Е.А. Русскевич

УГОЛОВНОЕ ПРАВО И «ЦИФРОВАЯ ПРЕСТУПНОСТЬ»: ПРОБЛЕМЫ И РЕШЕНИЯ

Монография

Москва
ИНФРА-М

2022

УДК 004.056: 343
ББК 67.408
Е92

Автор:
Русскевич Е.А., доктор юридических наук, профессор кафедры уголовного права Московского университета МВД России имени В.Я. Кикотя

Рецензенты:
1) **Букалерова Л.А.**, доктор юридических наук, профессор;
2) **Козаев Н.Ш.**, доктор юридических наук, доцент.

Русскевич Е.А.

Уголовное право и «цифровая преступность»: проблемы и решения: монография. 2-е изд., перераб. и доп. – М.: ИНФРА-М, 2022. – 000 с.

ISBN 978-5-16-

Монография посвящена комплексу теоретико-прикладных проблем приспосабливания отечественного механизма уголовно-правовой охраны к цифровизации преступности в условиях становления информационного общества. Наряду с общетеоретическими вопросами глубокому анализу подвергается зарубежное уголовное законодательство и положения норм международного права. В работе представлена уточненная уголовно-правовая характеристика преступлений в сфере компьютерной информации, в том числе новеллы российского уголовного законодательства – неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации (ст. 274^1 УК РФ).

Во втором издании отдельно проработаны вопросы дифференциации уголовной ответственности за цифровые преступления средствами Общей и Особенной части УК РФ. Проведен анализ проблем квалификации преступлений в сфере компьютерной информации, а также иных преступлений, совершаемых с использованием информационно-коммуникационных технологий, за пределами главы 28 УК РФ. С учетом полученных результатов представлен проект постановления Пленума Верховного Суда Российской Федерации «О судебной практике по делам о преступлениях в сфере компьютерной информации».

Монография рассчитана на научных сотрудников, преподавателей, практикующих юристов, студентов и аспирантов юридических вузов и факультетов.

ББК 67.408

ISBN 978-5-16-

Подписано в печать 25.11.2021. Формат 60x90/16.
Гарнитура Newton. Бумага офсетная. Усл. печ. л. 15,0. Уч.изд. л. 18,72.
Тираж 500 экз. Заказ № 00000
Издательский Дом «ИНФРА-М»
127282, Москва, ул. Полярная, д. 31в.
Тел.: (495) 3800540, 3800543. Факс: (495) 3639212
E-mail: books@infra-m.ru http://www.infra-m.ru

Посвящается моему учителю,
заслуженному деятелю науки Российской Федерации,
доктору юридических наук, профессору
Ветрову Николаю Ивановичу

Предисловие

На протяжении всей истории человеческая цивилизация подвергалась фундаментальным изменениям благодаря информации. Возникновение письменности, появление книгопечатания, а затем и первых технических средств коммуникации (телеграфа, телефона, радио и телевидения) оказали самое глубокое воздействие как на отдельного человека, так и на все сферы общественной жизни и государство. Появление электронно-вычислительных машин и распространение сети «Интернет» ознаменовало переход человечества уже в цифровую эпоху. Современный человек стал частью информационного (цифрового) общества, в котором его повседневная жизнедеятельность все более связана с компьютерами, сетевыми ресурсами и данными.

Сложно переоценить значение высокотехнологичных средств коммуникации в решении глобальных вызовов и угроз современного мира. Так, остановить атипичную пневмонию во многом стало возможным благодаря Интернету. Через несколько дней после вспышки смертельной эпидемии Всемирная организация здравоохранения (ВОЗ) запустила защищённый сайт, на котором проводились видеоконференции по проблеме, осуществлялся обмен рентгеновскими снимками лёгких, на основе чего был разработан протокол диагностики вместе с рекомендациями по карантину инфицированных пациентов. Несмотря на то что атипичная пневмония по длительности инкубационного периода, лёгкости распространения и смертности существенно превосходила известную эпидемию испанского гриппа[1], пострадало от неё лишь 8422 человек[2].

Вместе с тем стремительно развивающаяся архитектура виртуального пространства не только качественно улучшает нашу жизнь, но и параллельно с этим генерирует новые риски и угрозы. Негативным следствием глобальной информатизации явилось появление не только нового вида преступлений (преступлений в сфере компьютерной информации, как их принято именовать в отечественной уголовно-

[1] С 1918 по 1920 гг. около трети населения мира (полмиллиарда человек) заразилось смертельной формой гриппа, унёсшей около 50 миллионов жизней. См.: Jeffery Taubenberger, David Morens. 1918 Influenza: the Mother of all pandemics // Emerging infections diseases. 2006. № 12.

[2] World Health Organization, SARS: How a global epidemic was stopped (Geneva: WHO Press, 2006).

правовой доктрине), но и существенное изменение облика преступности в целом, которая в связи с использованием информационно-коммуникационных технологий приобрела несвойственные ей ранее признаки: экстерриториальность, гипертаргетированность, мультипликативность и др.

С одной стороны, ситуация мимикрирования преступности вполне типична, а такое ее свойство как историческая изменчивость знакомо любому специалисту в области криминологии. Вместе с тем, также известно и то, что качественное изменение преступности как правило обусловлено серьёзными социально-экономическими преобразованиями. Однако с преступностью нового поколения ситуация несколько иная. Их возникновению и продуцированию способствовали иные факторы.

Несмотря на весьма активное обсуждение этой проблемы, использование информационно-коммуникационных технологий в преступных целях в последние годы по-прежнему является серьёзным вызовом как для правоохранительных, так и законодательных органов. Жертвами преступлений, совершаемых с использованием информационно-коммуникационных технологий, ежегодно становятся миллионы людей и организаций, а также органы власти конкретных государств.

Вместе с ведущими странами мира Российская Федерация активно включилась в процесс построения информационного пространства. Планируемое перспективное развитие предполагает повсеместное внедрение технологий больших данных, нейротехнологий, искусственного интеллекта, систем распределенного реестра, квантовых технологий, компонентов робототехники, технологий виртуальной реальности и др. В соответствии с Указом Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» государство поставило своей целью обеспечить благоприятные условия для применения информационных и коммуникационных технологий, что также предполагает комплексное совершенствование законодательства[1].

Преступность, существующая в онлайн-пространстве или использующая достижения и возможности информационно-коммуникационных технологий («цифровая преступность»), проявляет себя как новое, слабо изученное негативное киберсоциальное явление, для противодействия которому требуются особый подход и инструментарий. Познание её характеристик, особенностей детерминации и выработка направлений уголовно-правового противодействия представляется важнейшей задачей современного общества для обеспечения национальной и международной безопасности.

[1] Собр. законодательства Рос. Федерации. – 2017. – № 20, ст. 2901.

РАЗДЕЛ I. ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ПРОТИВОДЕЙСТВИЯ «ЦИФРОВОЙ ПРЕСТУПНОСТИ»

Глава 1.
УГОЛОВНОЕ ПРАВО В УСЛОВИЯХ ЦИФРОВОЙ РЕАЛЬНОСТИ: ПОСТАНОВКА ПРОБЛЕМЫ

1.1. МЕХАНИЗМ УГОЛОВНО-ПРАВОВОЙ ОХРАНЫ В ЭПОХУ ИНФОРМАЦИОННОГО ОБЩЕСТВА

Основой противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий («цифровой преступности»), является формирование по возможности полного представления об информационном обществе и тех проблемах, которые оно ставит перед уголовно-правовым охранительным механизмом в целом. Как справедливо отмечает по этому поводу Д. А. Керимов: «…чем глубже и более всесторонне познана внешняя среда, чем рациональнее использованы добытые знания, чем в большей мере они отражают назревшие потребности этой среды, тем выше теоретический уровень правотворчества, тем эффективнее действие правовых норм, тем оптимальнее достижение целей и задач правового регулирования»[1].

В. Н. Кудрявцев также указывает, что «важнейшей предпосылкой любой правотворческой деятельности – это анализ объективных общественных процессов (негативных и позитивных), определяющих как саму необходимость в принятии законодательства или практики его применения, так и конкретное содержание этих изменений»[2].

Следует отметить, что на фоне нарастающих проявлений информатизации социальных отношений специалисты уже обратили внимание на совокупность системных противоречий, которые возникают между компьютерной преступностью XXI века и классическим механизмом уголовно-правового противодействия. Так, С. В. Власова небезосновательно резюмирует, что нельзя входить в цифровой мир с архаичной антикриминальной правовой моделью, то есть следственным уголовным процессом и уголовным правом, ориентированным на противодействие традиционной преступности. Не надо оцифровывать правовую архаику, которая сложилась ещё во времена средневековья[3].

---

[1] Керимов Д. А. Методология права (предмет, функции, проблемы философии права). С. 9 – 10.

[2] Кудрявцев В. Н. Закон, проступок, ответственность. М., 1986. С. 100.

[3] Власова С. В. К вопросу о приспосабливании уголовно-процессуального механизма к цифровой реальности // Библиотека криминалиста. 2018. № 1. С. 11.

Проблематика информационного общества разрабатывалась целым рядом отечественных и зарубежных специалистов[1]. Авторы отмечают, что общество цифрового мира сочетает в себе такие фундаментальные инновации как искусственный интеллект, роботизацию, «Интернет вещей» (Internet of Things (IoT), трёхмерную печать и др.[2] Изложение различных позиций о признаках, критериях, принципах построения и влиянии информационного общества на политические, экономические и социокультурные условия жизни человека, могло бы занять десятки страниц настоящей работы и видится не столь уж необходимым, поскольку фундаментальные аспекты информационного общества были зафиксированы на уровне ряда международных и отечественных документов стратегического значения.

Так, 22 июля 2000 г. была принята Окинавская хартия глобального информационного общества. В документе подчёркивается, что информационно-коммуникационные технологии являются одним из наиболее важных факторов, влияющих на формирование общества XXI века. Их революционное воздействие касается образа жизни людей, их образования и работы, а также взаимодействия правительства и гражданского общества. Информационно-коммуникационные технологии быстро становятся жизненно важным стимулом развития мировой экономики. Они также дают возможность частным лицам, фирмам и сообществам, занимающимся предпринимательской деятельностью, более эффективно и творчески решать экономические и социальные проблемы[3].

Следующим значимым документом явилась Декларация принципов «Построение информационного общества – глобальная задача в новом тысячелетии» (Женева, 2003 год), в которой было заявлено о стремлении построить общество, ориентированное на интересы людей, открытое для всех, в котором каждый мог создавать информацию и знания, иметь к ним доступ, пользоваться и обмениваться ими, на основе целей и принципов

---

[1] См., например: Белл Д. Социальные рамки информационного общества // Новая технократическая волна на Западе. М., 1986; Белл Д. Грядущее постиндустриальное общество. М., 2001; Кастельс М. Информационная эпоха: экономика, общество и культура. М., 2000; Каюмов А. Т. Информационное общество: концептуальное осмысление динамики социокультурного развития: дис. …д-ра филос. наук. Уфа, 2007; Полякова Т. А. Правовое обеспечение информационной безопасности при построении информационного общества в России: дис. …д-ра юрид. наук. М., 2008. и др.

[2] См., например: Шваб К. Четвёртая промышленная революция: перевод с английского. М., 2018. С. 9.

[3] Окинавская хартия глобального информационного общества // Дипломатический вестник. 2000. № 8. С. 51 – 56.

Устава Организации Объединённых Наций и Всеобщей декларации прав человека[1].

Несколько позднее в 2005 году Комитет министров Совета Европы утвердил Декларацию о правах человека и верховенстве права в информационном обществе. Одним из основных положений данного документа явился вывод о том, что реализация прав человека не должна подлежать иным ограничениям, кроме предусмотренных Всеобщей декларацией прав человека или прецедентным правом Европейского суда по правам человека, только потому, что они реализуются в цифровой среде. Одновременно должны быть приняты решительные меры для защиты граждан от новых, набирающих силу видов нарушения прав человека и использованием информационно-коммуникационных технологий[2].

В России первый стратегический документ, определивший принципы и направления развития информационного общества, был принят в 2008 году[3]. Целью Стратегии-2008 было общее повышение качества жизни, обеспечение конкурентоспособности страны на международной арене, развитие социально-политической, культурной и духовной сфер жизни общества, а также совершенствование государственного управления.

Спустя почти 10 лет была разработана новая Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы[4]. Согласно данному документу информационная природа общества определяется тем, что информация и уровень её применения и доступности кардинальным образом влияют на экономические и социокультурные условия жизни граждан. В целях реализации Стратегии-2017 была также утверждена программа «Цифровая экономика Российской Федерации»[5].

Если обобщить содержание приведённых выше документов и мнения отдельных специалистов, можно выделить следующие основополагающие характеристики информационного общества:

---

[1] [Электронный ресурс] // URL: http://www.un.org/ru/events/pastevents/pdf/decwsis.pdf (дата обращения: 06.05.2018).

[2] [Электронный ресурс] // URL: http://www.ifapcom.ru/files/Deklaratsiya_Komiteta_ministrov_o_pravah_cheloveka_i_verhovenstve_prava_v_informatsionnom_obschestve.pdf (дата обращения: 06.05.2018).

[3] Стратегия развития информационного общества в Российской Федерации (утв. Указом Президента РФ от 07.02.2008 № Пр-212) // Российская газета. – 16.02.2008. – № 34.

[4] Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы (утв. Указом Президента РФ 09.05.2017 № 203) // Собрание законодательства РФ. – 15.05.2017. – № 20. – Ст. 2901.

[5] Распоряжение Правительства РФ от 28.07.2017 № 1632-р «Об утверждении программы «Цифровая экономика Российской Федерации» // СПС «Консультант-Плюс».

- массовое распространение информационно-коммуникационной инфраструктуры и появление на этой основе информационной культуры у населения (в том числе навыков по эксплуатации информационных сетей);
- формирование единого информационного пространства, позволяющего практически без ограничений не только искать, получать информацию, но и осуществлять её распространение;
- существенное изменение национальных процессов политического управления ввиду мощного влияния субъектов, осуществляющих информационно-коммуникационное воздействие на государственные управленческие системы на глобальном (наднациональном) уровне;
- сращивание экономики с информационно-коммуникационной инфраструктурой, переходящей в зависимость уровня экономического развития государства от темпов внедрения передовых информационных технологий в деятельность хозяйствующих субъектов;
- формирование устойчивого социального запроса на обеспечение информационной безопасности для защиты интересов личности, общества и государства в информационной сфере.

Конечно же, нельзя говорить о том, что цифровая эра является данностью для всего населения земного шара. Разрыв между развитыми и развивающимися странами отчётливо проявляется и в аспекте построения информационного общества. Плотность использования информационно-коммуникационных технологий и прежде всего сети Интернет существенно разнится как в зависимости от региона, так и возраста населения. Наиболее активными пользователями глобальной сети традиционно выступают представители молодого поколения (в возрасте от 15 до 24 лет). При этом наивысшие показатели развития информационно-коммуникационной инфраструктуры демонстрируют страны Европы.

Россия не относится к числу аутсайдеров построения современного информационного общества. Предпринятые на государственном уровне меры позволили добиться значительных результатов в развитии электронного правительства и цифровой экономики.

Можно с уверенностью утверждать, что Россия, как страна, интегрированная в глобальное коммуникационное пространство, будет подвергаться влиянию новых технологий и форм массовой коммуникации, подобно другим технологически развитым державам. Как следствие, информационно-коммуникационная трансформация преступности на уровне российского государства является объективным и неизбежным следствием вступления в эпоху информационного общества.

При этом крайне важно учитывать те основные черты, которые характеризуют «цифровую преступность». Проведённое нами исследование позволяет говорить о следующих значимых свойствах преступлений, совершаемых с использованием информационно-коммуникационных технологий:

1) *экстерриториальность* – транснациональный характер компьютерной преступности является наиболее очевидным и одновременно обсуждаемым признаком. Глобальная доступность информационно-коммуникационных услуг означает, что преступность в информационном пространстве естественным образом имеет экстерриториальное измерение. При этом все больше компьютерных атак затрагивает одновременно две, три, десять и более стран;

2) *виртуальность* – информационно-коммуникационная среда является краеугольным признаком компьютерной преступности. Обеспечивая анонимность и физическую дистанцию от непосредственного потерпевшего, виртуальное пространство выступает значимым преимуществом и одновременно мощной детерминантой совершения преступления. В отличие от реального мира виртуальность снимает многие психологические барьеры на пути к осуществлению преступной деятельности прежде всего в связи с поддержанием чувства (и не всегда ложного) личной безопасности у преступника;

3) *гипертаргетированность* – преступлениям, совершаемым с использованием современных информационно-коммуникационных технологий, пожалуй, как никаким другим, свойственна нацеленность сразу на многих потерпевших и способность вызывать целые цепи многоуровневых общественно опасных последствий. При крупных вирусных атаках на финансовый сектор или банковские счета отдельных хозяйствующих субъектов или физических лиц количество потерпевших может измеряться сотнями и даже тысячами. Так, например, компьютерная атака с использованием компьютерного вируса-шифровальщика «WannaCry» началась 12 мая 2017 года и за достаточно короткий промежуток времени поразила свыше 500 тысяч компьютеров в 150 странах. Лидерами по количеству инфицированных систем стали Россия, Украина и Индия[1]. В данной связи следует сослаться на известную теорему Станислава Лема, согласно которой по мере технологического прогресса неуклонно возрастает разрушительная мощь малых групп. Ещё в начале 1960-х годов Лем предсказал, что в XXI веке новая производственная революция создаст условия, когда не только криминальные группы, но и отдельные преступники смогут ставить под угрозу нормальное функционирование и жизнь населения мегаполисов и даже государств[2];

4) *мультипликативность* – предыдущий признак во многом основывается на таком свойстве компьютерной преступности как способность к самовоспроизводству или свойстве мультипликативности. Наиболее ярко данный признак проявляется на примере распространения вредоносных компьютерных программ. Вирусная атака на конкретную

---

[1] Сборник исследований по практической безопасности АО «Позитив Текнолоджиз». М., 2018. С. 6.

[2] См.: Лем С. Сумма технологий. М., 2012.

организацию благодаря особенностям архитектуры глобальной информационной сети Интернет может обернуться колоссальными последствиями не только для отдельно взятой страны, но даже целой группы государств. Компьютерный вирус, распространяясь по открытым каналам связи, уже без участия человека будет поражать все доступные ему цели, включая объекты социального обеспечения (больницы, школы и т.д.) и государственного управления.

Другой стороной свойства мультипликативности является то, что появление какой-либо формы виртуальной преступной деятельности, как правило, вызывает новые посягательства на отношения информационной безопасности. Например, появление нового компьютерного вируса с нетипичным способом распространения порождает всплеск целевых атак на защищённые информационный ресурсы как отдельных граждан, так и государства;

5) *сверхизменчивость* – появление новой IT-технологии на массовом рынке товаров или услуг практически незамедлительно оборачивается очередной «перезагрузкой» преступности. Злоумышленники оценивают новации как поле очередных возможностей для совершения атак на граждан или организации. Учитывая, что технологии совершенствуются стремительно и непрерывно, это соответственно обусловливает такой же динамичный и перманентный процесс цифрового обновления преступности, когда какие-то относительно устоявшиеся формы виртуальной преступной деятельности уходят в небытие и замещаются другими;

6) *системная латентность (гиперлатентность)* – компьютерная преступность практически не поддаётся внятному количественному измерению. Объяснение этому имеет комплексный характер: противоречия действующего нормативного регулирования, несовершенство правоприменительной деятельности и механизмов статистического учёта, массовое несообщение о причинении вреда самими потерпевшими, а также бесчисленность и постоянно видоизменяющаяся природа «цифровой преступности». По оценкам специалистов, 85-97% компьютерных преступлений не обнаруживается[1]. При этом в современных научных работах латентность рассматривается как внутреннее репродуктивное свойство (внутренний источник самовоспроизводства) преступности[2], что отсылает нас к ранее выделенному признаку мультипликативности.

Выделенные атрибутивные свойства в своей совокупности позволяют вполне чётко представить насколько комплексно должен измениться

---

[1] См.: Агапов П. В., Борисов С. В., Вагурин Д. В., Коренюк А. Л., Меркурьев В. В., Побегайло А. Э., Халиуллин А. И. Противодействие киберпреступности в аспекте обеспечения национальной безопасности: монография. М., 2014. С. 35.

[2] См., например: Макаров В. В. Криминологическое исследование самодетерминации преступности: автореф. дис. …канд. юрид. наук. М., 2014. С. 8.

механизм уголовно-правовой охраны. В отечественной доктрине под таким механизмом предлагается понимать взаимодействие основных звеньев (элементов) уголовно-правовой системы в процессе осуществления задачи охраны наиболее важных общественных отношений от преступных посягательств[1]. В несколько ином (динамическом) аспекте его определяет Ю. С. Жариков – как систему необходимых и достаточных стадий правовой регламентации и упорядочения общественных отношений, позволяющую посредством реализации уголовно-правовых запретов, предписаний и дозволений обеспечивать эффективную охрану этих самих отношений от общественно опасных и противоправных посягательств[2].

Представление автора о стадийности механизма уголовно-правовой охраны в известном смысле является верным. Однако, на наш взгляд, стадии в большей мере характеризуют непосредственный процесс действия механизма, его этапы. Структуру же правильнее определять через его основные элементы. В качестве таковых в отечественной доктрине традиционно выделяют: 1) нормы уголовного права как нормативную основу механизма; 2) ответственность (наказание) как средство, при помощи которого решается задача уголовно-правовой охраны; 3) уголовно-правовое отношение как способ реализации уголовно-правовых норм, в том числе уголовное судопроизводство (уголовный процесс).

Уголовное законодательство являются ведущим звеном механизма уголовно-правовой охраны. Именно по этой причине вопрос об адаптации УК РФ к новым условиям и актуальным запросам информационного общества является первоочередным и базовым. Как справедливо отмечает Н. Ш. Козаев, «одной из важнейших проблем законодательной техники уголовного права на сегодняшний день является «запаздывание» правовой регламентации по отношению к бурно меняющимся социально-экономическим отношениям… Создание адекватной правовой базы противодействия преступности в условиях научно-технического прогресса является одной из гарантий не только национальной безопасности, но и уважения России, как стратегического партнёра во внешнеполитических и внешнеэкономических отношениях»[3].

Следует, однако, оговориться, что одной из проблем в решении задачи цифрового обновления отечественного уголовного законодательства является то, что развитие и внедрение новейших технологий связаны с высоким уровнем неопределённости – достаточно сложно спрогнозировать глубину и многосторонние последствия технологических преобразований в

---

[1] См.: Фефелов П. А. Механизм уголовно-правовой охраны (основные методологические проблемы). М., 1992. С. 66.

[2] Жариков Ю. С. Правоотношения в механизме уголовно-правового регулирования: монография. М., 2012. С. 88.

[3] Козаев Н. Ш. Современные технологии и проблемы уголовного права (анализ зарубежного и российского законодательства): монография. М., 2015. С. 7.

политике, экономике, культуре, социальной сфере и т.д. В связи с этим следует согласиться с М. М. Бабаевым и Ю. Е. Пудовочкиным, что такая ситуация характеризуется крайне высоким уровнем риска (как для субъектов уголовной политики и уголовного права, так и для граждан) и высокой степенью уязвимости самого уголовного права[1].

Вместе с тем, проникновение кибернетических методов, а также инструментария информационно-коммуникационных технологий в механизм преступления, на наш взгляд, уже сейчас позволяет выделить следующие фундаментальные аспекты модификации уголовного законодательства. Прежде всего таковым является определение оптимального (соответствующего современным угрозам) количества преступлений, посягающих на информацию и элементы информационно-коммуникационной инфраструктуры, то есть само содержание главы 28 УК РФ. Во-вторых, настоятельно необходимо очертить глубину «оцифровки» остальных разделов Особенной части УК РФ – насколько обширно следует изменить диспозиции традиционных составов преступлений путем детализации их совершения с использованием информационно-коммуникационных технологий. В-третьих, там, где адаптация традиционных составов преступлений будет явно недостаточной или невозможной для эффективного противодействия современным криминальным угрозам в виртуальной среде, необходимо определить ряд специальных норм. В-четвёртых, самостоятельным направлением модернизации УК РФ выступает формулирование научно-обоснованных критериев о значении использования информационно-коммуникационных технологий в сложившейся системе дифференциации уголовной ответственности.

В целом в разрешении указанных вопросов, на наш взгляд, необходимо ориентироваться на те основные направления в развитии технологий, в том числе негативные, которые с высокой долей вероятности и определят модель «оцифровки» уголовного права к условиям новой реальности.

Наиболее трудноразрешимым, своего рода системным, вызовом для механизма уголовно-правовой охраны информационного общества является ранее обозначенный глобализм преступлений, совершаемых с использованием информационно-коммуникационных технологий. Общество, в котором миллиарды людей связаны между собой мобильными устройствами, открывающими беспрецедентные возможности в сфере поиска, обработки и распространения информации, требует совершенно иного подхода как к правовому регулированию этих процессов, так и к охране наиболее значимых благ и интересов с ними связанных. Экстерриториальный характер интернет-коммуникаций заставляет

[1] Бабаев М. М., Пудовочкин Ю. Е. Неопределённость уголовного права в эпоху неопределённости // Законы России: опыт, анализ, практика. 2018. № 2. С. 6.

признать, что никакие региональные и тем более внутригосударственные меры не будут достаточными. Как справедливо отмечает по данному поводу М. А. Ефремова, «разграничение глобальной и национальной информационной безопасности довольно условно в современном мире, поскольку информационное пространство постепенно стирает границы»[1].

Полагаем, что цифровой гиперподключённый и гиперсвязанный мир потребует единого международного уголовного законодательства, построенного на общих стандартах противодействия киберпреступности. При этом признание юрисдикции такого «*Международного уголовного кодекса о киберпреступлениях*», устанавливающего минимальный перечень посягательств на безопасность данных и информационной инфраструктуры, должно выступать обязательным условием участия государства во всех значимых международных организациях и процессах[2].

Смежной проблемой является также то, что технологические преобразования, ознаменовавшие вступление человечества в эпоху четвёртой промышленной революции, изменили природу и характер международных конфликтов. Как справедливо отмечают исследователи: «…война будет всё меньше и меньше походить на войны прошлого… всё чаще конфликты будут происходить не на поле боя, а в киберпространстве…»[3]. Это в свою очередь обусловливает необходимость пересмотра критериев планирования, подготовки и развязывания агрессивной войны, а также применения запрещённых средств и методов её ведения. Очевидно, что подобное будет возможным, только при создании комплекса международных норм в отношении «*кибернетической войны»,* как это ранее имело место в отношении отдельных видов вооружений (ядерного, биологического, химического и др.).

Информационно-коммуникационная сфера выступает благоприятной площадкой для подрывной деятельности по разрушению традиционных ценностей и смысловых ориентиров общества. Навязывание стереотипов, выгодных тем или иным силам, уже показало свою эффективность на международной арене. «Арабская весна» и примеры других «цветных революций» явились наглядным свидетельством катастрофических последствии неэффективности органов безопасности отдельных государств в противодействии этому злу: эскалация нетерпимости и насилия,

---

[1] Ефремова М. А. Уголовно-правовая охрана информационной безопасности: монография. М., 2018. С. 78.

[2] С учётом современной геополитической обстановки едва ли можно говорить о скорой реализации подобной инициативы. В подтверждение можно лишь указать, что уже более десяти лет Российская Федерация безуспешно продвигает идеи и проекты по подготовке Конвенции Организации Объединённых Наций «О сотрудничестве в сфере противодействия информационной преступности».

[3] Овчинский В. С. Криминология цифрового мира: учебник для магистратуры. М., 2018. С. 55.

возникновение новых вооружённых конфликтов, многочисленные жертвы среди мирного населения, неконтролируемое распространение оружия, разрушение экономики и др. Как справедливо отмечает С. В. Володенков, «экстерриториальность коммуникационных технологий в интернет-пространстве приводит к тому, что национальные процессы политического управления подвергаются мощному влиянию политических акторов, осуществляющих информационно-коммуникационное воздействие на государственные управленческие системы на глобальном (наднациональном) уровне. По сути, универсальные модели интернет-коммуникации разрушают национальные особенности политического управления…»[1]. В связи с этим полагаем, что задачей ближайшего будущего также является совершенствование механизма уголовно-правовой защиты от наиболее опасных форм виртуального распространения криминогенной пропаганды, угрожающей политической стабильности государства, как на уровне ответственности модераторов данных, так и поставщиков услуг связи.

Информационное общество неразрывно ассоциируется со сквозным проникновением технологий в повседневную жизнь человека, то есть с так называемым «Интернетом-вещей» (IoT) и имплантируемыми устройствами с выходом в Интернет. Подключённость практически любого предмета быта (от кофеварки до автомобиля) к глобальному цифровому пространству должна произвести революцию в том, как мы работаем и живём. В целом «IoT» должен сделать нашу жизнь безопаснее, эффективнее и гораздо удобнее. Однако развитие «IoT-технологий» создаёт угрозу для безопасности личности, её основных прав и свобод. Стремительное развитие «Интернета-вещей» кардинально изменит привычную картину преступлений против личности и, следовательно, потребует определённых изменений в сфере уголовного законодательства.

Цифровое общество потребует уголовно-правового противодействия посягательствам на принципиально новые объекты – «*виртуальное имущество*». Так, например, одним из быстро развивающихся секторов экономики является рынок многопользовательских онлайн-игр («World of Tanks», «Worlds of Warcraft» и др.) и сервисов по предоставлению различного рода контента (фильмов, музыки, электронных книг и т.д.). При этом виртуальное пространство стремительно коммерциализируется и впитывает в себя всё большие денежные потоки. За реальные деньги пользователи информационных услуг приобретают игровые деньги, а равно иные объекты информационного характера, не имеющие физического (овеществлённого) выражения. Например, одной из первых громких покупок в среде онлайн-игр было приобретение в декабре 2004 года виртуального острова на планете Калипсо за 26 500 долларов США.

[1] Володенков С. В. Интернет-коммуникации в глобальном пространстве современного политического управления. М., 2015. С. 112.

Позднее, этот рекорд был перебит покупкой космической станции на одном из астероидов, вращающихся возле планеты за 100 000 долларов США[1].

Уже в современных условиях в сети Интернет присутствуют специальные сервисы (торговые площадки) по продаже виртуальных объектов, используемых игроками в многопользовательских онлайн-играх. Следует отметить, что правовая природа подобного рода объектов до настоящего времени чётко в науке не определена. Юристы спорят о том, могут ли такие объекты как электронные книги, библиотеки itunes, аккаунт в социальной сети или многопользовательской игре переходить в порядке наследования, а равно возможно ли возложить на подобное цифровое имущество обременение или использовать его в порядке исполнительного производства[2].

Следует отметить, что в США вопрос о правовом статусе виртуальных объектов и даже их наследовании уже практически решён. Так, с 1 января 2015 года в штате Делавэр вступил в силу нормативный акт (An act to amend Title 12 of the Delaware Code relating to fiduciary access to digital assets and digital accounts), позволяющий получать виртуальную собственность по наследству. Также на его основе в 2015 году был разработан унифицированный акт (Fiduciary access to digital assets act), рекомендуемый для принятия во всех штатах страны[3].

В связи с этим актуальным является вопрос о возможности признания виртуальных объектов предметом хищения по российскому уголовному законодательству. «Виртуальное имущество» в основе своей представляет собой всего лишь компьютерный код. Вместе с тем, в отличие от иных компьютерных данных, выражающих идеи, мысли и т.п., такой код направлен преимущественно на имитацию объектов реального (физического) мира (зданий, транспортных средств, предметов быта и т.д.). Хотя такие объекты и существуют лишь на экране компьютера, они могут приобретаться и отчуждаться и обладают явно выраженной потребительской ценностью. Сохранение нейтралитета уголовного права относительно оценки посягательств на виртуальные объекты едва ли является приемлемым подходом. Приобретение реальных и виртуальных

---

[1] Онлайн-аукцион – продажа космической станции // [Электронный ресурс] // URL: http://eve-online.info/forum/viewtopic.php? id=518 (дата обращения: 15.02.2018).

[2] См., например: Архипов В. В. Виртуальное право: основные проблемы нового направления юридических исследований // Известия высших учебных заведений. Правоведение. 2013. № 2; Лисаченко А. В. Право виртуальных миров: новые объекты гражданских прав // Российский юридический журнал. 2014. № 2; Семенюта Б. Онлайн-игры: правовая природа отношений // Интеллектуальная собственность. Авторское право и смежные права. 2014. № 8 и др.

[3] Uniform Law Comission // [Электронный ресурс] // URL:http://www.uniformlaws.org/Act.aspx?title=Fiduciary%20Access%20to%20Digital%20Assets% 20Act,%20Revised%20(2015) (дата обращения: 15.03.2018).

денег, накопление овеществлённого и интернет-имущества имеет одну общую черту – затрачиваемое на это реальное время человека, его труд и во многих случаях реальные финансовые ресурсы. В связи с этим можно сделать вывод, что такие объекты не должны и не могут быть исключены из-под уголовно-правовой охраны только потому, что обладают несколько иной природой, выражены в другой форме и выглядят, попросту говоря, незнакомыми. Как справедливо отмечает М. А. Кулезин, «дальнейшее абстрагирование от решения указанной проблемы в условиях столь молниеносно развивающихся информационных технологий и Интернета не является эффективным для бизнеса в целом и отдельных граждан в частности»[1]. Разумеется, в решении этого вопроса доктрина уголовного права в значительной степени зависит от развития науки цивилистической, которая, как представляется, должна выделить такие объекты в качестве особой категории объектов гражданских прав с использованием отдельных элементов правового режима вещей, как это сделано, например, в отношении бездокументарных ценных бумаг.

Развитие информационных технологий обусловит качественное преобразование транспортной преступности. Ещё в 2012 году штат Невада (США) принял закон, разрешающий движение автомобиля без водителя. Уже сейчас становится очевидным, что данный процесс связан с вполне конкретными угрозами. Так, при проведении испытаний в марте 2018 года беспилотный автомобиль Uber насмерть сбил пешехода[2]. В этих условиях перед отечественной доктриной уголовного права возникает необходимость в разработке принципиально нового подхода к юридической оценке происшествий с участием таких транспортных средств. Как справедливо отмечает М. М. Лапунин, «перед изготовителями транспорта, программистами и будущими «пассажирами-водителями» стоит важный юридический вопрос: кто и в каких пределах будет нести ответственность в случае причинения вреда с участием беспилотного транспортного средства»[3]. На настоящий момент понятно, только одно: традиционное положение об ответственности водителя в такой ситуации не сработает, поскольку его-то в такой ситуации попросту нет.

Указанные выше системные изменения общественных отношений (и не только они) оказывают дизруптивное воздействие на механизм уголовно-правовой охраны, вызывая состояние так называемой *дизрупции уголовного*

---

[1] Кулезин М. А. Реальные проблемы виртуальных объектов // Евразийская адвокатура. 2015. № 5 (18). С. 53.

[2] [Электронный ресурс] // URL: https://www.bbc.com/russian/news-43462646?ocid=vk (дата обращения: 08.02.2018).

[3] Лапунин М. М. Научно-технический прогресс и потребности в изменении уголовного закона // Уголовное право: стратегия развития в XXI веке: материалы XIV Международной научно-практической конференции (26-27 января 2017 г.). М., 2017. С. 97.

права – неспособности выполнять свои базовые функции ввиду перманентного и динамичного внешнесредового воздействия. В наиболее упрощённой форме это выражается в представлении о полной несостоятельности уголовно-правового механизма перед актуальными угрозами XXI века и обосновании необходимости совершенно новой модели противодействия преступности.

Пожалуй, в наименьшей степени (по крайне мере в ближайшей перспективе) информатизация преступности затронет проблематику следующего элемента механизма уголовно-правовой охраны – уголовного наказания. Полагаем, что процесс «цифровизации» уголовного права обойдёт стороной данный институт, оставив его практически в нетронутом виде со своим уже сложившимся комплексом традиционных проблем и противоречий. Вместе с тем, можно выделить два направления модернизации уголовного наказания, которые, безусловно, следует развивать с целью обеспечения соответствия наказательной практики ожиданиям и вызовам информационного общества. Первое касается разработки новых видов наказания, в том числе связанных с принудительным ограничением активности лица в информационном пространстве. Понятно, что законодательные инициативы здесь имеют вторичный характер и полностью зависят от программно-технической возможности обеспечить исполнение подобных наказаний, которая на современном этапе попросту отсутствует. Смежной проблемой выступает внедрение блокчейн-технологий для контроля за исполнением имеющихся видов наказания, а также разработка на основе технологии распределённых реестров совершенно новых видов уголовно-правового воздействия.

Второе направление касается внедрения информационно-коммуникационной инфраструктуры непосредственно в сам процесс исправления осуждённых, прежде всего в целях предупреждения их десоциализации. Так, П. В. Жестеров пишет по данному поводу: «…уголовно-исполнительная система также не может дольше оставаться в «цифровой» изоляции. Учитывая то обстоятельство, что десятки тысяч осуждённых отбывают наказание в регионах, недоступных для посещения их родными и близкими, в процедуре реализации уголовной ответственности в форме исполнения и отбывания лишения свободы назрела необходимость в обеспечении дозированного доступа осуждённых к наказанию в виде лишения свободы к современным информационным и коммуникационным технологиям»[1]. Подобные инициативы, на наш взгляд, должны получить всеобщую поддержку и по возможности скорейшую реализацию.

---

[1] Жестеров П. В. Четвёртая промышленная революция: трансформация содержания уголовной репрессии // Уголовное право: стратегия развития в XXI веке: материалы XV Международной научно-практической конференции. М., 2018. С. 625 – 626.

По меткому замечанию С. С. Алексеева, «энергию» механизму правового регулирования сообщает государство, а именно деятельность конкретных компетентных органов[1]. Следует констатировать, что данное звено отечественного механизма уголовно-правовой охраны испытывает значительные трудности в противодействии «цифровой преступности». Наряду с нехваткой экспертов, техническим отставанием и устаревшими тактиками противодействия, следует выделить и неготовность оперативных и судебно-следственных органов узреть в «старых» нормах уголовного закона новое цифровое измерение. В данном аспекте одной из главных задач является преодоление «традиционного», «не цифрового», видения уголовного права непосредственно правоприменителями. Это довольно сложная и многоаспектная проблема, которая касается не только первичной подготовки кадров в образовательных учреждениях, но и повышения квалификации действующих сотрудников. Вместе с тем, отметим, что ведущая роль так или иначе остаётся за отечественной доктриной уголовного права, которая должна предварительно описать, классифицировать и объяснить преступность информационного общества, и тем самым обеспечить соответствующее качественное наполнение образовательных программ.

Проблемы процессуальной формы реализации уголовно-правовых отношений в условиях информатизации преступности также многочисленны и сложны. Вместе с тем, сами по себе они не составляют предмет настоящего исследования. Следует лишь заметить, что перед наукой уголовно-процессуального права стоит фундаментальная научно-исследовательская задача, без успешного решения которой достижения доктрины уголовного права окажутся практически бесполезными. Как и ранее, эти родственные науки должны развиваться согласованно, не отставая и подкрепляя друг друга в решении актуальных проблем противодействия преступности.

С учётом изложенного и принимая во внимание особую значимость, которую приобрела компьютерная информация и информационно-коммуникационная инфраструктура в настоящее время, представляется необходимым дополнить общий объект уголовно-правовой охраны специальным указанием на информационную безопасность, изложив ч. 1 ст. 2 УК РФ в следующей редакции: «Задачами настоящего Кодекса являются: охрана прав и свобод человека и гражданина, собственности, общественного порядка, общественной и *информационной* безопасности, окружающей среды, конституционного строя Российской Федерации от преступных посягательств, обеспечение мира и безопасности человечества, а также предупреждение преступлений».

[1] Алексеев С. С. Проблемы теории права. Т. 1. Свердловск, 1972. С. 371.

Завершая рассмотрение проблем механизма уголовно-правовой охраны в эпоху информационного общества, можно сформулировать следующие основные выводы:

1) Российская Федерация, как страна, интегрированная в глобальное коммуникационное пространство, будет подвергаться влиянию новых технологий и форм массовой коммуникации, подобно другим технологически развитым державам. Как следствие, информационно-коммуникационная трансформация преступности на уровне российского государства является объективным и неизбежным следствием вступления в эпоху информационного общества;

2) с учётом стремительной «цифровизации» общественных отношений можно сделать вывод о дизруптивном воздействии информационно-коммуникационных технологий на механизм уголовно-правовой охраны (дизрупции уголовного права);

3) при определении стратегических направлений модернизации механизма уголовно-правовой охраны необходимо учитывать сущностные свойства преступлений, совершаемых с использованием информационно-коммуникационных технологий: а) экстерриториальность; б) виртуальность; в) гипертаргетированность; г) мультипликативность; д) сверхизменчивость; е) системную латентность (гиперлатентность);

4) проникновение кибернетических методов, а также инструментария информационно-коммуникационных технологий в механизм преступления позволяет выделить следующие фундаментальные аспекты модификации уголовного законодательства: а) определение оптимального количества составов преступлений, посягающих на информацию и элементы информационно-коммуникационной инфраструктуры; б) выделение критериев «оцифровки» остальных разделов Особенной части УК РФ, путём детализации совершения традиционных составов преступлений специфическим способом – с использованием информационно-коммуникационных технологий; в) в тех случаях, где адаптация традиционных составов преступлений будет явно недостаточной или невозможной для эффективного противодействия современным криминальным угрозам в виртуальной среде, определение специальных норм; г) разработка научно-обоснованных критериев о значении использования информационно-коммуникационных технологий в сложившейся системе дифференциации уголовной ответственности;

5) одной из главных задач приспосабливания уголовно-правового механизма к противодействию преступлениям, совершаемым с использованием информационно-коммуникационных технологий, является преодоление «традиционного», «не цифрового», видения уголовного права на правоприменительном уровне. Это довольно сложная и многоаспектная проблема, которая касается как первичной подготовки кадров в образовательных учреждениях, так и повышения квалификации действующих сотрудников. Ведущая роль так или иначе остаётся за

отечественной доктриной уголовного права, которая должна предварительно описать, классифицировать и объяснить преступность информационного общества, и тем самым обеспечить соответствующее качественное наполнение образовательных программ;

6) принимая во внимание особую значимость, которую приобрела компьютерная информация и информационно-коммуникационная инфраструктура в настоящее время, представляется необходимым дополнить общий объект уголовно-правовой охраны специальным указанием на информационную безопасность.

1.2. ПРЕСТУПЛЕНИЯ, СОВЕРШАЕМЫЕ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ («ЦИФРОВЫЕ ПРЕСТУПЛЕНИЯ»): ПРОБЛЕМЫ ИНТЕРПРЕТАЦИИ

Необходимой предпосылкой комплексного изучения проблем ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, является определение их понятия. Как справедливо подчёркивает Н. Ш. Козаев, «адаптация науки и отрасли уголовного права к изменениям, вызываемым научно-техническим прогрессом, подчиняется общим закономерностям генезиса правовой системы и может происходить посредством совершенствования юридической техники, введения в правовой оборот новых понятий и терминов, по возможности их нормативного дефинирования»[1].

Анализ современной отечественной и зарубежной литературы позволяет констатировать, что вопрос о категориальном определении подобного рода деяний далеко не решён. При этом проблема дефинирования преступлений, совершаемых с использованием информационно-коммуникационного оборудования, может быть представлена сразу на двух уровнях. Первый связан с отсутствием общего видения относительно самой терминологии. В трудах отечественных и зарубежных авторов можно обнаружить использование совершенно разных категорий: компьютерные преступления[2], информационные преступления[3], киберпреступления[1],

---

[1] Козаев Н. Ш. Противодействие злоупотреблениям современными технологиями: международно-правовые и уголовно-правовые аспекты: монография / под ред. докт. юрид. наук, проф. А. В. Наумова. М., 2016. С. 69.

[2] См.: Жмыхов А. А. Компьютерная преступность за рубежом и ее предупреждение : дис. … канд. юрид. наук. М., 2003; Лопатина Т. М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности : дис. ... д-ра юрид. наук. М., 2007 и др.

[3] См.: Букалерова Л. А. Информационные преступления в сфере государственного и муниципального управления: законотворческие и правоприменительные проблемы: дис. …д-ра юрид. наук. М., 2007; Крылов В. В. Информационные компьютерные преступления. М., 1997 и др.

преступления в сфере высоких технологий[2], интернет-преступления[3], cybercrime и computer-related crime[4].

Второй уровень касается самого наполнения данной группы преступлений – учёные существенно расходятся во мнениях относительно того, какие деяния следует признавать «компьютерными», а какие при внешней схожести таковыми всё же не являются.

Полагаем, что с методологической точки зрения эти проблемы должны решаться в обратной последовательности – только определившись с содержанием предмета, можно будет успешно разрешить вопрос о терминологии. Как справедливо отмечается в уголовно-правовой теории, определение круга преступлений и их классификация, позволяет осмыслить явление в его целостности, выявить внутренние взаимосвязи и соподчинения, прогнозировать наличие недостающих звеньев[5].

Одним из известных подходов является определение компьютерных преступлений как деяний, исключительно посягающих на безопасность компьютерной информации[6]. Вместе с тем, А. А. Жмыхов отмечает, что указания на направленность посягательства объективно недостаточно, поскольку таким образом к компьютерным преступлениям необходимо

---

[1] См.: Тропина Т. Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: понятие, состояние, уголовно-правовые меры борьбы: дис. …канд. юрид. наук. Владивосток, 2005; Чекунов И. Г. Криминологическое и уголовно-правовое обеспечение предупреждения киберпреступности: автореф. дис. …канд. юрид. наук. М., 2013 и др.

[2] См.: Козаев Н. Ш. Современные технологии и проблемы уголовного права (анализ зарубежного и российского законодательства): монография. М., 2015 и др.

[3] См.: Дремлюга Р. И. Интернет-преступность: монография. Владивосток, 2008; Гузеева О. С. Преступления, совершаемые в российском сегменте сети Интернет: монография. М., 2015 и др.

[4] См.: Dana L. Bazelon, Yun Jung Choi and Jason F. Conaty. Computer crimes. Am. Crim. L. Rev. 2006; Douglas H. Hancock. To what extent should computer related crimes be the subject of specific legislative attention? Alb. L.J. Sci. & Tech. 2001; Stephen P. Heymann, Legislating computer crime.Harv. J. On Legis. 1997.

[5] Кудрявцев В. Н., Лунеев В. В. О криминологической классификации преступлений // Государство и право. 2005. № 6. С. 54.

[6] Гаджиев М. С. Криминологический анализ преступности в сфере компьютерной информации (по материалам Республики Дагестан): автореф. дис. ...канд. юрид. наук. Махачкала, 2004. С. 9.

будет относить и уничтожение физических носителей информации[1]. В связи с этим он предпринимает попытку конкретизировать содержание явления, обосновывая, что это «не просто совокупность преступлений, посягающих на безопасность компьютерной системы или сети, но и совершаемых с помощью компьютерной системы или сети, а также в рамках компьютерной системы или сети»[2].

М. А. Ефремова выделяет преступления против безопасности информационно-телекоммуникационных технологий как «…совокупность запрещённых уголовным законом общественно опасных деяний, посягающих на общественные отношения, обеспечивающие безопасность процессов и методов поиска, сбора, хранения, обработки, предоставления, распространения информации посредством средств вычислительной техники и информационно-телекоммуникационных сетей»[3].

Используя другую терминологию (киберпреступность), однако похожим образом определяет данные преступления Т. Л. Тропина: «…совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, и против компьютерных систем, компьютерных сетей или компьютерных данных»[4].

Таким образом, по мнению данных авторов, компьютерная (кибернетическая, виртуальная, информационно-технологическая) природа преступления определяется как содержанием объекта посягательства, так и признаками средства и обстановки (виртуального пространства).

Полагаем, что такой подход нельзя признать удачным, так как в указанной интерпретации исследователи проблематику виртуальной преступности искусственно концентрируют на деяниях, посягающих исключительно на безопасность компьютерных данных и систем, то есть

---

[1] Следует отметить, что категорический отказ А. А. Жмыхова от возможности оценки противоправного воздействия на внешнюю оболочку хранения компьютерной информации (повреждение или уничтожение компьютера, внешних дисков и т.п.) как компьютерного преступления представляется дискуссионным. Полагаем, что имеющиеся стандарты юридической оценки посягательств на средства хранения, обработки или передачи компьютерной информации к сегодняшнему дню оказываются в значительной части малопригодными и требуют корректировки.

[2] Жмыхов А. А. Компьютерная преступность за рубежом и ее предупреждение: дис. …канд. юрид. наук. М., 2003. С. 18–19.

[3] Ефремова М. А. Уголовно-правовая охрана информационной безопасности: монография. М., 2018. С. 221 – 222.

[4] Тропина Т. Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. …канд. юрид. наук. Владивосток, 2005. С. 36.

предусмотренных главой 28 УК РФ. Вместе с тем, очевидно, что это, хотя и значимая, но лишь малая её часть.

В отечественной теории уголовного права можно обнаружить подход, связанный с определением компьютерных преступлений через своего рода «сетевой» аспект. Так, Н. В. Летелкин оперирует категорией «преступления, совершаемые с использованием информационно-телекоммуникационных сетей (включая сеть Интернет)». Автор раскрывает данную группу деяний как «умышленные, наказуемые деяния, запрещённые Особенной частью уголовного закона, наряду с основным объектом уголовно-правовой охраны, посягающие на общественные отношения в сфере правомерного использования информационно-телекоммуникационных сетей, отличающиеся повышенной степенью общественной опасности ввиду использования при их совершении технологических систем, предназначенных для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники»[1].

Как нетрудно заметить, Н. В. Летелкин выделяет два критерия признания преступления компьютерным – использование соответствующих технологических систем (различного рода сетей, в том числе сети Интернет), а также направленность деяния на причинение вреда дополнительному объекту уголовно-правовой охраны – отношениям в сфере информационной безопасности. Наиболее уязвимым моментом предлагаемого подхода является, пожалуй, тезис о необходимой двуобъектности преступления, поскольку, как известно, многие из современных преступлений, совершаемых с использованием сетевого оборудования, угрозы для самой информационной инфраструктуры не представляют. Например, сбыт наркотических средств, совершаемый путём так называемых «закладок» с использованием сети Интернет.

При определении круга преступлений, совершаемых с использованием информационно-коммуникационных технологий, можно опираться исключительно на формально-юридический аспект и относить к компьютерным преступлениям только те, в законодательном описании которых присутствует или подразумевается использование соответствующих средств. Именно подобным образом перечень киберпреступлений определяют авторы аналитического обзора «Комплексный анализ состояния преступности в Российской Федерации по итогам 2017 года и ожидаемые тенденции её развития», указывая, что к таковым относятся: 1) составы преступлений, включённых в главу 28 УК РФ «Преступления в сфере компьютерной информации», 2) ст. 159^6 УК РФ

[1] Летелкин Н. В. К вопросу об определении понятия преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет») // Уголовное право: стратегия развития в XXI веке: материалы XV Международной научно-практической конференции. М., 2018. С. 619.

«Мошенничество в сфере компьютерной информации», 3) ст. 187 УК РФ «Неправомерный оборот средств платежей», 4) составы, имеющие указание на использование электронных или информационно-телекоммуникационных сетей, в том числе сети Интернет при совершении преступления (ст. 171^2 «Незаконные организация и проведение азартных игр», ч. 1 ст. 185^3 «Манипулирование рынком», п. «б» ч. 2 ст. 228^1 «Незаконное производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества», п. «б» ч. 3 ст. 242 «Незаконные изготовление и оборот порнографических материалов или предметов», п. «г» ч. 2 ст. 242^1 «Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних» и п. «г» ч. 2 ст. 242^2 «Использование несовершеннолетнего в целях изготовления порнографических материалов или предметов» УК РФ)[1].

При наличии определённых достоинств, строго догматический подход обладает очевидным и существенным недостатком – он не позволяет учесть реальных масштабов проблемы, значительно и искусственно преуменьшая палитру компьютерной преступности. Это в свою очередь может привести к недостаточному вниманию теории уголовного права к охране общественных отношений, обеспечивающих личные и общественные интересы в информационной сфере, а также к недооценке тенденций развития отечественного уголовного законодательства. Кроме того, на наш взгляд, догматический подход не позволит построить эффективную стратегию предупреждения преступлений, совершаемых с использованием информационно-коммуникационных технологий.

Стремительное развитие информационных отношений существенно увеличивает их значимость для общества и государства. Учитывая масштабы «виртуализации жизнедеятельности», в социальном плане можно рассматривать такие общественные отношения как единые, обеспечивающие одновременно и физические блага личности, и экономические отношения, и общественные, а также государственные интересы. В уголовно-правовом смысле они представляют собой разные, но весьма взаимосвязанные отношения, одни из которых обеспечивают права и законные интересы личности, другие – конкретные общественные или государственные интересы. Поскольку на такие взаимосвязанные общественные отношения посягают преступления, совершаемые с

[1] Антонян Ю. М. Комплексный анализ состояния преступности в Российской Федерации по итогам 2017 года и ожидаемые тенденции её развития: аналитический обзор // Ю. М. Антонян, Д. А. Бражников, М. В. Гончарова, В. И. Коваленко, В. И. Шиян, Г. Э. Бицадзе, А. В. Евсеев. М.: ФГКУ «ВНИИ МВД России», 2018. С. 58.

использованием информационно-коммуникационных технологий, не входящие в главу 28 УК РФ, постольку с точки зрения повышения эффективности охраны подобного рода общественных отношений уголовным правом представляется целесообразным исходить из понимания анализируемых преступлений не в формально-догматическом понимании, а в более широком смысле.

Так, принципиально другим является определение компьютерной преступности как совокупности деяний, вообще совершаемых с использованием современного информационно-коммуникационного оборудования. Например, А. Г. Волеводз выделяет не только преступления в сфере компьютерной информации, посягающие на информационные компьютерные отношения, но и «иные преступления, для которых характерно использование компьютерной информации или составляющих ее элементов информационного пространства при совершении деяний, посягающих на иные охраняемые уголовным законом правоотношения (собственности, общественной безопасности и т.д.)»[1].

Т. М. Лопатина также относит к данным преступлениям все совершённые на определённой территории за определённый период деяния (лиц, их совершивших), непосредственно посягающие на отношения по сбору, обработке, накоплению, хранению, поиску и распространению компьютерной информации, а равно преступления с использованием компьютера в целях извлечения материальной выгоды или иной личной заинтересованности[2].

Следует отметить, что примерно такой же подход был сформулирован на 10-м Конгрессе ООН по предупреждению преступности и обращению с правонарушениями (2000 г., Вена), где были предложены сразу два определения киберпреступлений:1) в узком смысле – любое противозаконное поведение в форме электронных операций, направленное против безопасности компьютерных систем и обрабатываемых ими данных; 2) в широком смысле – любое противозаконное поведение, осуществляемое посредством или в связи с компьютерной системой или сетью, включая такие преступления, как незаконное владение, предложение или распространение информации посредством компьютерной системы или сети[3].

В 2013 году Министерство внутренних дел Великобритании (United Kingdom Home Office) приняло стратегию противодействия преступности (Serious and Organised Crime Strategy), в которой все «киберпреступления»

---

[1] Волеводз А. Г. Противодействие компьютерной преступности. М., 2002. С. 50.

[2] Лопатина Т. М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности: дис. ... д-ра юрид. наук. М., 2007. С. 39.

[3] [Электронный ресурс] // URL: http://www.un.org/ru/documents/decl_conv/declarations/vendec (дата обращения: 21.01.2018).

были классифицированы также на две группы: 1) «виртуально-зависимые»(cyber-dependent crimes) – преступления, которые могут быть совершены исключительно с использованием компьютерного оборудования, программного обеспечения, информации или сетей (cyber-dependent crimes can only be committed using computers, computer networks or other forms of information communication technology) и 2) «виртуально-возможные» (cyber-enabled crimes) – преступления, которые могут быть совершены и без использования современных информационно-коммуникационных технологий, однако демонстрируют тенденцию стремительной виртуализации (cyber-enabled crimes (such as fraud, the purchasing of illegal drugs and child sexual exploitation) can be conducted on or offline, but online may take place at unprecedented scale and speed)[1].

И. Г. Чекунов единственным критерием признания деяния «киберпреступлением» признаёт присутствие таких признаков объективной стороны, как средство или орудие, в качестве которых выступает вредоносная компьютерная программа или программно-техническое средство, подключённое к компьютерной сети или сотовому оператору связи[2].

А. Н. Савенков определяет киберпреступность как умышленные общественно опасные деяния, установленные уголовным законом государства, совершённые путём неправомерного доступа к электронной информации, содержащейся в компьютерных сетях и использующие их возможности в системах связи телекоммуникаций[3].

Нельзя не признать, что представленный выше подход к определению компьютерной преступности характеризуется некой амбивалентностью – такими преступлениями признают как деяния, совершаемые против безопасности компьютерных данных и информационной инфраструктуры, так и все остальные, которые могут быть и (или) фактически совершаются с использованием информационно-коммуникационных технологий. По мнению К. Н. Евдокимова, «дихотомический подход к пониманию компьютерной преступности, имея сторонников и противников в отечественной криминологической науке, остаётся всё же наиболее логичным, поскольку позволяет оценить всю сложность, многообразие разноуровневость рассматриваемого криминального явления и найти

---

[1] [Электронный ресурс] // URL: https://www.gov.uk/government/ publications/serious-organised-crime-strategy> accessed on 22 January 2015.[1 SEP] (дата обращения: 17.02.2018).

[2] Чекунов И. Г. Криминологическое и уголовно-правовое обеспечение предупреждения киберпреступности: автореф. дис. …канд. юрид. наук. М., 2013. С. 7.

[3] Савенков А. Н. Противодействие киберпреступности в финансово кредитной сфере как вектор обеспечения глобальной безопасности // Государство и право. 2017. № 10. С. 8.

определённый баланс среди существующих научных мнений»[1]. Вместе с тем, такая интерпретация порождает представление, что какой-либо значимой грани между простой (традиционной) и компьютерной преступностью попросту не существует – любое или практически любое деяние, предусмотренное Особенной частью УК РФ, можно рассматривать как компьютерное преступление при условии, что оно совершается с использованием соответствующих средств и в виртуальном пространстве. Во многом в связи с этим в отечественной теории уголовного права было высказано суждение, что попытки представить все преступления, совершаемые с использованием информационно-коммуникационных технологий, как некую обособленную группу общественно опасных деяний, самостоятельное уголовно-правовое явление, обладающее своими институциональными признаками, изначально обречены на провал. Так, Ю. М. Батурин и А. М. Жодзишский обосновывали, что «компьютерных преступлений, как преступлений специфических в юридическом смысле, попросту нет»[2].

Из этих же соображений В. М. Быков и В. Н. Черкасов резюмируют, что «компьютерных преступлений как самостоятельного вида не существует, их следует рассматривать лишь как квалифицирующий признак обычных, «традиционных» преступлений. При этом компьютер при совершении преступления выступает в качестве объекта преступления, орудия преступления, средства, на котором подготавливается преступление, или среды, в которой оно совершается»[3].

Как представляется, указанные авторы имеющиеся объективные сложности в определении понятия экстраполировали на само явление – если не поддаётся научному дефинированию, значит не существует. Вместе с тем, согласиться с тем, что компьютерной преступности «per se» не существует и, выражаясь метафорически, это не что иное как «старое вино в новых бутылках»[4], пожалуй, нельзя. И контраргументы здесь связаны не только с состоявшимся обособлением специфических посягательств на безопасность информационно-коммуникационной инфраструктуры (глава 28 УК РФ). «Цифровая надстройка» традиционной преступности представляет собой совершенно новое явление, характеризующееся своим

---

[1] Евдокимов К. Н. Противодействие компьютерной преступности в Российской Федерации: криминологические и уголовно-правовые аспекты. Иркутск, 2016. С. 16.

[2] Батурин Ю. М., Жодзишский А. М. Компьютерная преступность и компьютерная безопасность. М., 1991. С. 11.

[3] Быков В. М., Черкасов В. Н. Преступления в сфере компьютерной информации: криминологические, уголовно-правовые и криминалистические проблемы: монография. М., 2015. С. 102.

[4] Susan. W. Brenner Cybercrime metrics: old wine, new bottle? // Virginia journal of law and technology. 2004. vol. 9. P. 15.

уникальным комплексом доктринальных противоречий и прикладных проблем.

В связи с этим необходимо обсудить весьма важный вопрос: можно ли использование информационно-коммуникационных технологий рассматривать в качестве сигнификативного признака определённой группы преступлений. Принятая в Особенной части УК РФ классификация преступлений по объекту посягательства не содержит основания для дифференциации преступлений на «компьютерные», «насильственные», «вооружённые» и т.п. Вместе с тем, такая дифференциация представляется возможной и важной в целях как более глубокого их изучения, так и решения сугубо прикладных вопросов противодействия. При этом, конечно же, не следует относить к категории компьютерных преступлений общественно-опасные деяния, которые связаны с использованием виновным информационно-коммуникационного оборудования исключительно как объектов материального мира, посредством которых можно, например, причинить вред жизни или здоровью человека. Это решение обосновывается объективным отсутствием информационно-технологической составляющей в механизме преступного поведения субъекта.

Международный союз электросвязи в своих рекомендациях «Понимание киберпреступности: явление, задачи и законодательный ответ» выразил позицию, согласно которой отсутствие определения не является серьёзной проблемой в научном дискурсе, так как более правильным является использование подхода основанного на типологии[1].

В Докладе Управления Организации Объединённых Наций по наркотикам и преступности «Всестороннее исследование проблемы киберпреступности» также подчёркивается сложность определения понятия и отмечается, что более эффективным является определение перечня или набора деяний, которые входят в понятие киберпреступность[2].

Не соглашаясь с тезисом о невозможности выделения компьютерных преступлений, следует всё же признать, что все попытки сформулировать некое общее определение данного явления, которое смогло бы вобрать в себя столь обширную и пёструю палитру посягательств, пожалуй, заведомо обречены на провал. Так, в самом широком смысле под анализируемыми преступлениями можно было бы понимать совокупность предусмотренных уголовным законом общественно опасных деяний, совершаемых с использованием средств хранения, обработки или передачи компьютерной информации либо информационно-коммуникационных сетей и оконечного оборудования. Понятно, что поскольку в настоящее время, не говоря уже о

---

[1] [Электронный ресурс] // http://www.itu.int/ITU-D/cyb/cybersecurity/docs/CCL-R.pdf (дата обращения: 03.05.2018).

[2] [Электронный ресурс] // http://www.unodc.org/documents/organized-crime/cybercrime/ Cybercrime_Study_Russian.pdf (дата обращения: 07.05.2018).

ближайшем будущем, цифровизация жизнедеятельности обусловит обыденность цифровых аспектов практически всех преступлений, такое определение обладает крайне незначительным теоретико-прикладным функционалом или, говоря напрямую, мало что проясняет в содержании явления.

Полагаем, что в самом обобщенном виде *под преступлениями, совершаемыми с использованием информационно-коммуникационных технологий, следует понимать общественно опасные, уголовно-противоправные деяния, совершаемые в отношении и (или) посредством методов, процессов или программно-технических средств, интегрированных с целью хранения, обработки или передачи компьютерной информации.*

В условиях цифровизации можно выделить два качественно разных по своей природе процесса в уголовно-правовой сфере. Первый связан с усложнением информационных отношений, при котором появляются новые информационные ценности (информационные активы) и, как следствие, новые формы общественно опасных посягательств на них. Некоторые из этих новых форм уже осмыслены законодателем и вплетены в ткань отечественного уголовного законодательства. Примером здесь может выступать включение в ч. 3 ст. 141 УК РФ положений о неправомерном вмешательстве в работу Государственной автоматизированной системы Российской Федерации «Выборы», а также установление ответственности за неправомерное воздействие на объекты критической информационной инфраструктуры Российской Федерации (ст. 274^1 УК РФ).

Второй процесс связан с изменением традиционной преступности в связи с внедрением информационно-коммуникационной инфраструктуры в механизм совершения преступления, в результате чего она приобрела дополнительное компьютерное (виртуальное) измерение. Наиболее ярким примером подобной «цифровой мутации» преступления явилось кардинальное изменение практики по делам о распространении порнографии и сбыте наркотиков. Особенности глобальной сети Интернет открыли перед распространителями порнографии и наркотиков ранее не виданные возможности, главным из которых явилось отсутствие необходимости личного контакта с приобретателем запрещённых объектов.

Признавая взаимосвязь и взаимообусловленность этих процессов, можно говорить о формировании и развитии двух самостоятельных уголовно-правовых феноменов: *«компьютерной преступности»* и *«компьютеризированной преступности»*. При этом если компьютерная преступность сугубо состоит из посягательств на объекты информационно-коммуникационной инфраструктуры (в том числе компьютерную информацию), то компьютеризированная преступность представляет собой весьма неопределённое и в известном смысле подвижное явление – традиционную преступность, которая ввиду цифрового обновления

общества, демонстрирует тенденцию стремительной «виртуализации». Таким образом, многослойная природа преступлений, совершаемых с использованием информационно-коммуникационных технологий, может быть представлена следующими видами преступлений:

1) *компьютерные преступления* – общественно опасные посягательства на установленный порядок хранения, обработки или передачи компьютерной информации либо эксплуатации информационно-коммуникационных сетей и оконечного оборудования (глава 28 УК РФ). Данная группа деяний является своего рода краеугольным элементом преступлений, совершаемых с использованием информационно-коммуникационных технологий. Именно посягательства на безопасность информационных активов и элементов информационно-коммуникационной инфраструктуры символизируют качественное изменение уголовно-правовой сферы, связанное с формированием совершенно нового типа общественных отношений;

2) *компьютеризированные преступления по признакам объекта – общественно опасные посягательства на традиционно охраняемые уголовным законом общественные отношения, опосредуемые информационно-коммуникационной инфраструктурой (ч. 3 ст. 141, п. «г» ч. 3 ст. 158, ст.ст. 159^{3}, 159^{6}, 187 УК РФ).* Научно-технический прогресс, совершенствование производства и, как следствие, удешевление компьютерной техники, программного обеспечения и услуг связи обусловили процесс непрерывного роста использования информационно-коммуникационных технологий во всех сферах жизни общества: экономике, политике, культуре и др. В результате привычные социальные модели взаимодействия приобрели информационно-технологическое измерение – расчеты на бытовом уровне и между хозяйствующими субъектами все больше стали осуществляться с использованием электронных денег и средств платежа, в избирательный процесс было внедрено специализированное программно-техническое обеспечение, целые направления государственного контроля и управления также получили свою «цифровую прививку» путем внедрения централизованных баз данных. Такой переход от традиционных (межличностных, «бумажных») форм социального взаимодействия к новым цифровым формам не изменил сути самих отношений, но придал им другое измерение с новыми рисками и угрозами;

– *компьютеризированные преступления по признакам объективной стороны*, в свою очередь, подразделяются на две подгруппы:

1) простые – общественно опасные посягательства на традиционно охраняемые уголовным законом общественные отношения, для которых использование информационно-коммуникационных технологий является значимо распространенным (в отдельных случаях – единственно возможным) способом осуществления общественно опасного деяния (ст.ст. 137, 138, 138^{1}, 146, 171^{2}, 185^{3}, 282, 354^{1} УК РФ). Указанная группа

характеризуется тем, что информационно-технологический способ совершения преступления учитывается как возможный и не влияющий на степень общественной опасности самого деяния. Следует отметить, что определение перечня данных преступлений и представляет основной предмет научного дискурса об отграничении традиционных и компьютерных преступлений. Полагаем, что в качестве критерия следует опираться не только на конструкции диспозиций уголовно-правовых норм Особенной части УК РФ, но и на объективное состояние самой преступности в части ее «миграции» в виртуальное пространство. Именно по этой причине к данной группе преступлений мы относим нарушение неприкосновенности частной жизни (ст. 137 УК РФ), уголовно-правовая норма об ответственности за которое не содержит специальной оговорки об использовании информационно-коммуникационных технологий, однако состояние правоприменения объективно указывает на то, что именно такой способ является преобладающим по данной категории дел;

2) квалифицированные – общественно опасные посягательства на традиционно охраняемые уголовным законом общественные отношения, для которых использование информационно-коммуникационных технологий является не только распространенным, но и отягчающим способом осуществления общественно опасного деяния (п. «д» ч. 2 ст. 110, п. «д» ч. 3 ст. 110[1], ч. 2 ст. 110[2], п. «в» ч. 2 ст. 151[2], ст. 205[2], п. «б» ч. 2 ст. 228[1] УК РФ и др.). Сущность компьютеризированной преступности заключается также в том, что использование соответствующих информационных технологий является не просто распространенным, но и создает такой комплекс теоретико-прикладных противоречий, которые в своей совокупности позволяют сделать вывод о качественном изменении общественной опасности новой (информационно-технологической) формы традиционного преступления. Необходимо отметить, что состояние отечественного уголовного законодательства не всегда адекватно отражает фактическое состояние данной группы преступлений.

Все остальные преступления, условно – *потенциально компьютеризированные*, посягающие на традиционно охраняемые уголовным законом общественные отношения, для которых использование информационно-коммуникационных технологий хотя и является возможным, однако выступает крайне редким, не типичным, фиксируемым от случая к случаю способом («crimes in which the computer is incidental to the offence»[1]), и на современном историческом этапе не оказывает значимого влияния на степень общественной опасности деяния (ст. 105, 205, 281 УК РФ и др.), на наш взгляд, не следует рассматривать в ряду изучаемого явления. Все это можно отнести к числу так называемой смежной проблематики, не представляющей актуального значения для

[1] Grabosky P. Cybercrime: keynotes in criminology and criminal justice series. New York: Oxford university press, 2016. P. 8.

противодействия именно компьютеризированной преступности как уже сложившейся на текущий момент социально негативной практике.

Таким образом, границы преступлений, совершаемых с использованием информационно-коммуникационных технологий, хотя и весьма подвижны, но всё же могут быть очерчены. Понятно, что в их определении ключевым фактором выступает достоверность криминологического знания о конкретной форме преступного поведения – в каких проявлениях и насколько масштабно то или иное преступление демонстрирует тенденцию к информатизации, сместилось ли оно в виртуальное пространство, какие проблемы это вызвало на уровне нормативного и правоприменительного противодействия.

С течением времени потенциально компьютеризированные преступления, конечно же, могут изменить свой статус. Так, например, совершение убийства посредством вмешательства в работу кардиостимуляторов и кохлеарных имплантов в настоящее время имеет характер лишь теоретического дискурса. На конференции по безопасности «Breakpoint» в Мельбурне (17.10.2012 г.) исследователь Барнаби Джек выступил с докладом о том, что из-за недоработок в программном обеспечении имплантируемые кардиостимуляторы можно заставить нанести смертоносный удар током напряжением 830 вольт путём отправки команды с ноутбука, находящегося на расстоянии до 15 метров[1]. С. Бреннер в качестве подтверждения реальности подобных угроз ссылается на дело Доминика Раймера, имевшее место ещё в 1994 году в Великобритании. 21-летний Раймер взломал внутреннюю сеть медицинского учреждения и внёс заведомо ложные сведения о лечении двух пациентов. В цифровую карту 9-летнего пациента, страдающего от менингита, он в графе назначенных препаратов указал совокупность сильнодействующих средств от сердечной недостаточности и высокого артериального давления. Трагические последствия не наступили только благодаря опыту и бдительности медсестры, которая решила перепроверить имеющиеся в базе данные с лечащим врачом. Однако второму пациенту всё-таки осуществили не вызванную медицинской необходимостью инъекцию антибиотика, который по счастливому стечению обстоятельств значимо не повлиял на его здоровье. Раймер предстал перед судом, однако был осуждён только за неправомерный доступ к компьютерной информации. Суд счёл недоказанным, что у подсудимого был умысел на причинение вреда здоровью или лишение жизни человека[2]. Как бы то ни было, с высокой долей вероятности можно предположить, что стремительное развитие имплантируемых технологий

[1] [Электронный ресурс] // URL: http://hitech.newsru.com/article/17Oct2012/cardio (дата обращения: 08.02.2018).

[2] Brenner S. W. Cybercrime and the law: challenges, issues and outcomes. Boston: Northeastern University press. 2012. P. 115.

кардинально изменит привычную картину преступлений против личности и, следовательно, обусловит «миграцию» убийства в категорию компьютеризированных преступлений, а, возможно, и потребует определённых законодательных решений.

В дополнение к сказанному следует лишь отметить, что менее вероятна, но всё же допустима и обратная тенденция, когда то или иное общественно опасное посягательство утратит свойства компьютеризированной преступности, например, по причине успешного противодействия со стороны правоохранительных органов.

Для соблюдения требований моносемантичности научных юридических терминов, а также чёткого разделения преступлений, посягающих на установленный порядок хранения, обработки или передачи компьютерной информации, и деяний, направленных на причинение вреда другим охраняемым уголовным законом общественным отношениям посредством использования информационно-коммуникационных технологий, мы полагаем возможным оперировать двумя приведёнными выше терминами: «*компьютерное преступление*» и «*компьютеризированное преступление*».

Выбор первого по большому счёту обусловлен сложившейся языковой традицией именовать посягательства, предусмотренные главой 28 УК РФ, именно «компьютерными преступлениями». Технические нестыковки, на которые обращают внимание отдельные специалисты, в действительности не так уж и важны, когда мы говорим о термине, главным предназначением которого является достаточно чётко отражать в массовом сознании определённую группу посягательств. Заменив его на европейскую версию – «киберпреступления», мы, пожалуй, лишь навредим этой ассоциативной связи, специалистам и не являющимся таковыми придётся попросту привыкать к новой для себя терминологии.

Введение в научный оборот авторского термина «компьютеризированное преступление» имеет, на наш взгляд, следующие преимущества: 1) прежде всего, он позволяет выразить объективно существующую связь с компьютерными преступлениями; 2) с этимологической точки зрения термин достаточно чётко выражает суть подобного рода посягательств, а именно их производный характер от некоего прототипа преступного поведения, существовавшего ранее и видоизменившегося под влиянием компьютерных технологий и 3) термин находится в отечественной языковой традиции, которая с «компьютеризацией» ассоциирует развитие и внедрение всех информационно-коммуникационных технологий (не только компьютеров как таковых, но и смартфонов, смарт-вещей, Интернета и т.д.).

Завершая параграф, следует подчеркнуть его основные положения и выводы:

1) определение общего понятия преступлений, совершаемых с использованием информационно-коммуникационных технологий, представляет собой неразрешимую (утопическую) исследовательскую

задачу ввиду внутренне присущей амбивалентности данного социально негативного явления. При этом самое общее их дефинирование как совокупности предусмотренных уголовным законом общественно опасных деяний, совершаемых с использованием средств хранения, обработки или передачи компьютерной информации либо информационно-коммуникационных сетей и оконечного оборудования, обладает крайне незначительным теоретико-прикладным функционалом;

2) в самом обобщенном виде под преступлениями, совершаемыми с использованием информационно-коммуникационных технологий, следует понимать общественно опасные, уголовно-противоправные деяния, совершаемые в отношении и (или) посредством методов, процессов или программно-технических средств, интегрированных с целью хранения, обработки или передачи компьютерной информации;

3) дихотомия цифрового обновления уголовно-правовой сферы обусловила формирование и развитие двух самостоятельных уголовно-правовых феноменов: *«компьютерной преступности»* и *«компьютеризированной преступности»*;

4) с учетом вышеизложенного необходимо различать следующие группы преступлений, совершаемых с использованием информационно-коммуникационных технологий:

– *компьютерные преступления* – общественно опасные посягательства на установленный порядок хранения, обработки или передачи компьютерной информации либо эксплуатации информационно-коммуникационных сетей и оконечного оборудования (глава 28 УК РФ);

– *компьютеризированные преступления* – общественно опасные посягательства на традиционно охраняемые уголовным законом общественные отношения, опосредуемые информационно-коммуникационной инфраструктурой, либо для которых использование информационно-коммуникационных технологий является значимо распространенным (в отдельных случаях квалифицирующим) способом осуществления общественно опасного деяния;

5) все остальные преступления (*потенциально компьютеризированные*), посягающие на традиционно охраняемые уголовным законом общественные отношения, для которых использование информационно-коммуникационных технологий хотя и является возможным, однако выступает крайне редким, не типичным, фиксируемым от случая к случаю способом, и на современном историческом этапе не оказывает значимого влияния на степень общественной опасности деяния (ст. 105, 205, 281 УК РФ и др.), на наш взгляд, не следует рассматривать в ряду изучаемого явления. Их можно отнести к числу так называемой смежной проблематики, не представляющей актуального значения для противодействия именно

компьютеризированной преступности как уже сложившейся на текущий момент социально негативной практики.

Глава 2.
МЕЖДУНАРОДНО-ПРАВОВЫЕ СТАНДАРТЫ И СРАВНИТЕЛЬНО-ПРАВОВОЙ АНАЛИЗ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

2.1. МЕЖДУНАРОДНО-ПРАВОВЫЕ СТАНДАРТЫ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Преступления, совершаемые с использованием информационно-коммуникационных технологий, являются транснациональной проблемой. Ещё на заре формирования так называемого «информационного общества» эксперты признавали, что оно не имеет политических, социальных и экономических границ[1]. В связи с этим считается практически общепринятым, что эффективное противодействие киберпреступности возможно только путем объединения усилий всего мирового сообщества, которое должно установить единые основы юрисдикции и правила международного сотрудничества государств в этой сфере[2].

Следует сразу указать, что общего (универсального) соглашения, регулирующего противодействие преступлениям в сфере информационно-коммуникационных технологий, до настоящего времени не существует. Как справедливо пишет Т. Л. Тропина, имеющиеся международные инструменты, направленные на обеспечение кибербезопасности, характеризуются мозаичностью, являются фрагментарными и скорее конкурируют между собой, чем способствуют гармонизации уголовного и уголовно-процессуального законодательства государств[3].

В этом же ключе В. С. Овчинский резюмирует, что международно-правовые механизмы, позволяющие отстаивать суверенное право государств на регулирование информационного пространства, в том числе в национальном сегменте сети Интернет, не установлены. Большинство государств (в том числе Россия) вынуждены «на ходу» адаптировать

---

[1] Breivik P. S. Education for the information age // D.W. Farmer and T.F. Mech, eds. New Directions for Higher Education. № 78. 1992.

[2] См., например: Полякова Т. А. Базовые принципы правового обеспечения информационной безопасности // Труды ИГП РАН. 2016. № 3 (55). С. 17; Савенков А. Н. Противодействие киберпреступности в финансово кредитной сфере как вектор обеспечения глобальной безопасности // Государство и право. 2017. № 10. С. 6; Сидоренко Э. Л. Криминальное использование криптовалюты5 международные оценки // Международное уголовное право и международная юстиция. 2016. № 6. С. 8 –10. и др.

[3] Тропина Т. Л. Борьба с киберпреступностью: возможна ли разработка универсального механизма? // Международное правосудие. 2012. № 3.С.86 – 95.

государственное регулирование сферы информации и информационных технологий к новым обстоятельствам[1].

Одна из первых попыток формирования единого решения проблемы компьютерной преступности на международном уровне была реализована Организацией экономического сотрудничества и развития (ОЭСР)[2]. Немного позднее Комитет министров Совета Европы в своей рекомендация №R 89 (9) «О преступлениях, связанных с компьютерами»[3] от 13 сентября 1989 г. определил минимально необходимый к включению в национальное законодательство список киберпреступлений. Уже в 1991 году Интерпол ввёл в обиход кодификатор компьютерных преступлений и способов их совершения[4]. Согласно данному документу, каждому компьютерному преступлению соответствует определённый буквенный индекс, расположенный в порядке уменьшения общественной опасности совершенного деяния. Для описания деяния могут применяться до пяти кодов. По справедливому мнению О. М. Сафонова, «при разработке и интеграции новых составов, регламентирующих ответственность за совершение преступлений с использованием компьютерных технологий в отечественное законодательство использование данного кодификатора или разработка собственного на схожих принципах, смогло бы существенно упростить данную задачу»[5].

Советом Европы разработан ряд инструментов для гармонизации законодательства в сфере киберпреступности. Однако самый значимый и известный из них – Конвенция «О преступности в сфере компьютерной информации» (Будапешт, 23 ноября 2001 г.). Конвенция делит преступления на 4 группы и в каждой предусматривает несколько составов

---

[1] Овчинский В. С. Криминология цифрового мира: учебник для магистратуры. М., 2018. С. 11.

[2] [Электронный ресурс] // Computer-Related Crime: Analysis of Legal Polici. Paris: OECD. 1986 // URL: http://www.unicri.it/services/library_documentation/ catalogue_thesaurus/catalogue.php?id =7075&vw=f (дата обращения: 05.07.2017).

[3] [Электронный ресурс] // Рекомендация Совета Европы № 89 (9). О преступлениях, связанных с компьютерами от 13 сентября 1989 // URL: https://wcd.coe.int/ViewDoc.jsp?Ref=Rec%2889%299&Language=lanEnglish&Ver=original&Site=C%20M&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75 (дата обращения: 05.07.2017).

[4] [Электронный ресурс] // Классификация компьютерных преступлений по кодификатору международной уголовной полиции генерального секретариата Интерпола // URL: http://www.cyberpol.ru/cybercrime.shtml#p_04 (дата обращения: 25.06.2017).

[5] Сафонов О. М. Уголовно-правовая оценка использования компьютерных технологий при совершении преступлений: состояние законодательства и правоприменительной практики, перспективы совершенствования: дис. …канд. юрид. наук. М., 2015. С.156.

преступлений: 1) преступления против конфиденциальности, целостности и доступности компьютерных данных и систем; 2) правонарушения, связанные с использованием компьютерных средств; 3) правонарушения, связанные с содержанием данных; 4) правонарушения, связанные с нарушением авторского права и смежных прав[1].

Европейская конвенция о киберпреступности в качестве обязательной меры также предполагает установление уголовной ответственности юридических лиц. При этом условиями наступления ответственности организации названы: 1) совершение противоправных действий в целях получения выгоды для юридического лица; 2) действия должны быть выполнены лицом, занимающим руководящий пост (обладающим управленческими и (или) представительскими функциями); 3) действия должны быть сопряжены с использованием полномочий по представлению юридического лица, принятию решений или осуществлению контроля за его деятельностью. Конвенция также предписывает устанавливать ответственность юридических лиц и в случаях совершения противоправных действий иным работником под руководством лица, занимающего руководящий пост в организации.

Согласно ст. 13 Конвенции, к физическим лицам, совершившим преступления, предусмотренные конвенцией, должны применять эффективные, соразмерные и убедительные наказания, включая лишение свободы. К юридическим лицам возможно применение мер и неуголовного характера, включая денежные санкции.

Отдельно Будапештская конвенция о преступности в сфере компьютерной информации обязывают страны-участницы квалифицировать как преступные действия подстрекательство к совершению любого из предусмотренных ею преступлений, соучастие в нем, либо покушение. При этом установление ответственности за подстрекательство и соучастие является обязанностью государства-подписанта конвенции, а криминализация покушения является правом.

В настоящее время Конвенция Совета Европы «О преступности в сфере компьютерной информации» 2001 года, является, пожалуй, самым проработанным и значимым международным документом, направленным на объединение усилий мирового сообщества в борьбе с преступностью в информационном пространстве[2]. Несмотря на то, что Россия все ещё не присоединилась к ней, можно вполне уверенно утверждать, что наиболее существенные ее положения уже фактически имплементированы в

---

[1] Конвенция о преступности в сфере компьютерной информации (EST № 185) от 23 ноября 2001 // Режим доступа: СПС «Консультант-Плюс».

[2] С момента принятия конвенцию ратифицировали 29 из 47 государств - членов СЕ и США. Российская Федерация не ратифицировала ее из-за положений о трансграничном доступе к хранящимся компьютерным данным (пункт «b» статьи 32).

отечественное уголовное законодательство. Вместе с тем, на наш взгляд, подписание данной конвенции вывело бы на качественно другой уровень международное уголовное преследование лиц, совершивших киберпреступления.

Соглашение о сотрудничестве в области обеспечения международной информационной безопасности Шанхайской организации сотрудничества от 16 июня 2009 года содержит лишь общее определение информационной преступности, к которой данный документ также предлагает относить использование информационных технологий для совершения таких преступлений как мошенничество, вымогательство, контрабанда, незаконная торговля наркотиками, распространение детской порнографии и др.[1] К основным угрозам международной информационной безопасности соглашение относит: 1) разработку и применение информационного оружия, подготовка и ведение информационной войны;2) информационный терроризм;3) информационную преступность;4) использование доминирующего положения в информационном пространстве в ущерб интересам и безопасности других государств;5) распространение информации, наносящей вред общественно-политической и социально-экономической системам, духовной, нравственной и культурной среде других государств;6) угрозы безопасному, стабильному функционированию глобальных и национальных информационных инфраструктур, имеющие природный и (или) техногенный характер.

Нельзя не отметить, что положительной стороной Соглашения является определение основных понятий в области обеспечения информационной безопасности. Так, даётся понятие информационной преступности – использование информационных ресурсов и (или) воздействие на них в информационном пространстве в противоправных целях. Её признаками являются проникновение в информационные системы для нарушения целостности, доступности и конфиденциальности информации; умышленное изготовление и распространение компьютерных вирусов и других вредоносных программ; осуществление DOS-атак и иных негативных воздействий; причинение ущерба информационным ресурсам; нарушение законных прав и свобод граждан в информационной сфере, в том числе права интеллектуальной собственности и неприкосновенности частной жизни; использование информационных ресурсов и методов для совершения таких общеуголовных преступлений, как мошенничество, вымогательство, контрабанда, незаконная торговля наркотиками, распространение порнографии и т. д.

---

[1] [Электронный ресурс] // Соглашение между правительствами государств - членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности // URL: http://www.conventions.ru/ view _base.php?id=1979 (дата обращения: 28.07.2017).

Конвенция о борьбе с преступлениями в области информационных технологий Лиги арабских государств от 21 декабря 2010 года содержит следующий перечень информационных преступлений: 1) неправомерный доступ к компьютерной информации (ст.6); 2) неправомерный перехват компьютерной информации (ст. 7); 3) неправомерное воздействие на целостность компьютерной информации (ст. 8); 4) неправомерный оборот информационных технологий (ст. 9)[1]; компьютерный подлог (ст. 10); компьютерное мошенничество (ст. 11); незаконный оборот порнографии (ст.ст. 12, 13); нарушение неприкосновенности частной жизни (ст. 14); кибертерроризм (ст. 15); организованные формы информационной преступности, связанные с легализацией, незаконным оборотом наркотических средств и иных запрещённых веществ, торговлей людьми и незаконной трансплантацией (ст. 16), информационные преступления, связанные с посягательством на объекты интеллектуальной собственности (ст. 17); неправомерный оборот цифровых средств платежа (ст. 18)[2].

В июне 2014 года Африканский союз принял Конвенцию о кибербезопасности и защите персональных данных[3]. В соответствии со статьями 29 и 30 данной конвенции государства-участники должны принять все необходимые законодательные меры, чтобы предусмотреть уголовную ответственность за: 1) неправомерный доступ к компьютерным данным и (или) системе; 2) несанкционированное уничтожение, повреждение, модификацию или копирование компьютерных данных; 3) изготовление и распространение детской порнографии; 4) изготовление, приобретение (в оригинале «download», то есть копирование в память устройства), распространение любых сообщений, изображений или иной информации экстремистской направленности; 5) безоговорочное отрицание, одобрение или оправдание геноцида или иных преступлений против человечества путём использования компьютерной системы; 6) посягательства на собственность, совершаемых с применением

---

[1] В оригинале: «Article 9: Offence of Misuse of Information Technology Means 1. The production, sale, purchase, import, distribution or provision of: a) any tools or programmes designed or adapted for the purpose of committing the offences indicated in Articles 6 to 8; б) the information system password, access code or similar information that allows access to the information system with the aim of using it for any of the offences indicated in Articles 6 to 8. 2. The acquisition of any tools or programmes mentioned in the two paragraphs above with the aim of using them to commit any of the offences indicated in Articles 6 to 8».

[2] [Электронный ресурс] // League of Arab States, 2010. Arab Convention on Combating Information Technology Offences // URL: http://www.arableagueonline.org/ (дата обращения: 20.12.2017 г.).

[3] [Электронный ресурс] // URL: http://pages.au.int/sites/default/files/en_AU%20Convention% 20on%20CyberSecurity%20Pers%20Data%20Protec% 20AUCyC%20adopted%20Malabo.pdf. (дата обращения: 10.12.2017).

компьютерных данных. Отдельно отмечается, что использование компьютерной информации и информационно-коммуникационных технологий при совершении таких преступлений, как терроризм и легализация денежных средств, необходимо оценивать в качестве отягчающего обстоятельства (п. «b» ч. 1 ст. 30).

С 2001 г. в рамках Содружества Независимых Государств действовало Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере компьютерной информации [1]. Основными целями сотрудничества в рамках данного соглашения являлось обеспечение эффективной борьбы с преступлениями в сфере компьютерной информации и создание правовых основ сотрудничества правоохранительных и судебных органов стран-участников соглашения в борьбе с ними.

С 12 марта 2020 г. вступило в силу Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере информационных технологий (заключено в г. Душанбе 28.09.2018)[2]. Данное соглашение пришло на смену Соглашению СНГ 2001 г.

В соответствии с положениями Соглашения государства-подписанты должны признать в соответствии с национальным законодательством в качестве уголовно наказуемых следующие деяния в сфере информационных технологий:

а) уничтожение, блокирование, модификация либо копирование информации, нарушение работы информационной (компьютерной) системы путем несанкционированного доступа к охраняемой законом компьютерной информации;

б) создание, использование или распространение вредоносных программ;

в) нарушение правил эксплуатации компьютерной системы лицом, имеющим к ней доступ, повлекшее уничтожение, блокирование или модификацию охраняемой законом компьютерной информации, если это деяние причинило существенный вред или тяжкие последствия;

г) хищение имущества путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, либо путем введения в компью-

---

[1] [Электронный ресурс] // Соглашение о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере компьютерной информации от 01 июня 2001 г. // URL: http://www.cis.minsk. by/page.php?id=866 (дата обращения: 06.11.2017).

[2] Единый реестр правовых актов и других документов СНГ http://cis.minsk.by/(дата обращения: 02.04.2020).

терную систему ложной информации, либо сопряженное с несанкционированным доступом к охраняемой законом компьютерной информации;

д) распространение с использованием информационно-телекоммуникационной сети Интернет или иных каналов электрической связи порнографических материалов или предметов порнографического характера с изображением несовершеннолетнего;

е) изготовление в целях сбыта либо сбыт специальных программных или аппаратных средств получения несанкционированного доступа к защищенной компьютерной системе или сети;

ж) незаконное использование программ для компьютерных систем и баз данных, являющихся объектами авторского права, а равно присвоение авторства, если это деяние причинило существенный ущерб;

з) распространение с использованием информационно-телекоммуникационной сети Интернет или иных каналов электрической связи материалов, признанных в установленном порядке экстремистскими или содержащих призывы к осуществлению террористической деятельности или оправданию терроризма.

Следует отметить, что данные соглашения, имея рекомендательный характер, оставляют национальному законодателю возможность учитывать присущие той или иной стране особенности. Так, например, в итоговом документе Тринадцатого Конгресса Организации Объединенных Наций по предупреждению преступности и уголовному правосудию (Доха, 12–19 апреля 2015 г.) в качестве рекомендации специально указано, что в области киберпреступности государствам-членам следует руководствоваться сбалансированным правовым подходом, который предусматривает признание в качестве конкретных преступлений основных деяний против конфиденциальности, целостности и доступности компьютерных данных и компьютерных систем, при одновременном рассмотрении вопроса о применимости к деяниям, совершенным в режиме онлайн, положений, касающихся таких общеуголовных преступлений, как хищение, мошенничество, фальсификация и преступления против личности[1].

В завершение данного параграфа представляется необходимым сделать ряд значимых обобщений:

1) имеющиеся региональные международно-правовые документы создают определенную основу для формирования национального уголов-

[1] [Электронный ресурс] // URL: http://www.un.org/ru/events/crimecongress2015/cybercrime.shtml (дата обращения: 06.08.2017).

ного законодательства об ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий;

2) региональные международные документы хотя и незначительно, но все же расходятся в определении содержания и круга компьютерных преступлений, что не позволяет утверждать о наличии единого международного стандарта криминализации деяний, связанных с злоупотреблениями современными информационно-коммуникационными технологиями;

3) не только российское общество, но и современное человечество в целом, стоят перед необходимостью открыть для себя новые перспективы развития. Необходимо понять, что никакие локальные решения не смогут изменить направление существующего движения народов – к полной несостоятельности в обеспечении информационной безопасности. Решения должны быть общими для всех. В этих условиях только общепринятые международные стандарты, строго инкорпорированные национальными законодательствами государств, могут оказаться той базой, тем инструментом, который преобразует множество частных теоретических концепций и конкретных нормативных решений, в некоторую целостную программу уголовно-правового противодействия информационной преступности. В условиях взаимосвязанного и взаимозависимого мира необходимость принятия единого международного документа о противодействии преступлениям, совершаемым с использованием современных информационно-коммуникационных технологий, приобретает очевидный характер. Региональные документы никогда не смогут решить глобальную по содержанию проблему эффективного противодействия киберпреступности.

Представляется, что наиболее приемлемым решением было бы принятие документа на уровне ООН[1], который определил бы не только общепринятую классификацию компьютерных преступлений, но и представил бы единые рекомендации государствам по их криминализации в национальном законодательстве.

[1] Данный вывод находит свою поддержку и в отечественной теории уголовного права. См.: Ефремова М.А. Уголовно-правовая охрана информационной безопасности: монография. М., 2018. С. 88; Савенков А.Н. Противодействие киберпреступности в финансово-кредитной сфере как вектор обеспечения глобальной безопасности // Государство и право. – 2017. – № 10. – С. 10 и др.

2.2. СРАВНИТЕЛЬНО-ПРАВОВОЙ АНАЛИЗ УГОЛОВНОГО ЗАКОНОДАТЕЛЬСТВА ЗАРУБЕЖНЫХ СТРАН ОБ ОТВЕТСТВЕННОСТИ ЗА ПРЕСТУПЛЕНИЯ, СОВЕРШАЕМЫЕ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Экстерриториальный характер преступлений, совершаемых с использованием информационно-коммуникационных технологий, заставляет совершенно по-другому взглянуть на роль и значение сравнительного правоведения в решении конкретных отраслевых проблем отечественного уголовного права. Познание опыта зарубежных стран в противодействии таким преступлениям позволяет не только обогатить отечественную науку, но и критически осмыслить национальное законодательство, выявить его слабые и сильные стороны, указать на очевидные проблемы, а также предложить наиболее правильные пути их разрешения. Не менее важным является и то, что отчётливое понимание особенностей установления и реализации ответственности за компьютерные и компьютеризированные преступления является непременным условием эффективного взаимодействия с правоохранительными органами и правовыми системами других государств.

В связи с этим следует лишь отчасти согласиться с мнением М. А. Простосердова, что зарубежный опыт противодействия киберпреступности можно охарактеризовать как несогласованный и поэтому малоэффективный. На национальных уровнях сложились свои направления уголовно-правовой политики противодействия киберпреступности и подходы построения уголовно-правовых норм[1].

Несогласованность подходов различных стран в противодействии киберпреступности действительно является вполне очевидной. С другой стороны, можно говорить и о некоторых решениях, имеющих почти общепринятый характер. К тому же смешанный «нормативный ландшафт» современного мира сам по себе представляет значительную научную ценность. Разные законодательные модели необходимо исследовать и верифицировать на предмет их пригодности для решения актуальных проблем противодействия компьютерной и компьютеризированной преступности на национальном уровне. Как справедливо пишет по данному поводу М. А. Ефремова: «процесс информатизации нашёл своё отражение в уголовном законодательстве зарубежных стран раньше, чем в российском. В этой связи исследование уголовного законодательства зарубежных стран представляет научный интерес с позиции выявления перспективных

[1] Простосердов М. А. Экономические преступления, совершаемые в киберпространстве: монография. М., 2017. С. 41.

направлений развития уголовного законодательства в данной сфере, которые могли быть заимствованы отечественным законодателем»[1].

Законодательные подходы к определению преступлений, совершаемых с использованием информационно-коммуникационных технологий, в США, Канаде, Великобритании, Австралии, Новой Зеландии и Сингапуре

Значительный материал по теме, конечно же, содержит уголовное законодательство Соединённых Штатов Америки, которые, пожалуй, одними из первых обратили внимание на проблему действенного противодействия преступлениям, совершаемым с использованием компьютерных технологий.

Ответственность за неправомерный доступ к компьютеру, компьютерной системе или компьютерной информации, которые могут быть отнесены к так называемой критической информационной инфраструктуре, предусмотрена §1030 Свода законов США[2]. Данное преступление относится к категории так называемых федеральных преступлений. На уровне сводов законов отдельных штатов выделяются главы о киберпреступлениях (глава 16 Свода законов штата Южная Каролина, глава 815 Свода законов штата Флорида, глава 41 Свода законов штата Арканзас и др.), в рамках которых преступлениями преимущественно признаются неправомерный доступ к компьютерной информации, неправомерная модификация компьютерной информации, создание и распространение в любой форме компьютерной информации, которая заведомо предназначена для совершения преступлений, неправомерное распространение информации о сетевых идентификаторах.

Свод законов штата Джорджия в §16-9-93 устанавливает ответственность за компьютерное хищение (computer theft), компьютерное злоупотребление (computer trespass), компьютерное нарушение неприкосновенности частной жизни (computer invasion of privacy), компьютерный подлог (computer forgery), разглашение сведений о средствах доступа к компьютеру или компьютерной сети (computer password disclosure)[3].

Наибольшим сходством с отечественной нормой об уголовной ответственности за неправомерный доступ к охраняемой законом компьютерной информации является компьютерное злоупотребление, которое предполагает совершение лицом несанкционированных другим пользователем действий в целях 1) удаления (полного или временного)

---

[1] Ефремова М. А. Уголовно-правовая охрана информационной безопасности: монография. М., 2018. С. 89.

[2] [Электронный ресурс] // URL: https://www.law.cornell.edu/uscode/text/18 (дата обращения: 06.08.2017).

[3] [Электронный ресурс] // URL: https://law.justia.com/codes/georgia/2010/title-16/chapter-9/article-6/part-1/16-9-93 (дата обращения: 06.08.2017).

компьютерной программы, 2) воспрепятствования использованию компьютера, компьютерной программы или компьютерной информации, 3) повреждения компьютера, компьютерной сети или компьютерной программы, независимо от того, как долго сохраняются (длятся) соответствующие изменения или неисправности[1]. В качестве наказаний за данное преступление может быть назначен штраф на сумму не свыше 50 000 долларов США или лишение свободы на срок не свыше 15 лет.

Ответственность за разглашение сведений о паролях доступа к компьютерному оборудованию или сети наступает только в случае причинения материального ущерба потерпевшему на сумму свыше 500 долларов США[2].

Представляет интерес подход законодателя штата Джорджия к установлению ответственности за так называемый «спаминг». В соответствии с §16-9-102 лицо осуществляющее массовую рассылку электронных писем в коммерческих целях, осознававшее их заведомо ложный характер, наказывается штрафом на сумму не свыше 1000 долларов США или лишением свободы на срок до 1 года[3].

Квалифицирующими обстоятельствами «спамминга» Свод законов штата Джорджия называет: 1) осуществление рассылки в объёме свыше 10 000 получателей в любой 24-часовой период; 2) осуществление рассылки в объёме свыше 100 000 получателей в течение 30 дней; 3) если число получателей рассылки превысило 1 млн. в течение года; 4) если лицо получило доход от одного сообщения в размере свыше 1000 долларов США; 5) если лицо получило доход от всей рассылки в размере свыше 50 000 долларов США; 6) если в осуществление массовой рассылки электронных сообщений было вовлечено заведомо несовершеннолетнее лицо. При наличии данных отягчающих обстоятельств лицо наказывается

---

[1] «Any person who uses a computer or computer network with knowledge that such use is without authority and with the intention of:(1) Deleting or in any way removing, either temporarily or permanently, any computer program or data from a computer or computer network;(2) Obstructing, interrupting, or in any way interfering with the use of a computer program or data; or (3) Altering, damaging, or in any way causing them malfunction of a computer, computer network, or computer program, regardless of how long the alteration, damage, or malfunction persists shall be guilty of the crime of computer trespass».

[2] «Any person who discloses a number, code, password, or other means of access to a computer or computer network knowing that such disclosure is without authority and which results in damages (including the fair market value of any services used and victim expenditure) to the owner of the computer or computer network in excess of $500.00 shall be guilty of the crime of computer password disclosure».

[3] «Any person who initiates a commercial e-mail that the person knew or should have known to be false or misleading that is sent from, passes through, or is received by a protected computer shall be guilty of the crime of initiation of deceptive commercial e-mail».

штрафом в размере не более 50 000 долларов США или лишением свободы на срок не более 5 лет.

Свод законов штата Род-Айленд в §11-52-2 устанавливает ответственность за доступ к компьютеру в неправомерных (мошеннических) целях (access to computer for fraudulent purposes), умышленное уничтожение или повреждение компьютера либо компьютерной сети, умышленное уничтожение, модификацию или блокирование компьютерной информации (§11-52-3), компьютерную кражу (§11-52-4), компьютерное злоупотребление (§11-52-4.1), киберстокинг (§11-52-4.2), уничтожение или повреждение компьютерной информации, которую лицо было обязано хранить в силу требований закона (§11-52-8)[1].

Киберстокинг определяется законодателем Род-Айленда как умышленное преследование лица или членов его семьи путём отправки сообщений с помощью компьютера или другого электронного устройства, которые вызывают у потерпевшего чувство тревоги, раздражения или беспокойства, и не преследуют никакой законной цели[2].

Свод законов штата Миссисипи ответственность за компьютерные преступления регламентирует в главе 45 (раздел 97). Данная глава объединяет нормы об ответственности за компьютерное мошенничество (§97-45-3), распространение сведений о сетевых идентификаторах пользователя (§97-45-5), неправомерное воздействие на компьютер, компьютерные сети и компьютерную информацию (§97-45-7), киберстокинг (§97-45-15), распространение электронных сообщений для причинения ущерба (§97-45-17).

Примечательной особенностью уголовного законодательства штата Миссисипи является криминализация действий, связанных с регистрацией интернет-аккаунта от имени другого лица в отсутствие его согласия с целью причинения ущерба, запугивания или обмана кого бы то ни было

---

[1] [Электронный ресурс] // URL:https://law.justia.com/codes/rhode-island/2012/title-11/chapter-11-52/(дата обращения: 06.08.2017).

[2] «Whoever transmits any communication by computer or other electronic device to any person or causes any person to be contacted for the sole purpose of harassing that person or his or her family is guilty of a misdemeanor, and shall be punished by a fine of not more than five hundred dollars ($500), by imprisonment for not more than one year, or both. For the purpose of this section, «harassing» means any knowing and willful course of conduct directed at a specific person which seriously alarms, annoys, or bothers the person, and which serves no legitimate purpose. The course of conduct must be of a kind that would cause a reasonable person to suffer substantial emotional distress, or be in fear of bodily injury. «Course of conduct» means a pattern of conduct composed of a series of acts over a period of time, evidencing a continuity of purpose. Constitutionally protected activity is not included with in the meaning of «course of conduct».

(§97-45-33)[1]. Как следует из текста нормы, ответственность наступает не просто за регистрацию страницы на имя другого человека, например, в Facebook, а только при условии, что таким образом лицо желает обеспечить свою анонимность при осуществлении каких-либо противоправных действий.

Нельзя не отметить и другое важное обстоятельство. Свод законов штата Миссисипи содержит норму, которая специально оговаривает, что положения главы о компьютерных преступлениях не исключают возможности вменения других составов преступлений в случаях, когда неправомерные действия с компьютерной информацией по-сути выступали способом их осуществления[2].

Уголовные законодательства штатов позволяют выявить и другие примеры специального разрешения вопросов совокупности при юридической оценке компьютерных преступлений. Так, например, §16-16-20 (5) Свода законов штата Южная Каролина определяет, что самостоятельным компьютерным преступлением следует считать причинение вреда каждому отдельному компьютеру, компьютерной системе или компьютерной сети[3].

С точки зрения отечественной науки уголовного права такое решение представляется несколько прямолинейным и одновременно поверхностным. Множество пострадавших устройств не может автоматически предрешать невозможность квалификации содеянного как единичного сложного преступления. Так, например, однократное распространение лицом вируса-шифровальщика в течение короткого промежутка времени может вызвать заражение и блокирование компьютерной информации сотен и тысяч потерпевших. Понятно, что вменение здесь совокупности будет иметь несколько искусственный характер – никаких сотен и тысяч самостоятельных преступлений в действительности не совершалось. В связи с этим полагаем, что количественный критерий повреждённого компьютерного оборудования и (или) компьютерной информации должен учитываться, прежде всего, при дифференциации уголовной ответственности за преступления,

---

[1] «Noth with standing any other provision of law, any person who knowingly and without consent impersonates another actual person through or on an Internet website or by other electronic means for purposes of harming, intimidating, threatening or defrauding another rperson».

[2] «The criminal offenses created by this chapter shall not be deemed to supersede, or repeal, any other criminal offense».

[3] «Each computer, computer system, or computer network affected by the violation of this chapter constitutes a separate violation» // [Электронный ресурс] // URL: https://law.justia.com/codes/ south-carolina/2012/title-16/chapter-16/section-16-16-20/(дата обращения: 06.08.2017).

совершаемые с использованием информационно-коммуникационных технологий.

Примечательно, что большинство штатов не оперирует понятием «вредоносная компьютерная программа» и устанавливает ответственность за распространение программных продуктов или компьютерной информации вообще, однако с намерением причинить ущерб или вызвать прерывание или ухудшение надлежащего функционирования любого компьютера, компьютерной сети, компьютерной системы или ее части. Такой подход, в частности, реализован в §18-5.5-102 Свода законов штата Колорадо[1].

Свод законов штата Нью-Джерси особо отягчающими обстоятельствами неправомерного воздействия на компьютерную информацию называет существенное нарушение работы общественного транспорта, подачи воды, газа или электроэнергии или другой социальной службы. При этом под «существенным нарушением» предлагается понимать неправомерный доступ, который: 1) затронул 10 или более самостоятельных зданий и длился 2 и более часа либо 2) создал риск наступления смерти человека или последствий в виде тяжкого вреда здоровью; 3) повлёк ущерб или убыток на сумму свыше 250 000 долларов США; 4) повлёк причинение вреда здоровью человека[2].

В соответствии со Сводом законов штата Нью-Джерси неправомерное вмешательство в работу компьютерного оборудования и систем органов государственной власти является составом так называемой строгой ответственности, по которому обвинение освобождено от необходимости доказывания умысла лица на причинение вреда информационным ресурсам именно таких субъектов[3]. Такое законодательное решение, как известно, не соответствует классическим положениям отечественного уголовного права о возможности ответственности лица только при условии установления его виновного отношения ко всем юридически значимым признакам состава преступления. Полагаем, что в данном случае, впрочем как и по другим составам строгой ответственности, законодатель поступается стройностью

---

[1] Causes the transmission of a computer program, software, information, code, data, or command by means of a computer, computer network, or computer system or any part thereof with the intent to cause damage to or to cause the interruption or impairment of the proper functioning of or that actually causes damage to or the interruption or impairment of the proper functioning of any computer, computer network, computer system, or part thereof» // [Электронный ресурс] // URL: https://law.justia.com/codes/ colorado/2016/title-18/article-5.5/section-18-5.5-102 (дата обращения: 17.05.2018).

[2] [Электронный ресурс] // URL: https://law.justia.com/codes/new-jersey/2013/title-2c/section-2c-20-25/ (дата обращения: 06.05.2018).

[3] «The defendant shall be strictly liable under this subsection and it shall not be a defense that the defendant did not know or intend that the victim was a government agency, or that the defendant intended that there be other victims of the crime».

теоретико-правовых конструкций уголовного права в пользу социальной необходимости и практической целесообразности. Действительно, злоумышленник практически всегда может защититься тем, что, распространяя вредоносное программное обеспечение, он, желал заблокировать сайт конкретного интернет-магазина и не допускал экспансивное распространение вируса и наступление последствий для информационной инфраструктуры целого города. Такое объяснение с процессуальной и криминалистической точки зрения сложно будет поставить под сомнение, что делает практически невозможным вменение лицу фактически наступивших тяжких последствий и назначение справедливого наказания.

Помимо традиционных уголовно-правовых запретов можно выделить специфический состав преступления, предусмотренный §5-41-204 Свода законов штата Арканзас об ответственности за незаконное использование шифрования (unlawful use of encryption)[1].

Следует отметить, что в отдельных штатах законодатель уделил особое внимание регламентации обстоятельств, которые могут выступать в качестве должной защиты (anaffirmative defense) от уголовного преследования за совершение деяния, посягающего на безопасность компьютерных данных. Так, например, Свод законов штата Нью-Гемпшир в §638.17 специально оговаривает, что лицо не может подлежать уголовной ответственности в случаях, если: 1) лицо было добросовестно убеждено, что правообладатель компьютера или компьютерной информации уполномочил его или должен был уполномочить на доступ к ним; 2) лицо не знало, не должно было и не могло знать, что доступ был осуществлён вопреки воли правообладателя компьютера или компьютерной информации[2].

Законодатель Канады весьма бессистемно подходит к определению преступлений, совершаемых с использованием информационно-коммуникационных технологий. Прежде всего в структуре Уголовного кодекса Канады отсутствует специальная глава (часть или раздел), посвящённая посягательствам на отношения, связанные с оборотом компьютерной информации. Отдельные компьютерные преступления включены в главы о посягательствах на отношения собственности, здоровье населения и общественный порядок.

В ст. 342[1] установлена ответственность за неправомерное использование компьютера (unauthorized use of computer). В соответствии с данной нормой преступлением является получение без достаточных на то оснований компьютерных услуг (сервиса по получению, хранению, обработке и

---

[1] [Электронный ресурс] // URL: http://law.justia.com/codes/arkansas/2010/title-5/subtitle-4/chapter-41/subchapter-2/5-41-206 (дата обращения: 06.05.2018).

[2] [Электронный ресурс] // URL: http://law.justia.com/codes/new-hampshire/2015/title-lxii/chapter-638/section-638-17 (дата обращения: 06.05.2018).

передаче информации), несанкционированное вмешательство в работу компьютерной системы, использование компьютерного оборудования в целях вредоносного воздействия на компьютерную информацию, а также использование, хранение и распространение сетевых идентификаторов другого лица (логина и пароля) для совершения одного из деяний, предусмотренных данной статьёй[1].

В соответствии со ст. 430 преступлением является вредоносное воздействие на компьютерную информацию (mischief in relation to computer data). Необходимыми последствиями деяния названы: уничтожение или повреждение информации, приведение её в непригодное для использования состояние, а также блокирование доступа к информации. Наиболее строгим наказанием является лишение свободы на срок до 10 лет[2].

Не лишним будет отметить, что в данной статье не конкретизирован способ «вредоносного воздействия». Таким образом, при буквальном толковании такое воздействие может быть как информационно-технологическим, так и сугубо физическим (путём повреждения или уничтожения носителей компьютерной информации).

Законодатель Канады не устанавливает самостоятельную ответственность за изготовление, распространение и использование вредоносных компьютерных программ или компьютерной информации. Следует, однако, отметить, что в ст. 327 предусмотрена ответственность за изготовление, распространение, продажу, предложение о продаже, размещение в открытом доступе, приобретение в целях использования компьютерных программ, предназначенных для обеспечения неоплачиваемого доступа к телекоммуникационным услугам.

Кроме того, в ст. 342.01 преступлением является совершение по-сути аналогичных действий в отношении компьютерных программ, предназначенных для неправомерного получения информации о платёжных картах или изготовления поддельных банковских карт.

С точки зрения отечественного законодательства и науки уголовного права экзотичным решением является установление в ст. 326 УК Канады ответственности за хищение телекоммуникационных услуг (theft of telecommunication service).

До 1990 года в законодательстве Великобритании не было специальных положений об ответственности за совершение компьютерных и компьютеризированных преступлений. Специалисты сходились во мнениях, что информатизация преступности и появление «виртуальных» способов совершения преступлений, в целом не создаёт непреодолимых

---

[1] [Электронный ресурс] // URL: http://laws-lois.justice.gc.ca/eng/acts/C-46/page-76.html#h-97 (дата обращения: 06.05.2018).

[2] [Электронный ресурс] // URL: http://laws-lois.justice.gc.ca/eng/acts/C-46/section-430.html (дата обращения: 06.05.2018).

препятствий для применения классических конструкций о краже, мошенничестве, уничтожении и повреждении имущества и т.д.[1]

Вместе с тем, суды начинали всё чаще испытывать трудности при юридической оценке действий, направленных против компьютерных данных и систем. Так, в деле «Cox vs Rilley» подсудимый уничтожил информацию на карте памяти устройства и таким образом вывел его из строя. Сторона защиты ссылалась на то обстоятельство, что в физическом смысле устройство, как и собственно карта, не пострадали, поэтому применение норм об уголовной ответственности за повреждение чужого имущества является невозможным. Суд не согласился с такими доводами и вынес обвинительный приговор[2].

В 1988 году в деле «R vs Gold and Another» решение суда об осуждении лица за подлог было отменено вышестоящим судом со ссылкой на то обстоятельство, что неправомерный доступ к компьютерной информации, связанный с использованием чужих сетевых идентификаторов и модификацией данных, не подпадает под действие уголовно-правовой нормы о подлоге[3].

С целью устранения имеющихся противоречий между нормативной базой и потребностями правоприменения был принят Закон о неправомерном использовании компьютерных технологий (Computer misuse act 1990), который с учётом поправок 2006 и 2015 годов устанавливает ответственность за следующие деяния: неправомерный доступ к компьютерной информации (ст. 1), неправомерный доступ в целях совершения иных преступлений (ст. 2), неправомерные действия в отношении компьютерных данных или нарушение правил эксплуатации средств хранения или обработки компьютерной информации (ст. 3), неправомерные действия в отношении компьютерных данных или нарушение правил эксплуатации средств хранения или обработки компьютерной информации, которые повлекли угрозу наступления тяжких последствий (ст. 3ZA), создание, приобретение или распространение компьютерных программ или компьютерной информации для совершения преступлений, предусмотренных статьями 1, 3 или 3ZA (ст. 3A)[4].

Кроме того, приспосабливание уголовного законодательства Великобритании к виртуальной преступности выразилось в принятии поправок к Закону Великобритании о мошенничестве (England fraud act 2006), определивших признаки компьютерного мошенничества. В

---

[1] Charlesworth A. Legislating against Computer Misuse: The trials and tribunals of the UK Computer Misuse Act 1990 // Journal of law and information science. 1993. № 1. P. 81.

[2] Cox vs Rilley [1986].

[3] R vs Gold and Another [1988].

[4] [Электронный ресурс] // URL: http://www.legislation.gov.uk/ukpga/1990/18 /section/2 (дата обращения: 15.04.2018).

соответствии с британским законодательством лицо, совершая обманные действия, в том числе с использованием средств связи (информационных технологий), в целях незаконного обогащения и причинения ущерба третьим лицам, подлежит наказанию в виде лишения свободы на срок до 5 лет[1].

Закон о киберпреступлениях Австралии (Cybercrime act 2001) классифицирует все преступления, совершаемые с использованием информационно-коммуникационных технологий, на две группы: тяжкие компьютерные преступления (serious computer offences) и другие компьютерные преступления (other computer offences). К первой группе относятся: неправомерный доступ к компьютерной информации или компьютерной системе в целях совершения тяжкого преступления (ст. 477^1), неправомерная модификация компьютерной информации (ст. 477^2), неправомерное нарушение электронной связи (ст. 477^3). Нельзя не отметить строгость наказаний за данные преступления – от 5 лет до пожизненного лишения свободы. При этом специфической особенностью санкции ст. 477^1 является то, что она построена по ссылочному принципу – вид и размер наказания определяется санкцией конкретного тяжкого преступления, которое намеревалось совершить лицо, используя информационно-коммуникационные технологии[2].

К иным компьютерным преступлениям австралийский законодатель относит неправомерный доступ к защищённой компьютерной информации (ст. 478^1), неправомерную модификацию компьютерной информации (ст. 478^2), приобретение и хранение (ст. 478^3), а также создание или распространение компьютерной информации или программ с целью совершения киберпреступлений (ст. 478^4).

Практически идентичный перечень компьютерных преступлений определяет Уголовный кодекс Новой Зеландии (ст. 249 – 252)[3]. При этом норма об ответственности за неправомерный доступ к компьютерной системе (ст. 252) также обладает формальной конструкцией.

В Сингапуре ответственность за совершение компьютерных преступлений определяется Законом Сингапура о неправомерном использовании компьютерных технологий (Singapore computer misuse act) и уголовным законодательством (Singapore Penal Code). Преимущественно

---

[1] [Электронный ресурс] // URL: http://www.legislation.gov.uk/ukpga/2006/35 /section/2 (дата обращения: 21.04.2018).

[2] «A person who is guilty of an offence against this section is punishable, on conviction, by a penalty not exceeding the penalty applicable to the serious offence…serious offence means an offence that is punishable by imprisonment for life or a period of 5 or more years» // [Электронный ресурс] // URL: https://www.legislation.gov.au/ Details/C2004A00937 (дата обращения: 21.02.2018).

[3] [Электронный ресурс] // URL: http://www.legislation.govt.nz/act/public/1961/ 0043/latest/DLM327382.html (дата обращения: 15.03.2018).

заимствуя опыт Великобритании, Закон Сингапура о неправомерном использовании компьютерных технологий устанавливает ответственность за неправомерный доступ к компьютерной информации (ст. 3), неправомерный доступ к компьютерной информации с целью совершения другого преступления (ст. 4), неправомерную модификацию компьютерной информации (ст. 5), несанкционированный доступ к сетям или услугам связи (ст. 6), неправомерное воспрепятствование использованию компьютера (ст. 7), неправомерное предоставление паролей, кодов доступа или иных аналогичных данных (ст. 8)[1]. Следует отметить, что в соответствии со ст. 3 Закона Сингапура о неправомерном использовании компьютерных технологий, лицо подлежит ответственности за так называемое «чистое хакерство» (mere hacking), то есть преступление считается оконченным с момента самого неправомерного доступа и не требует наступления каких-либо общественно опасных последствий.

Законодательные подходы к определению преступлений, совершаемых с использованием информационно-коммуникационных технологий, в странах Европейского Союза

Уголовный кодекс Германии отдельно не выделяет группу компьютерных преступлений. В разных главах предусмотрена ответственность за фишинг (ст. 202b), неправомерную модификацию информации (ст. 303a), компьютерный саботаж (ст. 303b), а также выведение из строя особо важных объектов инфраструктуры (ст. 305a)[2].

Как представляется, особого внимания заслуживают положения немецкого законодательства об ответственности за компьютерный саботаж. В соответствии с буквальным толкованием ст. 303b, таковым необходимо признавать как повреждение, модификацию или уничтожение компьютерной информации, так и её физических носителей. Известно, что посягательства на технические средства обработки информации в отечественной теории уголовного права традиционно предлагают оценивать исключительно в проекции посягательства на отношения собственности. Полагаем, что данный подход требует ревизии в современных условиях. Возрастающая значимость информационного актива меняет акценты в том числе в части уголовно-правовой квалификации.

Следует отдельно указать, что законодатель Германии в специальной норме устанавливает ответственность за приготовление к фишингу и

[1] [Электронный ресурс] // URL: http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=DocId:8a3534de-991c-4e0e-88c5-4ffa712e72af%20%20Status:inforce%20Depth:0;rec=0 (дата обращения: 21.10.2017).

[2] [Электронный ресурс] // URL: https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html (дата обращения: 21.02.2018).

шпионажу данных (data espionage). Согласно ст. 202c уголовно-наказуемым является предоставление другим лицам сведений о сетевых идентификаторах (логинах и паролях), а также предоставление компьютерных программ для совершения фишинга или незаконного получения конфиденциальной информации.

Согласно ст. 263a УК Германии, подлежит привлечению к уголовной ответственности лицо, которое, действуя с намерением получить для себя или третьего лица имущественную выгоду, причиняет вред имуществу другого лица, воздействуя на результат обработки данных путем неправильного создания программ, использования неправильных или неполных данных, путем неправомочного использования данных или иного неправомочного воздействия на результат обработки данных (наказывается лишением свободы на срок до 5 лет или штрафом). В части 2 данной статьи предусмотрена ответственность по-сути за приготовительные действия к совершению компьютерного мошенничества: изготовление компьютерной программы, приобретение соответствующего оборудования (наказывается лишением свободы на срок до 3 лет или штрафом)[1].

Как справедливо отмечает А. Э. Жалинский, немецкий законодатель предельно четко разграничил два вида мошенничества: общеуголовное (традиционное) и информационное (компьютерное). Природа последнего заключается в том, что обману подвергается не человек, а программа, поскольку ущерб имуществу причиняется воздействием на процесс переработки информации и путем неправильного установления программы, использования неверных или неполных данных, а также путем неправомочного использования данных или неправомочного воздействия на процессы переработки данных[2].

В §107c УК Австрии предусмотрена ответственность за киберстокинг, при этом квалифицирующим обстоятельством деяния называется самоубийство потерпевшего. Противоправный доступ к компьютерной системе предусмотрен §118a. Вместе с тем, ответственность здесь наступает исключительно за доступ, связанный с ознакомлением с конфиденциальной информацией. Отдельно §119a говорится о нарушении конфиденциальности информации путём перехвата компьютерных данных. Таким образом, австрийский законодатель разделяет данные преступления по способу их совершения – доступ и перехват.

Ответственность за уничтожение, повреждение или иное несанкционированное изменение или использование компьютерной информации, предусмотрена в соответствии со §126a УК Австрии. Отягчающим обстоятельством является совершения данного преступления с использованием вредоносных компьютерных программ или специального

---

[1] Уголовный кодекс Германии // URL: http://www.gesetze-im-internet.de/englisch_stgb/ englisch_stgb.html#p2344(дата обращения: 21.04.2018).

[2] Жалинский А. Э. Современное немецкое уголовное право. М., 2006. С. 463.

оборудования, заведомо предназначенного для негативного воздействия на данные. Особо квалифицирующими признаками деяния названы: 1) причинение ущерба на сумму свыше 300 000 евро; 2) совершение преступления в отношении объектов критической информационно инфраструктуры и 3) совершения преступления в составе преступной организации[1].

Ответственность же за нарушение функционирования компьютерной системы регламентирована в рамках специальной нормы §126b.

В §126c УК Австрии регламентирована ответственность за изготовление и распространение вредоносных компьютерных программ, а также за распространение средств идентификации пользователей (логинов и паролей). Нельзя не указать на подход австрийского законодателя в части регламентации специального основания освобождения от уголовной ответственности лица, которое своими действиями или своевременным обращением в правоохранительные органы предотвратило наступление негативных последствий.

Уголовная ответственность за компьютерные преступления предусмотрена в главе «Преступления против автоматизированных систем обработки данных» УК Франции и характеризуется достаточно высоким уровнем детализации составов.

Нельзя согласиться с позицией М. А. Ефремовой, что ответственность за неправомерный доступ к автоматизированной системе обработки данных в соответствии со ст. 323-1 УК Франции наступает только при уничтожении или изменении данных либо ухудшении работы самого оборудования или системы[2]. Согласно буквальному толкованию данной статьи по части 1 лицо наказывается лишением свободы на срок до 2 лет или штрафом до 60 000 евро за сам неправомерный доступ. В случае если такие действия повлекли «удаление или модификацию данных, а равно ухудшение работы самой компьютерной системы» содеянное по части 2 наказывается лишением свободы на срок до 3 лет или штрафом до 100 000 евро. И наконец, особо квалифицирующим обстоятельством является совершение данного преступления против системы автоматизированной обработки данных, используемой государством (наказывается лишением свободы на срок до 5 лет и штрафом до 150 000 евро)[3].

---

[1] [Электронный ресурс] // URL: https://www.unodc.org/cld/document/aut/1974/austrianpenalcode2014.html (дата обращения: 21.02.2018).

[2] Ефремова М. А. Уголовно-правовая охрана информационной безопасности: монография. М., 2018. С. 99.

[3] [Электронный ресурс] // URL: https://www.legifrance.gouv.fr/affichCode.do;jsessionid=78FB2013EE0FE26E09BC533710AE4ABF.tplgfr26s_1?idSectionTA=LEGISCTA000006149839&cidTexte=LEGITEXT000006070719&dateTexte=20161231 (дата обращения: 01.06.2018).

Наряду с этим по французскому законодательству преступлениями являются: замедление или искажение функционирования автоматизированной системы обработки данных (ст. 323-2); введение заведомо ложных (недостоверных) данных в компьютерную систему (ст. 323-3); распространение оборудования или компьютерных программ, заведомо предназначенных для совершения преступлений против автоматизированных систем обработки данных (ст. 323-3-1); участие в группе, созданной для совершения одного или нескольких преступлений против автоматизированных систем обработки данных (ст. 323-4).

Статья 323-4-1 специально оговаривает, что если преступления, предусмотренные ст. 323-1 – 323-3-1, совершены организованной группой и в отношении систем автоматизированной обработки данных, используемых государством, содеянное наказывается лишением свободы на срок до 10 лет и штрафом до 300 000 евро. Следует отдельно указать, что в данной статье говорится именно о сочетании отягчающих обстоятельств.

По законодательству Италии ответственность за неправомерный доступ к компьютеру, компьютерной системе или сети предусмотрена в ст. 615-ter. Необходимо отметить ряд значимых особенностей данной нормы. Во-первых, по итальянскому законодательству наказуемым является сам несанкционированный доступ (наказывается до 3 лет лишения свободы). При этом в соответствии с примечанием к данной статье уголовное преследование за данное деяние является возможным только по заявлению самого потерпевшего. Иными словами, чистое хакерство законодатель Италии относит к категории дел частно-публичного обвинения. Однако при наличии квалифицирующих признаков уголовное дело может быть возбуждено и при отсутствии обращения заинтересованной стороны. К отягчающим обстоятельствам неправомерного доступа к компьютерной информации по УК Италии относятся: 1) совершение преступления должностным лицом, государственным или муниципальным служащим, а равно работников оператора связи; 2) если неправомерный доступ был сопряжён с применением насилия; 3) если неправомерный доступ повлёк уничтожение, повреждение, модификацию или блокирование информации, а также существенное нарушение функционирования компьютерной системы или сети (наказывается лишением свободы на срок от 1 года до 5 лет). И наконец, в третьих, к особо квалифицирующим признакам неправомерного доступа законодатель Италии относит его совершение в отношении автоматизированных систем вооружённых сил или органов общественного порядка или общественной безопасности, а также информационных систем, используемых для поддержания безопасности

здоровья населения(наказывается лишением свободы на срок от 3 до 8 лет)[1].

В ст. 615-quarter регламентирована ответственность за распространение средств идентификации пользователей (логинов, паролей, кодов доступа и т.д.). Отдельно в ст. 615-quinquies предусмотрена ответственность за распространение оборудования или компьютерных программ, заведомо предназначенных для несанкционированного воздействия на компьютерную информацию и объекты информационно-коммуникационной инфраструктуры.

В ст. 617-quinquies законодатель Италии устанавливает ответственность за установку оборудования, предназначенного для перехвата или блокирования компьютерной или телематической связи.

Следует отдельно указать на то, как законодатель Италии адаптирует классические положения уголовного законодательства к новым формам общественных отношений, связанных с использованием информационно-коммуникационных технологий. По тексту кодекса включены нормы, которые по-сути экстраполируют общие нормы УК Италии на посягательства с «цифровым» элементом. Так, ст. 491-bis Италии «Информационные документы» не регламентирует признаки какого-либо самостоятельного преступления, однако оговаривает, что все преступления, связанные с фальсификацией или подлогом официальных публичных документов, в полной мере относятся и к тем случаям, когда такие документы выражены в электронной форме.

В ст. 600-1 примерно из эти же целей законодатель Италии делает оговорку, что все уголовно-правовые запреты, связанные с незаконным оборотом порнографических материалов в равной мере распространяются на «виртуальную порнографию», то есть изображения, выполненные путём методов автоматизированной обработки данных, и не связанные с реальными людьми.

Уголовный кодекс Испании посягательства на отношения, связанные с обеспечением безопасности компьютерных данных, описывает в ст.ст. 197 – 199 и 278. При этом ответственность за компьютерное мошенничество регламентирована ст. 248[2]. В соответствии со ст. 249 УК Испании, если размер хищения превышает 400 евро, содеянное наказывается лишением свободы на срок от 6 месяцев до 3 лет. Статья 250 предусматривает перечень особо отягчающих обстоятельств: 1) если деяние совершено в отношении вещей первой необходимости, жилища или другого имущества,

---

[1] [Электронный ресурс] // URL: // http://europam.eu/?module=legislation&country=Italy(дата обращения: 05.06.2018).

[2] [Электронный ресурс] // URL: file:///C:/Users/%D0%96%D0%B5%D0%BD%D1%8F/Downloads/SpainCriminalCodeCodigoPenal.pdf (дата обращения: 21.04.2018).

обладающего особой социальной ценностью; 2) если деяние сопряжено с уничтожением или изменением компьютерной информации или официального документа любого вида; 3) если деяние совершено в отношении объектов, обладающих художественной, культурной или научной ценностью; 4) если деяние причинило значительный ущерб потерпевшему с учётом имущественного положения последнего и достатка его семьи; 5) если размер хищения превышает 50 тысяч евро; 6) если деяние сопряжено с использованием доверительных отношений, а равно служебного положения; 7) если деяние связано с фальсификацией доказательств, обусловивших вынесение судом неправосудного акта в ущерб собственнику или иному владельцу имущества. Наиболее строгим наказанием за особо квалифицированное мошенничество является лишение свободы на срок от четырех до восьми лет.

Уголовный кодекс Бельгии отдельно устанавливает ответственность за неправомерное получение (копирование) защищённой информации в электронной форме (ст. 143), неправомерный доступ к компьютеру или компьютерной сети (ч. 1 ст. 143), распространение сетевых идентификаторов пользователей, компьютерных программ и компьютерной информации, заведомо для виновного предназначенных для совершения неправомерного доступа к объектам информационно-коммуникационной инфраструктуры (ч. 2 ст. 143), несанкционированное уничтожение, повреждение или модификацию компьютерной информации (ст.144-bis).

Примечательно, что норма об ответственности за повреждение компьютерной информации расположена законодателем Бельгии сразу после положений об ответственности за уничтожение или повреждение чужого имущества (ст. 144). Такое смешение, на наш взгляд, является скорее недостатком, чем достоинством бельгийского законодательства. Некая схожесть в деянии мало сближает данные преступления, которые существенно отличаются друг от друга содержанием объекта посягательства.

В ст. 147 УК Бельгии специально предусмотрена ответственность за компьютерное мошенничество, которое в целом повторяет конструкцию отечественной ст. 159[6] УК РФ[1].

В целом почти идентичный подход к законодательному определению преступлений, совершаемых с использованием информационно-коммуникационных технологий, демонстрирует законодатель Швейцарии[2].

---

[1] [Электронный ресурс] // URL: http://europam.eu/?module=legislation &country=Switzerland (дата обращения: 11.06.2018).

[2] [Электронный ресурс] // URL: http://europam.eu/data/mechanisms/FOI/FOI %20Laws /Switzerland/ Switzerland_Criminal%20Code%201937%20EN.pdf (дата обращения: 11.06.2018).

Уголовное законодательство Дании в ст. 263 предусматривает ответственность за неправомерный доступ к охраняемой законом компьютерной информации. В соответствии со ст. 263а уголовно-наказуемым также является распространение «средств доступа к информационной системе», что, судя по всему, относится к средствам идентификации пользователя объектами информационно-коммуникационной инфраструктуры (логины, пароли и т.д.). Общим отягчающим обстоятельством по данным преступлениям признаётся их совершение в отношении «информационных ресурсов государственного значения». Нельзя не отметить, что данные составы преступлений находятся в главе о посягательствах на основные права и свободы человека, наряду с нарушением неприкосновенности частной жизни и жилища. Кроме того, датский законодатель также выделяет специальную норму об ответственности за компьютерное мошенничество (ст. 279а)[1].

Уголовный кодекс Норвегии регламентирует ответственность за неправомерный доступ к компьютерной информации (ст. 145)[2]. В ст. 146 (б) самостоятельно выделен запрет на распространение сведений о сетевых идентификаторах (логинах и паролях). Кроме того, в статье 151 (б) регламентирована ответственность до 10 лет лишения свободы за уничтожение, повреждение или блокирование компьютерной информации или информационно-коммуникационного оборудования, которые повлекли существенное нарушение деятельности органов государственной власти или общественного порядка.

Уголовный кодекс Финляндии также содержит положения об ответственности за посягательства на компьютерную информацию и средства её обработки, хранения и передачи[3]. Особо следует отметить, что в §9а главы 34 УК Финляндии криминализованы действия, связанные не только с сетевыми идентификаторами пользователей, но и с вредоносным программным обеспечением.

Значительную работу по приспосабливанию уголовного законодательства к современному цифровому обществу проделал законодатель Эстонии. Прежде всего в главе о преступлениях против собственности УК Эстонии содержит положения о неправомерном воздействии на компьютерную информацию (§206), неправомерном удалении или изменении идентификационного номера устройства, предназначенного для осуществления обмена данных (§206[1]),

---

[1] [Электронный ресурс] // URL: http://europam.eu/data/mechanisms/PF/PF%20Laws/Denmark/ Denmark_Criminal_Code_2005.pdf (дата обращения: 11.06.2018).

[2] [Электронный ресурс] // URL: http://www.un.org/depts/los/LEGISLATION ANDTREATIE S/PDFFILES/NORpenal_code.pdf (дата обращения: 11.06.2018).

[3] [Электронный ресурс] // URL:http://europam.eu/data/mechanisms/PF/PF%20 Laws/Finland/Finland_Penal%20Code1889_amended2016_FN.pdf (дата обращения: 11.06.2018 г).

неправомерное вмешательство в работу компьютерной системы (§207), а также компьютерное мошенничество (§213).

Отягчающими обстоятельствами неправомерного воздействия на компьютерную информацию и вмешательства в работу компьютерной системы являются: 1) если деяние сопряжено с использованием вредоносного программного обеспечения; 2) если преступление совершено группой лиц; 3) если преступление было направлено против критически значимых информационных ресурсов; 3) повлекло наступление тяжких последствий.

С 2015 года эстонский законодатель пересмотрел подход к регламентации ответственности за изготовление распространение вредоносного программного обеспечения. Упразднив §208 «Распространение вредоносных компьютерных программ», законодатель Эстонии дополнил УК новой нормой – §216[1] «Приготовление к компьютерному преступлению». В соответствии с данной нормой преступлением является изготовление, хранение или распространение компьютерных программ, специально изготовленных или приспособленных для совершения преступления, предусмотренного §206 «Неправомерное воздействие на компьютерную информацию»[1].

Отдельно в §217 УК Эстонии предусмотрена ответственность за неправомерный доступ к компьютерной системе, связанный с нейтрализацией средств программно-технической защиты. Таким образом, эстонский законодатель разделяет деяние, связанное с деструктивным воздействием на информацию, содержащейся в компьютерной системе, и сам несанкционированный доступ к такой защищённой системе.

Помимо этого, осознавая изменившийся характер угроз глобальной безопасности, законодатель Эстонии включил специальную оговорку о неправомерном воздействии на защищённую компьютерную систему в уголовно правовой норме об ответственности за террористический акт (§237).

Уголовная ответственность за несанкционированный доступ к автоматизированной системе обработки данных предусмотрена ст. 241 УК Латвии. Следует отметить, что состав по конструкции является материальным и предполагает наступление последствий в виде значительного ущерба. Квалифицирующими обстоятельствами преступления является наступление тяжких последствий или направленность на объекты критической информационной

[1] [Электронный ресурс] // URL: http://europam.eu/data/mechanisms/FD/FD%20Laws/Estonia/Estonia_Criminal%20code2001amended%202016_EN.pdf (дата обращения: 11.06.2018).

инфраструктуры[1]. В ст. 243 УК Латвии почти в идентичном виде с положениями УК Эстонии установлена ответственность за неправомерное воздействие на саму компьютерную информацию и вмешательство в работу компьютерной системы.

Отдельно в ст. 245 УК Латвии регламентирована ответственность за нарушение правил хранения или обработки защищённой информации, или других правил безопасности информационной системы, совершенное лицом, ответственным за их соблюдение, если это привело к похищению, уничтожению или повреждению информации или причинению материального ущерба.

Развёрнутую систему преступлений против защиты информации содержит глава 33 УК Польши (ст. 265 – 269b). Данная глава объединяет посягательства на информационные ресурсы как открытого, так и закрытого (конфиденциального) характера. Отдельно криминализованы действия, связанные с вредоносными компьютерными программами и сетевыми идентификаторами пользователей[2].

Исследование уголовно-правовых норм об ответственности за компьютерные и компьютеризированные преступления по законодательству стран Евросоюза можно было бы продолжить, однако оно не выявит каких-либо существенных отступлений от уже приведённых примеров. Полагаем, что проведённый анализ уже позволяет сделать вывод о наличии неких общих тенденций.

Прежде всего, следует заключить, что своего рода «европейская модель» не предполагает обязательного выделения специальной главы, раздела или иной части для самостоятельного определения преступлений, посягающих на отношения, связанные с обеспечением безопасности информационно-коммуникационной инфраструктуры. Посягательства на компьютерную информацию и нормальное функционирование средств её хранения, обработки или передачи, как правило, помещаются в главы о преступлениях против личности, собственности или общественной безопасности.

Европейская модель характеризуется дифференцированным установлением ответственности за посягательства на конфиденциальность, целостность и доступность самой компьютерной информации и за противоправные действия в отношении средств её хранения, обработки или передачи (средств автоматизированной обработки данных).

---

[1] [Электронный ресурс] // URL:http://europam.eu/data/mechanisms/COI/COI%20 Laws/Latvia/LatviaCriminal%20Codeamended%202016.pdf (дата обращения: 11.06.2018).

[2] [Электронный ресурс] // URL: http://europam.eu/data/mechanisms/COI/COI %20Laws/Poland/Poland_Penal%20Codeamended%202016.pdf (дата обращения: 21.10.2017).

В отличие от отечественного законодательства европейская модель уголовно-правового противодействия компьютерным преступлениям характеризуется установлением ответственности не только за изготовление, распространение и использование вредоносных компьютерных программ, но и за незаконные действия, связанные с оборудованием, заведомо предназначенным для совершения посягательств на безопасность данных и систем, а также за распространение сведений о сетевых идентификаторах (средств авторизации пользователя).

Наиболее распространёнными отягчающими признаками компьютерных преступлений по европейскому уголовному законодательству являются: 1) групповой способ совершения преступления; 2) совершение преступления в отношении объектов критической информационной инфраструктуры; 3) наступление тяжких последствий; 4) сопряжённость преступления с использованием вредоносных компьютерных программ или устройств, заведомо предназначенных для противоправного воздействия на компьютерную информацию или средства её хранения, обработки или передачи.

Немаловажным представляется и то обстоятельство, что за многие компьютерные и компьютеризированные преступления уголовные законодательства стран Евросоюза предполагают возможность возложения ответственности и на юридических лиц.

И наконец, примечательной особенностью отдельных стран Евросоюза является наличие норм, легитимирующих применение традиционных положений уголовного законодательства к новым «цифровым» формам совершения преступлений. Таким образом данные страны, не изменяя существующих юридических конструкций, как бы легально расширяют их действие, решая тем самым проблему предельной допустимости размывания признаков традиционных составов.

Уголовная ответственность за преступления, совершаемые с использованием информационно-коммуникационных технологий, по законодательству Китайской Народной Республики

Отдельного и внимательного рассмотрения, на наш взгляд, заслуживает китайский опыт уголовно-правового противодействия киберпреступности. Причины такого решения заключаются не только в том, что Китай является одним из ведущих государств с миллиардным населением и второй по значимости экономикой мира. Китайская модель предупреждения и противодействия преступной деятельности в виртуальном пространстве считается одной из наиболее сбалансированных и эффективных. Кроме того, немаловажным фактором выступают крепкие партнёрские отношения между Россией и Китаем.

В отечественной юридической науке изучению развития китайского права всегда уделялось значительное внимание[1]. Обращаясь к анализу правовой системы Китая, П. В. Трощинский обоснованно призывает учитывать своеобразие китайского права, правовой культуры и правосознания её граждан, которые были сформированы под глубоким влиянием нравственного учения великого Конфуция[2].

При этом В. В. Севальнев справедливо делает вывод, что правовую систему Китая нельзя полностью отнести к романо-германской (континентальной системе), она является смешанной и представляет собой симбиоз древних правовых традиций и современного законодательства, которое основано на идеях «социализма с китайской спецификой», принципах романо-германского права, и подвергалась серьёзному влиянию правовой модели СССР[3].

Как и в России, до середины 90-х годов прошлого века(до 1997 года) в уголовном законодательстве Китая не было специальных положений об ответственности за посягательства на компьютерную информацию, а также средства её хранения обработки или передачи. Суды разрешали возникающие проблемные ситуации на основе традиционных составов преступлений, прибегая, как правило, к крайне расширительному толкованию положений уголовного закона. Так, в 1986 году состоялось известное решение по делу Чена, которое считается первым приговором по киберпреступлению в Китае. Чен, работая операционистом в банке, воспользовался служебным доступом к информационной системе банка и изменил сведения о балансе принадлежащего ему банковского счёта. Вынося обвинительный приговор, суд применил положения УК Китая о краже[4].

Данное решение было неоднозначно воспринято в научном сообществе Китая и вызвало бурную полемику по поводу правильности применения положений о краже. Противники вынесенного решения указывали на то,

---

[1] См., например: Гудошников Л. М. Исследование политико-юридических проблем Китая в ИДВ РАН // Проблемы Дальнего Востока. 2005. № 6. С. 31 – 42; Трощинский П. В. Право Китая в зеркале российской науки // Государство и право. 2018. № 1. С. 82 – 95; Лузянин С. Г., Трощинский П. В., Суходолов Я. А. Особенности правового регулирования борьбы с преступностью в Китае // Всероссийский криминологический журнал. 2016. Т. 10. № 4. С. 812 – 824 и др.

[2] Трощинский П. В. К вопросу о традиционных взглядах на право в китайском обществе // Вестник Университета имени О. Е. Кутафина. 2016. № 3 (19). С. 146.

[3] Севальнев В. В. Правовое регулирование противодействия коррупции в Китае // Журнал зарубежного законодательства и сравнительного правоведения. 2018. № 2. С. 70.

[4] Пример приведён по: Qianyun Wang. A comparative study of cybercrime in criminal law: China, US, England, Singapore and the Council of Europe. Rotterdam, 2016. P. 42.

что Чен в сущности никакого имущества не изымал, им были неправомерно модифицированы сведения в информационной системе банка, и поэтому ответственность за кражу он нести не может[1]. Другие ссылались на то, что расширительное толкование состава общеуголовной кражи позволяет распространить его и на действия, совершённые с использованием современных информационный систем кредитно-финансовых учреждений, поскольку умысел виновного был направлен именно на получение материальной выгоды[2]. Так или иначе практически все специалисты соглашались в одном – уголовное законодательство Китая должно быть дополнено специальными положениями об ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий.

УК Китая в редакции 1997 года предусматривал три специальные статьи, связанные с компьютерными преступлениями:

- статья 285 регламентировала ответственность за неправомерный доступ к информационным ресурсам, связанным с деятельностью органов государственной власти, иных критически важных отраслей и обеспечением обороноспособности страны (объектам критической информационной инфраструктуры);
- в соответствии со ст. 286 уголовно-наказуемыми считались следующие действия: 1) неправомерное вмешательство в работу средств автоматической обработки данных и 2) изготовление и распространение вредоносных компьютерных программ;
- статья 287 не предусматривала самостоятельного уголовно-правового запрета и указывала на то, что «традиционные посягательства, совершаемые с использованием компьютерной техники, такие как мошенничество, кража, государственная измена и др., наказываются в соответствии с общими положениями уголовного законодательства об ответственности за данные преступления»[3].

Вместе с тем реализованная модель уголовной ответственности за посягательства на отношения, связанные с обеспечением безопасности компьютерных данных и систем, вызвала критику у представителей китайской науки, суть которой сводилась к тому, что указанные нормы не охватывают ситуацию неправомерного доступа к компьютерным системам

---

[1] Chen Lihua. The discussion on computer crime and its legislation // Legal science.1990. № 1. P. 42

[2] Ma Qiufeng. The concept of computer crime // China Academic Journal Electronic Publishing House.1992. P. 177.

[3] [Электронный ресурс] // URL: http://www.fmprc.gov.cn/ce/cgvienna/eng/dbtyw /jdwt/crimelaw/ t209043.htm (дата обращения: 21.05.2018).

частных лиц (граждан и организаций) при условии, что это никак не повлияло на работу средств автоматизированной обработки данных[1].

Действительно, при буквальном толковании ст. 286 УК Китая в редакции 1997 года следует сделать вывод, что она могла быть применена только в тех случаях, когда неправомерное вмешательство в работу компьютерной системы повлекло ухудшение её функционирования. Если же был осуществлён доступ без замедления работы системы или деструктивного воздействия на сами компьютерные данные, содеянное не могло быть признано преступлением, поскольку ст. 285 заведомо устанавливала ответственность только за неправомерный доступ к информационным ресурсам государственного и общественного значения.

В 2009 году были внесены первые поправки в уголовное законодательство Китая, связанные с ответственностью за преступления, совершаемые с использованием информационно-коммуникационных технологий. Так, ст. 285 УК Китая была дополнена частью 2, устанавливающей ответственность за неправомерную уничтожение, повреждение или модификацию данных, хранящихся в информационной системе частных лиц, и частью 3,криминализирующей распространение программно-технических средств, заведомо предназначенных для совершения преступлений, предусмотренных частями 1 и 2 данной статьи.

В целом данные изменения явились ответом на всё возрастающее значение компьютерных технологий в повседневной жизни граждан и деятельности хозяйствующих субъектов Китая.

В 2015 году была принята 9-я поправка к УК Китая, которая дополнила его ещё тремя новыми составами преступлений в сфере компьютерной информации:

- в соответствии со ст. 286A была установлена ответственность провайдеров за неисполнение решений контролирующих органов по блокированию соответствующих интернет-ресурсов и удалению запрещённой информации;
- статья 287A установила ответственность за использование интернет-ресурсов для распространения информации (обучения) о способах совершения преступлений;
- в соответствии со ст. 287B криминализовано виртуальное содействие совершению киберпреступлений[2].

Указанные изменения стали следствием реализации курса государства на борьбу с возрастающей криминализацией виртуального пространства, в том числе в части создания лицами специализированных информационных

[1] Zhao Bingzhiand Yu Zhigang. Computer crime and the response from legislation and legal theory // China legal science.2001. № 1. P. 149.

[2] [Электронный ресурс] // URL: http://www.fmprc.gov.cn/ce/cgvienna/eng /dbtyw/jdwt/crimelaw/t209043.htm (дата обращения: 21.05.2018).

ресурсов, предназначенных для обмена информацией и программно-техническими средствами для совершения преступлений[1].

Таким образом, действующее законодательство Китая содержит следующие уголовно-правовые нормы об ответственности за компьютерные преступления: неправомерный доступ (ст. 285), неправомерное вмешательство в работу (функционирование) компьютерной системы (ст. 286), неисполнение решения контролирующего органа о блокировании интернет-ресурса или удалении информации (ст. 286А),использование интернет-ресурсов для распространения информации о совершении преступлений (криминогенной информации) (ст. 287А) и содействие совершению киберпреступлений (ст. 287В). При этом ст. 287 УК Китая представляет собой гиперссылочную уголовно-правовую норму, легитимирующую применение традиционных положений китайского уголовного законодательства к случаям совершения иных общеуголовных преступлений с использованием современных информационно-коммуникационных технологий.

Цяньюнь Ван справедливо отмечает, что по смыслу ст. 285 УК Китая уголовно-наказуемым является противоправное преодоление средств программно-технической защиты информации (взлом сам по себе, так называемое «чистое хакерство»), совершённое только в отношении объектов критической информационной инфраструктуры. Взлом компьютерной системы частных лиц без последующего воздействия на компьютерную информацию (её уничтожение, повреждение, блокирование или модификацию) не является преступлением[2].

Нельзя не отметить очевидную близость в данном вопросе законодательства Китая отечественной уголовно-правовой норме об ответственности за неправомерный доступ к компьютерной информации (ст. 272 УК РФ), которая, как известно, в ряду обязательных конструктивных признаков состава также называет общественно-опасные последствия в виде уничтожения, блокирования, модификации или копирования компьютерной информации.

Вместе с тем, в отличие от китайской модели УК России предусматривает обязательность последствий (причинение вреда) и для неправомерного доступа к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации (ч. 2 ст. 2741).При этом вред, как конструктивный признак состава преступления, предусмотренного ч. 2 ст. 2741 УК РФ, не

---

[1] См.: Li Huaisheng. The evolution of cybercrime in three generations of the information network and the law-making // Legal forum. 2015. № 4. P. 94; Yu Zhigang.The Criminalization of training hackers in cyberspace // Law edition journal of Yunnan University. 2015. № 1. P. 86.

[2] Qianyun Wang. A comparative study of cybercrime in criminal law: China, US, England, Singapore and the Council of Europe. Rotterdam, 2016. P. 55.

конкретизирован, то есть является оценочным признаком. Системное толкование позволяет предположить, что таковым являются всё те же последствия в виде уничтожения, блокирования, модификации или копирования информации, содержащейся в критической информационной инфраструктуре.

Полагаем, что подход законодателя Китая в части уголовно-правовой охраны критической информационной инфраструктуры государства является более предпочтительным. Особая значимость таких ресурсов для обеспечения обороноспособности государства, общественной безопасности и поддержания общественного порядка позволяет сделать вывод о необходимости признания преступлением сами действия по их компьютерной атаке.

Отдельно следует уделить внимание китайскому подходу к определению «вредоносной компьютерной программы». В своей работе Цяньюнь Ван отмечает, что применение ч. 3 ст. 285 УК Китая вызвало ряд трудностей в части квалификации действий с так называемыми компьютерными программами двойного назначения. Такое программное обеспечение предназначено для тестирования специалистами компьютерных систем защиты информации, однако может быть использовано и при совершении преступлений[1].

В решении данной проблемы руководящее значение имеют разъяснения Верховного Суда КНР 2011 года, согласно которым «вредоносная компьютерная программа» должна соответствовать следующим обязательным критериям: 1) получение компьютерной информации и воздействие на средства автоматизированной обработки данных должны выступать основными функциями вредоносной компьютерной программы; 2) вредоносная компьютерная программа должна обладать возможностью (функционалом) по преодолению средств программно-технической защиты компьютерных данных и систем и 3) работа вредоносной компьютерной программы предполагает, что доступ к компьютерной информации или вмешательство в работу средств автоматизированной обработки данных имеет несанкционированный характер, то есть осуществляется без надлежащих на то правомочий[2].

Выделенные Верховным Судом КНР признаки позволяют решить многие проблемы квалификации преступления, связанного с оборотом вредоносных компьютерным программ. Вместе с тем указанное толкование

---

[1] Qianyun Wang. A comparative study of cybercrime in criminal law: China, US, England, Singapore and the Council of Europe. Rotterdam, 2016.P. 56.

[2] Interpretations of several issues on the application of law in handling criminal cases about endangering the security of computer information systems. 2011. № 19 // [Электронный ресурс] // URL: http://www.scio.gov.cn/xwfbh/qyxwfbh/document /1004368/1004368.htm. (дата обращения: 21.05.2018).

оставляет отдельные вопросы относительно содержания признака вредоносности. Так, например, китайская модель не позволяет признать вредоносной компьютерную программу, которая заведомо предназначена для автоматизированного изготовления самих компьютерных вирусов (так называемый «конструктор вирусов»).

Деяние, предусмотренное ст. 285А УК Китая, имеет очевидное сходство с положениями российского законодательства об ответственности за неисполнение оператором связи, оказывающим услуги по предоставлению доступа к информационно-телекоммуникационной сети «Интернет», обязанности по ограничению доступа к информации, доступ к которой должен быть ограничен на основании сведений, полученных от федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере связи, информационных технологий и массовых коммуникаций (ст. 13.34 КоАП РФ). Вместе с тем, необходимо отметить, что состав преступления, предусмотренный ст. 285А УК Китая, обладает материальной конструкцией и в качестве обязательных признаков называет следующие альтернативные последствия: 1) если неисполнение решение провайдером привело к «массовому распространению» запрещённой информации и 2) повлекло наступление тяжких последствий.

Несмотря на использование китайским законодателем оценочных признаков, которые закономерно вызовут определённые затруднения на практике, само решение о криминализации таких действий следует признать положительным. В этом отношении отечественное законодательство выглядит несогласованным и непоследовательным, поскольку, устанавливая административную ответственность за простое бездействие провайдера по удалению запрещённого контента или блокированию криминогенного интернет-ресурса, оно не определяет ответственность поставщика связи в случаях, когда такое неисполнение привело к тяжким последствиям, выразившимся, например, в гибели человека, массовых беспорядках, дезорганизации деятельности органов государственной власти и т.д.

В ст. 287А законодатель Китая весьма удачно решает проблему ответственности за виртуальное содействие в совершении преступлений без признаков соучастия. Как известно, в отечественной доктрине уголовного права масштабное распространение безадресного подстрекательства и предлагаемой по принципу «до востребования» помощи в совершении компьютерных преступлений позволило отдельным специалистам сделать вывод о необходимости переосмысления некоторых общетеоретических положений института соучастия. Так, А. Ю. Чупрова пишет, что особенностью подстрекательских действий в сети Интернет является то, что умысел лица не персонифицирован, его призыв к совершению преступления обращён к неопределённо большому кругу лиц.

Кто найдёт предложение заслуживающим внимания и одобрения и реализует его на практике, автору прокламации неизвестно[1].

Полагаем, что попытки переосмысления аксиоматичного положения о невозможности привлечения к ответственности за так называемое абстрактное соучастие, вряд ли являются оправданными. Подстрекательством может быть признано склонение другого лица к совершению конкретного преступления, а не пробуждение абстрактных преступных устремлений или интереса к противоправному поведению. Недостаточно дать кому-то совет заняться кражами: для признания лица подстрекателем необходимо, чтобы оно подстрекнуло совершить определённую кражу путем объяснения выгод от преступления, умаления трудностей и опасности, с которым сопряжено его выполнение[2]. В той же мере сказанное относится и к пособничеству. Современная судебная практика демонстрирует строгую приверженность данной концепции[3].

Тенденция к расширительному толкованию подстрекательских и пособнических действий по делам о компьютерных преступлениях, имеет своё объяснение – публичное размещение информации, склоняющей или облегчающей их совершение, объективно является общественно опасным и требует надлежащей оценки. Однако даже при решении самых злободневных проблем нельзя законность приносить в жертву «социальной необходимости», произвольно расширяя пределы действия уголовного закона. Полагаем, что отечественному законодателю необходимо обратить более пристальное внимание именно на ст. 287А УК Китая, которая в рамках специальной нормы устанавливает ответственность за виртуальное содействие в совершении преступлений без признаков соучастия.

В ст. 287 В УК Китая криминализована деятельность пособника в совершении преступления, посредством использования информационно-коммуникационных технологий. Таким образом, это как бы специальная норма о «виртуальном пособничестве». В отличие от ст. 287А, где лицо предоставляет вредоносные компьютерные программы «до востребования», в ст. 287В речь идёт именно о содействии совершению конкретного преступления. Как справедливо подчёркивает в своей работе Цяньюнь Ван, лицо должно достоверно знать о том, что пользователь, которому он оказывает помощь, намеревается совершить конкретное

---

[1] Чупрова А. Ю. Уголовно-правовые механизмы регулирования отношений в сфере электронной коммерции: дис. …д-ра юрид. наук. М., 2015. С. 259.

[2] Курс российского уголовного права. Общая часть / под ред. В. Н. Кудрявцева, А. В. Наумова. М., 2001. С. 359.

[3] Апелляционное определение Верховного Суда РФ от 27.04.2017 г. по делу № 89-АПУ17-3сп.; Апелляционное определение Верховного Суда РФ от 04.06.2015 г. по делу № 30-АПУ15-3.

преступление (..an actor obviously knows that the person to whom he providing help intends to commit a crime by means of a network)[1].

С точки зрения отечественной теории уголовного права данное решение является примером так называемого «избыточного законотворчества». Появление подобной нормы не решает проблему уголовной ответственности лица, поскольку таковая уже была возможной с учётом общих положений о наказуемости пособнических действий.

Проведённое исследование позволяет сделать несколько значимых выводов общего характера. Имея с Россией общую точку отсчёта (1997 г.) в построении уголовно-правового механизма противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий, Китай реализовал более сложную модель их криминализации.

Китайская модель уголовно-правового противодействия киберпреступности развивалась в три этапа: 1-й этап защиты критической информационной инфраструктуры (1997 г.), 2-й этап расширения защиты информационных ресурсов частных лиц (2009 г.) и 3-й этап установления ответственности провайдеров и виртуальных пособников (2015 г.).

Применительно к отечественной проблематике уголовно-правового противодействия киберпреступности наибольшим теоретико-прикладным значением обладают положения уголовного законодательства Китая об ответственности провайдеров и лиц, использующих интернет-ресурсы для распространения криминогенной информации и оказания не персонифицированной помощи для совершения преступлений.

Уголовная ответственность за преступления, совершаемые с использованием информационно-коммуникационных технологий, по законодательству Социалистической Республики Вьетнам

Российскую Федерацию и Социалистическую Республику Вьетнам связывают долгие годы всеобъемлющего стратегического партнерства. В честь 70-летия установления дипломатических отношений между странами и 25-летия подписания межгосударственного Договора об основах дружественных отношений в 2019 году было торжественно объявлено об открытии перекрестных годов России во Вьетнаме и Вьетнама в России. На церемонии открытия перекрестного года Дмитрий Медведев заявил, что между государствами сложилась тесная торгово-экономическая кооперация. Успешно реализуются крупные и перспективные проекты в

[1] Qianyun Wang. A comparative study of cybercrime in criminal law: China, US, England, Singapore and the Council of Europe. Rotterdam, 2016.P. 60.

энергетике, промышленности, инвестиционной и высокотехнологичных сферах[1].

Нельзя не отметить, что в 2015 году Вьетнам стал первой страной, подписавшей соглашение о свободной торговле с Евразийским экономическим союзом, ключевым членом которого является Россия, продемонстрировав особый приоритет в сотрудничестве между двумя странами[2].

Дальнейшее развитие стратегического партнерства и экономических отношений между Россией и Вьетнамом обусловливает значительный интерес к сравнительно-правовым исследованиям законодательств двух стран[3]. И в этом отношении особую актуальность представляет анализ подходов государств к установлению уголовной ответственности за преступления в сфере компьютерной информации. Трансграничный характер киберпреступности требует по возможности четкого представления об уровне согласованности подходов стран-партнеров к определению ответственности за наиболее опасные ее проявления.

До 1999 года в уголовном законодательстве Социалистической Республики Вьетнам не было специальных положений об ответственности за посягательства на компьютерную информацию, а также средства ее автоматизированной обработки или передачи. Как подчеркивает по этому поводу Нгуен Нгок Ань, по уголовному законодательству Вьетнама до 1999

---

[1] Дмитрий Медведев и Нгуен Суан Фук приняли участие в открытии перекрестных годов России во Вьетнаме и Вьетнама в России. Москва, 22 мая 2019 года / [Электронный ресурс] // URL: http://government.ru/news/36754/ (дата обращения: 28.06.2021 г.)

[2] Подписано Соглашение о свободной торговле между ЕАЭС и Вьетнамом. Бурабай, Республика Казахстан, 29 мая 2015 года / [Электронный ресурс] // URL: http://government.ru/news/18296/ (дата обращения: 28.06.2021 г.)

[3] См., например: Демидов Н.Н., Фам Ныы Хан. Проблемы, связанные со сбором и использованием электронных доказательств в уголовном деле во Вьетнаме // Закон и право. 2021. № 1. С. 86-88; Минбалеев А.В. Правовое обеспечение кибербезопасности во Вьетнаме // Вестник УрФО. Безопасность в информационной сфере. 2019. № 1 (31). С. 64-68; Чан Тхи Ту Ань. Уголовная ответственность по законодательству Российской Федерации и Социалистической Республики Вьетнам: возрастные ограничения // Журнал зарубежного законодательства и сравнительного правоведения. 2015. № 5 (54). С. 911-914; Вьонг Т.Л., Чан Т.Т.А. Виды и характеристика уголовно-процессуального задержания в праве Социалистической Республики Вьетнам // Журнал зарубежного законодательства и сравнительного правоведения. 2014. № 5 (48). С. 884-886; Ву Куанг Хуан. Планирование законотворческой деятельности во Вьетнаме // Журнал зарубежного законодательства и сравнительного правоведения. 2013. № 2 (39). С. 334-342 и др.

года компьютерное преступление – это просто преступление, которое совершается благодаря достижениям информационных технологий[1].

Уголовный кодекс Социалистической Республики Вьетнам (далее – УК СРВ) в редакции 1999 года изначально предусматривал три специальные статьи об ответственности за преступления в сфере компьютерной информации: статья 224 «Создание и распространение вредоносных компьютерных программ» предусматривала ответственность за создание и распространение вредоносных компьютерных программ, если это деяние повлекло блокирование, модификацию или уничтожение компьютерной информации или было совершенно лицом, которое ранее привлекалось к ответственности за такое деяние; статья 225 «Нарушение правил эксплуатации и использования компьютерных сетей» устанавливала ответственность за нарушение специальных правил в сфере информационной безопасности, если это повлекло блокирование, модификацию или уничтожение компьютерной информации или было совершенно лицом, которое ранее привлекалось к ответственности за такое деяние; статья 226 «Незаконное использование информации в сети Интернет и в компьютерах» предусматривала ответственность за несанкционированное использование информации, содержащейся в сети Интернет или на иных носителях, распространение в компьютерной сети информации, противоречащей действующему законодательству, если эти деяния повлекли наступление тяжких последствий или были совершенны лицом, которое ранее привлекалось к ответственности за такое деяние.

В 2009 году были внесены поправки в уголовное законодательство Вьетнама, в результате которых были изменены редакции действующих норм, а также список компьютерных преступлений был расширен до пяти составов: статья 224 «Распространение вирусных компьютерных программ, вредоносных компьютерных программ для функционирования компьютерных сетей, телекоммуникационных сетей, Интернета, цифрового оборудования»; статья 225 «Воспрепятствование или нарушение функционирования компьютерных сетей, телекоммуникационных сетей, Интернета, цифрового оборудования»; статья 226 «Незаконное использование информации в компьютерных сетях, телекоммуникационных сетях или Интернете»; статья 226-а «Незаконный доступ к компьютерным сетям, телекоммуникационным сетям, Интернету или цифровым устрой-

[1] Thiếu tướng, GS, TS. NGUYỄN NGỌC ANH - Cục trưởng V19 - Bộ Công an / Kỷ yếu hội thảo khoa học "Phòng, chống tội phạm sử dụng công nghệ cao - Những vấn đề đặt ra trong công tác đào tạo", Học viện CSND tháng 11/2014/ [Электронный ресурс] // URL: http://canhsatnhandan.vn/Home/Print/286/Mot-so-quy-dinh-cua-phap-luat-ve-toi-pham-cong-nghe-cao (дата обращения: 01.07.2021 г.)

ствам других лиц»; статья 226-б «Использование компьютерных сетей, телекоммуникационных сетей, Интернета или цифровых устройств с целью хищения имущества».

В 2015 г. был принят новый Уголовный кодекс Социалистической Республики Вьетнам. И уже в 2017 г. в него были внесены отдельные изменения, в том числе затрагивающие вопросы уголовной ответственности за преступления в сфере компьютерной информации. В действующей редакции Раздел 2 «Преступления против информационных технологий и телекоммуникационных сетей» предусматривает девять составов преступлений (ст. 292 УК СРВ утратила силу): статья 285 «Изготовление, сбыт, передача инструментов, оборудования, программного обеспечения, предназначенных для противоправных целей»; статья 286 «Распространение вредоносных компьютерных программ для компьютерных сетей, телекоммуникационных сетей или электронных устройств»; статья 287 «Воспрепятствование или нарушение работы компьютерных сетей, телекоммуникационных сетей или электронных устройств»; статья 288 «Незаконное предоставление или использование информации в компьютерных сетях или телекоммуникационных сетях»; статья 289 «Незаконное проникновение в компьютерную сеть, телекоммуникационную сеть или электронное устройство другого лица»; статья 290 «Использование компьютерной сети, телекоммуникационной сети или электронных устройств в целях совершения хищения»; статья 291 «Незаконный сбор, хранение, обмен, торговля, публикация информации о чужих банковских счетах»; статья 292 «Незаконное оказание услуг в компьютерных сетях или телекоммуникационных сетях» – утратила силу; статья 293 «Незаконное использование радиочастот, предназначенных для аварийно-спасательных служб, служб безопасности, поисково-спасательных служб, национальной обороны или общественной безопасности»; статья 294 «Умышленное создание вредных помех радиочастот».

В науке уголовного права Вьетнама отмечается, что принятый в 2015 г. УК СРВ существенно пересмотрел положения о пенализации преступлений в сфере компьютерной информации с учетом современных тенденций практики борьбы с киберпреступностью: значительно увеличены размеры наказания в виде штрафа (назначаемого как в качестве основного,

так и в качестве дополнительного вида наказания), предусмотрена возможность применения конфискации имущества[1].

Нельзя не отметить, что принятие УК СРВ 2015 г. во многом было направлено на достижение формально-юридической определенности составов компьютерных преступлений. Так, были исключены такие оценочные признаки как причинение ущерба или наступление иных тяжких последствий. В новой редакции все компьютерные преступления по УК СРВ получили довольно строгое описание альтернативных криминообразующих признаков: при незаконном получении прибыли или причинении ущерба с указанием размера в денежном эквиваленте; при заражении электронных устройств или информационной системы с указание точного количества пострадавших пользователей; при отключении или приостановке работы компьютерной сети, телекоммуникационной сети или электронного устройства с детализацией такого периода по минутам и часам; аналогично при приостановлении деятельности учреждений или организаций.

Статья 285 УК СРВ по своему содержанию является наиболее близкой уголовно-правовой норме об ответственности за незаконный оборот специальных технических средств, предназначенных для негласного получения информации (ст.138[1] УК РФ). В сравнении с УК РФ, следует отметить, что законодатель Вьетнама, пожалуй, более удачно определяет направленность и природу видового объекта данного преступления, помещая его в группе посягательств на информационную безопасность. Как известно, в отечественной доктрине уголовного права такое решение обосновывается рядом ученых уже на протяжении длительного времени[2].

В теории уголовного права Вьетнама разъясняется, что соответствующие инструменты и оборудование могут быть использованы для незаконного проникновения в компьютерные сети, подслушивания информации, модификации информации, вмешательства или нарушения работы

---

[1]ThS. Trần Đoàn Hạnh. Hoàn thiện khung khổ pháp lý xử phạt tội phạm công nghệ thông tin, mạng viễn thông / [Электронный ресурс] // URL: https://tapchitaichinh.vn/nghien-cuu--trao-doi/trao-doi-binh-luan/hoan-thien-khung-kho-phap-ly-xu-phat-toi-pham-cong-nghe-thong-tin-mang-vien-thong-112331.html) (дата обращения: 28.06.2021 г.).

[2] См., например: Русскевич Е.А. Уголовное право и «цифровая преступность»: проблемы и решения: монография. – М.: ИНФРА-М, 2019; Усов Е.Г. Уголовная ответственность за незаконный оборот специальных технических средств, предназначенных для негласного получения информации: дис. …канд.юрид.наук. Иркутск, 2020. С. 13.

компьютерных сетей, телекоммуникационных сетей, электронного оборудования, хищения имущества через компьютерную сеть и др. К предмету преступления, предусмотренного ст. 285 УК СРВ, следует относить вредоносные программы (вирусы, шпионские программы, рекламное и др.), электронные чипы для считывания карточных данных, цифровое оборудование для приема, вещания, цифровых или параллельных сигналов, микрочипы, периферийные устройства, программные модули ввода данных и др.[1]

Следует отметить, что субъективная сторона преступления, предусмотренного ст. 285 УК СРВ, также характеризуется специальной целью – совершение противоправных действий с соответствующими инструментами. Таким образом, если такое оборудование или программное обеспечение (даже с функциями осуществления компьютерной атаки), применяется в научных или учебных целях либо для тестирования средств программно-технической защиты информационных ресурсов, содеянное не может квалифицироваться как преступление.

В ст. 286 УК СРВ отдельно установлена ответственность за умышленное распространение вредоносных компьютерных программ. В некотором смысле данная норма дополняет положения ст. 285 УК СРВ. Вместе с тем, согласно ст. 286 УК СРВ уголовная ответственность за распространение вредоносных компьютерных программ наступает только при наличии следующих альтернативных криминообразующих признаков: а) лицом получен доход в размере от 50 000 000 до менее 200 000 000 донгов; б) деяние повлекло причинение ущерба на сумму от 50 000 000 до менее 300 000 000 донгов; в) вредоносная компьютерная программа поразила от 50 до 200 электронных устройств либо информационную систему с 50 – 200 пользователями; г) деяние совершено лицом, которое ранее привлекалось к административной ответственности за такое деяние или лицом, имеющим судимость за ранее совершенное преступление, предусмотренное данной статьей.

По ч. 1 ст. 286 УК СРВ лицо может быть подвергнуто наказанию в виде штрафа в размере от 50 000 000 до 200 000 000 донгов либо в виде принудительных работ на срок до 3 лет либо лишению свободы на срок от 6 месяцев года до 3 лет. В соответствии с частью 4 данной статьи лицу может быть так назначено дополнительное наказание в виде лишения пра-

---

[1] Уголовное право Вьетнама. Часть Особенная: учебник / под ред. Нгуен Нгок Хоа. 23 -е изд., перераб. и доп. Ханой.: Издательство народной милиции. 2017 / [Электронный ресурс] // URL:http://thuvien.hlu.edu.vn/KMETSNAVI/TocBookReader.aspx?mets_id=146&dmd_id=37217&locale=vi-VN (дата обращения: 28.06.2021 г.).

ва занимать определенные должности или заниматься определенной деятельностью на срок от 1 года до 5 лет.

Дифференциация уголовной ответственности за данное деяние реализована в зависимости от наличия следующих квалифицирующих признаков: по части 2 данной статьи (наказывается от 3 до 7 лет лишения свободы): а) преступление совершено организованной группой; б) лицом получен доход в размере от 200 000 000 до менее 500 000 000 донгов; в) деяние повлекло причинение ущерба на сумму от 300 000 000 до менее чем 1,000,000,000 донгов; г) вредоносная компьютерная программа поразила 200 – 500 электронных устройств либо информационную систему с 200 – 500 пользователей; д) опасный рецидив; по части 3 (наказывается от 7 до 12 лет лишения свободы): а) преступление совершено против системы данных, которая является государственной тайной или информационная система, служащая национальной обороне и безопасности; б) преступление совершено против национальной информационной инфраструктуры, информационной системы управления национальной электрической сетью, банковской или иной финансовой информационной системы, информационной системы управления движением транспорта; в) лицом получен доход в размере ≥ 500 000 000 донгов; г) деяние повлекло причинение ущерба на сумму ≥ 1 000 000 000 донгов; д) вредоносная компьютерная программа поразила ≥ 500 электронных устройств либо информационную систему с ≥ 500 пользователей.

Особое внимание следует уделить толкованию по уголовному праву Вьетнама такого признака как ущерб. В соответствии с принятыми разъяснениями при определении ущерба необходимо учитывать как прямой и непосредственный материальный вред, связанный с повреждением информационно-коммуникационной инфраструктуры, так и затраты потерпевшего на исправление повреждений компьютерных сетей, телекоммуникационных сетей или атакованных электронных средств, а также косвенный ущерб, связанный с прерыванием работы компьютерной сети, телекоммуникационной сети или атакованных электронных средств[1].

Приведенное толкование ущерба по делам о преступлениях в сфере компьютерной информации, на наш взгляд, в наибольшей степени соот-

---

[1] Thông tư liên tịch số 10/2012/TTLT-BCA-BQP-BTP-BTT&TT-VKSNDTC-TANDTC. Hướng dẫn áp dụng quy định của bộ luật hình sự về một số tội phạm trong lĩnh vực công nghệ thông tin và viễn thông / ngày 10 tháng 09 năm 2012 // [Электронный ресурс] // URL: https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Thong-tu-lien-tich-10-2012-TTLT-BCA-BQP-BTP-BTTTT-VKSNDTC-TANDTC-huong-dan-148869.aspx (дата обращения: 28.06.2021 г.).

ветствует современным вызовам и угрозам в части обеспечения информационной безопасности. Включение в понятие ущерба упущенной выгоды является вполне обоснованным, поскольку позволяет давать справедливую юридическую оценку во многих ситуациях, когда компьютерное оборудование физически не пострадало, ее функционирование было восстановлено усилиями самого потерпевшего (например, системными администраторами организации), однако сам он понес серьезные убытки за время вынужденного простоя.

Необходимо также обратить внимание на то, как в правоприменительной практике Вьетнама решается вопрос о количестве потерпевших по делам, связанным с изготовлением, использованием и распространением вредоносных компьютерных программ. Согласно сформулированным рекомендациям, в ходе расследования уголовных дел о преступлениях, связанных с использованием информационно-коммуникационных технологий, правоохранительные органы должны принимать меры по установлению всех потерпевших. В случае, когда по объективным причинам невозможно установить личность потерпевшего (потерпевший проживает за границей; потерпевшего невозможно идентифицировать; потерпевший уклоняется от сотрудничества, потому что не желать раскрывать свою личность и т.п.), но на основании собранных доказательств есть основания полагать, что конкретное лицо пострадало в результате совершенного преступления, не установление личности потерпевшего не влияют на квалификацию содеянное и вынесение приговора[1].

В ст. 287 УК СРВ предусмотрена самостоятельная ответственность за совершение лицом действий, направленных на уничтожение или модификацию компьютерной информации, а также на воспрепятствование нормальной работе компьютерного оборудования и информационно-коммуникационных сетей, если это деяние не подпадает под признаки распространения вредоносных компьютерных программ (ст. 286 УК СРВ) и неправомерного доступа к компьютерной информации (ст. 289 УК СРВ).

Уголовная ответственность по данной статье наступает только при наличии хотя бы одного из следующих дополнительных условий: 1) лицом получен доход в размере от 50 000 000 до менее 200 000 000 донгов;

---

[1] Thông tư liên tịch số 10/2012/TTLT-BCA-BQP-BTP-BTT&TT-VKSNDTC-TANDTC. Hướng dẫn áp dụng quy định của bộ luật hình sự về một số tội phạm trong lĩnh vực công nghệ thông tin và viễn thông / ngày 10 tháng 09 năm 2012 // [Электронный ресурс] // URL: https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Thong-tu-lien-tich-10-2012-TTLT-BCA-BQP-BTP-BTTTT-VKSNDTC-TANDTC-huong-dan-148869.aspx (дата обращения: 28.06.2021 г.).

2) деяние повлекло причинение ущерба на сумму от 100 000 000 до менее чем 500 000 000 донгов; 3) деяние повлекло отключение или приостановку работы компьютерной сети, телекоммуникаций сети или электронного устройства на период от 30 минут до 24 часов или с 03 до 10 раз в течение 24 часов; 4) деяние повлекло приостановление деятельности организации на срок от 24 часов до 72 часов; 5) деяние совершено лицом, которое ранее привлекалось к административной ответственности за такое деяние или лицом, имеющим судимость за ранее совершенное преступление, предусмотренное данной статьей.

Квалифицирующими признаками данного преступления выступают: по части 2 (наказывается от 3 до 7 лет лишения свободы): а) преступление совершено организованной группой; б) деяние совершено лицом, злоупотребляющим своим положением администратора компьютерной сети или телекоммуникационной сети; в) опасный рецидив; г) лицом получен доход в размере от 200 000 000 до 1 000 000 000 донгов; д) деяние повлекло причинение ущерба на сумму от 500 000 000 до 1 500 000 000 донгов; е) деяние повлекло отключение или приостановку работы компьютерной сети, телекоммуникаций сети или электронного устройства на срок от 24 часов до 168 часов или от 10 до 50 раз в течение 24 часов; ж) деяние повлекло приостановление деятельности организации на срок от 72 часов до менее 168 часов; по части 3 (наказывается от 7 до 12 лет лишения свободы): а) деяние совершено против системы данных, содержащей государственную тайну, или против информационной системы, служащей интересам национальной обороны и безопасности; б) преступление совершено против национальной информационной инфраструктуры, информационной системы управления национальной электрической сетью, банковской или иной финансовой информационной системы, информационной системы управления движением транспорта; в) лицом получен доход в размере ≥ 1 000 000 000 донгов; г) деяние повлекло причинение ущерба на сумму ≥ 1 500 000 000 донгов; д) деяние повлекло отключение или приостановку работы компьютерной сети, телекоммуникаций сети или электронного устройства на ≥ 168 часов или ≥ 50 раз в течение 24 часов; е) деяние повлекло приостановление деятельности организации на ≥ 168 часов.

В ст. 288 законодатель Вьетнама, на наш взгляд, весьма удачно решает проблему ответственности за виртуальное содействие в совершении преступления без признаков соучастия. В отечественной доктрине уголовного права масштабное распространение предлагаемой по принципу «до востребования» помощи в совершении компьютерных преступлений позволило отдельным специалистам сделать вывод о необходимости переосмысления некоторых общетеоретических положений института со-

участия. Однако, эти попытки отвергнуть аксиоматичное положение о невозможности привлечения к ответственности за так называемое абстрактное соучастие, вряд ли являются оправданными. Тенденция к расширительному толкованию пособнических действий по делам о компьютерных преступлениях, конечно же, имеет под собой основания – публичное размещение информации, облегчающей их совершение, объективно является общественно опасным и требует надлежащей оценки. Однако даже при решении самых злободневных проблем нельзя законность приносить в жертву «социальной необходимости», произвольно расширяя пределы действия уголовного закона. В связи с этим, полагаем, что отечественному законодателю необходимо обратить более пристальное внимание именно на ст. 287 УК СРВ, которая в рамках специальной нормы устанавливает ответственность за распространение значимой информации о физическом лице либо организации. Нельзя не отметить, что охранительный спектр данной нормы гораздо шире противодействия виртуальному пособничеству в совершении преступления, поскольку предполагает также самостоятельную защиту от распространения любой вредоносной (криминогенной) информации, которое в результате повлекло самоубийство потерпевшего, нарушение общественного порядка, в том числе проведение несанкционированных демонстраций либо ухудшение дипломатических отношений между странами.

Ответственность за неправомерный доступ к компьютерной информации установлена в ст. 289 УК СРВ. Законодатель Вьетнама определяет объективную сторону данного преступления как последовательную совокупность действий. Несанкционированный доступ к компьютерным сетям, телекоммуникационным сетям или электронным устройствам может быть признан преступлением, если он был альтернативно сопряжен: 1) с совершением действий по изменению идентификаторов доступа к системе, в результате чего потерпевший теряет такой доступ; 2) с неправомерным вмешательством в работу электронных устройств; 3) с копированием, изменением или уничтожением данных; 4) с неправомерным использованием услуг.

По ч. 1 ст. 289 УК СРВ лицо может быть подвергнуто наказанию в виде штрафа в размере от 50 000 000 до 300 000 000 донгов или лишению свободы на срок от 1 года до 5 лет. В соответствии с частью 4 данной статьи лицу может быть так назначено дополнительное наказание в виде лишения права занимать определенные должности или заниматься определенной деятельностью на срок от 1 года до 5 лет. Следует сделать вывод, что по законодательству Вьетнама само по себе преодоление средств программно-технической защиты компьютерной информации, так называе-

мое «чистое хакерство», не образует признаков уголовно-наказуемого неправомерного доступа. Подобный подход, как известно, реализован и в отечественной ст. 272 УК РФ.

Дифференциация уголовной ответственности за неправомерный доступ к компьютерной информации реализована по следующей модели: по части 2 данной статьи (наказывается от 3 до 7 лет лишения свободы): а) деяние совершено организованной группой; б) деяние совершено лицом, злоупотребляющим служебным положением; в) лицом получен доход в размере от 200 000 000 до менее 500 000 000 донгов; г) деяние повлекло причинение ущерба на сумму от 300 000 000 до 1 000 000 000; д) деяние совершено против национальной точки обмена Интернетом, базы данных доменных имен или национальная система серверов доменных имен; е) опасный рецидив; по части 3 (наказывается от 7 до 12 лет лишения свободы): а) деяние совершено против системы данных, содержащей секретную информацию или против информационной системы, служащей интересам национальной обороны и безопасности; б) деяние совершено против национальной информационной инфраструктуры; в) лицом получен доход в размере ≥ 500 000 000 донгов; г) деяние повлекло причинение ущерба на сумму ≥ 1 000 000 000 донгов.

Изучение УК СРВ позволяет сделать вывод, что законодатель Вьетнама уделяет особое внимание преступлениям, неправомерно воздействующим на критическую информационную инфраструктуру государства, признавая их особо тяжкими преступлениями, непосредственно затрагивающими нормальное функционирование страны. Нельзя не отметить, что Вьетнам уже сталкивался с серьезными компьютерными атаками в отношении критической информационной инфраструктуры. Так, 29 января 2016 года была совершена массовая компьютерная атака на аэропорты страны, в результате которых на информационных табло международного аэропорта Таншоннят, международного аэропорта Ной Бай, международного аэропорта Дананг, аэропорта Фукуок, появились изображения и текст, оскорбляющие Вьетнам и Филиппины. В то же время сайт вьетнамских авиалиний также был взломан и данные почти полумиллион пассажиров оказались утеряны[1].

Понятие критической информационной инфраструктуры раскрыто в Законе Социалистической Республики Вьетнам о кибербезопасности (2018). В соответствии со ст. 10 данного закона информационные систе-

[1] Взлом вьетнамских аэропортов / [Электронный ресурс] // URL: https://en.wikipedia.org/wiki/Vietnamese_airports_hackings) (дата обращения: 15.05.2021 г.).

мы, критически важные для национальной безопасности – это информационные системы, которые в случае инцидента, проникновения, захвата оперативного управления, искажения, прерывания, остановки, атаки или разрушения серьезно поставит под угрозу безопасность сети. Объекты критической информационной инфраструктуры включают: военные, охранные, дипломатические и шифровальные информационные системы; система хранения информации, обработки сведений, составляющих государственную тайну; информационные системы, служащие для хранения и сохранения объектов и данных, имеющих особое значение; информационные системы, служащие сохранению материалов и веществ, особо опасных для человека и окружающей среды; информационные системы, обслуживающие сохранение, производство и управление особо важными материальными, физическими объектами, имеющими отношение к национальной безопасности; важные критические информационные системы, обслуживающие деятельность центральных государственных учреждений и организаций; национальные информационные системы в секторах энергетики, финансов, банковского дела, телекоммуникаций, транспорта, природных ресурсов и окружающей среды, химической промышленности, здравоохранения, культуры и печати; автоматизированные системы управления и мониторинга на важных строительных работах[1].

В отличие от российского уголовного законодательства, в котором выделена специальная норма об ответственности за неправомерное воздействие на критическую информационную инфраструктуру (ст. 274^1 УК РФ), законодатель Вьетнама предусматривает ответственность за такие деяния, выделяя соответствующие квалифицированные составы преступлений: п. «а, б» ч.3 ст. 286, п. «а, б» ч. 3 ст. 287, п. «а, б» ч.3 ст.289 УК СРВ. Нельзя не отметить, что УК СРВ не предусматривает последствий в виде причинения вреда как обязательный признак в составе неправомерного доступа к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре.

Статья 290 УК СРВ устанавливает ответственность за ряд действий, совершаемых с использованием современных информационно-коммуникационных технологий, в целях хищения чужого имущества. Сразу следует указать, что данная норма обладает сходством с мошенничеством в сфере компьютерной информации (ст. 159^6 УК РФ). Объективная сторона преступления, предусмотренного ст. 290 УК СРВ выражена

[1] Luật an ninh mạng số: 24/2018/QH14 / ngày 12 tháng 6 năm 2018 / [Электронный ресурс] // URL: https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Luat-an-ninh-mang-2018-351416.aspx (дата обращения: 15.05.2021 г.).

следующими альтернативными действиями: 1) использование информации о банковском счете или банковской карте организации, юридического лица или физического лица в целях присвоения имущества владельца банковского счета или банковской карты либо в целях незаконной оплаты товаров и услуг; 2) изготовление, хранение, торговля, использование, распространение поддельных банковских карт с целью присвоения имущества владельца банковской карты либо в целях незаконной оплаты товаров и услуг; 3) незаконный доступ к банковскому счету организации, юридического лица или физического лица в целях хищения имущества; 4) обман в сфере электронной торговли, электронных платежей, онлайн-торговли валютой, онлайн-привлечения капитала, онлайн-многоуровневого маркетинга или онлайн-торговли ценными бумагами в целях хищения имущества.

Нельзя не отметить, что ст. 290 УК СРВ по конструкции объективной стороны охватывает не только отечественную норму об ответственности за компьютерное мошенничество (ст. 159^6 УК РФ), но и кражу с банковского счета и в отношении электронных денежных средств (п. «г» ч. 3 ст. 158 УК РФ), общий состав мошенничества, когда хищение денежных средств осуществляется дистанционно с использованием методов так называемой «социальной инженерии» (ст. 159 УК РФ), а также мошенничество с использованием электронных средств платежа (ст. 159^3 УК РФ). Такое решение о выделении специального состава хищения в сфере информационных технологий заслуживает пристального внимания, учитывая те трудности, которые в настоящее время испытывает отечественная правоприменительная практика при отграничении указанных выше составов преступлений.

Статья 291 УК СРВ предусматривает ответственность за незаконное получение и разглашение сведений, составляющих банковскую тайну. Обращает на себя внимание, что в отличие от ст. 183 УК РФ, по вьетнамскому уголовному законодательству лицо будет нести ответственность за незаконное собирание, хранение и разглашение информации о чужих банковских счетах только при наличии одного из альтернативных условий: 1) деяние совершено в отношении от 20 до 50 банковских счетов и 2) лицом получен доход в размере от 20 000 000 до 50 000 000 донгов.

Дифференциация ответственности по данной статье реализована в зависимости от количества скомпрометированных банковских счетов (от 50 до 200 счетов и свыше 200 счетов), систематичности действий виновного, совершения преступления в соучастии (организованной группой) и от размера полученного дохода от преступной деятельности.

Уголовное законодательство Вьетнама также предусматривает самостоятельную ответственность за незаконное использование радиочастот специальных служб (ст. 293 УК СРВ), а равно за умышленное создание помех нормальной работе радиоинформационной системы (ст. 294 УК СРВ). Составы указанных преступлений сконструированы с использованием альтернативных криминообразующих признаков: 1) причинение имущественного ущерба в размере от 200 000 000 до 500 000 000 донгов и 2) совершение деяния лицом, ранее привлекавшимся к ответственности за аналогичное правонарушение.

В отечественном уголовном законодательстве аналоги подобных составов преступлений отсутствуют. Вместе с тем, следует отметить, что Кодекс Российской Федерации об административных правонарушениях в ст. 13.4 предусматривает ответственность за нарушение требований к использованию радиочастотного спектра, правил радиообмена или использования радиочастот, несоблюдение норм или параметров радиоизлучения.

Важно отметить, что за совершение отдельных преступлений в сфере компьютерной информации уголовное законодательство Вьетнама устанавливает ответственность с 14-летнего возраста. Согласно ч. 1 ст. 12 УК СРВ общий возраст уголовной ответственности составляет 16 лет. Вместе с тем, в ч. 2 ст. 12 УК СРВ за совершение преступлений, предусмотренных ст.ст. 285, 286, 287, 289 и 290 УК СРВ, относящихся к тяжкой или особо тяжкой категории, лицо подлежит уголовной ответственности с 14 лет. В соответствии со ст. 9 УК СРВ тяжкими признаются преступления, за совершение которых максимальное наказание составляет от 7 до 15 лет лишения свободы, особо тяжкими – от 15 до 20 лет или более строгое наказание.

Как известно, российское уголовное законодательство преступные посягательства на безопасность компьютерных данных и систем связывает с достижением лицом общего возраста уголовной ответственности. В конце второго десятилетия XXI в. такое положение, на наш взгляд, вряд ли выражает осмысленную уголовно-политическую позицию и, по сути, является проявлением инерции в правовом регулировании. При принятии в 1996 году нового УК РФ проблема киберпреступности в России имела, мягко говоря, периферийный характер – предусмотрев соответствующую главу о преступлениях в сфере компьютерной информации, законодатель, не имея выраженного социального запроса, не особо вникал в тонкости (в том числе касающиеся криминологической характеристики личности киберпреступника) данного негативного явления. В современных же условиях положение об общем возрасте уголовной ответственности за посяга-

тельства на безопасность компьютерных данных и систем (гл. 28 УК РФ) не соответствует специфике данной преступности, которая изначально и до настоящего времени характеризуется существенной вовлеченностью именно представителей молодого поколения.

При этом наивным заблуждением является тезис о том, что несовершеннолетние в возрасте от 14 до 16 лет еще не могут в полной мере понимать характер совершаемого ими киберпреступления, а также сущность тех негативных последствий, которые за этим последуют. Ученые отмечают, что социализация детей сегодня происходит не только в материально-вещественном мире и привычной среде социальных взаимодействий, но и в цифровой среде. Причем с течением времени значение цифровой социализации только усиливается[1]. Следует признать, что представители «цифрового поколения» (или поколения «Z») начала 2000-х гораздо более ясно воспринимают ценность информационных активов и разрушительные последствия вредоносного поведения в виртуальном пространстве, чем мы привыкли о том судить.

В 2015 году Национальное агентство по борьбе с преступностью в Великобритании (NCA) опубликовало данные, согласно которым средний возраст киберпреступника снизился с 24 до 17 лет. По этой причине агентство инициировало социальную программу «#CyberChoices», направленную на предупреждение вовлечения несовершеннолетних в совершение преступлений с использованием современных информационно-коммуникационных технологий. Программа преимущественно ориентирована на подростков 12–15 лет и их родителей. По данным агентства, именно в этом возрасте несовершеннолетние зачастую начинают проявлять активность в использовании вредоносного программного обеспечения, в том числе для получения материальной выгоды[2].

В 2018 году заместитель председателя правления ПАО «Сбербанк России» Станислав Кузнецов представил журналистам результаты исследования банка и компании, специализирующейся в сфере информационной безопасности, «Bi.Zone», посвященного проблемам киберпреступности в мире. В ходе доклада С. Кузнецов отметил, что около 10 % кибер-

---

[1] См.: Плешаков В.А. Теория киберсоциализации человека: монография. М., 2011.

[2] [Электронный ресурс] // URL: https://nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime/cyber-crime-preventing-young-people-from-gettinginvolved? (дата обращения: 15.05.2019).

преступников имеют достаточно юный возраст (14–15 лет). При этом 85–90 % киберпреступников в мире – это молодые люди не старше 20 лет[1].

Анализ современной литературы позволяет сделать вывод, что идея снижения возраста уголовной ответственности за компьютерные преступления находит свою поддержку и в науке. Так, А.Ж. Кабанова, ссылаясь на происходящие процессы компьютеризации всех сфер общественной жизни, в своей работе обосновывает необходимость понижения возраста уголовной ответственности за преступления в сфере компьютерной информации с 16 до 14 лет[2]. Согласно результатам социологического исследования, проведенного К.Н. Евдокимовым в 2009 и 2017 гг., большинство прокурорских работников (53,1 %), сотрудников органов предварительного расследования (60 %) и компьютерных пользователей (73,3 %) поддерживают идею о снижении возраста уголовной ответственности за совершение преступлений в сфере компьютерной информации[3].

Изложенное позволяет сделать вывод, что в современных условиях имеются достаточные основания для принятия решения о снижении возраста уголовной ответственности за преступления против компьютерных данных и систем до 14 лет путем внесения соответствующих изменений в ч. 2 ст. 20 УК РФ. Вместе с тем, полагаем, что данное решение должно учитывать объективную неоднородность соответствующих составов, которая выявляется в наличии специальных норм об ответственности за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации (ст. 274 УК РФ), и за посягательства на нормальное функционирование объектов критической информационной инфраструктуры (ст. 274[1] УК РФ). Учитывая довольно сложное бланкетное содержание данных уголовно-правовых норм, а также размеры санкций ст. 274[1] УК РФ, возраст уголовной ответственности за соответствующие деяния, на наш взгляд, должен остаться общим.

---

[1] В Сбербанке рассчитали долю совершенных детьми киберпреступлений // [Электронный ресурс] // URL: https://www.rbc.ru/society/04/07/2018/5b3ceb009a7947b19e91997e (дата обращения: 15.05.2019).

[2] Кабанова А.Ж. Преступления в сфере компьютерной информации: уголовно-правовые и криминологические аспекты: автореф. дис. … канд. юрид. наук. Ростов-на-Дону, 2004. С. 4.

[3] Евдокимов К.Н. Проблемы квалификации и предупреждения нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ): монография. Иркутск, 2018. С. 54.

Проведенное исследование позволяет сделать несколько значимых выводов общего характера. Имея с Россией практически единую точку отсчета в построении уголовно-правового механизма противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий, Вьетнам реализовал более сложную модель как в криминализации, так и в части дифференциации ответственности.

Вьетнамская модель уголовно-правового противодействия киберпреступности развивалась в три этапа: 1-й этап характеризуется отсутствием специальных норм о компьютерных преступлениях и применением для квалификации компьютерных инцидентов общих положений уголовного законодательства (до 1999 года); 2-й этап связан с установлением ответственности за основные преступления против информационных технологий (до 2009 года) и 3-й этап характеризуется последовательным расширением защиты информационных ресурсов (реформы УК СРФ 2009, 2015 и 2017 гг.).

Применительно к отечественной проблематике уголовно-правового противодействия киберпреступности наибольшим теоретико-прикладным значением обладают положения уголовного законодательства Вьетнама в части дифференциации ответственности за совершение преступлений в сфере компьютерной информации в зависимости от незаконного получения прибыли или причинения ущерба с указанием размера в денежном эквиваленте; заражения электронных устройств или информационной системы с указанием точного количества пострадавших пользователей; отключения или приостановки работы компьютерной сети, телекоммуникационной сети или электронного устройства с детализацией такого периода по минутам и часам.

Законодательные подходы к определению преступлений, совершаемых с использованием информационно-коммуникационных технологий, в странах Содружества Независимых Государств

Ввиду многих причин политического, экономического, социального и культурного характера при проведении сравнительного исследования наиболее пристальное внимание традиционно уделяется законодательству стран Содружества Независимых Государств[1]. Нельзя не отметить, что в этом есть и сугубо практический смысл – учитывая сложившиеся процессы миграции населения, судебно-следственные органы стран Содружества гораздо чаще вынуждены взаимодействовать друг с другом в рамках

[1] Далее по тексту – Содружество или СНГ.

правовой помощи по уголовным делам. Как известно, в рамках СНГ в 2001 году было принято Соглашение о сотрудничестве в борьбе с преступлениями в сфере компьютерной информации, которое рекомендовало странам-участницам признавать уголовно наказуемыми следующие деяния, если они совершены умышленно: 1) осуществление неправомерного доступа к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети;2) создание, использование или распространение вредоносных программ;3) нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлёкшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред или тяжкие последствия;4) незаконное использование программ для ЭВМ и баз данных, являющихся объектами авторского права, а равно присвоение авторства, если это деяние причинило существенный ущерб[1].

В общем и целом, на первоначальном этапе все страны Содружества так или иначе регламентировали ответственность за три традиционных компьютерных преступления: 1) неправомерный доступ к компьютерным данным; 2) незаконное создание и распространение вредоносного программного обеспечения и 3) нарушение правил эксплуатации средств хранения, обработки и передачи компьютерных данных.

Однако, за прошедшее время «правовой ландшафт» противодействия компьютерной преступности в рамках СНГ претерпел существенные изменения. Следует констатировать, что в основной массе страны пошли по пути детализации уголовной ответственности за посягательства на отношения информационной безопасности и, как следствие, расширения перечня соответствующих составов. В настоящее время УК Республики Молдова содержит уже 10 составов компьютерных преступлений, УК Республики Казахстан – 9, УК Армении– 7, УК Республики Беларусь – 7, УК Республики Таджикистан – 7, УК Республики Узбекистан – 6, УК Азербайджана – 5. Пожалуй, наименее проработанным в части обеспечения информационной безопасности является УК Кыргызской Республики, который в настоящее время содержит лишь уголовно-правовой запрет на создание, использование и распространение вредоносных программ для ЭВМ (ст. 290). Следует, однако, отметить, что в проекте нового УК Кыргызстана (вступает в силу с 1 января 2019 года) регламентированы уже 3 преступления против информационной безопасности (глава 42): неправомерный доступ к компьютерной информации (ст. 304), создание

[1] Электронный ресурс // Соглашение о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере компьютерной информации от 01 июня 2001 г. // URL: http://www.cis.minsk.by/page.php?id=866 (дата обращения: 06.10.2017).

вредоносных компьютерных программ (ст. 305) и компьютерный саботаж (ст. 306)[1].

В настоящее время наиболее развёрнутую систему компьютерных преступлений содержит Уголовный кодекс Республики Молдова – всего 10 составов. Глава XI «Информационные преступления и преступления в области электросвязи» объединяет уголовно-правовые нормы об ответственности за: несанкционированный доступ к компьютерной информации (ст. 259), неправомерные производство, импорт, продажу или предоставление технических средств или программных продуктов, адаптированных для совершения преступлений (ст. 260), неправомерный перехват передачи информационных данных (ст. 260^1), нарушение целостности информационных данных, содержащихся в информационной системе (ст. 260^2), воздействие на функционирование информационной системы (ст. 260^3), неправомерные производство, импорт, продажа или предоставление паролей, кодов доступа или иных аналогичных данных (ст. 260^4), подлог информационных данных (ст. 260^5), информационное мошенничество (ст. 260^6), нарушение правил безопасности информационных систем (ст. 261), несанкционированный доступ к сетям или услугам электросвязи (ст. 261^1)[2].

В соответствии со ст. 259 УК Молдовы неправомерный доступ к информационным активам будет оконченным преступлением только при условии наступления двухуровневых последствий: 1) уничтожение, повреждение, модификации, блокирования или копирования информации, нарушения работы компьютеров, информационной системы или сети и 2) причинение ущерба в крупном размере[3]. Очевидно, что на практике установление причинно-следственной связи между самим неправомерным доступом и имущественными потерями потерпевшего может вызывать значительные трудности. С другой стороны, при подобной конструкции уголовно-правовой нормы нельзя будет квалифицировать как оконченное преступление в случаях, когда потерпевший своевременными действиями смог предотвратить наступление ущерба (например, восстановив утраченные данные).

Следует отметить, что действия, охватываемые ст. 272 УК РФ, в абсолютном большинстве национальных законодательств пространства СНГ рассредоточены сразу по нескольким составам. Как метко замечает по этому поводу О. И. Семыкина, законодательствам стран Содружества

---

[1] Сведения приведены на основании обращения к текстам нормативных актов, размещённых в справочных правовых системах или на официальных сайтах правительств соответствующих государств.

[2] [Электронный ресурс] // URL: http://online.zakon.kz/Document/?docid=30394923 #pos=2668;-85 (дата обращения: 21.03.2018).

[3] [Электронный ресурс] // URL: http://lex.justice.md/ru/331268/ (дата обращения: 21.03.2018).

характерен подход так называемого «распиливания» признаков неправомерного доступа к компьютерной информации на самостоятельные составы преступления путём конкретизации в них общественно опасных последствий[1]. Так, УК Республики Беларусь отдельно устанавливает ответственность за несанкционированный доступ (ст. 349), модификацию компьютерной информации, сопряжённую с несанкционированным доступом (ч. 2 ст. 350), умышленное уничтожение, блокирование, приведение в непригодное состояние компьютерной информации (компьютерный саботаж), сопряжённые с неправомерным доступом (ч. 2 ст. 351), несанкционированное копирование либо иное неправомерное завладение информацией (ст. 352). Сопоставление санкций показывает, что по белорусскому законодательству наименее тяжким является неправомерное копирование (завладение) компьютерными данными (наказывается лишением свободы на срок до двух лет), в то время как наиболее строгое наказание предусмотрено за компьютерный саботаж, сопряжённый с неправомерным доступом (наказывается лишением свободы на срок от трёх до десяти лет)[2].

Практически таким же образом дифференцирует посягательства на информационные данные законодатель Казахстана, отдельно устанавливая ответственность за неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций (ст. 205), неправомерное уничтожение или модификацию информации (ст. 206), неправомерное завладение информацией (ст. 208), неправомерное изменение идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента (ст. 213)[3]. Похожий подход реализован в уголовных кодексах Азербайджана, Армении, Молдовы, Таджикистана и Узбекистана.

Полагаем, что курс указанных государств на дифференциацию ответственности в зависимости от последствий неправомерного доступа к компьютерным данным следует оценить положительно. Такое решение в большей мере способствует реализации основополагающих принципов уголовного права и прежде всего принципа справедливости. Кроме того, наличие специальных норм об ответственности за уничтожение (блокирование), модификацию и копирование информационных данных, на наш взгляд, обладает значительно большим превентивным зарядом. Как справедливо писал В. Н. Кудрявцев, общая, абстрактная норма значительно удобнее для квалифицированного юриста. Но ведь уголовные законы

---

[1] Семыкина О. И. Противодействие киберпреступности за рубежом // Журнал зарубежного законодательства и сравнительного правоведения. 2016. № 6. С. 112.

[2] [Электронный ресурс] // URL: http://www.pravo.by/document /?guid=3871&p0=Hk9900275 (дата обращения: 05.03.2018).

[3] [Электронный ресурс] // URL: http://online.zakon.kz/m/Document /?docid=31575252# subid=2050000 (дата обращения: 07.03.2018).

создаются не только для юристов. Они имеют воспитательное и предупредительное значение. Простой и понятный текст закона, устанавливающего ответственность за конкретные действия, смысл которых ясен для любого гражданина, имеет важное профилактическое значение. Поэтому наряду с общими нормами, которые уже имеются в законодательстве, в некоторых случаях оправдано появление новых законов, подчёркивающих общественную опасность тех или иных форм поведения, причиняющих вред социалистическому обществу[1].

Уголовный кодекс Республики Казахстан содержит 9 составов преступлений, посягающих на отношения в сфере информатизации и связи (глава 7 УК РК): неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций (ст. 205), неправомерное уничтожение или модификация информации (ст. 206), нарушение работы информационной системы или сетей телекоммуникаций (ст. 207), неправомерное завладение информацией (ст. 208), принуждение к передаче информации (ст. 209), создание, использование или распространение вредоносных компьютерных программ и программных продуктов (ст. 210), неправомерное распространение электронных информационных ресурсов ограниченного доступа (ст. 211), предоставление услуг для размещения Интернет-ресурсов, преследующих противоправные цели (ст. 212), неправомерные изменение идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства (ст. 213)[2].

По уголовному законодательству Казахстана неправомерный доступ к охраняемой законом компьютерной информации должен быть сопряжён с общественно опасными последствиями в виде «существенного нарушения прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства». Белорусский законодатель в ряду альтернативных последствий несанкционированного доступа называет «существенный вред».

Активное использование таких оценочных признаков вряд ли следует признать обоснованным. Как известно, в теории уголовного права нет общепринятого толкования «существенности» нарушения или вреда, что

[1] Кудрявцев В. Н. Общая теория квалификации преступлений. М., 1972. С. 248 – 249.

[2] [Электронный ресурс] // URL: http://online.zakon.kz/m/Document /?docid=31575252 #subid=2050000 (дата обращения: 21.04.2018).

закономерно порождает неоднозначную правоприменительную практику, когда тождественные по-сути деяния получают разную правовую оценку[1].

Глава 33 «Преступления в сфере информатики и связи» раздела XIII «Преступления в сфере компьютерной информации» УК Республики Туркменистан также объединяет 9 преступлений, связанных с использованием информационно-коммуникационных технологий: неправомерный доступ к информации, в информационную систему или информационно-телекоммуникационную сеть (ст. 333), незаконное уничтожение информации или изменение её формата (ст. 334), нарушение нормальной работы информационной системы и информационно-телекоммуникационной сети (ст. 334^1), незаконное присвоение информации (ст. 334^2), распространение заведомо сфальсифицированной информации (ст. 334^3), создание, использование и распространение вредоносных программ (ст. 335), незаконное распространение электронных источников информации с ограниченным разрешением (ст. 335^1), оказание услуг по размещению Интернет-ресурсов, преследующих незаконные цели (ст. 335^2), неправомерное изменение идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства (ст. 335^3)[2].

Уголовный кодекс Армении устанавливает ответственность за следующие 7 компьютерных преступлений: несанкционированный доступ (проникновение) к системе компьютерной информации (ст. 251), изменение компьютерной информации (ст. 252), компьютерный саботаж (ст. 253), неправомерное завладение компьютерной информацией (ст. 254), изготовление или сбыт специальных средств для неправомерного доступа (проникновения) к компьютерной информации (ст. 255), разработка, использование и распространение вредоносных программ (ст. 256), нарушение правил эксплуатации компьютерной системы или сети (ст. 257)[3].

Практически идентичный список уголовно-правовых запретов содержит Уголовный кодекс Республики Беларусь: несанкционированный доступ к компьютерной информации (ст. 349), модификация компьютерной информации (ст. 350), компьютерный саботаж (ст. 351), неправомерное

---

[1] Как известно, неопределённость признака существенного нарушения прав и законных интересов граждан или организаций, либо охраняемых законом интересов общества или государства становилась предметом рассмотрения Конституционно Суда Российской Федерации. См., например: Определение Конституционного Суда РФ от 23 марта 2010 г. № 368-О-О // СПС «Консультант-Плюс».

[2] [Электронный ресурс] // URL: http://online.zakon.kz/Document/ ?docid=31295286#pos =2801;-159 (дата обращения: 21.04.2018).

[3] [Электронный ресурс] // URL: http://www.parliament.am/legislation.php?ID= 1349&sel= show&lang=rus#24 (дата обращения: 21.04.2018).

завладение компьютерной информацией (ст. 352), изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети (ст. 353), разработка, использование либо распространение вредоносных программ (ст. 354), нарушение правил эксплуатации компьютерной системы (ст. 355)[1].

Придерживается данной модели и УК Таджикистана (глава 28), выделяя следующую систему компьютерных преступлений: неправомерный доступ к компьютерной информации (ст. 298), модификация компьютерной информации (ст. 299), компьютерный саботаж (ст. 300), незаконное завладение компьютерной информацией (ст. 301), изготовление и сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети (ст. 302), разработка, использование и распространение вредоносных программ (ст. 303), нарушение правил эксплуатации компьютерной системы или сети (ст. 304)[2].

Как представляется, следует отметить удачное определение законодателем Таджикистана ответственности за нарушение правил эксплуатации компьютерной системы или сети. В диспозиции статьи содержится прямое указание на форму вины данного преступления – «…если это повлекло по неосторожности уничтожение, блокирование, модификацию компьютерной информации, нарушение работы компьютерного оборудования или причинение иного значительного ущерба». При этом деяния, связанные с умышленным посягательством на целостность и (или) доступность компьютерных данных должны квалифицироваться либо как модификация компьютерной информации, либо как компьютерный саботаж.

Уголовный кодекс Республики Узбекистан насчитывает 6 составов преступлений, посягающих на отношения в сфере обеспечения безопасности информационных технологий (глава XXI): нарушение правил информатизации (ст. 278^1), незаконный (несанкционированный доступ к компьютерной информации (ст. 278^2), изготовление с целью сбыта либо сбыт и распространение специальных средств для получения незаконного (несанкционированного) доступа к компьютерной системе (ст. 278^3), модификация компьютерной информации (ст. 278^4), компьютерный саботаж (ст. 278^5), создание, использование или распространение вредоносных программ (ст. 278^6)[3].

Следует отметить, что законодатель Республики Узбекистан использует идентичный подход, реализованный в ст. 272 УК РФ, – в качестве

---

[1] [Электронный ресурс] // URL: http://www.pravo.by/document/?guid=3871&p0=Hk9900275 (дата обращения: 21.04.2018).

[2] [Электронный ресурс] // URL: http://online.zakon.kz/Document/?docid=30397325#pos= 3041;-130 (дата обращения: 21.04.2018).

[3] [Электронный ресурс] // URL: http://www.lex.uz/pages/getact.aspx?lact_id=111457 (дата обращения: 21.04.2018).

обязательных последствий неправомерного доступа к компьютерной информации названы уничтожение, блокирование, модификация, копирование либо перехват информации.

Сравнительно-правовой анализ показывает, что не все государства Содружества используют такой конструктивный признак диспозиции ст. 272 УК РФ как охраняемая законом информация. Так, диспозиция ст. 278[2] УК Республики Узбекистан не содержит указания на то, что компьютерная информация, к которой осуществляется неправомерный доступ, должна быть охраняемой законом[1]. УК Республики Беларусь в ст. 349 указывает лишь на несанкционированный доступ к «информации, хранящейся в компьютерной системе, сети или на машинных носителях».

Уголовное законодательство Украины выделяет следующие преступления в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей, сетей электросвязи (раздел XVI): несанкционированное вмешательство в работу электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей либо сетей электросвязи (ст. 361), создание с целью использования, распространения или сбыта вредных программных либо технических средств, а также их распространение или сбыт (ст. 361[1]), несанкционированные сбыт или распространение информации с ограниченным доступом, сохраняющейся в электронно-вычислительных машинах (компьютерах), автоматизированных системах, компьютерных сетях или на носителях такой информации (ст. 361[2]), несанкционированные действия с информацией, обрабатывающейся в электронно-вычислительных машинах (компьютерах), автоматизированных системах, компьютерных сетях или сохраняющейся на носителях такой информации, совершенные лицом, имеющим право доступа к ней (ст. 362), нарушение правил эксплуатации электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей либо сетей электросвязи или порядка либо правил защиты информации, обрабатывающейся в них (ст. 363), воспрепятствование работе электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей либо сетей электросвязи путем массового распространения сообщений электросвязи (ст. 363[1])[2].

Достоинством украинского законодательства, на наш взгляд, является довольно успешное определение в ст. 362 субъекта преступления. Как известно, в науке уголовного права схожая проблема применительно к ст. 274 УК РФ до настоящего времени выступает предметом

---

[1] [Электронный ресурс] // URL: http://www.lex.uz/pages/getact.aspx?lact_id=111457 (дата обращения: 17.04.2018).

[2] [Электронный ресурс] // URL: http://online.zakon.kz/Document/?doc_id=30418109# pos=2981;-97 (дата обращения: 21.04.2018).

бескомпромиссной дискуссии. Кроме того, удачной представляется криминализация в ст. 363[1] так называемых DDOS-атак.

Уголовное законодательство Азербайджана в главе 30 «Киберпрестпления» содержит 5 составов: неправомерный доступ к компьютерной системе (ст. 271), неправомерное завладение компьютерной информацией (ст. 272), неправомерное вмешательство в компьютерную систему или компьютерную информацию (ст. 273), оборот средств, изготовленных для совершения киберпреступлений (ст. 273[1]), фальсификация компьютерных данных (ст. 273[2])[1].

В ряду квалифицирующих признаков совершения компьютерных преступлений УК Азербайджана содержится указание на «инфраструктурные объекты общественного значения». В соответствии с примечанием к ст. 271 УК Азербайджана под такими объектами подразумеваются государственные учреждения, предприятия, организации, неправительственные организации (общественные объединения и фонды), кредитные организации, страховые компании, инвестиционные фонды, которые представляют большую значимость для государства и общества.

Уголовный кодекс Грузии в главе XXXV предусматривает 3 состава преступления: самовольное проникновение в компьютерную систему (ст. 284), незаконное использование компьютерных данных или (и) компьютерных систем (ст. 285) и посягательство на компьютерные данные или (и) компьютерную систему (ст. 286).

В ряду особенностей грузинского законодательства, пожалуй, можно назвать установление ответственности юридических лиц в случае их причастности к киберпреступлениям. Возможными наказаниями выступают: штраф и лишение права заниматься определённой деятельностью или ликвидация и штраф[2].

Пожалуй, наименее проработанным в части обеспечения информационной безопасности является Уголовный кодекс Кыргызской Республики, который в настоящее время содержит лишь уголовно-правовой запрет на создание, использование и распространение вредоносных программ для ЭВМ (ст. 290). Следует, однако, отметить, что в проекте нового Уголовного кодекса Кыргызстана (вступает в силу с 1 января 2019 года)регламентированы уже 3 преступления против информационной безопасности (глава 42): неправомерный доступ к компьютерной информации (ст. 304), создание вредоносных компьютерных программ (ст. 305) и компьютерный саботаж (ст. 306)[3].

---

[1] [Электронный ресурс] // URL: http://online.zakon.kz/m/Document /?docid=30420353#subid=2710000 (дата обращения: 22.04.2018).

[2] [Электронный ресурс] // URL: https://matsne.gov.ge/ka/document/download /16426/ 143/ru/pdf (дата обращения: 22.04.2018).

[3] [Электронный ресурс] // URL: http://online.zakon.kz/Document/ ?docid=30222833#pos=0;0 (дата обращения: 22.04.2018).

Следует положительно оценить подход отдельных стран СНГ, дифференцировавших ответственность за неправомерный доступ к компьютерной информации в зависимости от содержания психического отношения субъекта. Так, статья 349 Республики Беларусь предусматривает ответственность за несанкционированный доступ к компьютерной информации, совершенный умышленно (ч. 2) и по неосторожности (ч.1).

УК Армении описывает несанкционированный доступ к компьютерной информации в целом как неосторожное преступление: «Несанкционированный доступ (проникновение) к какой-либо части системы информации или ко всей системе информации, хранящейся в компьютере, компьютерной системе, сети или на машинных носителях и охраняемой законом, совершенный с нарушением системы защиты и повлёкший *по неосторожности* (выделено мной – *Е.Р.*) изменение, копирование, уничтожение или блокирование информации, либо вывод из строя компьютера, компьютерной системы, сети или компьютерного оборудования либо иной значительный ущерб»[1]. Вместе с тем, умышленные посягательства на конфиденциальность, целостность и доступность компьютерных данных предусмотрены ст. 252 (изменение компьютерной информации), ст. 253 (компьютерный саботаж), и ст. 254 (неправомерное завладение компьютерной информацией).

Отсутствие чёткого разделения ответственности за неосторожное и умышленное уничтожение, блокирование, модификацию или копирование информации при неправомерном доступе является серьёзным изъяном действующей редакции ст. 272 УК РФ. Как представляется, заимствование опыта приведённых выше стран Содружества могло бы способствовать успешному устранению данной проблемы.

Проведённое исследование позволило выявить следующие типичные для пространства СНГ обстоятельства, усиливающие ответственность за преступления в сфере компьютерной информации: 1) совершение преступления группой лиц по предварительному сговору или организованной группой (ст. 271.2.2 УК Азербайджана, ч. 2 ст. 252 УК Армении, ч. 2 ст. 349 УК Белоруссии, ч. 2 ст. 206 УК Казахстана, п. «б» ч. 2 ст. 259 УК Молдовы, п. «а» ч. 2 ст. 278^2 УК Узбекистана); 2) наступление в результате совершения преступления тяжких последствий (ч. 3 ст. 251 УК Армении, ч. 3 ст. 349 УК Белоруссии, ч. 3 ст. 205 УК Казахстана, ч. 3 ст. 298 УК Таджикистана); 3) совершение преступления из корыстных побуждений (ч. 2 ст. 349 УК Белоруссии) 4) совершение преступления лицом с использованием своего служебного положения (ст. 271.2.3 УК Азербайджана, ч. 2 ст. 251 УК Армении, п. «в» ч. 2 ст. 278^2 УК

[1] [Электронный ресурс] // URL: http://www.parliament.am/legislation.php?ID =1349&sel= show&lang =rus#24 (дата обращения: 21.04.2018).

Узбекистана); 5) совершение преступления повторно (ст. 271.2.1 УК Азербайджана, п. «б» ч. 2 ст. 278^3 УК Узбекистана).

Следует констатировать, что отечественное уголовное законодательство в целом отражает главенствующий в пространстве СНГ подход к конструированию квалифицирующих признаков.

По УК Азербайджана отягчающим обстоятельством неправомерного доступа к компьютерной информации является совершение данного деяния в отношении «инфраструктурных объектов общественного значения». В соответствии с примечанием к ст. 271 УК Азербайджана под такими объектами подразумеваются государственные учреждения, предприятия, организации, неправительственные организации (общественные объединения и фонды), кредитные организации, страховые компании, инвестиционные фонды, которые представляют большую значимость для государства и общества. Можно с удовлетворением констатировать, что отечественное законодательство в этом аспекте уже было доработано. Как известно, с 1 января 2018 г. вступил в силу Федеральный закон от 26 июля 2017 г. №194-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»[1], которым глава 28 УК РФ была дополнена специальной нормой об ответственности за неправомерное воздействие на объекты критической информационной инфраструктуры Российской Федерации (ст. 274^1).

Подводя итог рассмотрению норм уголовного законодательства стран СНГ, можно сделать вывод, что отечественное законодательство об ответственности за компьютерные преступления требует совершенствования. Заслуживающими внимания мерами, на наш взгляд, являются: криминализация компьютерного саботажа и разделение ответственности за неправомерный доступ к компьютерной информации в зависимости от психического отношения субъекта к наступлению общественно опасных последствий (умысла или неосторожности); дифференциацию ответственности за неправомерный доступ в зависимости от наступивших последствий: а) уничтожение, блокирование, приведение в непригодное состояние компьютерной информации, б) её модификация (изменение), и в) копирование (завладение).

Подводя итог рассмотрению норм уголовного законодательства зарубежных стран, посвящённых ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, можно сделать следующие общие выводы:

1) в связи с активным ростом распространенности информационных способов совершения преступлений многие государства современного

[1] Российская газета. №167. 31.07.2017 г.

мира предприняли соответствующие меры по изменению (цифровизации) национального уголовного законодательства;

2) в современных условиях уголовно-правовое противодействие компьютерным и компьютеризированным преступлениям реализуется в следующих основных направлениях: а) путем применения общих норм на основе расширительного толкования сложившихся правовых категорий и конструкций; б) посредством закрепления использования информационных технологий в качестве конструктивных или квалифицирующих признаков; в) путем регламентации специальных норм об ответственности за посягательства на компьютерную информацию, а также средства ее хранения, обработки и передачи;

3) можно выделить основные модели уголовно-правового противодействия компьютерным и компьютеризированным преступлениям в зарубежных странах:

– *умеренная*, заключающаяся в выделении в уголовном законе специальных норм об ответственности за отдельные посягательства на компоненты информационной среды: компьютерную информацию, а также средства ее хранения, обработки и передачи;

– *экспоненциальная*, связанная с возрастающей во времени тенденцией к закреплению использования информационно-коммуникационных технологий в качестве конструктивных и (или) квалифицирующих признаков отдельных уголовно-правовых норм.

При этом в современных условиях наиболее предпочтительной является последняя модель. Вместе с тем, ее реализация требует соблюдения ряда фундаментальных требований, обеспечивающих системное единство отрасли;

4) в отличие от отечественной правовой традиции, американская, европейская и китайская модели противодействия компьютерным преступлениям исходят из разделения ответственности за деяния, связанные с воздействием на информацию, и деяния, посягающие на нормальное функционирование средств автоматизированной обработки данных;

5) сравнительный анализ показал, что преобладающими видами наказания за преступления, совершаемые с использованием информационно-коммуникационных технологий, выступают штраф и лишение свободы. При этом, в зависимости от отсутствия или наличия отягчающих обстоятельств, срок наказания в виде лишения свободы варьируется от нескольких месяцев до 10 лет.

РАЗДЕЛ II. ДИФФЕРЕНЦИАЦИЯ ОТВЕТСТВЕННОСТИ ЗА «ЦИФРОВЫЕ ПРЕСТУПЛЕНИЯ» КАК ОСНОВНОЕ НАПРАВЛЕНИЕ МОДЕРНИЗАЦИИ ОТЕЧЕСТВЕННОГО УГОЛОВНОГО ЗАКОНОДАТЕЛЬСТВА

ГЛАВА 1. ТЕОРЕТИКО-ПРАВОВЫЕ ОСНОВЫ ДИФФЕРЕНЦИАЦИИ ОТВЕТСТВЕННОСТИ ЗА «ЦИФРОВЫЕ ПРЕСТУПЛЕНИЯ»

Дифференциация уголовной ответственности является ключевым (основополагающим) направлением развития уголовного законодательства и уголовно-правовой политики Российской Федерации в решении стратегической задачи приспосабливания отечественного механизма уголовно-правовой охраны к условиям информационного общества. Отечественная доктрина уголовного права характеризуется наличием целого ряда фундаментальных исследований сущности, видов, средств и критериев дифференциации уголовной ответственности[1]. Вместе с тем, нельзя утверждать, что все значимые проблемы решены исчерпывающе, позиции авторов даже по принципиальным вопросам в отдельных случаях противоположны либо требуют некоторого переосмысления в современных условиях. Одно из классических определений дифференциации уголовной ответственности принадлежит Т.А. Лесниевски-Костаревой, которая раскрывает данное явление как «градацию, разделение, расслоение ответственности в уголовном законе, в результате которой законодателем устанавливаются различные уголовно-правовые последствия в зависимости от типовой степени общественной опасности преступления и личности виновного»[2].

Другие многочисленные определения дифференциации уголовной ответственности во многом повторяют приведенную выше дефиницию. А.В. Васильевский, например, характеризует ее как «изменение преду-

---

[1] См.: Васильевский А.В. Дифференциация уголовной ответственности и наказания в Общей части уголовного права : дис. … канд. юрид. наук. Ярославль, 2000; Грибов А.С. Дифференциация ответственности за экономические преступления в России, ФРГ и США: сравнительно-правовое исследование : автореф. дис. … канд. юрид. наук. Ярославль, 2011; Лесниевски-Костарева Т.А. Дифференциация уголовной ответственности : дис. ... д-ра юрид. наук. М., 1999; Рогова Е.В. Учение о дифференциации уголовной ответственности : дис. ... д-ра юрид. наук. М., 2014 и др.

[2] Лесниевски-Костарева Т.А. Дифференциация уголовной ответственности: теория и законодательная практика. М., 1998. С. 52.

смотренного законом вида, размера и характера меры ответственности в зависимости от изменения общественной опасности деяния и лица, его совершившего, а также с учетом принципа гуманизма и других важных обстоятельств»[1].

Экстравагантное, но в целом похожее определение формулирует Е.В. Рогова: «…разделение мер уголовно-правового характера, применяемых за совершение деяния, содержащего все признаки состава преступления, на основании характера и степени общественной опасности преступления и личности виновного в целях достижения баланса между строгостью ответственности за тяжкие и особо тяжкие преступления и мягкостью за преступления небольшой и средней тяжести»[2].

В определении Е.В. Роговой некоторые возражения вызывает цель дифференциации уголовной ответственности как некоего «баланса» строгости ответственности между разными категориями преступлений. Не совсем понятно, о каком балансе ведет речь автор, и может ли он выступать в качестве цели вообще. Полагаем, что некая стройность ответственности за разнокатегорированные преступления если и может выступать в качестве цели, то исключительно промежуточной, носящей при этом факультативный характер. Усилия законодателя по дифференциации ответственности, на наш взгляд, направлены к достижению более общей и отнюдь не формальной цели – надлежащего, соответствующего современным вызовам и угрозам, обеспечения уголовно-правовой охраны наиболее значимых благ и интересов от общественно опасных посягательств.

Среди представителей науки уголовного права нет общепринятого вȉдения относительного инструментария дифференциации уголовной ответственности, то есть того набора юридико-технических средств, посредством которых она, собственно, реализуется.

О.Н. Чупрова выделяет следующие средства дифференциации уголовной ответственности: в общей части УК РФ: 1) категории преступлений; 2) множественность преступлений; 3) неоконченное преступление; 4) соучастие в преступлении; 5) несовершеннолетие виновного; 6) смягчающие и отягчающие обстоятельства; 7) освобождение от уголовной ответственности и от наказания; в Особенной части УК РФ: 1) привилегиро-

[1] Васильевский А.В. Дифференциация уголовной ответственности и наказания в Общей части уголовного права : дис. … канд. юрид. наук. Ярославль, 2000. С. 4.

[2] Рогова Е.В. Учение о дифференциации уголовной ответственности : дис. ... д-ра юрид. наук. М., 2014. С. 161.

ванные и квалифицированные составы; 2) санкции статей; 3) специальные основания освобождения от уголовной ответственности[1].

В.С. Минская существенно расширяет круг средств дифференциации уголовной ответственности и относит к ним практически все положения Общей части, в том числе формы вины, добровольный отказ, виды наказаний и др.[2] В свою очередь, М.С. Румянцев к числу средств дифференциации уголовной ответственности уже относит сами разделы и главы Особенной части УК РФ[3].

Отмежевавшись от большинства, Е.В. Рогова подчеркивает системообразующий характер категоризации преступлений и называет ее не «средством», а «основой» дифференциации уголовной ответственности[4].

В теории уголовного права предметом бескомпромиссной дискуссии является отнесение к средствам дифференциации уголовной ответственности института освобождения от последней. М.Н. Каплин отмечает по этому поводу, что «уголовной ответственностью может являться лишь реальная мера, а не освобождение от нее. Соответственно, дифференцировать то, чего нет, невозможно»[5].

Противоположной точки зрения придерживаются Т.А. Лесниевски-Костарева[6] и Е.В. Рогова[7], которые относят к средствам дифференциации основания освобождения от уголовной ответственности, предусмотренные как в Общей, так и Особенной части УК РФ.

Полагаем, что институт освобождения от уголовной ответственности отнюдь не противоречит правовой природе средств дифференциации. В связи с этим категоричное утверждение М.Н. Каплина вызывает возражение ввиду того обстоятельства, что автор понимает дифференциацию в весьма ограничительном аспекте: дифференцировать – значит определить меру ответственности, но не освободить от нее. Вместе с тем, дифферен-

---

[1] Чупрова О.Н. Средства дифференциации уголовной ответственности // Юрист-Правовед. – 2007. – № 6. – С. 31.

[2] Минская В.С. Дифференциация уголовной ответственности в УК РФ // Уголовное право. – 1998. – № 3. – С. 18–24.

[3] Румянцев М.С. Особенности регламентации средств дифференциации ответственности в УК РФ // Российский следователь. – 2013. – № 2. – С. 29.

[4] Рогова Е.В. Учение о дифференциации уголовной ответственности : дис. ... д-ра юрид. наук. М., 2014. С. 198.

[5] Каплин М.Н. Сущность дифференциации уголовной ответственности // Юридические записки Ярославского государственного университета имени П.Г. Демидова. – 2001. – № 5. – С. 177.

[6] Лесниевски-Костарева Т.А. Дифференциация уголовной ответственности: теория и законодательная практика. М., 1998. С. 135.

[7] Рогова Е.В. Учение о дифференциации уголовной ответственности … С. 206.

циация предполагает определение законодателем всех юридически значимых оснований, влияющих на реализацию ответственности в принципе.

Многообразие позиций на определение средств дифференциации уголовной ответственности выявляет наличие расхождения в ответе на один основополагающий вопрос: следует ли относить к таковым средствам положения уголовного законодательства, с которыми законодатель связывает само *основание* уголовной ответственности: возраст уголовной ответственности, виды соучастников, стадии неоконченного преступления?

Полагаем, что ответ на поставленный вопрос не может быть исключительно отрицательным либо положительным. С одной стороны, положения ст.ст. 20, 30 и 33 УК РФ лежат в основе самой возможности ответственности по уголовному праву России за соучастие в преступлении, при его незавершенном характере, а равно с точки зрения возрастной зрелости человека. В этом проявляется не дифференцирующая, а криминообразующая природа данных положений. Не согласись мы с этим, к средствам дифференциации уголовной ответственности необходимо будет причислить практически все: правила действия уголовного закона во времени, пространстве и по кругу лиц, невменяемость, казус и т.д. Ложность такого пути очевидна – в действительности мы будем определять не средства градации уголовной ответственности, а признаки, с помощью которых очерчиваются ее пределы, внешние (межотраслевые) границы.

Вместе с тем, следует указать на то очевидное обстоятельство, что возраст уголовной ответственности в отечественном уголовном законе используется и как средство дифференциации ответственности. Так, например, возраст субъекта используется законодателем при разрешении вопроса о пределах ответственности за хищение предметов, имеющих особую ценность (ст. 164 УК РФ), посягательство на жизнь сотрудника правоохранительного органа (ст. 317 УК РФ) и др. В указанных случаях законодатель решает вопрос не о криминализации (поскольку ответственность за такие деяния уже установлена так называемыми общими нормами), а о дифференциации ответственности – с какого возраста лѝца должны нести сравнительно более строгую ответственность по соответствующим специальным нормам. Это позволяет сделать вывод, что возраст уголовной ответственности все же следует рассматривать как одно из средств ее дифференциации. При этом следует, безусловно, согласиться с тем, что дифференцирующим функционалом обладают положения, которые определяют особенности ответственности и наказания несовершеннолетних (гл. 14 УК РФ), соучастников (ст. 67 УК РФ) и при неоконченном пре-

ступлении (ст. 66 УК РФ). Однако эти нормы имеют отношение к наказанию, специальным правилам его назначения.

Значимым для настоящего исследования и в некотором смысле удивительным представляется то обстоятельство, что к самостоятельным средствам дифференциации уголовной ответственности, закрепленным в УК РФ, специалисты не относят специальные нормы и нормы об ответственности за составные преступления. Появление таких норм, как известно, не связано с криминализацией – до выделения специальной нормы или нормы с учтенной совокупностью уголовный закон уже признает такие действия преступными. В связи с этим выделение специального уголовно-правового запрета – это всегда своего рода «перекраивание» уже существующего порядка ответственности.

Пожалуй, одной из причин такого положения является то, что проблематика специальных норм традиционно позиционируется авторами в контексте оснований и критериев выделения квалифицирующих и привилегирующих признаков основных составов преступлений. Так, А.В. Архипов пишет, что специальные нормы в Особенной части УК РФ могут выделяться из общих по различным признакам. Решающее значение для выделения специального состава из общего должно иметь наличие существенной разницы в общественной опасности деяний, подпадающей под действие специальной нормы, по сравнению с общей. При этом само выделение специального состава должно производиться с целью дифференциации уголовной ответственности. Иными словами, специальная норма за совершение запрещенных ею деяний должна устанавливать уголовную ответственность, отличную от общей нормы. В противном случае, отмечает автор, выделение специальной нормы из общей становится просто бессмысленным[1].

Однако утверждать, что феномен специальных норм Особенной части УК РФ исчерпывается теорией квалифицирующих и привилегирующих признаков, будет крайне дискуссионным. Современное уголовное законодательство России позволяет выделить множество примеров, когда такие нормы регламентируются при очевидном отсутствии каких-либо отягчающих или смягчающих обстоятельств. В качестве примера можно хотя бы привести ст.ст. 285^1, 285^2, 285^3 и 285^4 УК РФ, каждая из которых, по сути, является специальной формой злоупотребления должностными полномочиями (ст. 285 УК РФ). Таким образом, почти аксиоматичное

[1] Архипов В.П. К вопросу о необходимости специальной нормы, предусматривающей уголовную ответственность за мошенничество при получении выплат // Вестник Томского государственного университета. – 2013. – № 377. – С. 96.

представление о том, что дифференциация уголовной ответственности – это *всегда* проблема «подвижности» общественной опасности деяния, приобретает дискуссионный характер. В современных условиях дифференциация уголовной ответственности может иметь и другие – уголовно-политические, формально-юридические, а иногда и сугубо утилитарные (обусловленные обеспечением эффективности правоприменения) основания. Этим, в частности, объясняется появление дополнительных видов мошенничества. И в данном аспекте «дробление» общих норм, главным образом, служит гарантией обеспечения принципа законности. Кроме того, оно также положительно сказывается на решении задачи общего предупреждения преступности. Судя по всему, в этом же контексте следует рассматривать появление специальных видов организаторских, подстрекательских и пособнических действий в Особенной части УК РФ. Очевидно, что появление соответствующих уголовно-правовых запретов не решало проблему криминализации, то есть определения *нового* общественно опасного деяния в качестве преступления. Законодатель, очевидно, стремился к достижению совершенно других целей.

Отказ теоретиков от признания уголовно-правовых норм об ответственности за составные преступления одним из средств дифференциации, возможно, объясняется крайне противоречивым к ним отношением. Так, А.П. Козлов, аргументируя искусственную природу составных преступлений, отмечает, что внутреннее единство содеянного не создает единого преступления, поскольку обусловлено лишь желанием законодателя объединить несколько преступлений в одной диспозиции нормы, и не более того[1].

Полагаем, что позиция автора о надуманном характере составных преступлений (при этом А.П. Козлов говорит даже не о составных преступлениях, а о составных диспозициях) является весьма дискуссионной. Объясняя наличие таких деяний в отечественном уголовном законодательстве, А.П. Козлов ссылается лишь на правотворческую инициативу, «голую» волю законодателя, и тем самым, на наш взгляд, крайне упрощает суть явления, игнорирует его глубинные криминологические предпосылки. Формализация составных преступлений – отнюдь не следствие «выдумки» законодателя, в основе их специального определения в Особенной части УК РФ лежит познание объективных закономерностей преступной деятельности.

---

[1] Козлов А.П. Юридическая природа составных и альтернативных «преступлений» // Вестник КрасГАУ. – 2006. – № 10. – С. 361.

Деяния, входящие в составное преступление, взаимосвязаны друг с другом, обладают внутренним единством, в реальной действительности часто совершаются в сочетании одного с другим и обладают специфической общественной опасностью именно в таком их сочетании[1]. Учитывая типичность, распространенность устойчивых сочетаний нескольких деяний и специфическую общественную опасность комбинации последних, образующей качественно новое образование, законодатель обобщает их, сводит в единое целое, отражая в соответствующем уголовно-правовом запрете в виде сложной, но единой законодательной конструкции. Как справедливо отмечает по этому поводу В.В. Питецкий: «…причин образования составных норм в законе несколько. Первая причина (юридическая) заключается в тесной взаимосвязи составов преступлений, образующих составную норму. Взаимосвязь составов обнаруживается на объективном уровне – причинно-следственные и обуславливающе-опосредованные связи, и на субъективном уровне – на уровне вины. Вторая причина (социальная) заключается в том, что такое сочетание преступлений достаточно распространено и типично, что во многом обусловливается общественными отношениями. Важнейшей причиной является повышенная общественная опасность такого рода актов преступного поведения, что, в частности, и приводит к закреплению составных норм. Процессуальной причиной является то, что образование составных норм существенно облегчает процессуальную деятельность судебных органов и органов расследования»[2].

Общетеоретические аспекты дифференциации ответственности получают иное, более конкретизированное, содержание в свете уголовно-правового противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий. Нельзя не отметить, что в теории уголовного права уже высказывались предложения по «цифровой» модернизации уголовного закона России. Так, О.М. Сафонов формулирует следующие направления дифференциации ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий: 1) закрепление в уголовном законе квалифицирующего признака «с использованием компьютерных технологий», в составах преступлений, которые могут совершаться с использованием таких технологий, и без них; 2) введение отдельных составов для деяний, которые без высоких технологий совершаться не могут (например,

[1] Гулиева Н.Б. Составные преступления в российском уголовном праве : дис. … канд. юрид. наук. Кемерово, 2006. С. 8.

[2] Питецкий В.В. Составные нормы в уголовном праве России : дис. … канд. юрид. наук. Красноярск, 2004. С. 9.

мошенничество в сфере компьютерной информации – ст. 159[6] УК РФ); 3) выделение в отдельную главу преступлений, в которых основным объектом являются отношения в сфере безопасности компьютерных систем[1].

Разработанные О.М. Сафоновым направления при очевидных достоинствах обладают и некоторыми недостатками. Прежде всего, остается неясным масштаб внедрения квалифицирующего способа совершения традиционных преступлений – требуется ли охватить все статьи Особенной части УК РФ или лишь отдельные составы? Стилистически неудачным представляется и редакция признака – «с использованием компьютерных технологий». Указание именно на «компьютерные» технологии является крайне казуальным и грозит многочисленными проблемами интерпретационного и прикладного характера.

С учетом теоретико-правовых основ дифференциации уголовной ответственности, модель ее реализации за преступления, совершаемые с использованием информационно-коммуникационных технологий, может быть представлена следующими блоками:

– *Совершенствованием дифференциации ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, средствами Общей части УК РФ.*

Первый блок предлагаемой модели затрагивает вопросы «настройки» общих положений отечественного уголовного законодательства к условиям трансформирующего влияния цифровизации на состояние и динамику современной преступности. Следует сразу отметить, что, учитывая фундаментальный характер институтов Общей части уголовного права, нельзя говорить о необходимости ее принципиального реформирования (по крайней мере, в обозримом будущем).

– *Совершенствованием дифференциации ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, средствами Особенной части УК РФ путем:*

а) выделения в Особенной части УК РФ специальных уголовно-правовых норм об ответственности за посягательства на традиционно охраняемые уголовным законом общественные отношения, опосредуемые информационно-коммуникационной инфраструктурой.

Указанный элемент дифференциации уголовной ответственности за преступления, совершаемые с использованием информационно-

[1] Сафонов О.М. Уголовно-правовая оценка использования компьютерных технологий при совершении преступлений: состояние законодательства и правоприменительной практики, перспективы совершенствования : дис. … канд. юрид. наук. М., 2015. С. 184.

коммуникационных технологий, охватывает деятельность по разработке и закреплению виртуальных форм, по сути, традиционных преступлений. Их особенностью является специфическое содержание объекта посягательства, который под влиянием информатизации жизнедеятельности приобрел дополнительное (цифровое) измерение. В определенном смысле данный блок является наиболее футурологическим, поскольку он основан на экстраполяции существующих информационно-коммуникационных тенденций на будущее состояние уголовно-правового механизма в целом и уголовное законодательство в частности. Пожалуй, наиболее ярким примером выступает установление уголовной ответственности за мошенничество в сфере компьютерной информации (ст. 159^6 УК РФ). Преступление объективное, невозможное еще в относительно недавнем прошлом, стало данностью нашего времени в связи с цифровизацией экономики и корреспондирующей этому модернизацией отношений собственности. Специальные нормы так или иначе будут связаны с появлением новых «цифровых сущностей» и формированием негативной практики посягательств на них;

б) выделения в Особенной части УК РФ уголовно-правовых норм с учтенной совокупностью (составных преступлений), где способом совершения посягательства на традиционно охраняемые уголовным законом общественные отношения выступает компьютерное преступление (деяние, предусмотренное главой 28 УК РФ).

Современное состояние преступности со всей очевидностью указывает на то, что многие посягательства на традиционно охраняемые уголовным законом общественные отношения «сращиваются» с преступлениями в сфере компьютерной информации. Так, в настоящее время такая тенденция отчетливо прослеживается по делам о нарушении неприкосновенности частной жизни (ст. 137 УК РФ), нарушении тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138 УК РФ), нарушении авторских и смежных прав (ст. 146 УК РФ) и др. В каждом таком случае правоприменитель прибегает к вменению совокупности преступлений, дополнительно квалифицируя действия субъекта по ст. 272 УК РФ. Вместе с тем, неправомерный доступ к охраняемой законом компьютерной информации стал настолько типичным для определенного круга традиционных составов преступлений, что имеются все основания для конкретизации этих компьютеризированных форм непосредственно в соответствующих статьях Особенной части УК РФ. Реализованным в настоящее время примером такой дифференциации является установление в ч. 3 ст. 141 УК РФ ответственности за специальный случай воспрепятствования осуществлению избирательных прав или работе из-

бирательных комиссий путем неправомерного вмешательства в работу Государственной автоматизированной системы Российской Федерации «Выборы»;

в) дополнения статей Особенной части УК РФ указанием на специфический способ совершения преступления – с использованием информационно-коммуникационных технологий – в качестве квалифицирующего признака.

Сложно поставить под сомнение то очевидное обстоятельство, что использование информационно-коммуникационных технологий, как говорится, «per se», во многом облегчает совершение посягательства на охраняемые уголовным законом общественные отношения. Виртуальное пространство обеспечивает анонимность злоумышленника, экстерриториальный характер существенно осложняет решение задачи раскрытия и расследования преступления. С другой стороны, очевидность данных доводов заставляет задуматься над вопросом о том, почему до настоящего времени они не легли в основу дифференциации ответственности за совершение многих других традиционных преступлений, например, вымогательства или угрозы убийством? Является ли это следствием некой инерции (архаики) отечественной уголовной политики или имеется какое-то другое объяснение?;

г) совершенствования норм об ответственности за преступления, посягающие на безопасность информационно-коммуникационной инфраструктуры (глава 28 УК РФ).

Данный элемент в целом касается содержания главы 28 УК РФ и затрагивает вопросы оптимального количества уголовно-правовых норм об ответственности за посягательства на отношения, обеспечивающие безопасность информационно-коммуникационной инфраструктуры; обоснованности учета традиционных квалифицирующих обстоятельств (групповой способ совершения преступления, служебное положение субъекта, тяжесть наступивших последствий и др.); выделения специфических отягчающих признаков, не свойственных другим группам преступлений; конструирования специальных оснований освобождения от уголовной ответственности за преступления, совершаемые против безопасности данных и информационно-коммуникационных систем.

В завершение данной части работы следует выделить ее основные положения и выводы:

1) дифференциация уголовной ответственности является ключевым (основополагающим) направлением развития уголовного законодательства и уголовно-правовой политики Российской Федерации в решении

стратегической задачи приспосабливания отечественного механизма уголовно-правовой охраны к условиям информационного общества;

2) наряду с традиционно выделяемыми в доктрине уголовного права к средствам дифференциации уголовной ответственности также следует относить специальные нормы и нормы об ответственности за составные преступления (преступления с учтенной совокупностью);

3) с учетом теоретико-правовых основ дифференциации уголовной ответственности, модель ее реализации за преступления, совершаемые с использованием информационно-коммуникационных технологий, может быть представлена следующими блоками:

– совершенствованием дифференциации ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, средствами Общей части УК РФ;

– совершенствованием дифференциации ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, средствами Особенной части УК РФ путем:

а) выделения в Особенной части УК РФ специальных уголовно-правовых норм об ответственности за посягательства на традиционно охраняемые уголовным законом общественные отношения, опосредуемые информационно-коммуникационной инфраструктурой;

б) выделения в Особенной части УК РФ уголовно-правовых норм с учтенной совокупностью (составных преступлений), где способом совершения посягательства на традиционно охраняемые уголовным законом общественные отношения выступает компьютерное преступление (деяние, предусмотренное главой 28 УК РФ);

в) дополнения статей Особенной части УК РФ указанием на специфический способ совершения преступления – с использованием информационно-коммуникационных технологий – в качестве квалифицирующего признака;

г) совершенствования норм об ответственности за преступления, посягающие на безопасность информационно-коммуникационной инфраструктуры (глава 28 УК РФ).

ГЛАВА 2. ДИФФЕРЕНЦИАЦИЯ ОТВЕТСТВЕННОСТИ ЗА «ЦИФРОВЫЕ ПРЕСТУПЛЕНИЯ» СРЕДСТВАМИ ОБЩЕЙ ЧАСТИ УГОЛОВНОГО ПРАВА

2.1. ДИФФЕРЕНЦИАЦИЯ ОТВЕТСТВЕННОСТИ ЗА «ЦИФРОВЫЕ ПРЕСТУПЛЕНИЯ» СРЕДСТВАМИ ИНСТИТУТА ПРЕСТУПЛЕНИЯ

Дифференциация ответственности реализуется законодателем в рамках всего уголовного закона путем комплексного и сбалансированного применения средств его Общей и Особенной частей. При этом логично сделать вывод, что своего рода «глубинная» дифференциация проводится именно в Общей части, поскольку она затрагивает ключевые (фундаментальные) отраслевые механизмы. Следует сразу оговориться, что проблематика дифференциации ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, средствами Общей части уголовного права будет нами представлена в двух перспективах: 1) в актуально-прикладном значении, объединяющем насущные (уже оформившиеся) проблемы модернизации Общей части уголовного права в условиях цифровизации преступности и 2) в прогностико-футурологическом контексте, объединяющем комплекс вопросов эволюции Общей части уголовного права в свете прогнозируемых с учетом технологических, экономических и социальных тенденций экспоненциальных преобразований общества.

В актуально-прикладной перспективе проблемы дифференциации ответственности за исследуемые посягательства средствами института преступления, на наш взгляд, преимущественно касаются возраста уголовной ответственности и соучастия.

Отечественное уголовное законодательство преступные посягательства на безопасность компьютерных данных и систем связывает с достижением лицом общего возраста уголовной ответственности. В конце второго десятилетия XXI в. такое положение, на наш взгляд, вряд ли выражает осмысленную уголовно-политическую позицию и, по сути, является проявлением инерции в правовом регулировании. При принятии в 1996 году нового УК РФ проблема киберпреступности в России имела, мягко говоря, периферийный характер – предусмотрев соответствующую главу о преступлениях в сфере компьютерной информации, законодатель, не имея выраженного социального запроса, не особо вникал в тонкости (в том числе касающиеся криминологической характеристики личности киберпреступника) данного негативного явления. В современных же условиях положение об общем возрасте уголовной ответственности за посягатель-

ства на безопасность компьютерных данных и систем (гл. 28 УК РФ) не соответствует специфике данной преступности, которая изначально и до настоящего времени характеризуется существенной вовлеченностью именно представителей молодого поколения.

При этом наивным заблуждением является тезис о том, что несовершеннолетние в возрасте от 14 до 16 лет еще не могут в полной мере понимать характер совершаемого ими киберпреступления, а также сущность тех негативных последствий, которые за этим последуют. Проведенное нами исследование показало, что лица в возрасте от 14 до 18 лет, как правило, демонстрируют более глубокие познания в принципах построения и функционирования информационно-коммуникационной инфраструктуры, чем представители старших групп. Уровень компьютерной грамотности несовершеннолетних позволяет им довольно легко ориентироваться в предлагаемых виртуальной средой продуктах и услугах. При этом абсолютное большинство из них обладают навыками по обеспечению собственной информационной безопасности. Приверженность данной группы к «информационной гигиене» складывается преимущественно по той причине, что несовершеннолетние хорошо осведомлены об имеющихся рисках, связанных с компьютерными инцидентами, в том числе с теми, которые касаются использования и распространения вредоносных компьютерных программ. В отличие от представителей старших групп лѝца данного возраста более осведомлены о принципах функционирования «анонимайзеров», «вирусов-шифровальщиков», а равно так называемой скрытой сети «DarkNet».

Ученые отмечают, что социализация детей сегодня происходит не только в материально-вещественном мире и привычной среде социальных взаимодействий, но и в цифровой среде. Причем с течением времени значение цифровой социализации только усиливается[1]. Следует признать, что представители «цифрового поколения» (или поколения «Z») начала 2000-х гораздо более ясно воспринимают ценность информационных активов и разрушительные последствия вредоносного поведения в виртуальном пространстве, чем мы привыкли о том судить.

Полученные нами результаты в целом корреспондируют данным более масштабных исследований, проведенных российскими и зарубежными правительственными структурами и компаниями. Так, в 2015 году Национальное агентство по борьбе с преступностью в Великобритании (NCA) опубликовало данные, согласно которым средний возраст киберпреступ-

[1] См.: Плешаков В.А. Теория киберсоциализации человека : монография. М., 2011.

ника снизился с 24 до 17 лет. По этой причине агентство инициировало социальную программу «#CyberChoices», направленную на предупреждение вовлечения несовершеннолетних в совершение преступлений с использованием современных информационно-коммуникационных технологий. Программа преимущественно ориентирована на подростков 12–15 лет и их родителей. По данным агентства, именно в этом возрасте несовершеннолетние зачастую начинают проявлять активность в использовании вредоносного программного обеспечения, в том числе для получения материальной выгоды[1].

В 2018 году заместитель председателя правления ПАО «Сбербанк России» Станислав Кузнецов представил журналистам результаты исследования банка и компании, специализирующейся в сфере информационной безопасности, «Bi.Zone», посвященного проблемам киберпреступности в мире. В ходе доклада С. Кузнецов отметил, что около 10 % киберпреступников имеют достаточно юный возраст (14–15 лет). При этом 85–90 % киберпреступников в мире – это молодые люди не старше 20 лет[2].

Анализ современной литературы позволяет сделать вывод, что идея снижения возраста уголовной ответственности за компьютерные преступления находит свою поддержку и в науке. Так, А.Ж. Кабанова, ссылаясь на происходящие процессы компьютеризации всех сфер общественной жизни, в своей работе обосновывает необходимость понижения возраста уголовной ответственности за преступления в сфере компьютерной информации с 16 до 14 лет[3].

В свою очередь, С.В. Скляров и К.Н. Евдокимов считают возможным снизить возраст уголовной ответственности физических лиц за совершение неправомерного доступа к компьютерной информации, если

---

[1] [Электронный ресурс] // URL: https://nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime/cyber-crime-preventing-young-people-from-gettinginvolved? (дата обращения: 15.05.2019).

[2] В Сбербанке рассчитали долю совершенных детьми киберпреступлений // [Электронный ресурс] // URL: https://www.rbc.ru/society/04/07/2018/5b3ceb009a7947b19e91997e (дата обращения: 15.05.2019).

[3] Кабанова А.Ж. Преступления в сфере компьютерной информации: уголовно-правовые и криминологические аспекты : автореф. дис. … канд. юрид. наук. Ростов н/Д, 2004. С. 4.

данное деяние повлекло наступление тяжких последствий (ч. 4 ст. 272 УК РФ)[1].

Согласно результатам социологического исследования, проведенного
К.Н. Евдокимовым в 2009 и 2017 гг., большинство прокурорских работников (53,1 %), сотрудников органов предварительного расследования (60 %) и компьютерных пользователей (73,3 %) поддерживают идею о снижении возраста уголовной ответственности за совершение преступлений в сфере компьютерной информации[2].

Изложенное позволяет сделать вывод, что в современных условиях имеются достаточные основания для принятия решения о снижении возраста уголовной ответственности за преступления против компьютерных данных и систем до 14 лет путем внесения соответствующих изменений в ч. 2 ст. 20 УК РФ. Вместе с тем, полагаем, что данное решение должно учитывать объективную неоднородность соответствующих составов, которая выявляется в наличии специальных норм об ответственности за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации (ст. 274 УК РФ), и за посягательства на нормальное функционирование объектов критической информационной инфраструктуры (ст. 274[1] УК РФ). Учитывая довольно сложное бланкетное содержание данных уголовно-правовых норм, а также размеры санкций ст. 274[1] УК РФ, возраст уголовной ответственности за соответствующие деяния, на наш взгляд, должен остаться общим[3].

Применительно к составу мошенничества в сфере компьютерной информации, С.С. Медведев делает вывод, что возраст наступления уголовной ответственности за данный вид мошенничества необходимо понизить до 14 лет. Автор аргументирует свою позицию преимущественно тем, что процесс социализации в современном обществе значительно ускорен[4].

---

[1] Скляров С.В., Евдокимов К.Н. Актуальные вопросы совершенствования судебной практики по уголовным делам о хищении чужого имущества путем ввода, удаления, блокирования, модификации компьютерной информации (ст. 159.6 УК РФ) // Российский судья. – 2017. – № 7. – С. 28–32.

[2] Евдокимов К.Н. Проблемы квалификации и предупреждения нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ) : монография. Иркутск, 2018. С. 54.

[3] Такое предложение нашло свою поддержку у 69 % опрошенных респондентов.

[4] Медведев С.С. Мошенничество в сфере высоких технологий : автореф. дис. … канд. юрид. наук. Краснодар, 2008. С. 15.

Полагаем, что идея о снижении возраста уголовной ответственности за хищение, совершаемое посредством неправомерного вмешательства в функционирование информационно-коммуникационных систем, прежде всего, систем дистанционного банковского обслуживания, заслуживает всяческой поддержки. Вместе с тем, нельзя не отметить, что вопрос о возрасте уголовной ответственности за компьютеризированные преступления всегда должен решаться системно, то есть исключительно в контексте ответственности за группу однородных посягательств в целом. Снижение возраста уголовной ответственности, например, за мошенничество в сфере компьютерной информации, закономерно породит вопрос о том, почему за другие виды мошенничества (хотя мы и не считаем, что преступление, предусмотренное ст. 159[6] УК РФ, по своей сути является видом мошенничества) ответственность наступает с общего возраста.

Компьютерная преступность характеризуется специфической архитектурой криминальных связей. В абсолютном большинстве случаев лѝца не знают друг друга в реальной жизни, и их взаимодействие реализуется посредством виртуальных средств идентификации. При этом площадками для построения и поддержания преступных связей, как правило, выступают специальные сайты, на которых осуществляется обмен сведениями о способах совершения компьютерных преступлений, предлагаются услуги по взлому электронной почты, распространяется вредоносное программное обеспечение, принимаются заказы и продается ботнет, специальное оборудование, базы данных с реквизитами клиентов кредитных организаций и т.д. В данной связи можно сослаться на меткое наблюдение Н.Ш. Козаева: «Переход по первой же ссылке, – пишет он, – привел на форум, где некое лицо предлагает оптом в 50 шт. приобрести карты оператора сотовой связи «Билайн» и беззастенчиво указывает цели: «если их пробивают, то показывают, что такого номера не существует, идеально подходит для создания киви, регистрации в соцсетях или для «мама срочно отправь на этот номер 500 руб., позже все объясню»[1].

В качестве отдельной проблемы следует также указать на получающие все большую популярность онлайн-курсы для программистов («hacker schools»). Формально заявляя о реализации образовательных программ для тех, кто хочет приобрести знания и навыки в программировании, отдельные из них фактически являются площадками для подготовки к совершению компьютерных преступлений[2].

---

[1] Козаев Н.Ш. Современные технологии и проблемы уголовного права (анализ зарубежного и российского законодательства). М., 2015. С. 187.

[2] Qianyun Wang. A comparative study of cybercrime in criminal law of China, US, England, Singapore and the Council of Europe. Rotterdam, 2016. P. 46.

Масштабное распространение безадресного подстрекательства и предлагаемой по принципу «до востребования» помощи в совершении компьютерных преступлений позволило отдельным специалистам сделать вывод о необходимости переосмысления некоторых общетеоретических положений института соучастия. Так, по мнению А.Ю. Чупровой, особенностью подстрекательских действий в сети «Интернет» является то, что умысел лица не персонифицирован, его призыв к совершению преступления обращен к неопределенно большому кругу лиц. Кто найдет предложение заслуживающим внимания и одобрения и реализует его на практике, автору прокламации неизвестно[1].

В свою очередь, М.Д. Фролов уже напрямую пишет, что лицо, склоняющее к совершению преступления в сфере информационно-коммуникационных технологий или оказывающее тому содействие неограниченному и не персонифицированному числу лиц, имеет не абстрактное, а вполне конкретное намерение. Абстрактность самого исполнителя не меняет общего вывода о наличии причинной обусловленности и реальной взаимосвязи таких действий, то есть о наличии признаков соучастия[2].

Вряд ли следует признать оправданным отказ от запрета на привлечение к ответственности за так называемое абстрактное соучастие. Подстрекательством может быть признано склонение другого лица к совершению конкретного преступления, а не пробуждение абстрактных преступных устремлений или интереса к противоправному поведению. Недостаточно дать кому-то совет заняться кражами: для признания лица подстрекателем необходимо, чтобы оно подстрекнуло совершить определенную кражу путем объяснения выгод от преступления, умаления трудностей и опасности, с которыми сопряжено его выполнение[3]. В той же мере сказанное относится и к пособничеству.

Современная судебная практика демонстрирует строгую приверженность данной концепции. Так, оправдывая Ч. в совершении преступления, суд указал, что пособник осознает, в совершении какого конкретного преступления он оказывает содействие, предвидит возможность наступления в результате действий исполнителя общественно опасных последствий и желает либо сознательно допускает наступление таких последствий,

---

[1] Чупрова А.Ю. Уголовно-правовые механизмы регулирования отношений в сфере электронной коммерции : дис. ... д-ра юрид. наук. М., 2015. С. 259.

[2] Фролов М.Д. О некоторых проблемах квалификации мошенничества в сфере компьютерной информации // Адвокат. – 2016. – № 6. – С. 57.

[3] Курс российского уголовного права. Общая часть / под ред. В.Н. Кудрявцева, А.В. Наумова. М., 2001. С. 359.

…каких-либо фактов, свидетельствующих о том, что передавая С. и М. информацию о потерпевших, Ч. осознавал, что этим он способствует совершению преступлений в их отношении, не установлено[1].

По другому делу, соглашаясь с выводом об отсутствии в действиях Аджиева состава преступления, предусмотренного ч. 4 ст. 33 п. «б» ч. 2 ст. 105 УК РФ, суд указал, что призывы и пожелания общего характера, которые непосредственно не направлены на склонение лица к конкретному противоправному деянию, не являются подстрекательством. Отсутствует оно и в том случае, если лицо в общей форме выражает мысль о желательности совершения того или иного преступления, однако она не обращена к другому лицу как к избранному (предполагаемому) исполнителю этого преступления[2].

Согласимся, пожалуй, что попытки расширительного толкования подстрекательских и пособнических действий по делам о компьютерных преступлениях имеют свое объяснение – публичное размещение информации, склоняющей или облегчающей их совершение, объективно является общественно опасным и требует надлежащей оценки. Вместе с тем, даже при решении самых злободневных проблем нельзя законность приносить в жертву «социальной необходимости», произвольно расширяя пределы действия уголовного закона. Пожалуй, отечественному законодателю необходимо обратить более пристальное внимание на опыт других государств, которые пошли по пути выделения специальных норм об ответственности за подобное поведение[3].

Следует с сожалением констатировать, что потенциал уголовно-правовых средств реагирования на организованные формы преступной деятельности в виртуальном пространстве существенным образом купирован вследствие современной редакции ч. 4 ст. 35 УК РФ. Действующее законодательное определение преступного сообщества не позволяет распространить его (с последующим применением ст. 210 УК РФ) на совершаемые структурированными организованными группами или объединениями организованных групп преступления, не относящиеся к тяжким или особо тяжким. Вместе с тем, хорошо известно, что совершением заказных

---

[1] Апелляционное определение Верховного Суда Российской Федерации от 27 апреля 2017 г. по делу № 89-АПУ17-3сп.

[2] Апелляционное определение Верховного Суда Российской Федерации от 04 июня 2015 г. по делу № 30-АПУ15-3.

[3] Например, с 2015 года ответственность за такие действия предусмотрена ст. 287 (Б) УК Китайской Народной Республики. См.: Qianyun Wang. A comparative study of cybercrime in criminal law of China, US, England, Singapore and the Council of Europe. Rotterdam, 2016. P. 42.

DDOS-атак на информационные ресурсы физических и юридических лиц занимаются организованные группы, структурированные по функциональному принципу на: 1) разработчиков вредоносного программного обеспечения, 2) его распространителей для создания бот-сетей, 3) лиц, отвечающих за поиск клиентов и 4) курирующих вопросы обналичивания/распределения полученных доходов, а также их легализацию. С внешней стороны такие организованные группы напоминают IT-компанию, у которой имеется также руководство и даже свой отдел кадров, занимающийся на постоянной основе поиском талантливых специалистов в сфере информационной безопасности.

В результате, значительное количество высокоорганизованной преступной деятельности получает оценку исключительно в рамках квалифицированных видов ст.ст. 272 и 273 УК РФ по признаку совершения соответствующих преступлений организованной группой. Полагаем, что для решения данной проблемы необходимо внести изменения в ч. 4 ст. 35 УК РФ (соответственно и в ч. 1 ст. 210 УК РФ) путем исключения указания на такую цель создания преступного сообщества, как совершение именно тяжких и особо тяжких преступлений.

Развитие и внедрение цифровых технологий связаны с высоким уровнем неопределенности. Это означает, что мы не имеем четкого представления, как в условиях четвертой промышленной революции будет трансформироваться уголовное право. В свою очередь, сама сложность процесса цифровизации уголовно-правовой сферы предполагает повышенную ответственность научного сообщества, которое должно обеспечить надлежащий уровень осмысления формирующихся тенденций. Указанные обстоятельства и обусловили постановку нами вопросов прогнозирования эволюции института преступления Общей части уголовного права на основе экстраполяции наблюдаемых технологических, экономических и социальных тенденций преобразования общества.

В конце второго десятилетия XXI в. как никогда ранее ощущается, что технологии обратного проектирования человеческого мозга приведут к созданию искусственного интеллекта и, соответственно, к появлению «разумных машин», а также обеспечат клонирование (продолжение жизни) человека в цифровой форме. Само по себе это станет точкой невозврата, когда, как метко замечает по этому поводу Г. Леонгард, «наши тела перестанут быть центром нашей идентичности»[1].

Появление «цифровой личности», на наш взгляд, завершит начавшийся переход от традиционного уголовного права индустриального об-

[1] Леонгард Г. Технологии против человека. М., 2018. С. 69.

щества XX в. к уголовному праву цифрового мира XXI в. («Уголовному праву 2.0»). Это подтверждается тем, что искусственный интеллект и «цифровая личность» принципиально изменят сферу уголовно-правовой охраны. Как известно, уже сегодня люди обращают в цифру все, что может быть виртуализировано. На первоначальном этапе это затронуло музыку, фильмы, книги, газеты и т.п. Сейчас этот процесс охватил кредитно-финансовый сектор, страхование, здравоохранение и транспорт. Параллельно с этим привычные объекты преступных посягательств последовательно приобретают дополнительное (цифровое) измерение. Юридическая практика уже «привыкла» к цифровым аналогам почтовых сообщений, объектов интеллектуальной собственности, денежных средств, ценных бумаг, платежных карт, официальных документов и др. Квалификация преступных посягательств на такие предметы в рамках действующего Уголовного кодекса Российской Федерации не вызывает значимых затруднений у правоприменителей.

Появление технологии эмуляции биологического мозга человека будет означать возможность совершенно новой формы жизни, когда само понятие о человеке больше не будет связано с его биологической оболочкой. Понятно, что эта жизнь в облаке потребует такой же уголовно-правовой защиты, как и в реальном физическом мире, поскольку здесь мы будем иметь дело не просто с компьютерным кодом, а с человеком. В результате нам необходимо будет распространить действие традиционных уголовно-правовых запретов (об убийстве, похищении человека, торговле людьми и др.) на все посягательства против «цифровой личности». Сам момент наступления смерти человека потеряет свое исключительно биологическое определение, получив дополнительное содержание в том, что в настоящее время мы именуем заурядным уничтожением компьютерной информации.

Смежной проблемой выступает защита субъектов, которые будут обладать человекоподобным сознанием небиологического происхождения. Обращаясь к данному вопросу, один из самых известных профессиональных футурологов современности – технический директор компании «Google» Рэй Курцвейл – пишет: «…сегодня мало кто беспокоится по поводу страданий, причиняемых нами компьютерным программам (зато мы часто жалуемся на муки, которые компьютерные программы доставляют нам), но если в будущем компьютерное обеспечение получит интеллектуальные, эмоциональные и моральные качества человека, на этом месте возникнет проблема»[1].

[1] Курцвейл Р. Эволюция разума. М., 2019. С. 244.

В продолжение своих мыслей Р. Курцвейл подчеркивает, что такие сущности «…станут неотличимы от живого человека, которого мы считаем сознательным существом, и, следовательно, будут разделять все те духовные ценности, что мы связываем с сознанием. Это не унижение достоинства человека, а скорее возвышение нашей оценки некоторых машин будущего. Возможно, для этих существ понадобится выбрать другую терминологию, поскольку это будут совсем другие машины»[1].

Разумеется, вопрос о модели уголовно-правовой охраны таких «умных машин» целиком зависит от выражения позиции всего человечества (полагаем, в лице универсальных международных организаций) относительно их природы и статуса. Будут ли такие сущности признаны равными человеку, то есть новой небиологической формой разумной жизни, или в целом их положение будет сравнимо, например, с животными, уголовно-правовую охрану которых мы реализуем в контексте защиты общественной нравственности, предсказать достаточно сложно. С высокой долей вероятности возможен смешанный сценарий, когда в зависимости от уровня воспроизведения интеллектуальных и эмоциональных качеств человека такие киберфизические системы будут определены в правовом поле дифференцированно – как равные человеку, то есть полноценные участники общественных отношений, новые субъекты права, и как автоматизированные системы с ограниченными функциями (способностями) искусственного интеллекта, то есть как высокотехнологичные устройства, вещи.

П.М. Морхат полагает, что в зависимости от функционально-целевого назначения и возможностей искусственный интеллект должен обладать гетерогенной правосубъектнстью. При этом автор указывает на возможность выделения соответствующего субъекта права – электронного лица, обладающего признаками «формализованного технико-юридического образа, воплощающего модальную фреймизацию персонифицированного юнита искусственного интеллекта, обособленную от человеческого субстрата»[2].

Индикатором перехода к «Уголовному праву 2.0» станет изменение традиционного представления о субъекте и субъективной стороне преступления. В отечественной юридической науке данная проблема уже была озвучена, хотя и в самом общем виде. Так, Э.В. Талапина пишет, что появление «цифровой личности», нового субъекта права наряду с человеком, закономерно обусловливает возникновение важного для юристов во-

---

[1] Курцвейл Р. Там же. С. 256.

[2] Морхат П.М. Правосубъектность искусственного интеллекта в сфере права интеллектуальной собственности: гражданско-правовые проблемы : автореф. дис. ... д-ра юрид. наук. М., 2018. С. 20–21.

проса об ответственности за действия роботов (несет ли ее собственник, пользователь или разработчик)[1]. Полагаем, что здесь следует внести определенную ясность. Вопрос об ответственности роботов, лишенных когнитивных возможностей и используемых человеком в качестве удобных помощников в быту или производстве, сам по себе несостоятелен. Речь идет о ГОСТ Р ИСО 8373-2014 «Роботы и робототехнические устройства. Термины и определения», в котором «робот» определяется как «приводной механизм, программируемый по двум и более осям, имеющий некоторую степень автономности, движущийся внутри своей рабочей среды и выполняющий задачи по предназначению».

При внешней автономности такие машины являются и останутся ничем иным, как орудием в руках человека. Следовательно, за вред, причиненный в процессе их использования, ответственность должен нести либо владелец, либо разработчик. Здесь срабатывает традиционная модель реализации ответственности в отношении субъекта, поведение которого (активное или пассивное) во взаимодействии со сложной технологической системой явилось непосредственной причиной наступления негативных последствий. Вместе с тем, «цифровая личность» и искусственный интеллект (в любой форме своего существования), несомненно, будут самостоятельными носителями интеллектуально-волевых качеств человека, то есть полноценными субъектами права. Это означает, что они же должны быть признаны и субъектами уголовной ответственности. Таким образом, теория уголовного права о субъекте преступления перейдет на принципиально новый этап развития, когда субъектом преступления будет признаваться не только физическое и (или) юридическое лицо, но и клон физического лица в цифровой форме, а также небиологический субстрат человека с искусственным интеллектом. Данный подход к проблеме обосновывает А.Г. Кибальник: «…пока технический объект любой степени сложности связан с человеческим поведением и контролируется человеком, он, по существу, является орудием причинения уголовно значимого вреда. Гипотетически ситуация может измениться, когда физический носитель искусственного интеллекта получит возможность полной «автономии» от человека. Если такой носитель приобретет свои «личные» способности осмысливать свое фактическое поведение, его возможные результаты и произ-

[1] Талапина Э.В. Право и цифровизация: новые вызовы и перспективы // Журнал российского права. – 2018. – № 2. – С. 9.

вольно руководить своей собственной активностью, в этом случае можно будет говорить о том, что «лед тронулся»[1].

Расширение представлений о субъекте закономерно породит проблему пересмотра таких категорий, как вина, мотив и цель совершения преступления. Психологическая теория вины останется приемлемой только для физических представителей Homo Sapiens. Для искусственного интеллекта и физических лиц, продолживших свою жизнь в цифровой форме, она может быть применена лишь при использовании своего рода юридической фикции, когда мы договоримся, что такие субъекты также обладают психикой, позволяющей им «осознавать, предвидеть и желать». Как справедливо отмечается в современной литературе: «…вопрос о том, могут ли действия робота рассматриваться как сознательные, переходит в серьезную философскую плоскость…Однако в случае с роботом, действия которого определяются без непосредственного участия человека, соотносятся с какой-либо целью и предполагают корректировку модели действий в соответствии с поступающими данными, в юридическом контексте потенциально допустимо говорить о некой аналогии с волевыми действиями»[2].

Здесь необходимо лишь указать, что авторы ставят вопрос о возможности признания наличия волевых процессов у киберфизической системы с так называемым «сильным» искусственным интеллектом (робота). Однако, как уже было показано выше, этот вопрос, прежде всего, необходимо будет поставить и решить в отношении лиц, продолживших свою жизнь в цифровом мире.

Следует также сделать вывод, что переход к уголовному праву нового поколения будет связан с изменением наших представлений о ключевом признаке преступления – общественно опасном деянии. С появлением новых субъектов оно потеряет свою человекоцентричную физическую интерпретацию. Можно будет говорить о деянии применительно к любым манипуляциям с компьютерной информацией, совершаемой «цифровой личностью». Эта «деятельность», в результате которой могут пострадать как члены физического, так и облачного мира, станет новой цифровой формой общественно опасного поведения субъекта преступления. Аналогичный модифицирующий процесс будет реализован и в отношении таких

---

[1] Кибальник А.Г. Как уголовное право будет реагировать на появление искусственного интеллекта // Уголовное право: стратегия развития в XXI веке: материалы XVI международной научно-практической конференции. М., 2019. С. 62–63.

[2] Архипов В.В., Наумов В.Б. О некоторых вопросах теоретических оснований развития законодательства о робототехнике: аспекты воли и правосубъектности // Закон. – 2017. – № 5 ; СПС «КонсультантПлюс».

объективных признаков, как место, обстановка, орудие и средство совершения преступления.

В завершение данного параграфа подведем его основные итоги:

1) в современных условиях имеются достаточные основания для принятия решения о снижении возраста уголовной ответственности за совершение преступлений, предусмотренных ст.ст. 272, 273 УК РФ, до 14 лет путем внесения соответствующих изменений в ч. 2 ст. 20 УК РФ;

2) встречающийся в отечественной науке уголовного права подход, связанный с расширительным толкованием подстрекательских и пособнических действий по делам о компьютерных преступлениях, противоречит принципу законности, произвольно расширяя пределы уголовной репрессии. Полагаем, что в решении проблемы установления ответственности за содействие совершению преступлений в сфере компьютерной информации при отсутствии признаков соучастия отечественному законодателю необходимо обратить более пристальное внимание на опыт других государств, которые пошли по пути выделения соответствующих специальных норм в Особенной части уголовного закона;

3) потенциал уголовно-правовых средств реагирования на организованные формы преступной деятельности в виртуальном пространстве существенным образом купирован вследствие современной редакции ч. 4 ст. 35 УК РФ. Действующее законодательное определение преступного сообщества не позволяет распространить его (с последующим применением ст. 210 УК РФ) на совершаемые структурированными организованными группами или объединениями организованных групп преступления, не относящиеся к тяжким или особо тяжким. В связи с этим представляется необходимым внести изменения в ч. 4 ст. 35 УК РФ (соответственно и в ч. 1 ст. 210 УК РФ) путем исключения указания на такую цель создания преступного сообщества, как совершение именно тяжких и особо тяжких преступлений;

4) изучение тенденций развития технологий обратного проектирования человеческого мозга и в области искусственного интеллекта позволяет обосновать вывод, что появление «цифровой личности» завершит начавшийся переход от традиционного уголовного права индустриального общества XX в. к уголовному праву цифрового мира XXI в., интегративными признаками которого является изменение традиционного представления о субъекте и субъективной стороне преступления, а равно об общественно опасном деянии, которые потеряют свою человеко-центричную физическую интерпретацию.

2.2. ДИФФЕРЕНЦИАЦИЯ ОТВЕТСТВЕННОСТИ ЗА «ЦИФРОВЫЕ ПРЕСТУПЛЕНИЯ» СРЕДСТВАМИ ИНСТИТУТА НАКАЗАНИЯ

Несмотря на значительное внимание профессионального сообщества к проблеме развития уголовного права в условиях цифровизации общества и, как следствие, преступности, вопросы эволюции института уголовного наказания остаются практически неразработанными, находясь в некотором смысле вдалеке от «столбовой дороги» многочисленных тематических форумов, конференций и семинаров[1]. Чем объясняется подобное равнодушие науки? Прежде всего, следует указать на традиционную вторичность проблемы пенализации. Поясним, что здесь вовсе нет попытки приуменьшить значимость института наказания в механизме уголовно-правовой охраны. Однако так уж сложилось, что фокус уголовно-правовой науки, как правило, сконцентрирован на решении вопроса: «а что наказывать?», нежели на вопросе: «Как наказывать?». Как справедливо отмечают по этому поводу М.М. Бабаев и Ю.Е. Пудовочкин: «…вопрос о конструировании санкций является одним из наиболее дискуссионных и, к сожалению, наименее исследованных. При этом его сложность определяется множеством параметров не только уголовно-правового, но и уголовно-политического характера»[2]. По этой причине в современной литературе можно встретить множество исследований, посвященных разработке перспективных направлений модернизации отечественного уголовного закона в свете актуальных угроз компьютерной преступности исключительно в части конструирования новых составов преступлений либо цифровой модернизации имеющихся. Другой причиной является, пожалуй, то, что ин-

[1] Такое положение представляется по меньшей мере удивительным, учитывая, что данная проблема, как заслуживающая пристального внимания отечественной науки уголовного права, выделялась учеными-криминалистами еще с середины прошлого века. М.Д. Шаргородский в своих работах неоднократно формулирует вывод, что возможности для практической юридической деятельности в области уголовного права, связанные с использованием кибернетических машин, не вызывают сомнения. Ссылаясь на работу В. Кнаппа (Кнапп В. О возможности использования кибернетических методов в праве. М., 1965), автор обосновывает необходимость использования кибернетических методов не только для познания государства и права (накопления, систематизации и анализа эмпирических данных), но и для непосредственного руководства обществом при помощи права. См.: Курс советского уголовного права (Часть Общая). Т. 1 / отв. ред. Н.А. Беляев, М.Д. Шаргородский. Л. : Изд. Ленингр. ун-та, 1968.

[2] Бабаев М.М., Пудовочкин Ю.Е. Проблемы российской уголовной политики. М., 2014. С. 166.

ститут уголовного наказания сам по себе крайне консервативен. При значительных количественно-качественных колебаниях преступности система наказаний демонстрирует неизменность, способность сохранять свою структуру, значительно реагируя лишь на переломные социально-политические преобразования, сопровождаемые принятием нового уголовного закона в целом. В связи с этим оформилось некое общее представление, что цифровизация уголовно-правовой сферы, конечно же, повлияет на состояние и содержание УК РФ, но обойдет стороной институт наказания, оставив его практически в нетронутом виде со своим уже сложившимся комплексом традиционных проблем и противоречий. И наконец, неразработанность проблемы пенализации в цифровую эпоху, на наш взгляд, объясняется также тем, что виртуальная сфера сама по себе характеризуется низким уровнем правительственного контроля. По этой причине реальная исполнимость неких новых видов уголовного наказания в интернет-пространстве видится как утопическая задача.

Полагаем, что вопрос эволюции уголовного наказания в период построения цифрового общества все же заслуживает самого пристального внимания науки и обладает значительным теоретико-прикладным потенциалом. Здесь также можно привести несколько аргументов. Во-первых, существуют обоснованные сомнения, что цифровизация не повлияет на саму модель государственно-правового принуждения, не заставит ее меняться и подстраиваться под новые условия гиперсвязанного и гиперподключенного мира. Как справедливо отмечает по данному поводу Клаус Шваб, четвертая промышленная революция сочетает разнообразные цифровые технологии, обусловливающие беспрецедентные изменения парадигм в экономике, бизнесе, социуме и в каждой отдельной личности. Она имеет фундаментальный и глобальный характер, являясь неотъемлемой частью всех стран, экономических систем и людей[1]. Во-вторых, современные технологии потенциально могут решить многие проблемы низкой эффективности традиционных мер уголовно-правового принуждения, обеспечив тем самым не только более эффективное достижение целей наказания, но и существенную экономию бюджетных расходов на пенитенциарную систему. В-третьих, учитывая, что развитие виртуальной сферы сопровождается усилением роли так называемых «цифровых прав и свобод» пользователей, закономерно возникает вопрос о перспективах уголовной репрессии в этой части. И в этом смысле появление новых видов наказания, направленных на их ограничение, выступает как законо-

[1] Шваб К. Четвертая промышленная революция: перевод с английского. М., 2018. С. 11–12.

мерный этап эволюционного развития уголовного права в цифровую эпоху.

Проблему трансформирующего влияния цифровых технологий на институт уголовного наказания можно представить двумя основными сценариями (вероятностными направлениями), которые, полагаем, заслуживают пристального внимания и проработки с целью обеспечения соответствия наказательной практики ожиданиям и вызовам информационного общества. В зависимости от глубины модифицирующего воздействия на уголовное наказание, на наш взгляд, можно выделить *умеренный* (адаптивно-линейный) сценарий эволюции наказания и *взрывной* (революционный). Умеренный сценарий цифровизации уголовного наказания предполагает поступательное внедрение информационно-коммуникационной инфраструктуры непосредственно в процесс исполнения имеющихся видов наказания в целях предупреждения десоциализации осужденных. В отечественной литературе справедливо отмечается, что уголовно-исполнительная система России не может оставаться в цифровой изоляции. Принимая во внимание, что тысячи осужденных отбывают наказание в виде лишения свободы в регионах, недоступных для посещения близкими, назрела необходимость в обеспечении их доступа к современным информационно-коммуникационным технологиям[1]. Подобные инициативы, на наш взгляд, должны получить всеобщую поддержку и по возможности скорейшую реализацию.

Адаптивно-линейный сценарий также охватывает внедрение современных информационно-коммуникационных технологий с элементами искусственного интеллекта для контроля за исполнением отдельных видов наказания. Эффективное использование таких технологий для замены процессов, которые сегодня выполняются вручную, предполагается, будет способствовать объективности надзора за осужденными, снижению коррупционных рисков, а также экономии бюджетных средств. Так, например, внедрение интеллектуальных систем в деятельность учреждений исполнения наказания позволило бы автоматизировать фиксацию допущенных осужденными нарушений установленного порядка отбывания наказания (мелкое хулиганство, хранение запрещенных предметов и др.). «Умная» программа в режиме реального времени определяла бы личность осужденного, время, место и характер допущенного нарушения, формировала на этой основе соответствующий документ и направляла для непо-

[1] Жестеров П.В. Четвертая промышленная революция: трансформация содержания уголовной репрессии // Уголовное право: стратегия развития в XXI веке : материалы XV Международной научно-практической конференции. М., 2018. С. 625–626.

средственного исполнения должностному лицу. Равным образом подобная интеллектуальная система позволила бы в автоматизированном режиме принимать решения о применении мер поощрения к осужденным, характеризующимся хорошим поведением, добросовестным отношением к труду и обучению.

Нельзя не отметить, что при очевидных преимуществах цифровизации исполнения имеющихся видов наказаний этот процесс сам по себе сопряжен с дополнительными трудностями и угрозами. Создание и обслуживание такой системы потребует не только финансовых затрат, но и соответствующего кадрового обеспечения, способного поддерживать ее работоспособность и защиту от вредоносного воздействия. При этом изначально необходимо учитывать, что наивысшая степень ответственного отношения к делу не исключит возможных отказов работы подобной системы. Так, например, согласно сообщению Министерства юстиции и безопасности Нидерландов, некорректное обновление прошивки вывело из строя сотни электронных браслетов слежения, используемых полицией Нидерландов. Обновление нарушило передачу данных с устройств на пункты управления, из-за чего сотрудники правоохранительных органов не смогли отслеживать местоположение подозреваемых, находящихся под домашним арестом, и лиц, отпущенных под залог. В качестве превентивной меры многие подследственные и осужденные, находящиеся в группе повышенного риска, были арестованы. О сбое в работе системы мониторинга были уведомлены жертвы преступлений и их родственники[1].

Значимым вопросом дифференциации ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, средствами института наказания является совершенствование системы отягчающих обстоятельств (ст. 63 УК РФ), посредством указания на специфический способ осуществления посягательства. Здесь нельзя не обратить внимание на то важное обстоятельство, что информационно-коммуникационный способ не всегда предопределяет повышение степени общественной опасности деяния. Так, распространение сведений, составляющих коммерческую тайну, с использованием обыкновенной электронной почты либо аккаунта в социальной сети мало отличается от аналогичных действий, совершаемых виновным в процессе личного общения. В отдельных случаях лицо может и сочетать способы передачи данных – передавая документы заказчику лично, отправляя ему сообщения в популярных мессенджерах и социальных сетях. Как бы то ни

[1] [Электронный ресурс] // URL: https://www.securitylab.ru/news/499060.php (дата обращения: 15.05.2019).

было, ключевым аспектом выступает не форма коммуникации – было ли информационное взаимодействие вербальным, либо реализовывалось посредством обыкновенных или электронных писем, а то обстоятельство – обеспечивала ли она анонимность злоумышленника, тем самым существенно затрудняя последующее раскрытие и расследование преступления.

В связи с этим полагаем, что в качестве отягчающего наказание обстоятельства в п. «к[1]» ст. 63 УК РФ следует закрепить не просто использование информационно-телекоммуникационных сетей, а *«совершение преступления с неправомерным сокрытием либо изменением идентификаторов оконечного оборудования пользователя информационно-коммуникационных технологий».*

Нельзя не отметить, что в отечественной теории уголовного права высказываются и гораздо более прогрессивные предложения о совершенствовании системы отягчающих обстоятельств в рамках ст. 63 УК РФ. Так, например, авторы предлагают расширить список отягчающих обстоятельств, предусмотренных ст. 63 УК РФ, указанием на использование *высокотехнологичного способа*. При этом отмечается, что в статьях главы 28 УК РФ указанный признак может быть использован как квалифицирующий[1].

Здесь хотелось бы отметить следующее. Полагаем, что авторы из правильных посылок, к сожалению, вывели ошибочное итоговое решение. Высокотехнологичный способ с юридико-технической точки зрения породит множество вопросов сугубо теоретических и, как следствие, практических проблем. Смысловая неопределенность данного признака, на наш взгляд, не выдерживает критики. С другой стороны, авторы совершенно обоснованно рассмотрели проблему (и обстоятельно осветили ее) о необходимости дифференциации уголовной ответственности в зависимости от того, использовал ли виновный при совершении преступления технологии искусственного интеллекта.

Революционный сценарий трансформации уголовного наказания в условиях цифровой реальности касается изменения самой системы наказаний. Понятно, что законодательные инициативы здесь всецело зависят от программно-технической возможности обеспечить исполнение подобных наказаний, которая на современном этапе, думается, отсутствует. Вместе с тем, прикладное значение науки во многом состоит в том, чтобы,

---

[1] Букалерова Л.А., Уторова Т.Н., Сизов Д.О. К вопросу о значении искусственного интеллекта в уголовном праве // Пенитенциарная наука. – 2020. – Т. 14. – № 1. – С. 74.

выявив и оценив закономерности развития и функционирования права и государственно-правовой сферы жизни общества в условиях цифровой реальности, уже сейчас спрогнозировать состояние интересующих правовых институтов в будущем.

Следует отметить, что, осознавая необходимость ограничения цифрового присутствия лица, признанного виновным в совершении преступления с использованием информационно-коммуникационных технологий, суды в рамках действующей системы наказаний пытаются решить данную проблему путем применения положений ст. 47 УК РФ. При этом анализ конкретных решений не позволяет утверждать о единообразном подходе. Так, в судебной практике можно найти примеры назначения в качестве дополнительного наказания: 1) лишения права заниматься деятельностью, сопряженной с использованием информационно-телекоммуникационной сети «Интернет»[1]; 2) лишения права пользования информационно-телекоммуникационной сетью «Интернет»[2]; 3) лишения права заниматься деятельностью, связанной с администрированием сайтов с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет»[3]; 4) лишение права заниматься деятельностью, связанной с размещением обращений и иных материалов в информационно-телекоммуникационных сетях общего пользования, включая сеть «Интернет»[4].

Из приведенных выше формулировок наглядно явствует, что суды, применяя один и тот же вид наказания, устанавливают для осужденного принципиально разные по характеру репрессивного воздействия ограничения: от запрета распространения информации в общедоступных сетях до запрета на само использование таких сетей. Нетрудно представить, что последний наиболее строгий подход существенным образом умаляет общую правоспособность лица: начиная от возможности приобретения необходимых товаров онлайн и заканчивая доступом к сервисам электронного правительства. В этом нет ничего удивительного, учитывая то обсто-

---

[1] Приговор Старооскольского городского суда Белгородской области от 16 октября 2017 г. по делу № 1-311/2017.

[2] Приговор Хасавюртовского районного суда Республики Дагестан от 22 ноября 2017 г. по делу № 1-173/2017.

[3] См.: Апелляционное определение Судебной коллегии по делам военнослужащих Верховного Суда Российской Федерации от 15 марта 2018 г. № 201-АПУ18-8; Приговор Волжского районного суда Самарской области от 12 ноября 2018 г. по делу № 1-220/2018.

[4] Апелляционное определение Судебной коллегии по делам военнослужащих Верховного Суда Российской Федерации от 28 февраля 2019 г. № 208-АПУ19-1.

ятельство, что суды, эксплуатируя интерпретационную емкость ст. 47 УК РФ, изначально принятой для ограничения активности лица в физическом мире, пытаются механически переложить данную норму на виртуальную сферу. Полагаем, что в условиях интенсивной цифровизации жизнедеятельности и, как следствие, преступности, отечественная система наказаний должна быть дополнена специальным наказанием, заключающимся в *ограничении права на цифровое присутствие*. Содержание такого ограничения, а равно его пределы с учетом тяжести совершенного лицом преступления должны быть четко определены непосредственно в уголовном законе.

Следует отметить, что проблема применения в качестве уголовного наказания ограничения на использование сети «Интернет» уже на протяжении длительного времени обсуждается в зарубежной литературе[1]. При этом в практике американских судов можно найти позицию, согласно которой общий запрет на использование компьютерной техники и (или) сети «Интернет» в современных условиях является неуместным ввиду значительной зависимости повседневной жизни человека от объектов информационно-коммуникационной инфраструктуры. Так, в деле «Соединенные Штаты против Холма» (2003 г.) судья Дайан Вуд специально отметила, что полный запрет на использование сети «Интернет» «сделает жизнь любого человека исключительно сложной, учитывая, что сегодня правительство настоятельно рекомендует налогоплательщикам подавать свои декларации в электронном виде, все больше и больше коммерции осуществляется в «Интернете», а огромные объемы правительственной информации передаются через веб-сайты»[2]. В связи с этим считается, что подобное ограничение может применяться в качестве уголовного наказания, но не может быть абсолютным, и должно иметь строго предметный характер.

С учетом изложенного полагаем, что уголовно-правовая норма о новом виде наказания, связанном с ограничением права лица на осуществление деятельности в информационно-коммуникационной сети «Интернет», может быть представлена в следующей редакции:

«Статья 47[1]. Ограничение права на цифровое присутствие

---

[1] См., например: Smith R. Criminal forfeiture and restriction-of-use orders in sentencing high tech offenders // Trends & issues in crime and criminal justice. – 2004. – № 286. Canberra: Australian Institute of Criminology / [Электронный ресурс] // URL: https://aic.gov.au/publications/tandi/ tandi286 (дата обращения: 12.02.2019).

[2] Пример приведен по: Smith R. Criminal forfeiture and restriction-of-use orders in sentencing high tech offenders // Trends & issues in crime and criminal justice 2004. №. 286. Canberra: Australian Institute of Criminology / [Электронный ресурс] // URL: https://aic.gov.au/publications/tandi/tandi286 (дата обращения: 12.02.2019).

1. Ограничение права на цифровое присутствие состоит в запрещении использования отдельных информационных ресурсов, а также в запрещении искать, получать, передавать, производить и распространять информацию в сети «Интернет».

2. Указанные в части первой настоящего Кодекса ограничения не могут затрагивать право лица на свободный доступ к информационным ресурсам органов власти, в том числе деятельность в сети «Интернет», связанную с получением государственных или муниципальных услуг (исполнением обязанностей) в электронной форме.

3. Ограничение права на цифровое присутствие устанавливается на срок от одного года до пяти лет в качестве основного вида наказания и на срок от шести месяцев до трех лет в качестве дополнительного вида наказания. В случаях, специально предусмотренных соответствующими статьями Особенной части настоящего Кодекса, ограничение права на цифровое присутствие в информационно-коммуникационной сети «Интернет» устанавливается на срок до двадцати лет в качестве дополнительного вида наказания.

4. Ограничение права на цифровое присутствие может назначаться в качестве дополнительного вида наказания и в случаях, когда оно не предусмотрено соответствующей статьей Особенной части настоящего Кодекса в качестве наказания за соответствующее преступление, если с учетом характера и степени общественной опасности совершенного преступления и личности виновного суд признает невозможным сохранение за ним права использовать отдельные информационные ресурсы, а также искать, получать, передавать, производить и распространять информацию в сети «Интернет».

5. В случае назначения этого вида наказания в качестве дополнительного к обязательным работам, исправительным работам, ограничению свободы, а также при условном осуждении его срок исчисляется с момента вступления приговора суда в законную силу. В случае назначения ограничения права на цифровое присутствие в качестве дополнительного вида наказания к аресту, содержанию в дисциплинарной воинской части, принудительным работам, лишению свободы оно распространяется на все время отбывания указанных основных видов наказаний, но при этом его срок исчисляется с момента их отбытия».

Значительный интерес представляет прогнозирование эволюции уголовного наказания в аспекте развития и внедрения технологий «больших данных». Желаем мы того или нет, но цифровой мир характеризуется беспрецедентным усилением контроля над отдельной личностью. Судя по

всему, этот процесс следует принять как неизбежность. Еще несколько лет назад мы не могли себе представить, что обеспечение безопасности дорожного движения в основном будет обеспечиваться автоматизированными системами фиксации нарушений, а значительное количество преступлений будет раскрываться благодаря «цифровым следам», оставленным злоумышленниками. Сервисы электронного правительства, кредитно-финансовый сектор, интернет-провайдеры, операторы мобильной связи, социальные сети и многочисленные мобильные приложения ежедневно собирают сведения об отдельном пользователе, формируя тем самым не только образ его цифрового присутствия, но и некое досье на лицо в реальном мире (законопослушность, потребительское поведение, круг общения, интересы и др.). Логично, что с течением времени особую значимость приобрел вопрос об использовании соответствующих данных в процессе государственного контроля и управления. Наиболее известным примером использования технологий анализа «больших данных» в осуществлении публично-властного контроля является китайская система социального кредита.

В 2014 году правительство Китая обнародовало документ «О планировании строительства системы социального кредита (2014–2020)». Главной целью системы является «построение гармоничного социалистического общества»[1]. Алгоритм системы предполагает, что каждому гражданину Китая присваивается изначальный (базовый) рейтинг общественной благонадежности. Отсутствие нарушений закона, дисциплинированность при исполнении финансовых обязательств (при погашении кредитов, уплате налогов, алиментов, коммунальных платежей и др.), благотворительность и иная общественно полезная деятельность способствуют росту индивидуального рейтинга гражданина, что, в свою очередь, предоставляет ему преимущества в получении образования и государственных услуг, учитывается при трудоустройстве, кредитовании и даже при бронировании билетов на общественном транспорте. Напротив, снижение рейтинга влечет за собой многочисленные правоограничения: запрет на работу на государственной службе, а также в пищевой и фармацевтической промышленности, отказ в получении ряда государственных услуг и социального обеспечения, невозможность получения услуг кредитных организаций, отказ в бронировании авиабилетов, мест в определенных гостиницах и ресторанах.

---

[1] [Электронный ресурс] // URL: https://chinacopyrightandmedia.wordpress.com/2014/06/14/ planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/ (дата обращения: 06.02.2019).

Китайский эксперимент был воспринят неоднозначно. Данный проект называют «цифровой диктатурой» XXI в., а саму модель селекции граждан на благонадежных и «с низкой степенью надежности» сравнивают с фашизмом. Полагаем, что отношение к использованию технологий «больших данных» в осуществлении государственного контроля и управления может быть более сдержанным. Пока такой рейтинг основывается на оценке внешнего (социального) поведения лица и не посягает на неприкосновенность его частной жизни, сложно утверждать об умалении фундаментальных международно-правовых гарантий правового статуса личности. С другой стороны, «большие данные» сами по себе не имеют тоталитарного подтекста, а являются одним из проявлений гиперподключенного цифрового общества, членами которого мы уже все являемся. Государственные структуры так или иначе не смогут (и вряд ли должны) игнорировать их потенциал в решении актуальных задач социального контроля.

Если допустить (а тому, как видим, есть веские основания), что в ближайшем будущем цифровой рейтинг общественной благонадежности найдет свое воплощение в России, перспективным видится дополнение уголовного закона новым видом наказания – *снижение рейтинга общественной благонадежности.* Очевидно, что такая форма уголовной репрессии имеет много общего с такими традиционными видами уголовного наказания, как лишение права занимать определенные должности и заниматься определенной деятельностью, а также ограничение свободы. Вместе с тем, если данные виды наказания имеют срочный характер и предполагают установление строго конкретных ограничений в отношении осужденного, понижение лица в рейтинге общественной благонадежности фактически представляет собой одномоментное общее ограничение субъекта в правоспособности. Учитывая всеобъемлющий характер такого ограничения, полагаем, что понижение лица в рейтинге общественной благонадежности (например, на одну, две, три категории) будет представлять собой более строгое наказание, чем лишение права занимать определенные должности и заниматься определенной деятельностью, а также ограничение свободы.

Анализ зарубежной литературы позволяет сделать вывод, что научное сообщество активно прорабатывает философские, этические и правовые проблемы куда более фантастических сценариев эволюции наказания. Так, например, Ребекка Роуч останавливается на возможности применения в качестве уголовного наказания принудительного медицинского вмешательства с целью удаления имплантированного в организм осужденного чипа, выполняющего функции современного мобильного телефо-

на. Стремительное развитие технологий в данном направлении действительно не позволяет иронично отнестись к такой постановке проблемы. Так, подкожные чипы, которые можно использовать для оплаты покупок, в качестве пропуска или проездного, массово начали вживлять гражданам Швеции. Более трех с половиной тысяч человек уже выразили желание стать обладателями таких «устройств», а многие уже успешно ими пользуются[1]. Рассматривая этот процесс как естественный ход эволюции человека, полагаем, что принудительное извлечение чипа будет неоправданным насилием над личностью. С другой стороны, с точки зрения развития института уголовного наказания, значительным потенциалом обладает использование таких технологий в установлении контроля над поведением осужденного.

Ребекка Роуч, опираясь на работы известных футурологов в области цифрового воспроизведения и управления разумом человека (преимущественно на исследования Ника Бострома), также анализирует проблему применения подобных технологий в аспекте исправления осужденных. Автор пишет, что при доступности технологии и необходимой вычислительной мощности можно будет ускорить работу загруженного на компьютер сознания человека. Таким образом, появится возможность менять саму проекцию времени – годы в виртуальном пространстве можно будет уравнять часам в реальном (физическом) мире. Загрузка индивидуального сознания преступника и его ускорение позволят исполнить наказание в несколько десятков лет за считанные часы, обеспечив при этом субъективное переживание виновным всех тягот и лишений нахождения в исправительном учреждении. В результате между восходом и закатом самые опасные преступники могут вернуться с опытом отбытия полноценного наказания либо в реальный мир (если технология позволяет их переход обратно в биологический субстрат), либо в смоделированный компьютером мир (как новую форму жизни)[2].

Конечно же, в современных условиях ускоренное ментальное отбывание квазилишения свободы можно причислить к неактуальным или даже надуманным проблемам. Вместе с тем, в таком подходе, на наш взгляд,

---

[1] Жителям Швеции начали массово вживлять чипы под кожу / [Электронный ресурс] // URL: https://www.mk.ru/science/2018/06/26/zhitelyam-shvecii-nachali-massovo-vzhivlyat-chipy-pod-kozhu.html (дата обращения: 18.01.2019).

[2] Roache R. How Technology Could Make «Life in Prison» a Much Longer, Tougher Sentence // Slate. 2013 // [Электронный ресурс] // URL: https://slate.com/technology/2013/08/daniel-pelka-ariel-castro-how-life-extending-technology-could-make-a-life-sentence-tougher-and-longer.html (дата обращения: 20.01.2019).

есть неоправданное пренебрежение объективно развивающимися процессами. Радикальные изменения технологий происходят на наших глазах. Вчерашние фантастические проекты отдельных ученых сегодня становятся реальным предметом работы инновационных компаний, а уже завтра обыденным явлением, без которого становится невозможной жизнь отдельного человека. Так было с персональными компьютерами и «Интернетом», и то же самое может произойти с технологиями цифрового воспроизведения и управления разумом человека.

ГЛАВА 3. ДИФФЕРЕНЦИАЦИЯ ОТВЕТСТВЕННОСТИ ЗА «ЦИФРОВЫЕ ПРЕСТУПЛЕНИЯ» СРЕДСТВАМИ ОСОБЕННОЙ ЧАСТИ УГОЛОВНОГО ПРАВА

3.1. ДИФФЕРЕНЦИАЦИЯ ОТВЕТСТВЕННОСТИ ЗА КОМПЬЮТЕРИЗИРОВАННЫЕ ПРЕСТУПЛЕНИЯ

Фокусируя внимание на влиянии цифровизации на сферу уголовно-правового регулирования, резонно задаться вопросом: как данный процесс повлияет или должен повлиять на состояние Особенной части УК РФ в целом? Следует сразу оговориться, что приспосабливание Особенной части УК РФ к цифровизации преступности нельзя воспринимать не только как задачу, реально достижимую в ближайшей перспективе, но и вообще как некий возможный результат, конечную цель. Неопределенность и перманентность информационного преображения общественной жизни требуют совершенно иного подхода к проблеме – пониманию цифровизации отечественного уголовного законодательства как процесса. В связи с этим следует согласиться с мнением С.А. Белоусова, что «достичь в системе законодательства абсолютного баланса всех его составных частей и внутрисистемных связей, а также полного ее соответствия запросам правовой системы и общества в целом не представляется возможным. Баланс в законодательстве может быть лишь относительным»[1].

Отмечая значимость упреждающего развития отечественного уголовного права, И.Я. Козаченко и Е.Б. Козаченко небезосновательно констатировали, что «…отечественный уголовный закон хранит достойное удивления спокойствие. Создается впечатление, что он боится запутаться в безжалостной «всемирной паутине». А отечественный законодатель делает вид, что в этой сфере ничего неординарного нет. Не опоздать бы!»[2].

Н.Ш. Козаев отмечает, что попытки законодателя выделить отдельные составы, где в качестве квалифицирующего обстоятельства выступает использование электронной (компьютерной) информации, следует оценить как эпизодические и бессистемные[3]. Согласимся с данным утверждением. Вместе с тем, в защиту законодателя следует указать, что доктрина

---

[1] Белоусов С.А. Законодательный дисбаланс: доктрина, теория, практика : автореф. дис. ... д-ра юрид. наук. Саратов, 2005. С. 25.

[2] Козаченко И.Я., Козаченко Е.Б. Инновационное безволие уголовного закона // Уголовное право: истоки, реалии, переход к устойчивому развитию: материалы Российского конгресса уголовного права (26–27 мая 2011 г.). М., 2011. С. 444.

[3] Козаев Н.Ш. Современные технологии и проблемы уголовного права (анализ зарубежного и российского законодательства). М., 2015. С. 193.

уголовного права, пожалуй, так и не смогла решить проблему разработки модели системного обновления отечественного уголовного законодательства в условиях информационного общества, не сформулировала общих правил и не предложила четких критериев его осуществления. Во многом именно по этой причине соответствующие решения законодателя воспринимаются специалистами не как последовательный курс по «оцифровке» отечественного уголовного законодательства, а как спонтанный ответ на актуальные потребности правоприменения, реакция на так называемый «криминализационный повод».

Более того, сама наука не лишена указанной эклектичности. В литературе можно обнаружить довольно локальные (фрагментарные) решения по более «точному» формулированию отдельных уголовно-правовых норм. Так, например, Д.А. Ковлагина предлагает изменить редакцию ст. 205 УК РФ путем включения части 1.1 следующего содержания: «Совершение взрыва, поджога или иных устрашающих население действий, сопряженных с посягательством на автоматизированные системы критически важных объектов и (или) потенциально опасных объектов государства, создающих опасность гибели человека, причинения значительного имущественного ущерба, аварийной ситуации, техногенной аварии либо иных тяжких последствий, с помощью информационных технологий»[1].

В свою очередь И.М. Рассолов считает, что необходимо не просто уточнить основной состав, а установить повышенную уголовную ответственность за совершение террористического акта, сопряженного с несанкционированным доступом к компьютерным системам или информационно-коммуникационным сетям, осуществляющим автоматизированное управление опасными технологическими производствами и предприятиями жизнеобеспечения, с целью нарушения их функционирования и создания аварийной ситуации и угрозы технической катастрофы[2].

Приведенные предложения по казуальному уточнению совершения преступления специфическим способом – путем использования информационно-коммуникационных технологий – как представляется, не учитывают интерпретационного потенциала действующих статей Особенной части УК РФ. Следует с удовлетворением констатировать, что отечественный уголовный закон в большей части свободен от казуистики и оперирует конструкциями, достаточно широкими для того, чтобы охватить всю

---

[1] Ковлагина Д.А. Информационный терроризм: понятие, уголовно-правовые и иные меры противодействия : монография. М., 2017. С. 106.

[2] Рассолов И.М. Киберпреступность: понятие, основные черты, формы проявления // Юридический мир. Общероссийский научно-практический правовой журнал. – 2008. – № 2 (134) // СПС «КонсультантПлюс».

совокупность конкретных форм общественно опасного поведения личности, имеющих между собою общие черты. Подобную абстрактность следует оценить положительно, поскольку, как справедливо писал М.Д. Шаргородский, излишние подробности в тексте закона усложняют пользование им и с точки зрения технической делают закон неудовлетворительным[1]. При этом С.С. Алексеев абстрактный прием изложения нормативного материала оценивал как признак «высокого уровня юридической культуры и развития науки»[2].

В связи с этим, дискуссионным представляется категоричное утверждение М.А. Ефремовой, что «…такое явление как кибертерроризм сегодня нельзя квалифицировать по ст. 205 УК РФ»[3]. Непонятно, почему диспозиция уголовно-правовой нормы об ответственности за террористический акт, под которым, как известно, понимается совершение в том числе *иных действий,* устрашающих население и создающих опасность гибели человека, причинения значительного имущественного ущерба либо наступления иных тяжких последствий, не может быть применена к компьютерным атакам на информационные объекты общественного значения, если они совершались в целях дестабилизации деятельности органов власти или международных организаций либо воздействия на принятие ими решений.

Полагаем, что приспосабливание Особенной части УК РФ к условиям информационного общества не должно быть связано с конструированием многочисленных «виртуальных копий», «цифровых двойников» традиционных уголовно-правовых запретов. Такая модернизация отечественного уголовного законодательства неминуемо приведет к избыточному дублированию его положений, выражающемуся в наличии значительного количества норм, конкурирующих друг с другом исключительно на стыке проблемы разграничения виртуального и реального в праве.

Абстрактный метод построения уголовного закона лежит в основе практически единодушного мнения специалистов относительно возможности квалификации причинения вреда компьютерному оборудованию путем использования вредоносной программы как уничтожения или повреждения чужого имущества по ст. 167 УК РФ. Данное суждение справедливо распространить и на составы приведения в негодность объектов жизнеобеспечения (ст. 215^2 УК РФ), приведения в негодность нефтепро-

---

[1] Шаргородский М.Д. Техника и терминология уголовного закона // Советское государство и право. – 1948. – № 1. – С. 60.

[2] Алексеев С.С. Проблемы теории права. Т. 2. С. 149.

[3] Ефремова М.А. Уголовно-правовая охрана информационной безопасности : дис. ... д-ра юрид. наук. М., 2017. С. 326.

водов, нефтепродуктопроводов и газопроводов (ст. 215^3 УК РФ), уничтожения или повреждения объектов культурного наследия (памятников истории и культуры) народов Российской Федерации, выявленных объектов культурного наследия, природных комплексов, объектов, взятых под охрану государства, или культурных ценностей (ст. 243 УК РФ), приведения в негодность транспортных средств или путей сообщения (ст. 267 УК РФ) и др.

Дистанционное отключение системы жизнеобеспечения конкретного пациента, совершенное посредством неправомерного вмешательства в функционирование программного обеспечения медицинского оборудования и с учетом действующей редакции ст. 105 УК РФ, может быть квалифицировано как убийство. Равным образом это касается всех составов умышленного причинения вреда здоровью.

Развитие систем беспилотного управления транспортными средствами с высокой долей вероятности обусловит возможность неправомерного завладения автомобилем, совершенного путем вмешательства в работу его бортовых систем управления. Вместе с тем, уже сейчас можно сделать вывод, что редакция ст. 166 УК РФ вполне применима и к таким случаям.

Демонстрацию конкретных примеров можно было бы продолжить и дальше, однако в этом мало практического смысла. Общая идея предстает достаточно ясно – феномен компьютеризации преступности по большому счету охватывается действующим уголовным законодательством России. Следовательно, в конструировании специальных составов «киберубийства», «киберугона», «кибертерроризма» и т.п. попросту нет необходимости.

Довольно распространенный тезис о том, что толкование права само по себе не может создавать нормативную новизну применительно к проблеме противодействия компьютеризированной преступности, объективно вызывает научную дискуссию. Как метко отмечает Ж. Карбонье, метод эволюционного толкования всегда имел один и тот же смысл: толкователь должен адаптировать закон к социальным изменениям[1]. Примерно в этом же аспекте Ю.А. Гаврилова обосновывает, что толкование может выявлять ценностную и мировоззренческую новизну, в результате чего формулируется итоговая смысловая новизна соответствующего правового предписания[2]. Полагаем, что в настоящее время отечественный механизм уго-

[1] Карбонье Ж. Юридическая социология. М., 1986. С. 311.

[2] Гаврилова Ю.А. Правоприменительная практика: особенности смыслообразования // Журнал российского права. – 2018. – № 5. – С. 54.

ловно-правовой охраны находится в процессе перехода от типичного правоприменения, связанного с выявлением «основного» смысла буквы уголовного закона, заложенного законодателем изначально, к нетипичному (цифровому), при котором правоприменитель фактически создает новое смысловое содержание уголовно-правового запрета, подчиненного потребностям динамично развивающегося информационного общества.

Ключевую роль в этом модифицирующем смыслообразовании отечественного уголовного права должна сыграть разъяснительная деятельность Верховного Суда Российской Федерации. Как справедливо пишет К.В. Ображиев: «…для постановлений Пленума Верховного Суда Российской Федерации разрешение неопределенности и конкретизация уголовного закона являются основной и регулятивной функцией. Однако содержание указанных постановлений не ограничивается интерпретацией – практически в каждом из них можно обнаружить предписания, не выводимые из уголовного закона, которые разрешают сложные уголовно-правовые вопросы, не имеющие однозначного законодательного решения, тем самым достигается компенсация имеющихся пробелов в УК РФ»[1]. В данном аспекте насущно необходимым представляется активизация Пленумом работы по разработке постановления о судебной практике по делам о преступлениях в сфере компьютерной информации, в рамках которого можно было бы разрешить не только дискуссионные вопросы применения норм, предусмотренных гл. 28 УК РФ, но и целый ряд смежных проблем, возникающих при квалификации посягательств на конституционные права граждан, отношения собственности, общественную безопасность и др.

Вместе с тем, интерпретационные возможности приспосабливания отечественного уголовного законодательства к проявлениям компьютеризированной преступности небезграничны. Недопустимым будет такое толкование, результат которого объективно выходит за пределы системного смысла закона, восполняя так называемый «системный семантический пробел». В этом случае, как справедливо отмечает В.Ф. Щепельков, речь идет уже об аналогии закона или об аналогии права, которые в соответствии со ст. 3 УК РФ (принцип законности Уголовного кодекса) запрещены[2]. Под аналогией в праве традиционно понимают восполнение неполноты системы правовых предписаний путем применения уже уста-

[1] Ображиев К.В. Система формальных (юридических) источников российского уголовного права: монография. М., 2015. С. 280–282.

[2] Щепельков В.Ф. Уголовный закон как формально-логическая система : дис. ... д-ра юрид. наук. СПб., 2003. С. 93.

новленной нормы к деяниям, не содержащим ее признаков[1]. В стремлении адаптировать классическое уголовно-правовое установление к компьютеризированной форме совершения того или иного посягательства нельзя переступать эту грань, недопустимо произвольно толковать понятие или юридическую конструкцию, которые по своей природе не могут быть применимы к виртуальной сфере. Так, например, дискуссионым представляется имеющееся в отечественной доктрине предложение о приравнивании хакерских атак к захвату органов власти. Авторы в обоснование данной позиции ссылаются на то, что «в настоящее время в рамках действующего УК РФ для группы лиц, взламывающей сайты, наказание предусматривается до пяти лет лишения свободы, а статья о захвате органов государственной власти предусматривает лишение свободы на срок до 20 лет. Между тем взлом сайтов государственных органов по своей сути может рассматриваться как их захват, так как доступ к ним закрыт»[2]. Здесь, на наш взгляд, в противоречие системному смыслу закона необоснованного отождествляются разные по содержанию деяния – физический захват зданий и сооружений государственных органов и блокирование деятельности их информационных ресурсов.

Подобные проблемы интерпретационного характера рельефно вырисовываются при рассмотрении ст. 215[4] УК РФ, предусматривающей ответственность за незаконное проникновение на охраняемый объект. В современной юридической литературе проникновение раскрывается как тайное или открытое вторжение. При этом подчеркивается, что проникновение может быть осуществлено и тогда, когда виновный незаконно использует какие-либо предметы без вхождения в соответствующее помещение[3]. В связи с этим закономерно возникает вопрос: следует ли квалифицировать как незаконное проникновение вмешательство лица в систему видеонаблюдения такого объекта, совершенное дистанционно? Иными словами, применима ли данная норма к случаям не физического, а «виртуального вторжения» на охраняемый объект? Полагаем, что ответ на дан-

---

[1] При применении закона по аналогии нет места толкованию в собственном смысле слова, поскольку отсутствует объект толкования. При этом уясняются нормы, при помощи которых восполняется неполнота. См.: Пиголкин А.С. Толкование норм права и правотворчество: проблемы соотношения // Закон: создание и толкование. М., 1998. С. 70.

[2] Криминализация и декриминализация как формы преобразования уголовного законодательства : монография / [И.С. Власов и др.]; отв. ред. В.П. Кашепов. М. : ИЗиСП, КОНТРАКТ, 2018 // СПС «КонсультантПлюс».

[3] Уголовное право России : учебник в 2 т. Т. 2: Особенная часть / под ред. д-ра юрид. наук, проф. Н.Г. Кадникова. М., 2018. С. 412.

ный вопрос может быть положительным. Вместе с тем, вполне очевидны те сложности, с которыми может быть связана такая интерпретация термина «проникновение».

Еще бóльшие сложности возникают при оценке посягательств на общественные отношения, складывающиеся в связи с реализацией прав человека в виртуальном пространстве, либо связанных с использованием нетипичных объектов (цифровых вещей, криптовалют и др.), а равно сопряженных с погружением в виртуальное пространство субъектов государственного управления. Так, например, возникает вопрос о возможности применения уголовно-правовой нормы об ответственности за клевету (ст. 128[1] УК РФ) к случаям распространения заведомо порочащих сведений о так называемой «цифровой личности», то есть по-сути о гипертекстовых компонентах сетевого облика индивида, формируемого им в рамках онлайн-среды с целью самопрезентации. Понятно, что говорить о наличии чести и достоинства у «цифровой личности» можно весьма условно, подразумевая их только у реального носителя подобных качеств – человека-владельца соответствующего «никнейма». Распространяя заведомо ложные и порочащие сведения о «цифровой личности», злоумышленник так или иначе направляет указанные действия против конкретного пользователя того или иного интернет-ресурса, то есть совершает уголовно наказуемую клевету. Однако проблема приобретает совершенно другое измерение, когда «цифровая личность» имеет искусственное происхождение и принадлежит одновременно сразу нескольким пользователям (например, создавалась и используется в социальной сети для коммерческих целей). Полагаем, что при подобных обстоятельствах клеветнические действия виновного не могут причинить вред общественным отношениям, обеспечивающим защиту чести и достоинства человека. С точки зрения общей теории уголовного права, такие действия правильно квалифицировать как покушение на негодный объект, то есть по ч. 3 ст. 30 ч. 2 ст. 128[1] УК РФ.

Н.А. Поветкина справедливо отмечает, что «сфера публичных финансов успешно проходит всестороннюю «оцифровку», и это, в свою очередь, позволяет говорить о федеральном бюджете как о «цифровом бюджете»[1]. Данное мнение автора основывается на активном внедрении и использовании различных государственных информационных систем: государственная интегрированная информационная система управления обще-

[1] Поветкина Н.А. Правовая форма интеграции информационных систем и информационных технологий в сферу публичных финансов // Журнал российского права. – 2018. – № 5. – С. 111.

ственными финансами «Электронный бюджет», государственная информационная система о государственных и муниципальных платежах (ГИС ГМП), информационно-аналитическая система Федерального казначейства, государственная автоматизированная информационная система «Управление» и др.

Неправомерное вмешательство в процесс функционирования указанных государственных информационных систем, конечно же, будет затрагивать не только отношения, связанные с обеспечением информационной безопасности, но, прежде всего, отношения, складывающиеся в процессе деятельности органов государственной власти. В связи с этим полагаем, что одним из значимых направлений цифровизации Особенной части УК РФ будет выделение специальных норм, которые ввиду специфического содержания основного непосредственного объекта не встраиваются в систему гл. 28 УК РФ.

В отдельных случаях обеспечение задачи эффективного противодействия компьютерной и компьютеризированной преступности может быть достигнуто только путем конкретизации диспозиций статей Особенной части УК РФ. Так, следует в целом поддержать позицию М.А. Простосердова, который обосновывает необходимость дополнения основного состава вымогательства (ст. 163 УК РФ) и принуждения к совершению сделки или отказу от ее совершения (ст. 179 УК РФ) таким признаком, как совершение указанных преступлений: «под угрозой удаления, блокирования либо модификации компьютерной информации, а равно под угрозой иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, которое может причинить существенный вред правам или законным интересам потерпевшего или его близких»[1].

Следует лишь указать, что представляется уязвимым решение автора о включении признака создания угрозы причинения существенного вреда правам и законным интересам потерпевшего. Такая оговорка мало что проясняет в разрешении проблемы отграничения таких требований от малозначительного деяния. С другой стороны, предлагаемая М.А. Простосердовым конструкция создает дополнительные трудности для правоприменителя, которому в каждом случае необходимо будет установить и «объяснить» суду, что угроза имела не формальный характер, а была сопряжена с возможностью причинения именно существенного вреда правам и законным интересам потерпевшего.

---

[1] Простосердов М.А. Экономические преступления, совершаемые в киберпространстве. М., 2017. С. 143.

Применительно к теме проводимого исследования решение о «цифровой конкретизации» составов вымогательства и принуждения к совершению сделки или отказу от ее совершения, конечно же, выглядит полумерой. Такое уточнение должно затронуть по крайней мере и основной состав понуждения к действиям сексуального характера (ст. 133 УК РФ).

З.И. Хисамова в своей работе делает вывод, что ст. 187 УК РФ не применима к криптовалюте, так как она представляет собой аналог денежной валюты, иными словами, «денежный суррогат», а не устройство, предназначенное для неправомерного приема, выдачи и перевода денежных средств. В связи с этим автор обосновывает необходимость дополнения УК РФ ст. 187[1] «Оборот денежных суррогатов»[1]. Данное предложение, на наш взгляд, имеет под собой существенные основания, однако только при условии достижения определенности относительно правового статуса криптовалюты в России в целом.

Отечественный механизм уголовно-правовой охраны объективно «не срабатывает» во многих других случаях, связанных с посягательствами на отношения, опосредуемые современными информационно-коммуникационными технологиями. Так, например, в соответствии с УК РФ можно квалифицировать как преступление неправомерный доступ к личной странице другого человека в социальной сети, однако весьма затруднительно дать правовую оценку созданию и использованию подобной страницы от имени другого человека без его согласия. Вместе с тем, такие действия могут причинить существенный вред правам и законным интересам личности, повлиять на принятие решений по трудоустройству, продвижению по службе и т.п.

Равным образом положения действующего уголовного законодательства не дают внятного ответа на вопрос о квалификации использования технологий реконструкции лица другого человека в режиме реального времени (технологий замены лиц). Вместе с тем, такое программное обеспечение позволяет, попросту выражаясь, «похищать» лицо другого человека, использовать его при изготовлении тех или иных материалов (условно компрометирующих или даже порнографических).

Замедленность цифрового обновления уголовно-правовых норм об ответственности за традиционные преступления, на наш взгляд, обусловлена объективными факторами и в целом связана с общими закономерностями развития права. В отечественной доктрине уголовного права обос-

[1] Хисамова З.И. Уголовная ответственность за преступления, совершаемые в финансовой сфере с использованием информационно-телекоммуникационных технологий. М., 2017. С. 124–125.

новано, что закреплять в законе единичные обстоятельства в качестве признака состава, даже в случаях, если они существенно влияют на общественную опасность, не имеет смысла[1]. Э.Ф. Побегайло, рассматривая проблемы дифференциации уголовной ответственности за тяжкие насильственные преступления, справедливо отмечает, что «…в процессе дифференциации законодатель учитывает *типичные* (выделено мной – *Е.Р.*) специфические признаки отдельных видов общественно опасных деяний и существенное изменение такими признаками уровня общественной опасности таких деяний»[2].

На сравнительную распространенность обстоятельства указывает А.И. Свинкин[3].

Т.А. Лесниевски-Костарева также пишет, что «квалифицирующими (привилегирующими) признаками следует считать указанные в законе *характерные для некоторых преступлений* (выделено мной – *Е. Р.*) соответствующего вида существенные обстоятельства, отражающие типовую значительно измененную в сравнении с основным составом преступления степень общественной опасности содеянного и личности виновного и влияющие на законодательную оценку (квалификацию) содеянного и меру ответственности»[4].

При этом А.Н. Трайнин уже напрямую указывает, что нет смысла закреплять в законе в качестве признака преступления единичные обстоятельства даже в случаях, если они существенно влияют на общественную опасность деяния[5]. Таким образом, для признания использования информационно-коммуникационных технологий в качестве квалифицирующего признака конкретного состава преступления необходимо учитывать степень распространенности этого способа в реальности.

---

[1] См., например: Рогова Е.В. Правила построения квалифицирующих и привилегирующих признаков состава преступления // Пробелы в российском законодательстве. – 2013. – № 5. – С. 172–178; Трайнин А.Н. Состав преступления по советскому уголовному праву. М., 1951. С. 88 и др.

[2] Побегайло Э.Ф. Проблемы дифференциации уголовной ответственности за тяжкие насильственные преступления // Совершенствование правовых мер борьбы с преступностью. Владивосток, 1986. С. 24–25.

[3] Свинкин А.И. Оптимальное конструирование квалифицированных составов по признакам повторности и рецидива // Проблемы эффективности уголовного закона. Свердловск, 1975. С. 35–37.

[4] Лесниевски-Костарева Т.А. Дифференциация уголовной ответственности : дис. ... д-ра юрид. наук. М., 1999. С. 17.

[5] Трайнин А.Н. Состав преступления по советскому уголовному праву. М., 1951. С. 88.

В этой связи следует поставить под сомнение позицию О.М. Сафонова, который пишет: «…сам процесс усиления ответственности за преступления, сопряженные с использованием компьютерных технологий, учитывая, что многие преступления могут быть совершены с использованием именно этого способа, не должен сопровождаться введением норм, содержащих данный признак в качестве квалифицирующего обстоятельства, в статьи Особенной части. Целесообразно ограничиться введением в ст. 63 УК РФ такого отягчающего наказание обстоятельства, как использование компьютерных технологий при совершении преступления»[1]. Данным решением О.М. Сафонов, по сути, отказывается от самой идеи дифференциации уголовной ответственности в зависимости от совершения преступления с использованием информационно-коммуникационных технологий и переводит проблему в плоскость индивидуализации наказания. При этом предлагаемая корректировка ст. 63 УК РФ весьма в общей форме решает проблему, когда в каждом конкретном случае судья будет решать, каким образом и насколько использование соответствующих средств влияет на меру ответственности личности.

В теории уголовного права мнения специалистов значительно разнятся по вопросу о том, какие именно составы преступлений требуют специальной оговорки об их совершении с использованием информационно-коммуникационных технологий. Так, А.Ж. Кабанова в 2004 году в своей работе обосновывала включение такого квалифицирующего признака, как «совершение преступления с использованием компьютерной техники, в том числе путем ввода компьютерных программ и информации, их модификации, уничтожения, блокирования либо иного вида вмешательства в процесс обработки информации, влияющего на результат обработки информации» в следующие составы преступлений: клевета, оскорбление, нарушение неприкосновенности частной жизни, нарушение тайны сообщений, нарушение авторских и смежных прав, мошенничество, изготовление или сбыт поддельных денег или ценных бумаг, поддельных кредитных либо расчетных карт, незаконное получение кредита, терроризм, хулиганство, незаконное распространение порнографических материалов и предметов, служебный подлог, фальсификация доказательств, подделка,

[1] Сафонов О.М. Уголовно-правовая оценка использования компьютерных технологий при совершении преступлений: состояние законодательства и правоприменительной практики, перспективы совершенствования : дис. …канд. юрид. наук. М., 2015. С. 141.

изготовление или сбыт поддельных документов, публичные призывы к развязыванию агрессивной войны[1].

Спустя более чем 10 лет А.Ю. Чупрова пишет, что в целях предупреждения посягательств на жизнь и здоровье личности путем нарушения работы медицинской аппаратуры и медицинских жизнеобеспечивающих приборов посредством информационно-телекоммуникационных сетей или применения компьютерных технологий необходимо дополнить п. «е» ч. 2 ст. 105, п. «в» ч. 2 ст. 111, ч. 2 ст. 112 УК РФ новым квалифицирующим признаком – с использованием компьютерных технологий или информационно-телекоммуникационных сетей[2]. Аналогичный признак автор предлагает включить и в ч. 2 ст. 127[1] УК РФ[3].

Полагаем, что несмотря на масштаб и сложность проблемы эффективного противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий, модернизация уголовного закона должна осуществляться обдуманно и по принципу минимизации вносимых поправок. Нет никакой необходимости сплошного «насыщения» диспозиций уголовно-правовых норм указанием на возможность их совершения посредством использования объектов информационной инфраструктуры. Такие оговорки должны иметь место только в случаях пробельности уголовного закона, его очевидного несоответствия современным угрозам. Очевидно, что далеко не всякое применение информационных технологий (сети «Интернет», например) влияет на степень общественной опасности деяния. Включение квалифицирующего признака в состав преступления необходимо в случаях, когда он объективно повышает вероятность наступления вредных последствий, что является важнейшим показателем опасности действия. Как справедливо писал по этому поводу В.Н. Кудрявцев, «опасность действия заключается в том, что оно может вызвать определенные вредные последствия. Однако эти последствия наступают не во всех случаях. Естественно, что действия будут сравнительно тем опаснее, чем выше степень вероятности наступления вредных последствий»[4]. Например, Федеральным законом от 01 марта 2012 г. № 18-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» система квалифицирующих признаков сбыта

---

[1] Кабанова А.Ж. Преступления в сфере компьютерной информации: уголовно-правовые и криминологические аспекты : автореф. дис. …канд. юрид. наук. Ростов н/Д, 2004. С. 5.

[2] Чупрова А.Ю. Уголовно-правовые механизмы регулирования отношений в сфере электронной коммерции : дис. ... д-ра юрид. наук. М., 2015. С. 21.

[3] Там же. С. 308.

[4] Кудрявцев В.Н. Объективная сторона преступления. М., 1960. С. 102.

наркотических средств, психотропных веществ или их аналогов была обоснованно дополнена указанием на использование электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет»). Дело здесь не только в том, что использование информационно-телекоммуникационных сетей существенно осложняет выявление и раскрытие сбыта наркотических средств, но, что более важно, оно существенно облегчает его совершение (предоставляет неограниченные возможности для формирования клиентской базы, гарантирует анонимность, упрощает расчеты и т.д.).

Таким образом, критерии определения границ признания использования информационно-коммуникационных технологий квалифицирующим (особо квалифицирующим) признаком преступления следует искать в характере охраняемых общественных отношений, свойствах уголовного права как специфического регулятора социальной жизни и самой преступности. Как справедливо отмечает С.Я. Лебедев, тональность уголовно-правовым технологическим инновациям задает сама преступность, которая, как главный объект превентивного контроля уголовной политики, демонстрирует сегодня обществу действительно инновационные сюжеты своего активного развития[1].

М.А. Ефремова в своей работе предлагает включить квалифицирующий признак «использование информационно-телекоммуникационных технологий» в ст.ст. 137, 138, 144, 146, 147, 158, 160, 163, 176, 183, 185[6], 205, 207, 275, 276 УК РФ. Аргументация автора в целом сводится к тому, что «…использование средств вычислительной техники существенно упрощает процесс совершения преступления»[2].

Вместе с тем, в каком-то смысле информационные технологии упрощают все – от приобретения продуктов питания в супермаркете до проведения выборов главы государства. Должно ли это выступать базовым критерием дифференциации уголовной ответственности? Необходимо учитывать, что появление информационного способа совершения преступления не свидетельствует априорно о том, что он является более опасным, чем традиционный, а во многом указывает на проблему отстава-

---

[1] Лебедев С.Я. Перспективы модернизации уголовного закона как средства обеспечения безопасного развития цифровой экономики // Обеспечение национальной безопасности – приоритетное направление уголовно-правовой, криминологической и уголовно-исполнительной политики : материалы XI Российского Конгресса уголовного права, посвященного памяти доктора юридических наук, профессора Владимира Сергеевича Комиссарова. М., 2018. С. 157.

[2] Ефремова М.А. Уголовно-правовая охрана информационной безопасности : дис. ... д-ра юрид. наук. М., 2017. С. 22.

ния социального контроля от развития общества и изменения преступности. Так, современный следователь может легко понять и построить тактику расследования незаконного собирания сведений, составляющих коммерческую тайну, связанного со взломом офисного помещения и физическим изъятием соответствующих документов. Привычная форма преступного поведения позволит следователю построить следственные версии, определиться с порядком формирования доказательственной базы и т.п. Ситуация кардинально меняется, когда незаконное собирание той же информации было осуществлено путем неправомерного вмешательства в работу офисного принтера, когда все документы, отправляемые на печать, в электронном виде отправлялись также на компьютер злоумышленника, находящегося, возможно, на другом конце света. Можно ли сказать уверенно, что первый способ незаконного получения сведений, составляющих коммерческую тайну, является менее опасным, чем второй?

Признание использования информационно-коммуникационных технологий квалифицирующим признаком преступления, конечно же, должно соответствовать обоснованным в науке критериям дифференциации уголовной ответственности.

Полагаем, что основанием безусловного характера является признание использования информационно-коммуникационных технологий квалифицирующим признаком преступления в соответствии с нормами международного права. В этом отношении отечественное уголовное законодательство имеет определенный потенциал для развития.

Безусловным поводом для принятия решения о дифференциации уголовной ответственности по анализируемому признаку является констатация того обстоятельства, что использование информационно-коммуникационных технологий приобрело значительную распространенность при совершении преступления и существенным образом повлияло на состояние защищенности прав и законных интересов граждан, охраняемых законом интересов общества и государства. Такая ситуация, например, имела место при корректировке ст. 228^1 УК РФ. Соглашаясь с приведенным решением, закономерно возникает вопрос о последовательной реализации уголовно-политического курса и распространении такого подхода к дифференциации ответственности за сбыт оружия, взрывчатых веществ и взрывных устройств (ст.ст. 222 и 222^1 УК РФ), сильнодействующих или ядовитых веществ (ст. 234 УК РФ), новых потенциально опасных психоактивных веществ (ст. 234^1 УК РФ).

Признание того, что правоохранительные органы испытывают затруднения при раскрытии и расследовании преступления, которое в отдельных случаях совершается с использованием информационно-

коммуникационных технологий, не может выступать должной основой для принятия решения об усилении ответственности.

В качестве общего итога данной части работы представляется возможным представить следующие обязательные криминализационные основания для принятия такого решения:

1) приспосабливание Особенной части УК РФ к условиям информационного общества не должно быть связано с конструированием «цифровых двойников» традиционных уголовно-правовых запретов. Такая модернизация отечественного уголовного законодательства неминуемо приведет к избыточному дублированию его положений, выражающемуся в наличии значительного количества норм, конкурирующих друг с другом исключительно на стыке проблемы разграничения виртуального и реального в праве;

2) внесение соответствующих поправок в Особенную часть УК РФ является обусловленным только в тех случаях, когда адаптационная емкость отечественного уголовного законодательства к проявлениям компьютеризированной преступности исчерпывает себя, и толкование нормы выходит за пределы системного смысла закона, восполняя системный семантический пробел, что свидетельствует уже об аналогии закона или об аналогии права, которые в соответствии со ст. 3 УК РФ запрещены;

3) появление нового (информационного) способа совершения преступлений не свидетельствует априорно о том, что он является более опасным, чем традиционный, а во многом указывает на проблему отставания социального контроля от развития общества и изменения преступности;

4) признание использования информационно-коммуникационных технологий квалифицирующим признаком преступления в целом должно соответствовать обоснованным в науке критериям дифференциации уголовной ответственности. При этом обязательными криминализационными основаниями (предпосылками) для принятия такого решения являются: 1) необходимость признания использования информационно-коммуникационных технологий квалифицирующим признаком преступления установлена нормами международного права и 2) использование информационно-коммуникационных технологий приобрело значительную распространенность при совершении конкретного преступления и существенным образом повлияло на состояние защищенности прав и законных интересов граждан, охраняемых законом интересов общества и государства.

3.2. ДИФФЕРЕНЦИАЦИЯ ОТВЕТСТВЕННОСТИ ЗА ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ (КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ)

Очевидной проблемой дифференциации ответственности за преступления в сфере компьютерной информации (компьютерные преступления) является отсутствие системного подхода к построению их квалифицирующих признаков. Как известно, в целях обеспечения системности уголовного законодательства в теории уголовного права был обоснован «блоковый» подход к изложению квалифицирующих признаков для отдельных групп преступлений[1]. Его сущность заключается в унифицированном построении отягчающих обстоятельств преступлений определенного вида, когда конкретный набор квалифицирующих признаков единообразно влияет на изменение их типовой общественной опасности. Анализ уголовно-правовых норм об ответственности за преступления в сфере компьютерной информации позволяет сделать вывод, что такая системность при их построении не была выдержана. В связи с этим в теории уголовного права высказываются многочисленные предложения по совершенствованию ст.ст. 272–274 УК РФ. Так, В.Г. Степанов-Егиянц в своем исследовании небезосновательно предлагает новые редакции ст.ст. 272 и 273 УК РФ, построенных на основе однотипного дифференцирующего воздействия конкретного набора квалифицирующих признаков[2].

В отечественной доктрине уголовного права предложения, связанные с дифференциацией ответственности за преступления в сфере компьютерной информации, высказывались неоднократно. В самом общем виде они могут быть сведены к двум основным группам: 1) заключающиеся в конкретизации («дроблении») существующих уголовно-правовых запретов; 2) связанные с включением дополнительных квалифицирующих признаков в действующие статьи об ответственности за компьютерные преступления.

Ярким представителем первого направления является А.Ю. Чупрова, которая обосновала комплексную модернизацию главы 28 УК РФ путем включения сразу нескольких новых составов преступлений: ст. 273[1] «Неза-

---

[1] Грибов А.С. Дифференциация ответственности за экономические преступления в России, ФРГ и США: сравнительно-правовое исследование : автореф. дис. … канд. юрид. наук. Ярославль, 2011. С. 11.

[2] Степанов-Егиянц В.Г. Методологическое и законодательное обеспечение безопасности компьютерной информации в Российской Федерации: уголовно-правовой аспект : автореф. дис. ... д-ра юрид. наук. М., 2016. С. 14–16.

прашиваемые массовые рассылки электронных сообщений»; ст. 273^2 «Подстрекательство или пособничество в совершении преступления с использованием средств массовой информации или информационно-телекоммуникационных сетей»; ст. 273^3 «Хищение персональных данных или иной идентификационной информации»; ст. 273^4 «Использование информационно-телекоммуникационных сетей (в том числе сети «Интернет») для распространения порнографических материалов»[1].

Обстоятельного рассмотрения заслуживает предложение А.Ю. Чупровой о криминализации в ст. 273^1 УК РФ такой деятельности, как спаминг. Автор обосновывает необходимость установления ответственности за «неоднократные массовые рассылки электронных сообщений, не позволяющие определить их отправителя, доставляемые получателю без его предварительного согласия». Признак неоднократности раскрывается автором с использованием административной преюдиции – «если лицо ранее в течение года было привлечено к административной ответственности за совершение аналогичного деяния».

Соглашаясь с общим выводом о своевременности положительного разрешения вопроса о криминализации спаминга[2], вызывает возражение позиция А.Ю. Чупровой в части использования такого конструктивного признака, как анонимность отправителя. При реализации такого подхода спаминг будет отсутствовать, если незапрашиваемые массовые рассылки будет осуществлять лицо, предоставляющее о себе полные и достоверные сведения. Вместе с тем, опасность данной деятельности определяется далеко не тем, что рассылка сама по себе носит анонимный характер. Спаминг существенно увеличивает нагрузку на почтовые сервера, затрудняя тем самым работу информационно-коммуникационных систем. Как отмечается в Резолюции 52 «Противодействие распространению спама и борьба со спамом» Всемирной ассамблеи по стандартизации электросвязи: «…спам стал широко распространенной проблемой, влекущей потерю доходов поставщиков услуг «Интернета», операторов электросвязи, опера-

---

[1] Чупрова А.Ю. Уголовно-правовые механизмы регулирования отношений в сфере электронной коммерции : дис. ... д-ра юрид. наук. М., 2015. С. 23–25.

[2] Так, согласно исследованию «Лаборатории Касперского» и «B2B International», в России 75 % опрошенных считают спам одной из главных угроз информационной безопасности (первое место респонденты оставили за вредоносными программами – 78 %). При этом результаты международного опроса меняют расстановку: спам – 64 % и вредоносные компьютерные программы – 61 % (всего было опрошено 4 438 респондентов) // [Электронный ресурс] // URL: https://media.kaspersky.com/en/IT_Security_Risks_Survey_2014_Global_report.pdf (дата обращения: 10.06.2018).

торов подвижной электросвязи и корпоративных пользователей. Противодействие спаму с помощью технических средств ложится тяжелым бременем на организации, включая операторов сетей, поставщиков услуг, а также пользователей, которые не по своей воле получают спам. Спам создает проблемы для безопасности информационных сетей и сетей электросвязи и все чаще используется в качестве средства фишинга и распространения вирусов, шпионского программного обеспечения, других видов вредоносных программ»[1].

Следует также отметить, что в указанной Резолюции отмечается как отсутствие единого подхода к определению спама в различных странах, так и то, что государствам-членам следует принять все необходимые меры в рамках своих национальных правовых систем по борьбе со спамом и его распространением.

Определение спама сформулировано в п. 3.37 ГОСТа Р ИСО/МЭК 27033-1-2011 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей», в соответствии с которым под ним предлагается понимать «незапрашиваемые сообщения электронной почты, содержание которых может быть вредоносным и (или) мошенническим»[2].

В данной трактовке вызывает возражение указание на вредоносность самих сообщений. С одной стороны, спам действительно выступает проводником компьютерных вирусов и мошеннической активности в киберпространстве. Но по большому счету это лишь часть анализируемого явления, не раскрывающая его сущности. Более удачная формулировка того, что следует называть спамингом, представлена в ст. 18 Федерального закона от 13 марта 2006 г. № 38-ФЗ «О рекламе»: «распространение рекламы по сетям электросвязи, в том числе посредством использования телефонной, факсимильной, подвижной радиотелефонной связи, допускается только при условии предварительного согласия абонента или адресата на получение рекламы. При этом реклама признается распространенной без предварительного согласия абонента или адресата, если рекламораспространитель не докажет, что такое согласие было получено. Рекламораспространитель обязан немедленно прекратить распространение рекламы в

---

[1] [Электронный ресурс] // URL: http://search.itu.int/history/HistoryDigitalCollectionDocLibrary/ 4.311.43.ru.600.pdf (дата обращения: 10.06.2018).

[2] ГОСТ Р ИСО/МЭК 27033-1-2011 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей» (утв. и введен в действие Приказом Росстандарта от 01.12.2011 № 683-ст) // СПС «КонсультантПлюс».

адрес лица, обратившегося к нему с таким требованием. Не допускается использование сетей электросвязи для распространения рекламы с применением средств выбора и (или) набора абонентского номера без участия человека (автоматического дозванивания, автоматической рассылки)».

Таким образом, определяющими общественную опасность спаминга выступают такие признаки, как: 1) массовость, свидетельствующая о способности такой рассылки оказывать существенное влияние на нормальное функционирование информационно-коммуникационной инфраструктуры; 2) отсутствие предварительного согласия абонента на получение сообщений. Достоверность (ложность) самих сведений, наличие данных об отправителе отнюдь не определяют природу анализируемого явления.

Вызывает возражение решение А.Ю. Чупровой о криминализации спаминга с использованием административной преюдиции. В абсолютном большинстве случаев спаммеры – это лица, занимающиеся распространением незапрашиваемого рекламного контента на профессиональной основе, достаточно осведомленные о том непосредственном и косвенном ущербе, который они причиняют владельцам информационных систем и ресурсов. В связи с этим предварительное привлечение к административной ответственности вероятнее всего никак не повлияет на достижение цели предупреждения спаминга и вызовет лишь применение злоумышленниками многочисленных механизмов уклонения от ответственности, в том числе с использованием так называемых «номиналов» (формальных руководителей юридических лиц без фактических организационно-распорядительных и административно-хозяйственных полномочий), которые будут сменять друг друга при необходимости.

В проекте ст. 273^1 УК РФ есть еще один уязвимый аспект. В части второй А.Ю. Чупрова выделяет квалифицированный вид спаминга: «Те же действия, повлекшие сбои или прекращение функционирования компьютерной системы в целом или ее части». Учитывая, что диспозиция основного состава спаминга сконструирована автором с административной преюдицией, получается, что квалифицированный спаминг будет иметь место лишь в случае, когда лицо, ранее в течение года привлеченное к административной ответственности за незапрашиваемую рассылку, повторно совершит указанное деяние и вызовет нарушение функционирования компьютерной системы. Вместе с тем, при значительном нарушении нормального функционирования объектов информационно-коммуникационной инфраструктуры, на наш взгляд, ответственность должна наступать независимо от повторности действий лица по незапрашиваемой рассылке.

Ключевой проблемой уголовно-правового определения ответственности за спаминг является признак массовости рассылки. А.Ю. Чупрова решает ее путем заимствования американского опыта, раскрывая массовость как направление «по одному адресу более 100 писем в течение суток, или 1 000 писем в течение 30 дней, или 10 000 писем в течение одного года». Важно отметить, что в основе подобных чисто математических критериев общественной опасности незапрашиваемой рассылки лежит мнение профессионального сообщества о том объеме электронных сообщений, который может оказывать значимое негативное влияние на работу поставщиков услуг «Интернета», операторов электросвязи, операторов подвижной электросвязи и рядовых пользователей. Понятно, что в целом такая оценка субъективна и с течением времени может подлежать пересмотру хотя бы по причине развития технологий высокоскоростной передачи информации и снижения расходов на это.

Уже сейчас подходы государств в определении количественных критериев уголовно наказуемого спама не единообразны. Так, Закон Гвианы «О киберпреступности» 2016 г. массовость рассылки определяет как отправление в течение 24 часов незапрашиваемых писем более чем 50 получателям[1]. Следует обратить внимание, что здесь в количественном выражении говорится именно о получателях, а не об отправленных сообщениях. Несбалансированность последнего подхода выражается в том, что при видимой большей строгости Закона Гвианы в сравнении с американской моделью определения спама в расчете за одни контрольные сутки в действительности он гораздо мягче в целом. Так, если злоумышленник будет отправлять ежедневно незапрашиваемые сообщения 49 получателям в течение года, то ответственность за спаминг по законодательству Гвианы он не понесет ни при каких обстоятельствах, хотя с точки зрения американской модели такое лицо превысит допустимые месячные (1 470 сообщений) и годовые (17 885 сообщений) значения.

[1] «For the purposes of this section, «multiple electronic mail messages» means unsolicited data messages, including electronic mail and instant messages sent to more than fifty recipients within twenty-four hours» // [Электронный ресурс] // URL: https://www.google.ru/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwjm2cDKidPbAhVLjiwKHUD3CYQQFggnMAA&url=http%3A%2F%2Fparliament.gov.gy%2Fdocuments%2Fbills%2F6033-cybercrime_bill_2016-__no_17_of_2016.doc&usg=AOvVaw03RGFrDVlxoWTd6jMrBhe0 (дата обращения: 14.06.2018).

Законы ряда африканских стран (Нигерии, Танзании и др.), предусматривая ответственность за спаминг, вообще никак не конкретизируют признак массовости рассылки незапрашиваемых сообщений.

Полагаем, что признак массовости рассылки незапрашиваемых сообщений должен быть определен в УК РФ бланкетным способом через указание на ее незаконность. Причина главным образом кроется в том, что актуальные критерии массовости должны определить профильные ведомства с учетом мнения всей отрасли. Кроме того, в отличие от прямой регламентации в уголовном законе такой подход обеспечит необходимую подвижность соответствующих критериев и оперативность в изменении объемов уголовной репрессии за спаминг.

В своей работе А.Ю. Чупрова обосновывает также целесообразность включения в УК РФ ст. 273^2 «Подстрекательство или пособничество в совершении преступления с использованием средств массовой информации или информационно-телекоммуникационных сетей». Прежде всего, следует четко обозначить, что автор предлагает установить ответственность не за подстрекательство и пособничество по смыслу ст. 33 УК РФ, а за самостоятельные формы общественно опасного поведения в киберпространстве: 1) призывы к совершению тяжких или особо тяжких преступлений с использованием средств массовой информации или информационно-телекоммуникационных сетей (включая сеть «Интернет»); 2) размещение в информационно-телекоммуникационных сетях (включая сеть «Интернет») информации, содержащей рекомендации относительно методов совершения хищений с использованием компьютерной информации, разработки, изготовления, применения или приобретения наркотических средств, психотропных веществ и их прекурсоров, оружия, взрывчатых веществ и взрывных устройств, ядерных материалов и радиоактивных веществ, а равно способах выведения из строя объектов жизнеобеспечения.

Таким образом, предлагаемая А.Ю. Чупровой новелла предусматривает более широкий круг деяний, нежели нормы об ответственности за подстрекательство или пособничество в совершении преступлений, позволяя квалифицировать целый ряд проявлений содействия преступной деятельности, которые не охватываются нормами об ответственности за соучастие.

Как уже отмечалось ранее, практика борьбы с преступностью в киберпространстве показывает, что лица, снабжающие злоумышленников вредоносным программным обеспечением, сетевыми идентификаторами пользователей и другой необходимой информацией, по соображениям конспирации не ставятся в известность о том, каким образом, в отношении кого и когда будут применены соответствующие средства. Таким образом,

задача, например, разработчиков вредоносных компьютерных программ заключается лишь в том, чтобы предоставить преступникам соответствующие объекты; знать же все планы получателей им вовсе не обязательно. Это в полной мере относится и к лицам, осуществляющим обучение навыкам по созданию компьютерных вирусов, преодолению программно-технических средств защиты интернет-ресурсов и т.п. Где и при каких обстоятельствах обучающиеся будут применять полученные ими знания, умения и навыки, сам инструктор не знает.

Соглашаясь с социально-правовой обусловленностью криминализации таких действий, мы не можем в полной мере принять ту модель, которую предлагает реализовать А.Ю. Чупрова. Возражения касаются как названия нормы, которая не отражает сущности ее содержания, так и описания самого деяния. Во-первых, преждевременным видится установление ответственности за призывы к совершению тяжких и особо тяжких преступлений с использованием информационно-коммуникационных технологий. Данное решение во многом является уязвимым по той причине, что в отечественном уголовном законодательстве нет общей нормы об ответственности за призывы к преступной деятельности в целом, криминализованы лишь призывы к конкретным ее видам – террористической и экстремистской деятельности. Аргументом не в пользу такого решения также выступает опасение относительно соблюдения права на свободу слова. Столь общий (абстрактный) запрет может легко породить ситуацию, когда обмен повседневной информацией, репосты тех или иных новостей, а также комментарии к ним могут быть расценены правоохранительными органами как призывы к преступной деятельности.

Социально и криминологически обоснованным решением видится включение в российское законодательство уголовно-правовой нормы об ответственности за содействие совершению преступлений, предусмотренных статьями 159^3, 159^6, а равно главой 28 УК РФ. Полагаем, что такая мера существенно расширит арсенал уголовно-правовых средств противодействия компьютерным и компьютеризированным преступлениям, создаст нормативную основу для раннего уголовно-правового реагирования на факты оказания помощи в их совершении при отсутствии признаков соучастия.

С учетом реализации данной законотворческой инициативы теряет смысл предложение А.Ю. Чупровой о целесообразности выделения ст. 273^3 «Хищение персональных данных или иной идентификационной информации». Незаконное завладение сетевыми идентификаторами пользователей в целях последующего сбыта является, по сути, приготовлением к содействию совершению преступлений с использованием информацион-

но-коммуникационных технологий, а фактический сбыт – уже совершением данного преступления в форме предоставления информации.

Дискуссионным представляется решение А.Ю. Чупровой о криминализации «использования информационно-телекоммуникационных сетей (в том числе сети «Интернет») для распространения порнографических материалов». Во-первых, и, пожалуй, это самое значимое замечание, такой запрет не будет соответствовать содержанию видового объекта преступлений в сфере компьютерной информации, поскольку распространение порнографических материалов никоим образом не угрожает состоянию защищенности компьютерной информации, а также нормальному функционированию средств ее автоматизированной обработки. Во-вторых, включив предлагаемую автором ст. 273^4 в УК РФ, мы закономерно породим конкуренцию с действующей ст. 242 УК РФ, что не будет способствовать решению проблем правоприменения.

Справедливости ради, следует указать, что А.Ю. Чупрова предлагает установить в этой норме ответственность не только за рассылку через «Интернет» порнографических материалов, но и за «использование ложных доменных имен с целью привлечения иных лиц для просмотра сайтов с порнографическими материалами». Действительно, такая деятельность в определенном смысле нарушает «сетевой» порядок. Такие «киберловушки», мимикрируя под новостные ресурсы, программы оздоровления или предложения по трудоустройству, позволяют злоумышленникам существенно увеличивать посещаемость и соответственно популярность сайтов, распространяющих порнографию. Однако представляется очевидным, что использование таких доменных имен образует собой типичную форму пособничества в совершении преступления, предусмотренного ст. 242 УК РФ. В тех же случаях, когда подобное совершает сам владелец порнографического сайта, то его действия как исполнителя полностью охватываются диспозицией все той же ст. 242 УК РФ.

К.Н. Евдокимов обосновывает необходимость дополнения главы 28 УК РФ статьей 272^1 «Незаконное завладение носителем компьютерной информации с целью осуществления неправомерного доступа к компьютерной информации»[1]. Данное предложение автора представляется дискуссионным. Во-первых, очевидно, что тем самым будут криминализованы приготовительные действия к неправомерному доступу к охраняемой законом компьютерной информации, что представляется излишним ввиду

[1] См.: Евдокимов К.Н. Проблемы квалификации и предупреждения компьютерных преступлений: монография. Иркутск, 2009. С. 94; Евдокимов К.Н. Противодействие компьютерной преступности в Российской Федерации: криминологические и уголовно-правовые аспекты: монография. Иркутск, 2016. С. 83.

наличия общих правил уголовной ответственности за неоконченную преступную деятельность. Во-вторых, наличие признака специальной цели при завладении материальным носителем информации с высокой долей вероятности сделает невозможным применение данного уголовно-правового запрета на практике. Злоумышленник всегда сможет сослаться на то, что его деяние было направлено на хранилище информации как на имущество. И наконец, в-третьих, сразу возникает вопрос о квалификации действий лица, которое сначала завладело носителем компьютерной информации и впоследствии осуществило неправомерный доступ к ней. Требуется ли в данном случае квалифицировать содеянное по совокупности? Если да, то налицо ситуация сверхкриминализации, поскольку лицу одновременно вменяют и оконченное преступление, и отдельную стадию его совершения.

М.А. Ефремова предлагает разделить ответственность за создание вредоносных программ (ст. 273) и использование или распространение вредоносных программ (ст. 273[1])[1]. Оценивая эту научную позицию, необходимо отметить, что ее практическая реализация вряд ли имеет под собой должное криминологическое обоснование. Нельзя однозначно утверждать, что действия по созданию вредоносной компьютерной программы всегда представляют бóльшую общественную опасность, нежели ее фактическое использование, и тем более распространение. Лицо, которое из профессионального интереса изготовило опасный компьютерный вирус без намерения его дальнейшего использования, заслуживает гораздо меньшего наказания в сравнении с тем, кто, распространив такую программу, причинит многомиллиардный ущерб миллионам пользователей сети «Интернет».

М.А. Простосердов в целях противодействия субкультуре хакеров, а также рынку вредоносного программного обеспечения предлагает дополнить ст. 273 УК РФ новой частью: «2.1. Сбыт компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации»[2].

Нами уже отмечалась необходимость конкретизации диспозиции ст. 273 УК РФ в части включения такого альтернативного деяния, как сбыт вредоносных компьютерных программ или компьютерной информации.

---

[1] Ефремова М.А. Уголовно-правовая охрана информационной безопасности : дис. ... д-ра юрид. наук. М., 2018. С. 351–352.

[2] Простосердов М.А. Экономические преступления, совершаемые в киберпространстве : монография. М., 2017. С. 143.

Вместе с тем, наша аргументация связана с противоречивым толкованием признака распространения вредоносного программного обеспечения. В свою очередь, М.А. Простосердов полагает, что сбыт обладает повышенной опасностью в сравнении с распространением, с чем сложно согласиться. В отличие от сбыта, распространение заведомо обращено не к конкретному приобретателю, а к неограниченному кругу лиц, что в большей мере угрожает нормальному функционированию объектов автоматизированной обработки данных.

Применительно ко второму направлению, связанному с совершенствованием системы квалифицирующих признаков преступлений в сфере компьютерной информации, можно также выделить основные позиции в отечественной доктрине уголовного права. Так, весьма распространенной является мысль о необходимости дополнения ст.ст. 272 и 273 УК РФ таким квалифицирующим признаком как, совершение указанных преступлений «с целью скрыть другое преступление или облегчить его совершение»[1]. К.Н. Евдокимов, обосновывая подобную инициативу, ссылается на то обстоятельство, что преступления в сфере компьютерной информации часто выступают способом совершения хищения, государственной измены, шпионажа и т. п.[2]

При этом нельзя не отметить, что у теоретиков нет общего взгляда на то, насколько данная цель повышает степень общественной опасности преступлений, в сфере компьютерной информации. Так, например, Д.А. Ковлагина полагает, что данный квалифицирующий признак следует указать в частях вторых ст.ст. 272 и 273 УК РФ[3]. В свою очередь, З. И. Хисамова предлагает включить такой квалифицирующий признак в ч. 3 ст. 273 УК РФ[4].

Действительно, нельзя оспорить то обстоятельство, что неправомерный доступ к охраняемой законом компьютерной информации довольно часто совершается с целью обеспечения выполнения объективной сторо-

---

[1] См., например: Степанов-Егиянц В.Г. Методологическое и законодательное обеспечение безопасности компьютерной информации в Российской федерации (уголовно-правовой аспект) : автореф. дис. ... д-ра юрид. наук. М., 2016. С. 14.

[2] Евдокимов К.Н. Проблема уголовно-правовой квалификации преступлений в сфере компьютерной информации // Российский следователь. – 2012. – № 6. – С. 20.

[3] Ковлагина Д.А. Информационный терроризм: понятие, уголовно-правовые и иные меры противодействия : монография. М., 2017. С. 113.

[4] Хисамова З.И. Уголовная ответственность за преступления, совершаемые в финансовой сфере с использованием информационно-телекоммуникационных технологий. М., 2017. С. 120.

ны другого преступления. Например, лицо, которое незаконно получает доступ к системе дистанционного банковского обслуживания коммерческой организации делает это ради дальнейшего хищения денежных средств потерпевшего. Можно продолжить: неправомерный доступ довольно часто предшествует совершению таких преступлений, как нарушение неприкосновенности частной жизни, нарушение тайны переписки или иных сообщений, вымогательство, принуждение к совершению действий сексуального характера, нарушение авторских и смежных прав, принуждение к совершению сделки или отказу от ее совершения, незаконное получение сведений, составляющих коммерческую или банковскую тайну и др.

Кроме того, использование вредоносной компьютерной программы или информации, как правило, связано с посягательством либо на компьютерную информацию, либо на нормальное функционирование средств ее хранения, обработки или передачи, то есть совершением преступления, предусмотренного ст. 272 УК РФ. Кроме того, как показывает современная правоприменительная практика, значительная доля случаев использования вредоносных компьютерных программ сопряжена с посягательством на объекты интеллектуальной собственности (ч. 2 ст. 146 УК РФ), когда преступник осуществляет незаконную нейтрализацию встроенной системы защиты лицензионного программного обеспечения. Включив такой квалифицирующий признак в систему дифференциации ответственности по ст. 273 УК РФ, мы фактически от этой же дифференциации откажемся применительно к такому деянию, как использование. Практически каждый случай использования вредоносной компьютерной программы или информации будет подпадать под действие ч. 3 ст. 273 УК РФ.

Таким образом, следует заключить, что анализируемое предложение вступает в противоречие с общетеоретическим положением учения о дифференциации уголовной ответственности, согласно которому квалифицирующий признак должен быть типичным, но в то же время нехарактерным для большинства деяний, зафиксированных в основном составе. Как справедливо отмечают по данному поводу Л.Л. Кругликов и О.Е. Спиридонова, «обстоятельства, которым придается статус квалифицирующих признаков, не должны быть нормой для большинства преступлений с основным составом»[1].

Полагаем, что недостаточно продуманной выглядит дифференциация ответственности за преступления в сфере компьютерной информации

[1] Кругликов Л.Л., Спиридонова О.Е. Юридические конструкции и символы в уголовном праве. СПб., 2005. С. 100.

в зависимости от формы соучастия. Как известно, общественная опасность преступления, совершенного организованной группой, всегда выше той, которую представляет преступление, совершенное группой лиц по предварительному сговору. Это обстоятельство, как правило, учитывается законодателем, который при построении квалифицированных составов довольно часто использует связку «совершение преступления группой лиц по предварительному сговору» – совершение преступления организованной группой». В отечественной доктрине уголовного права такую модель оценивают как оправданную, поскольку «с появлением второго звена связок происходит резкий скачок в уровне (типовой степени) общественной опасности соответствующих видов преступного поведения и возникает необходимость в установлении новых законодательных пределов наказуемости»[1].

Поэтому последовательная дифференциация уголовной ответственности за групповое совершение преступлений в сфере компьютерной информации предполагает установление различной наказуемости такого рода деяний в зависимости от формы соучастия. Так, например, было бы логично в ч. 2 ст. 273 УК РФ установить ответственность за создание, использование и распространение вредоносных компьютерных программ группой лиц по предварительному сговору, а в ч. 3 ст. 273 УК РФ – организованной группой.

Обращаясь к квалифицирующим признакам преступления, предусмотренного ст. 274[1] УК РФ, дискуссионными, пожалуй, можно назвать два реализованных решения. Во-первых, законодатель проявил малопонятную последовательность в регламентации совершения преступления предварительно сговорившейся и организованной группами в рамках одной части. Очевидно, что уравнивание таких качественно разных по опасности форм соучастия вряд ли отвечает научно обоснованным критериям дифференциации ответственности. Во-вторых, все преступления в сфере компьютерной информации в качестве особо отягчающего обстоятельства называют наступление тяжких последствий или *создание угрозы их наступления*. Вместе с тем, уголовно-правовая норма, предусмотренная ст. 274[1] УК РФ, такой оговорки не содержит, что, учитывая особую значимость объектов посягательства, представляется по меньшей мере ошибочным.

Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

---

[1] Кругликов Л.Л., Спиридонова О.Е. Юридические конструкции и символы … С. 127.

предполагает категорирование всех объектов в зависимости от социальной, политической, экономической значимости, а также значимости объекта критической информационной инфраструктуры для обеспечения обороны страны, безопасности государства и правопорядка. К сожалению, действующая редакция ст. 274[1] УК РФ не учитывает данное деление, что представляется существенным упущением не только с точки зрения игнорирования критериев дифференциации уголовной ответственности, но и что, пожалуй, более значимо, – анализируемая уголовно-правовая новелла не позволяет должным образом оценить различия в объеме и значимости социальных последствий криминальных посягательств на объекты критической инфраструктуры. Возможности учета опасности указанного деяния только лишь посредством дифференциации уголовного наказания, как представляется, явно недостаточны. Полагаем, что в этой части уголовно-правовая норма об ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации требует корректировки.

Как уже отмечалось при проведении сравнительно-правового исследования законодательств зарубежных стран, значимой проблемой дифференциации ответственности за преступления в сфере компьютерной информации по отечественному законодательству является конкретизация и разделение ответственности за неправомерный доступ к компьютерной информации. С точки зрения рекомендаций Будапештской конвенции о киберпреступности 2001 г., ст. 272 УК РФ представляет собой некий симбиоз, не вполне удачное сочетание сразу нескольких компьютерных преступлений. Закономерно, что такое положение не способствует единообразному пониманию данной уголовно-правовой нормы, порождает крайне противоречивую правоприменительную практику и, как следствие, не служит эффективной защите информационной безопасности.

Прежде всего в целях реализации принципа справедливости и обеспечения надлежащей дифференциации ответственности за качественно разные деяния с точки зрения содержания основного непосредственного объекта и их общественной опасности представляется целесообразным упразднить самостоятельную ответственность за неправомерный доступ к компьютерной информации, повлекший ее копирование. Подобные последствия в наименьшей степени затрагивают безопасность информационных отношений, поскольку не связаны с непосредственным деструктивным воздействием на данные или средства их автоматизированной обработки. В сущности, потерпевший терпит ущерб при копировании компьютерной информации, только если она относилась к тому или иному виду тайны, что, как известно, охватывается и, полагаем, должно охваты-

ваться исключительно специальными уголовно-правовыми нормами (ст.ст. 137, 138, 183, 275, 276, 283^1 и др.). В связи с этим представляется обоснованным дополнить соответствующие уголовно-правовые нормы специальным отягчающим обстоятельством – если деяние было совершено путем неправомерного доступа к компьютерной информации.

Самостоятельного законодательного определения требует деяние, связанное с умышленным уничтожением, блокированием либо модификацией компьютерной информации, в том числе посредством воздействия на средства ее хранения, обработки или передачи, при отсутствии признаков неправомерного доступа. Современная правоприменительная практика каждый раз испытывает серьезные затруднения в случае необходимости оценки действий лица, которое уничтожило либо модифицировало компьютерную информацию, однако до этого было допущено к компьютерной системе самим владельцем. Понятно, что говорить о неправомерном доступе здесь весьма сложно. Только, пожалуй, при самом расширительном толковании диспозиции ст. 272 УК РФ можно предположить, что лицо в определенном смысле превысило пределы такого доступа, то есть действовало уже неправомерно. Очевидно, насколько непрочны аргументы такой квалификации и, следовательно, сомнительны перспективы уголовного преследования в свете положений ст. 3 УК РФ.

Из общей нормы, предусмотренной ст. 272 УК РФ, настоятельно необходимо выделить уголовно-правовой запрет неправомерного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации. Одним из значимых аргументов в пользу такого решения является обеспечение межотраслевой преемственности ответственности за схожие деяния. Так, Кодекс об административных правонарушениях Российской Федерации в ст. 13.18 устанавливает ответственность за воспрепятствование уверенному приему радио- и телепрограмм, а также работе сайтов в сети «Интернет». Кроме того, значимым доводом выступает распространенность общественно опасного поведения в киберпространстве, направленного не на данные, а сам процесс работы объектов информационно-коммуникационной инфраструктуры. Наиболее яркой иллюстрацией данной проблемы являются так называемые DDOS-атаки на информационные ресурсы организаций и частных лиц, которые сами по себе не связаны с преодолением программно-технических средств защиты информации, то есть не предполагают осуществление неправомерного доступа к ней, а лишь влекут сбои в работе соответствующих интернет-ресурсов.

Отсутствие специальной уголовно-правовой нормы о неправомерном вмешательстве в работу автоматизированных средств хранения, обра-

ботки и передачи компьютерной информации породило весьма противоречивую практику применения ст. 272 УК РФ в случаях незаконного подключения лицом к сети «Интернет» с использованием чужих сетевых идентификаторов. Так, например, Б. в процессе использования персонального компьютера, подключенного к сети «Интернет», обнаружил возможность неправомерного и бесплатного подключения к сети «Интернет». Обладая полученными знаниями о возможности неправомерного и бесплатного осуществления подключения к сети «Интернет», не желая осуществлять подключение к сети «Интернет» законным способом, а именно с использованием сетевых реквизитов, принадлежащих его родному брату, вызванного значительными затратами денежных средств на лицевом счете, нуждаясь в использовании ресурсов сети «Интернет», путем подбора цифровых значений с использованием программы для сканирования компьютерных сетей «LanScope» получил сведения о сетевых реквизитах доступа к сети «Интернет» абонента краевого государственного бюджетного учреждения «Корякский фольклорный ансамбль танца «Ангт» в виде логина и пароля с целью последующего их использования и обеспечения себе бесплатного доступа к сети «Интернет». Реализуя возникший преступный умысел, Б. из корыстной заинтересованности, с целью обеспечения себе бесплатного доступа к сети «Интернет», при помощи персонального компьютера, подключенного к сети «Интернет» посредством оператора связи, осознавая, что имеющийся логин и пароль принадлежат действующему абоненту, предвидя возможность наступления общественно опасных последствий в виде искажения (модификации) информации в базе учетно-статистических данных, а также возможность блокирования доступа к компьютерной информации законного пользователя, используя сетевые реквизиты доступа к сети «Интернет», осуществил неправомерное подключение и работу в сети «Интернет» в указанный период времени со следующими параметрами сетевого соединения. Таким образом, Б. из корыстной заинтересованности, осуществил неправомерный доступ к охраняемой Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ, Указом Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» компьютерной информации, а именно: информации о сетевых реквизитах КГБУ «Ангт», что повлекло искажение (модификацию) информации в базе учетно-статистических данных, а именно: информации о времени начала, продолжительности и стоимости работы в сети «Интернет» абонента КГБУ «Ангт», а также блокирование доступа к компьютерной информации, выразившееся в невозможности подключения сотрудников КГБУ

«Ангт» к сети «Интернет» в указанное время и использовании предоставленного указанному учреждению внешнего трафика по технологии DSL[1].

Как справедливо отмечает У.В. Зинина, при подобных обстоятельствах действия лица приводят лишь к изменению статистической информации в биллинговой системе – программно-аппаратном комплексе, предназначенном для учета потребления услуг связи, управления расчетами за такие услуги, управления самими услугами, одновременно с хранением информации об абонентах, которым оператор связи оказывает эти услуги[2]. Подобная автоматизированная модификация информации, конечно же, не образует последствий, предусмотренных ст. 272 УК РФ. В действительности данная ситуация представляет собой типичный пример неправомерного воздействия именно на объекты информационно-коммуникационной инфраструктуры, в результате которого потерпевший либо полностью лишается возможности получать услуги связи, либо существенно теряет в их качестве (например, в скорости передачи данных). У.В. Зинина небезосновательно резюмирует, что тем самым в официальную статистику преступности в сфере компьютерной информации включаются случаи не вполне корректного применения правоприменительными органами уголовного закона, свидетельствующие о расширительном толковании элементов состава преступления, предусмотренного ст. 272 УК РФ[3]. В защиту подобной практики следует лишь сослаться на то, что такое положение во многом обусловлено несовершенством нормативной базы.

Таким образом, действующая уголовно-правовая норма об ответственности за неправомерный доступ к компьютерной информации должна быть разделена на три самостоятельных преступления: ст. 272 «Неправомерный доступ к компьютерной информации»; ст. 272^1 «Умышленное уничтожение, блокирование либо модификация компьютерной информации»; ст. 272^2 «Неправомерное воздействие на средства хранения, обработки или передачи компьютерной информации».

И наконец, с учетом предлагаемых поправок главы 28 УК РФ окончательного решения требует имеющаяся неопределенность конструкции ст. 274 УК РФ в части содержания субъективной стороны данного преступления. Полагаем, что диспозиция указанной уголовно-правовой нормы должна быть дополнена прямым указанием на неосторожную форму вины субъекта по отношению к общественно опасным последствиям. Та-

---

[1] Обвинительное заключение по уголовному делу № 423731 // Архив СО Корякского МО МВД России.

[2] Зинина У.В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве : автореф. дис. … канд. юрид. наук. М., 2007. С. 23.

[3] Там же.

кое решение позволит провести четкое разграничение данного деяния от неправомерного доступа к компьютерной информации, совершаемого лицом с использованием своего служебного положения, а также от умышленного уничтожения, блокирования либо модификации компьютерной информации.

Симметрично такая поправка должна быть включена в уголовно-правовую норму об ответственности за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, которую в силу специфики данного преступления следует определить в специальной статье со своей системой квалифицирующих признаков (ст. 274^2 УК РФ).

Возвращаясь к проблеме межотраслевой дифференциации ответственности за посягательства в сфере компьютерной информации, следует указать на отсутствие преемственности в части правовой оценки действий, связанных с неисполнением решения федерального органа исполнительной власти об ограничении доступа к определенному контенту в сети «Интернет». В настоящее время такая ответственность предусмотрена исключительно ст. 13.34 КоАП РФ. При этом понятно, что такого рода бездействие руководителей оператора связи может повлечь за собой причинение значительного материального ущерба гражданам или организациям либо наступление иных тяжких последствий (гибель человека, массовые беспорядки и т.п.). Криминализация подобного поведения является распространенной практикой в законодательстве зарубежных стран. В связи с этим представляется необходимым специально определить ответственность за бездействие операторов связи в УК РФ при условии наступления общественно опасных последствий.

Просчеты законодателя в конструировании санкции конкретной уголовно-правовой нормы либо ненадлежащее ее применение способны породить множество дополнительных социальных проблем и противоречий. По этой причине одной из главных задач современной науки уголовного права является изучение эффективности правовых мер, используемых в борьбе с преступностью, научное обоснование дальнейшего совершенствования системы и практики применения наказаний, установленных уголовном законодательством. Как справедливо замечает Л.Л. Кругликов, крайне важно, чтобы «физиономия» каждой санкции была определена законодателем четко, однозначно, соответствовала бы по виду и размерам

описанного в ней наказания типовым, а равно прогнозируемым индивидуальным свойствам содеянного и личности виновного[1].

Изучение современной наказательной практики по делам о преступлениях в сфере компьютерной информации позволяет утверждать о наличии следующих основных противоречий. Прежде всего, несмотря на выраженную и признаваемую в теории корыстную направленность компьютерных и компьютеризированных преступлений, санкции уголовно-правовых норм, предусмотренных главой 28 УК РФ, не содержат указаний об обязательном дополнительном наказании в виде штрафа.

Близкая по своей сути проблема связана также с тем, что в санкциях статей об ответственности за исследуемые преступления в качестве дополнительного наказания не включено лишение права занимать определенные должности или заниматься определенной деятельностью. Такое положение не отвечает той общей закономерности, что довольно часто компьютерные и компьютеризированные преступления совершаются лицами, как правило, профессионально занятыми в сфере IT-технологий.

Кроме того, санкции уголовно-правовых норм с учтенной совокупностью (составных преступлений), где способом совершения посягательства на традиционно охраняемые уголовным законом общественные отношения выступает компьютерное преступление, не всегда отражают усиление карательных функций государства. Так, в действующем УК РФ наглядным тому примером может выступать сопоставление санкций ч. 3 ст. 141 УК РФ и ч. 2 ст. 274^1 УК РФ.

С учетом изложенного можно предложить следующий проект главы 28 УК РФ, состоящий из 10 статей:

«Статья 272. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование либо модификацию компьютерной информации, –

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. То же деяние,

---

[1] Кругликов Л.Л. Сбои в конструировании санкций в уголовном законодательстве // Юридическая техника. 2008. № 2. С. 110.

а) совершенное группой лиц по предварительному сговору;

б) причинившее крупный ущерб;

в) совершенное из корыстной заинтересованности, –

наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные организованной группой либо лицом с использованием своего служебного положения, –

наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на срок до шести лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, –

наказываются лишением свободы на срок до восьми лет.

Примечания. 1. Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

2. Крупным ущербом в статьях настоящей главы признается ущерб, сумма которого превышает один миллион рублей.

Статья 272[1]. Умышленное уничтожение, блокирование либо модификация компьютерной информации

1. Умышленное уничтожение, блокирование либо модификация компьютерной информации при отсутствии признаков состава преступления, предусмотренного статьей 272 настоящего Кодекса, –

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. То же деяние,

а) совершенное группой лиц по предварительному сговору;

б) причинившее крупный ущерб;

в) совершенное из корыстной заинтересованности, –

наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные организованной группой либо лицом с использованием своего служебного положения, –

наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на срок до шести лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, –

наказываются лишением свободы на срок до восьми лет.

Статья 272[2]. Неправомерное воздействие на средства хранения, обработки или передачи компьютерной информации

1. Неправомерное воздействие на средства хранения, обработки или передачи компьютерной информации, если это повлекло нарушение и (или) прекращение их функционирования, –

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. То же деяние,

а) совершенное группой лиц по предварительному сговору;

б) причинившее крупный ущерб;

в) совершенное из корыстной заинтересованности, –

наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до

четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные организованной группой либо лицом с использованием своего служебного положения, –

наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на срок до шести лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, –

наказываются лишением свободы на срок до восьми лет.

Статья 273. Создание, использование или распространение вредоносных компьютерных программ

1. Создание, использование или распространение вредоносных компьютерных программ либо иной вредоносной компьютерной информации, –

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. Те же деяния,

а) совершенные группой лиц по предварительному сговору;

б) причинившие крупный ущерб;

в) совершенные из корыстной заинтересованности, –

наказываются штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные организованной группой либо лицом с использованием своего служебного положения, –

наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на срок до шести лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, –

наказываются лишением свободы на срок до восьми лет.

Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-коммуникационных сетей

1. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-коммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-коммуникационным сетям, повлекшее по неосторожности уничтожение, блокирование либо модификацию компьютерной информации, –

наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. То же деяние, причинившее крупный ущерб, –

наказывается ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года

3. Деяние, предусмотренное частью первой настоящей статьи, если оно повлекло тяжкие последствия или создало угрозу их наступления, –

наказывается принудительными работами на срок до пяти лет либо лишением свободы на срок до шести лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

Статья 274[1]. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации

1. Неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, если он повлек причинение вреда критической информационной инфраструктуре Российской Федерации, –

наказывается принудительными работами на срок до пяти лет со штрафом в размере от пятисот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет и с ограничением свободы на срок до двух лет или без такового либо лишением свободы на срок от двух до шести лет со штрафом

в размере от пятисот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет.

2. Деяние, предусмотренные частью первой настоящей статьи:

а) совершенное группой лиц по предварительному сговору;

б) причинившее крупный ущерб;

в) совершенное из корыстной заинтересованности, –

наказываются лишением свободы на срок от трех до восьми лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные:

а) в отношении объекта критической информационной инфраструктуры второй категории;

б) организованной группой;

в) лицом с использованием своего служебного положения, –

наказываются лишением свободы на срок от пяти до десяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет.

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, если они совершены в отношении объекта критической информационной инфраструктуры первой категории либо повлекли тяжкие последствия или создали угрозу их наступления, –

наказываются лишением свободы на срок от шести до двенадцати лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти.

Статья 274[2]. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации

1. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, или информационных систем, информационно-коммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к критической информационной инфраструктуре Российской Федерации, либо правил доступа к указанным информации, информационным системам, информационно-коммуникационным сетям, автоматизированным системам управления, сетям электросвязи, если оно повлекло по неосторожности причинение вреда критической информационной инфраструктуре Российской Федерации, –

наказывается принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового либо лишением свободы на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

2. То же деяние, если оно совершено в отношении объекта критической информационной инфраструктуры второй категории либо причинило крупный ущерб, –

наказывается лишением свободы на срок до шести лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет.

3. Деяние, предусмотренное частью первой или второй настоящей статьи, если оно совершено в отношении объекта критической информационной инфраструктуры первой категории либо повлекло тяжкие последствия или создало угрозу их наступления, –

наказывается лишением свободы на срок до восьми лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет.

Статья 274³. Незаконная массовая рассылка незапрашиваемых электронных сообщений (спаминг)

1. Незаконная массовая рассылка незапрашиваемых сообщений по сетям электросвязи либо посредством использования телефонной, факсимильной, подвижной радиотелефонной связи, в том числе с применением средств выбора и (или) набора абонентского номера без участия человека (автоматического дозванивания, автоматической рассылки), –

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до од-

ного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. То же деяние, совершенное группой лиц по предварительному сговору, –

наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до трех лет, либо принудительными работами на срок до трех лет, либо лишением свободы на тот же срок со штрафом в размере до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года.

3. Деяние, предусмотренное частью первой или второй настоящей статьи, совершенное организованной группой либо лицом с использованием своего служебного положения, –

наказывается ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

Статья 274[4]. Содействие совершению преступлений с использованием информационно-коммуникационных технологий

1. Умышленное содействие совершению преступлений, предусмотренных пунктом «г» частью 3 статьи 158, статьями 159[3], 159[6], а равно статьями настоящей главы, советами, указаниями, предоставлением информации, средств или орудий совершения преступления, при отсутствии признаков соучастия, –

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. То же деяние, совершенное группой лиц по предварительному сговору, –

наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет либо ограничением свободы на срок до трех лет, либо принудительными работами на срок до четырех лет, либо

лишением свободы на тот же срок срок со штрафом в размере до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года.

3. Деяние, предусмотренное частью первой или второй настоящей статьи, совершенное лицом с использованием своего служебного положения, –

наказывается принудительными работами на срок до пяти лет, либо лишением свободы на срок до шести лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

Статья 274[5]. Неисполнение требований федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере связи, информационных технологий и массовых коммуникаций

1. Неисполнение обязанности по ограничению или возобновлению доступа к информации, доступ к которой должен быть ограничен или возобновлен на основании сведений, полученных от федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере связи, информационных технологий и массовых коммуникаций, причинившее крупный ущерб, –

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок до четырехсот восьмидесяти часов, либо принудительными работами на срок до двух лет либо лишением свободы на тот же срок.

2. Деяние, предусмотренное частью первой настоящей статьи, если оно повлекло тяжкие последствия или создало угрозу их наступления, –

наказывается принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет либо лишением свободы на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет».

В завершение данной части работы необходимо также указать на следующее. Анализируя положения Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» в аспекте ст. 274[1] УК РФ, можно сделать

вывод, что законодателю не удалось добиться единства позитивного и охранительного механизмов. В УК РФ не были включены значимые правила, нарушение которых объективно представляет опасность не только для критической информационной инфраструктуры Российской Федерации, но и для иных охраняемых уголовным законом интересов (жизни, здоровья, собственности и т.д.).

В ряду таковых особо следовало бы выделить обязанности соответствующих субъектов, заключающиеся в: 1) незамедлительном информировании о компьютерных инцидентах федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации; 2) оказании содействия должностным лицам федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, в обнаружении, предупреждении и ликвидации последствий компьютерных атак, установлении причин и условий возникновения компьютерных инцидентов; 3) обеспечении выполнения порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты; 4) реагировании на компьютерные инциденты в порядке, утвержденном федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации; 5) обеспечении беспрепятственного доступа должностных лиц федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, к значимым объектам критической информационной инфраструктуры при реализации этими лицами полномочий, предусмотренных законом.

Указанные положения закона в целом направлены на достижение транспарентности и кооперации. Практика сокрытия проблем в сфере информационной безопасности хорошо известна. Специалисты отмечают, что компании неохотно сообщают об инцидентах, связанных с утечкой пользовательской информации. Это влечет за собой репутационные и неизбежные финансовые потери. Те же, кто решается на откровенность, зачастую не спешат с неприятными новостями. Между обнаружением

бреши в безопасности и ее обнародованием в некоторых случаях проходят месяцы[1].

Неисполнение указанных выше обязанностей соответствующими субъектами объективно создает угрозу причинения вреда не только состоянию защищенности критической информационной инфраструктуры Российской Федерации, но и правам и свободам отдельных граждан и организаций. Замалчивание компьютерных инцидентов дает фору преступникам, позволяет им осуществлять новые компьютерные атаки.

Принимая во внимание необходимость неукоснительного исполнения субъектами критической информационной инфраструктуры требований регулятивного законодательства в данной сфере, отдельные страны устанавливают уголовную ответственность. Так, например, Закон о кибербезопасности 2018 г. Сингапура предусматривает значительное количество составов преступлений, связанных с ненадлежащим исполнением правил и стандартов, касающихся функционирования объектов критической информационной инфраструктуры, совершаемых их владельцами/операторами: 1) невыполнение предписания уполномоченного органа, касающегося действий, которые должны быть предприняты владельцем или владельцами в отношении: угрозы кибербезопасности; соблюдения стандартов деятельности, применимых к владельцу; назначения аудитора, утвержденного уполномоченным органом; других вопросов, которые уполномоченный орган может счесть необходимыми или целесообразными для обеспечения безопасности критически важной информационной инфраструктуры (ст.12) – наказывается штрафом в размере до 100 000 долларов США или лишением свободы на срок до 2 лет; 2) не сообщение владельцем критически важной информационной инфраструктуры уполномоченному органу о наступлении любого из следующих событий в установленной форме и в установленном порядке в течение установленного периода: инцидент кибербезопасности в отношении критически важной информационной инфраструктуры; инцидент кибербезопасности в отношении любого компьютера или компьютерной системы, находящейся под контролем владельца, которая взаимосвязана или взаимодействует с критически важной информационной инфраструктурой; любой другой тип инцидента кибербезопасности в отношении критически важной информационной инфраструктуры (ст.14) – наказывается штрафом в размере до 100 000 долларов США или лишением свободы на срок до 2 лет; 3) уклонение от обязательного аудита состояния защищенности объектов крити-

[1] Сборник исследований по практической безопасности АО «Позитив Текнолоджиз». М., 2018. С. 68.

ческой информационной инфраструктуры (ст.15) – наказывается штрафом в размере до 100 000 долларов США или лишением свободы на срок до 2 лет; 4) уклонение владельца критически важной информационной инфраструктуры от выполнения обязательных требований уполномоченного органа в условиях, требующих обнаружения и предупреждения угроз для национальной безопасности, обороны, международных отношений, экономики, общественного здравоохранения, общественной безопасности или общественного порядка Сингапура (ст.23) – наказывается лишением свободы на срок до 10 лет[1].

Данный подход не реализован в отечественном правовом поле. Положения ч. 3 ст. 274[1] УК РФ не распространяются на случаи неисполнения приведенных выше обязанностей, поскольку в целом обращены к *эксплуатационным* правилам и требованиям средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре.

В отечественной теории уголовного права справедливо подчеркивается, что появление новых технических, военных систем и другие факторы предопределяют дальнейшее расширение сферы действия института ответственности за нарушение специальных обязанностей. Наличие указанного института является необходимым условием реализации субъективных прав и свобод граждан, нормального функционирования общественных отношений в целом, эффективного и безопасного использования различных технических средств[2]. В этом отношении перспективным видится дополнение главы 28 УК РФ специальной нормой об ответственности за нарушение требований в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации.

Однако, процесс криминализации требует взвешенного подхода. Полагаем, что установление уголовной ответственности за уклонение от исполнения отдельных обязанностей лицами, ответственными за обеспечение безопасности объектов критической информационной инфраструктуры, может быть реализовано двумя способами: 1) путем построения соответствующего состава с административной преюдицией (в этом случае дополнения потребует и отечественный закон об административных правонарушениях); 2) посредством определения состава преступления с материальной конструкцией, включив в качестве криминообразующих при-

---

[1] [Электронный ресурс] // URL: https://sso.agc.gov.sg/Acts-Supp/9-2018/Published/20180312?DocDate=20180312 (дата обращения: 15.09.2020 г.).

[2] Уголовная ответственность за преступления, связанные с нарушением специальных правил: монография / Колл. Авт. Андрианов В.К., Боровиков В.Б., Мотин О.А. и др.; под ред. Ю.Е. Пудовочкина. М.: РГУП, 2018. С. 19.

знаков причинение крупного ущерба либо наступление тяжких последствий.

Согласимся, что в стремлении избежать декларативности отдельных положений закона о критической информационной инфраструктуре Российской Федерации, обеспечить их эффективным средством правового принуждения, не обязательно сразу прибегать к очередной модернизации УК РФ. Запретить под страхом ответственности не значит решить проблему государственно-частного партнерства в сфере обеспечения информационной безопасности. Несомненно одно – затронутая проблема нуждается в обстоятельной проработке и обсуждении профессиональным сообществом.

РАЗДЕЛ III. ЮРИДИЧЕСКИЙ АНАЛИЗ И ПРОБЛЕМЫ КВАЛИФИКАЦИИ «ЦИФРОВЫХ ПРЕСТУПЛЕНИЙ»

ГЛАВА 1. ЮРИДИЧЕСКИЙ АНАЛИЗ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ (КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ)

1.1. НЕПРАВОМЕРНЫЙ ДОСТУП К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ (СТ. 272 УК РФ)

Уголовно-правовой запрет неправомерного доступа является краеугольным пунктом в группе преступлений, посягающих на безопасность компьютерных данных и систем. Это своего рода протонорма – изначальный момент, отправная точка построения всей системы внутренне взаимосвязанных юридических конструкций (в нашем случае – уголовно-правовых норм о преступлениях в сфере компьютерной информации). Данный вывод подтверждается и тем обстоятельством, что во всех зарубежных странах независимо от фактически реализованной модели противодействия киберпреступности, изначальным вопросом криминализации всегда было установление ответственности именно за неправомерный доступ к защищённой компьютерной информации.

Вместе с тем, полагаем, что данные официальной статистики весьма неполно отражают реальное состояние проблемы. По ряду причин объективно-субъективного свойства подавляющее число компьютерных атак на ресурсы граждан и организаций попросту не отражается в системе учёта правоохранительных органов. Так, М. В. Старичков уровень

латентности преступлений, предусмотренных ст. 272 УК РФ, определяет на уровне 99,7%[1].

С. М. Иншаков на основе проведённого исследования определяет коэффициент латентности неправомерного доступа к компьютерной информации на уровне 4,8. При этом отмечается, что из данного количества латентных преступлений, от 70% до 80% не были заявлены потерпевшими, а от 30% до 20% процентов были укрыты. Прогнозируемое значение фактического количества преступных деяний на 2011 г. в исследовании оценивается от 47,2 тыс. до 52,3 тыс.[2]

Главным фактором гиперлатентности, пожалуй, выступает высокий уровень терпимости самих потерпевших, которые либо пытаются решить проблему утраты данных альтернативными способами (например, обращаясь за восстановлением аккаунта непосредственно к администраторам интернет-ресурса), либо не спешат заявлять об этом в полицию, поскольку не желают тратить собственное время на разбирательство, не верят в возможности правоохранительных органов по поимке злоумышленников, не желают огласки каких-либо компрометирующих сведений при исследовании предшествующей виртуальной активности самого потерпевшего в сети Интернет и др.

В отечественной доктрине уголовного права высказываются различные мнения относительно понимания объекта неправомерного доступа к компьютерной информации. Так, по мнению Т. Г. Смирновой, «непосредственным объектом преступлений в сфере компьютерной информации является часть информационных отношений, непосредственно связанных с операциями над компьютерной информацией, в частности общественные отношения по соблюдению и обеспечению требований безопасности, законных способов получения, обработки и использования компьютерной информации, а также нормального функционирования компьютерной техники»[3].

Похожим образом непосредственный объект компьютерных преступлений предлагает понимать Т. М. Лопатина: «общественные отношения, обеспечивающие: а) конфиденциальность охраняемой законом

---

[1] Старичков М. В. Умышленные преступления в сфере компьютерной информации: уголовно-правовая и криминологическая характеристики: дис. …канд.юрид.наук. Иркутск, 2006. С. 109-112.

[2] См.: Теоретические основы исследования и анализа латентной преступности: монография / под ред. С. М. Иншакова. М., 2011.

[3] Смирнова Т. Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации: дис. …канд. юрид. наук. М., 1998. С. 12.

компьютерной информации; б) безопасность компьютерной информации и компьютеров; в) безопасность эксплуатации ЭВМ или их сети»[1].

О. М. Сафонов непосредственный объект анализируемого преступления раскрывает как «совокупность общественных отношений в сфере информационной безопасности, связанных с реализацией прав собственника или иного законного владельца компьютерной информации по реализации своих полномочий в отношении данной информации, и защите её от неправомерного воздействия»[2].

О. С. Гузеева объектом преступления, предусмотренного ст. 272 УК РФ, называет общественные отношения, обеспечивающие правомерный доступ, создание, хранение, модификацию, использование компьютерной информации самим создателем, потребление её иными пользователями[3].

М. А. Ефремова определяет непосредственный объект анализируемого преступления как «общественные отношения, обеспечивающие безопасность процессов хранения, обработки, предоставления информации посредством средств вычислительной техники и информационно-телекоммуникационных сетей»[4].

В позициях О. С. Гузеевой и М. А. Ефремовой определённые возражения возникают в связи с использованием формулировки «обеспечивающих отношений». Как справедливо отмечает Г. П. Новоселов, понятие объекта преступления нередко увязывается не только с правовыми благами, охраняемыми законом интересами, субъективными правами и т.п., но и с такими общественными отношениями, которые либо что-то регулируют…, что-то обеспечивают… Подобного рода трактовка «непосредственного» объекта преступления породила конструкции, которые, хотя формально и не вступают в очевидное противоречие с исходным тезисом, явно имеют «налёт» искусственности и схоластичности и, самое главное, ничего не дают для практики применения уголовно-правовых норм[5].

При определении непосредственного объекта преступления, предусмотренного ст. 272 УК РФ, необходимо также учитывать изменения,

---

[1] Лопатина Т. М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности: дис. …д-ра юрид. наук. М., 2006. С. 197.

[2] Сафонов О. М. Уголовно-правовая оценка использования компьютерных технологий при совершении преступлений: состояние законодательства и правоприменительной практики, перспективы совершенствования: дис. …канд. юрид. наук. М., 2015. С. 83.

[3] Гузеева О. С. Квалификация преступлений в сфере компьютерной информации. М., 2016. С. 29.

[4] Ефремова М. А. Уголовно-правовая охрана информационной безопасности: автореф. дис. …д-ра юрид. наук. М., 2018. С. 47.

[5] Новоселов Г. П. Учение об объекте преступления. М., 2001. С. 24 – 25.

которые были внесены Федеральным законом от 07.12.2011 г. № 420-ФЗ. Как известно, из диспозиции ч. 1 ст. 272 УК РФ была исключена оговорка о нарушении работы ЭВМ, системы ЭВМ или их сети. Помимо отказа от использования ряда терминов, значимым (хотя и небесспорным) решением явилась декриминализация неправомерного доступа к компьютерной информации, повлёкшего нарушение нормального функционирования средств автоматизированной обработки данных. Таким образом, отношения, складывающие в связи и по поводу функционирования средств автоматизированной обработки компьютерной информации, как бы выпали из сферы охранительного действия уголовно-правовой нормы об ответственности за неправомерный доступ к компьютерной информации.

В связи с этим, полагаем, что с учётом действующей редакции ст. 272 УК РФ, объектом анализируемого преступления выступают исключительно *общественные отношения, возникающие в связи и по поводу хранения, использования, обработки и передачи охраняемой законом компьютерной информации.*

Другим дискуссионным вопросом является наличие специфического предмета посягательства при неправомерном доступе к компьютерной информации. По мнению В. С. Комиссарова, компьютерная информация не может рассматриваться в качестве предмета преступления. Аргументация автора главным образом заключается в том, что информация не отвечает одному из основных признаков предмета преступления – «не обладает физическим признаком, не объективирована в конкретно осязаемой форме»[1]. Похожую позицию занимает А. Н. Ягудин, указывая, что компьютерная информация не является вещью материального мира[2].

В свою очередь Р. М. Айсанов пишет, что предметом преступления, предусмотренного ст. 272 УК РФ, является не только компьютерная информация, но и компьютерные микросхемы и *компьютерные услуги* (выделено мной – *Е. Р.*)[3]. К. Н. Евдокимов также полагает, что предметом анализируемого преступления является компьютерная информация[4].

---

[1] См.: Уголовное право. Особенная часть: учебник / под ред. А. И. Рарога. М., 2009. С. 209.

[2] Ягудин А. Н. Уголовная ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей: дис. …канд. юрид. наук. М., 2013. С. 47.

[3] Айсанов Р. М. Состав неправомерного доступа к компьютерной информации в российском, международном и зарубежном уголовном законодательстве: автореф. дис. …канд. юрид. наук. М., 2006. С. 7.

[4] Евдокимов К. Н. Проблемы квалификации и предупреждения компьютерных преступлений. Иркутск, 2009. С. 47.

М. А. Ефремова занимает тождественную позицию, однако предлагает заменить термин «компьютерная информация» на «электронная информация»[1].

В отечественной теории уголовного права высказывались прямо противоположные мнения о содержании предмета преступления в целом. Так, Н. А. Беляев таковым считал любой из элементов общественного отношения, охраняемого уголовным законом, вне зависимости от того, материальный он или идеальный. Вещи, лица, а также их деятельность могут выступать в качестве предмета преступления. На этом основании автор утверждал, что беспредметных преступлений не существует, так как невозможно совершить посягательство на общественное отношение без воздействия на его элементы. Различие заключается лишь в том, что в некоторых составах предмет введён в качестве обязательного признака, а в других только подразумевается[2].

Со временем господствующей позицией всё же стало определение предмета именно как вещи, существующей в материальном мире, противоположной нематериальным элементам охраняемого общественного отношения[3].

Такая концепция предмета преступления, по большому счёту, была пригодна для XX века. Экспансивное развитие компьютерных технологий в 2000-е вызвало появление цифровых «сущностей», которые стали выражать социально значимые отношения между субъектами, не обладая при этом материальной (овеществлённой) природой. Как справедливо пишет Ю. Е. Пудовочкин, потребности сегодняшнего дня настоятельно требуют отказаться от ставшего догмой понимания предмета только и исключительно как вещи (предмета материального мира)[4]. Таким образом, нематериальный характер компьютерной информации, как представляется, не может выступать веским аргументом в пользу отрицания возможности её рассмотрения в качестве предмета неправомерного доступа по смыслу ст. 272 УК РФ.

---

[1] Ефремова М. А. Уголовно-правовая охрана информационной безопасности: автореф. дис. …д-ра юрид. наук. М., 2018. С. 47.

[2] Курс советского уголовного права. Часть общая / под ред. Н. А. Беляева, М. Д. Шаргородского. Л., 1968. С. 303 – 305.

[3] См., например: Загородников Н. И. Советское уголовное право. М., 1975. С. 56 – 58; Кравцов С. Ф. Предмет преступления: автореф. дис. …канд. юрид. наук. Л., 1976. С. 8; Наумов А. В. Российское уголовное право: курс лекций. В 3 т. Т.1. Общая часть. 4-е изд., перераб и доп. М., 2007. С. 310.

[4] Пудовочкин Ю. Е. Учение о составе преступления. Учебное пособие. М., 2009. С. 61.

Более прикладным значением обладает вопрос о том, что следует понимать под «охраняемой законом информацией»[1]. В теории уголовного права нет единства мнения относительно ответа на него. Так, высказана та точка зрения, что неправомерный доступ к компьютерной информации имеет место при обращении к любой информации вопреки воли её владельца[2], а предметом анализируемого преступления является компьютерная информация, в отношении которой собственник явным образом объявил об ограничениях по её использованию[3].

Вместе с тем всё большее распространение стала получать позиция, согласно которой под «охраняемой законом информацией» следует понимать лишь закрытую информацию, к которой относятся государственная, служебная, коммерческая, банковская, врачебная, нотариальная, адвокатская тайны, персональные данные и т.д.[4] В Методических рекомендациях Генеральной прокуратуры Российской Федерации, в частности, указано, что по смыслу ст. 272 УК РФ охраняемой законом информацией являются лишь сведения, в отношении которых установлен специальный режим правовой защиты (например, государственная, служебная и коммерческая тайна, персональные данные и т.д.)[5].

Отсутствие общепринятого толкования термина «охраняемая законом информации» закономерно обусловило неоднообразную практику применения ст. 272 УК РФ. Отдельные суды, придерживаясь рекомендаций Генеральной прокуратуры РФ, указывают, что неправомерные манипуляции с открытой (общедоступной) информацией не подпадают под действие данной статьи. Так, отменяя обвинительный приговор, вышестоящий суд указал: «…по смыслу закона под охраняемой законом понимается информация, для которой установлен специальный режим её правовой защиты… то есть информация ограниченного доступа… При этом судом сделаны выводы, что указанная информация (новости, советы

---

[1] Следует отметить, что законодательства ряда стран используют более общую категорию – «информация, хранящаяся в компьютерной системе, сети или на машинных носителях». См., например: Швед Н. А. Неправомерный доступ к компьютерной информации: уголовно-правовая защита в РФ и Республике Беларусь // Информационное право. 2016. № 2. С. 32.

[2] См.: Доронин А. М. Уголовная ответственность за неправомерный доступ к компьютерной информации: автореф. дис. …канд. юрид. наук. М., 2003. С. 6.

[3] Малышенко Д. Г. Уголовная ответственность за неправомерный доступ к компьютерной информации: дис. …канд. юрид. наук. М., 2002. С. 58.

[4] См.: Гузеева О. С. Квалификация преступлений в сфере компьютерной информации. М., 2016. С 30.

[5] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации // СПС «КонсультантПлюс».

логопеда, психолога и т.п.) охраняется законом – статьёй 6 Федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»… Однако данные выводы противоречат содержанию вышеуказанных законодательных актов Российской Федерации… Информация на сайте, в редактировании и удалении которой признана виновной К., является общедоступной информацией, к которой относятся общеизвестные сведения и для которой отсутствует необходимость установления специального режима её правовой защиты… Указанное закреплено и в пунктах 1.7 и 3.2 Положения о сайте МБДОУ «1», утверждённого приказом заведующей учреждения, согласно которому информационный ресурс сайта является открытым и общедоступным, информация на сайте является открытой и общедоступной, если иное не определено специальными документами. При этом таковых в материалах уголовного дела не имеется»[1].

Можно, однако, найти многочисленные примеры применения ст. 272 УК РФ при оценке действий, связанных с неправомерным доступом к общедоступной информации, хранящейся в сети Интернет. Так, С., прекратив свою трудовую деятельность в организации, в которой занимал должность генерального директора, и утратив в связи с этим право доступа к учётной записи администратора сайта, принадлежащего организации и используемого в деловых и маркетинговых целях, испытывая неприязненное отношение к руководству, желая опорочить деловую репутацию юридического лица, умышленно уничтожил и модифицировал часть компьютерной информации: изменил изображение слайдера, удалив исходные изображения, но добавив другие изображения, порочащие деловую репутацию организации, удалил контактный телефон и сведения об имеющихся сертификатах, изменил сведения о производстве и качестве сырья, удалил информацию о партнёрах, экологической безопасности продукции и т.д.[2]

Другим примером может послужить дело в отношении А., который, располагая сведениями о логине и пароле администратора сайта образовательного учреждения, из любопытства и желания проверить навыки владения компьютерными программами, удалил имеющуюся на указанном сайте информацию, заменив графическим изображением чёрного флага с арабской вязью, то есть совершил уничтожение и модификацию общедоступной информации на официальной странице организации в сети Интернет[3].

---

[1] Апелляционный приговор Судебной коллегии по уголовным делам Верховного суда Чувашской Республики от 3 июня 2015 года по делу № 22-1054/2015.

[2] Приговор Октябрьского районного суда г. Архангельска от 14 декабря 2015 года по делу № 1-352/2015.

[3] Приговор Волжского городского суда Волгоградской области от 17 ноября 2016 года по делу № 1-1105/2016.

Принимая подобные решения, суды, как правило, ссылаются на то обстоятельство, что виновное лицо осуществило неправомерное уничтожение, модификацию или блокирование общедоступной информации, охраняемой Федеральным законом № 149-ФЗ от 27 июля 2006 года «Об информации, информационных технологиях и о защите информации».

Согласно ст. 16 данного закона защита информации представляет собой принятие правовых, организационных и технических мер, направленных на: 1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации; 2) соблюдение конфиденциальности информации ограниченного доступа; 3) реализацию права на доступ к информации. При этом в соответствии с ч. 3 ст. 6 указанного закона обладатель информации, если иное не предусмотрено федеральными законами, вправе разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа.

Нельзя не отметить, что данные положения в целом корреспондируют Рекомендациям по стандартизации, разработанным Государственным научно-исследовательским испытательным институтом проблем технической защиты информации Гостехкомиссии России, определяющим безопасность информации как состояние защищённости информации, при котором обеспечивается её конфиденциальность, доступность и целостность[1].

Общедоступная информация отнюдь не является информацией, лишённой защиты. Положения об обязательном характере технологической и программной защиты общедоступной информации, размещаемой в сети Интернет, содержатся во многих подзаконных нормативно-правовых актах. Так, в соответствии с Приказом Минкомсвязи России от 27.06.2013 года «Об утверждении Требований к технологическим, программным и лингвистическим средствам, необходимым для размещения информации государственными органами и органами и местного самоуправления в сети Интернет в форме открытых данных, а также для обеспечения её использования»[2] общедоступная информация, размещаемая на сайте в форме открытых данных, должна быть защищена от уничтожения, модификации, блокирования, а также от иных неправомерных действий в отношении такой информации. Аналогичное требование предусмотрено постановлением Правительства РФ от 10.07.2013 года № 582 «Об

[1] Рекомендации по стандартизации Р 50.1.053-2005 «Информационные технологии. Основные термины и определения в области технической защиты информации» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 6 апреля 2005 г. № 77-ст).

[2] Российская газета. № 187, 23.08.2013.

утверждении Правил размещения на официальном сайте образовательной организации информационно-телекоммуникационной сети Интернет и обновления информации об образовательной организации»[1].

Таким образом, положения ст. 6 и ст. 16 Федерального закона № 149-ФЗ от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации» в своей взаимосвязи позволяют сделать вывод о том, что по смыслу ст. 272 УК РФ к «охраняемой законом информации» следует относить не только информацию ограниченного доступа, но и общедоступную информацию, в отношении которой её обладателем приняты меры по защите от несанкционированного уничтожения, модификации, блокирования или копирования.

Более того, с точки зрения отечественного учения об объекте преступления конфиденциальная информация должна прежде всего охраняться специальными нормами и в рамках тех разделов, которые выражают связь такой информации с тем или иным родовым объектом. Информационная безопасность при посягательствах на конфиденциальную компьютерную информацию, конечно же, тоже страдает, однако она далеко не выражает направленность и сущность таких деяний. В связи с этим позволим себе обосновать вывод, что *само наличие ст. 272 УК РФ обусловлено необходимостью надлежащей уголовно-правовой охраны защищённой владельцем, но общедоступной информации, в целях обеспечения таких её свойств как целостность и доступность.*

Объективная сторона преступления выражается в неправомерном доступе к компьютерной информации. При этом его способы могут быть самыми разнообразными и, как правило, не влияют на юридическую оценку поведения виновного лица. Весьма удачную систематизацию способов неправомерного доступа к компьютерной информации приводит А. Г. Волеводз, выделяя: «1) использование специальных технических или аппаратно-программных средств, позволяющих преодолеть установленные системы защиты; 2) незаконное использование действующих паролей или кодов для проникновения в компьютер либо совершение иных действий в целях проникновения в систему или сеть под видом законного пользователя; 3) хищение носителей машинной информации при условии, что были приняты меры к их охране, если это деяние повлекло уничтожение или блокирование информации»[2].

Приведённый перечень, конечно же, не раскрывает всего многообразия форм осуществления неправомерного доступа. Таковым, в частности, следует признавать и совершение неправомерных действий в отношении компьютерной информации лицом, которое попросту воспользовалось

---

[1] Собрание законодательства РФ, 22.07.2013. № 29, ст. 3964.

[2] Волеводз А. Г. Противодействие компьютерным преступлениям. М., 2002. С. 61.

временным отсутствием законного владельца включённого компьютера в кафе или ином общественном месте.

Следовательно, неправомерный доступ это не всегда «проникновение», сопряжённое с преодолением программно-технической защиты информации, как о том пишут отдельные авторы[1]. Нельзя его раскрывать и как «ознакомление»[2] с компьютерной информацией, поскольку это деяние является самостоятельным и последующим за доступом.

В самом обобщённом виде неправомерный доступ к компьютерной информации следует определить как *совершение любых высокотехнологичных либо примитивно-бытовых действий, предоставляющих лицу возможность распоряжения информацией (её уничтожения, модификации, блокирования, копирования) по собственному усмотрению без согласия на то законного владельца.*

В теории уголовного права непрестанно подчёркивается, что воздействие на внешнюю оболочку хранения компьютерной информации (повреждение или уничтожение компьютера, внешних дисков и т.п.) не подпадает под признаки неправомерного доступа и требует квалификации по уголовно-правовым нормам об ответственности за посягательства на собственность. Например, М. А. Ефремова пишет, что «…уничтожение компьютера в физическом смысле, в результате чего утрачивается компьютерная информация, должно быть квалифицировано как преступление против собственности»[3].

Вместе с тем, представим себе ситуацию, когда лицо умышленно завладевает и уничтожает USB-диск, однако главной целью этого деяния являлось не причинение материального ущерба потерпевшему (следует отметить, весьма незначительного), а определённой информации. Очевидно, что в данном случае злоумышленник направляет свои усилия на причинение вреда прежде всего отношениям в сфере законного оборота информации. В условиях удешевления компьютерного оборудования, мобильных телефонов и внешних накопителей информации потерпевший, как правило, выражает недовольство не в связи с имущественным ущербом, а ввиду невосполнимой утраты важной информации (списка контактов, клиентской базы, текста дипломной работы, диссертации), которая по своей ценности

---

[1] См.: Воробьев В. В. Особенности квалификации преступлений в сфере компьютерной информации // Российское право в период социальных реформ. Н. Новгород, 1998. С. 70; Малышенко Д. Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации: дис. …канд. юрид. наук. М., 1998. С. 63.

[2] Дворецкий М. Ю. Преступления в сфере компьютерной информации (уголовно-правовое исследование): дис. …канд. юрид. наук. Волгоград, 2001. С. 72

[3] Ефремова М. А. Уголовная-ответственность за преступления, совершаемые с использованием информационно-телекоммуникационных технологий. М., 2015. С. 86.

может в несколько раз превосходить стоимость того носителя, на котором она хранилась.

Рассмотрим ещё один пример. Преступник похищает ноутбук, находясь у себя дома, включает его и удаляет всю информацию прежнего владельца. За исключением неизвестных автору примеров, практика до настоящего времени сконцентрирована на оценке подобного рода действий исключительно как хищения в той или иной форме, оставляя без надлежащей квалификации тот ущерб, который был причинён общественным отношениям в сфере обеспечения информационной безопасности.

Сомнительность квалификации посягательств на объекты информационно-коммуникационной инфраструктуры только лишь как преступлений против собственности частично подтверждается и обоснованными в науке уголовного права правилами квалификации иных преступлений. Так, как известно, убийство, совершённое путем поджога жилища, Пленум Верховного Суда РФ в своём постановлении «О судебной практике по делам об убийстве (ст. 105 УК РФ)» от 27 января 1999 года № 1 предлагает квалифицировать не только по ст. 105 УК РФ, но и по ч. 2 ст. 167 УК РФ.

Чтобы разобраться в обозначенной проблеме, нельзя не обратиться и к наработкам общей теории уголовного права о так называемых негативных признаках совокупности. Считается, что совокупность преступлений отсутствует, если: 1) совершение двух или более преступлений предусмотрено статьями Особенной части УК РФ в качестве обстоятельства, влекущего более строгое наказание; 2) совершенное деяние одновременно подпадает под признаки составов преступлений, предусмотренных общей и специальной нормами; 3) совершенные лицом деяния образуют последовательно выполненные стадии одного и того же преступления; 4) имеются признаки единого сложного преступления (продолжаемого, составного, с альтернативными действиями и т.д.); 5) при «перерастании» преступления в более тяжкое преступление[1].

Последовательный анализ приведённых обстоятельств позволяет констатировать, что они отсутствуют в случаях совершения лицом деяния, связанного с уничтожением носителя охраняемой законом компьютерной информации, или его хищения с последующим удалением компьютерных данных.

Как представляется, имеющиеся стандарты юридической оценки посягательств на средства хранения, обработки или передачи компьютерной информации к сегодняшнему дню оказываются в значительной части малопригодными и требуют корректировки.

---

[1] Совокупность преступлений: проблемы теории и практики квалификации. Монография / Под ред. Ю. Е. Пудовочкина. М., 2016. С. 92 – 101.

В связи с этим полагаем, что *наряду с традиционными способами, под неправомерным доступом к компьютерной информации следует понимать посягательства на средства её хранения, обработки или передачи. При этом подобного рода деяния необходимо квалифицировать по соответствующим статьям УК РФ об ответственности за посягательства на собственность и по ст. 272 УК РФ.*

Следует, конечно же, оговориться, что применение ст. 272 УК РФ к ситуациям уничтожения компьютерных данных посредством воздействия на цифровой носитель или средство обработки информации, не является идеальным решением и во многом обусловлено современным состоянием отечественного уголовного законодательства. В данном аспекте глава 28 УК РФ остро нуждается в выделении специальной нормы, о чём еще будет сказано в заключительном параграфе настоящей главы.

Отдельного рассмотрения требует также признак «неправомерности» доступа к охраняемой законом компьютерной информации. Следует согласиться с мнением В. С. Карпова, который указывает, что «доступ будет являться неправомерным, если: 1) лицо не имеет права на доступ к компьютерной информации; 2) лицо имеет право на доступ к данной информации, однако осуществляет его помимо установленного порядка, с нарушением правил её защиты»[1].

Использование лицом своих служебных или профессиональных полномочий отнюдь не исключает возможности признания доступа к компьютерной информации неправомерным. Это объясняется тем, что право лица на доступ к информационной базе данных носит не общий характер, а возникает только в связи с строго определёнными (нормативно регламентированными) основаниями[2]. Такое расширительное толкование признака «неправомерности» при доступе к защищённым информационным базам находит свою поддержку и на уровне

---

[1] Карпов В. С. Уголовная ответственность за преступления в сфере компьютерной информации: дис. …канд. юрид. наук. Красноярск, 2002. С. 87.

[2] Так, например, приказом МВД России № 1144 от 03.12.2007 г. «О системе информационного обеспечения Госавтоинспекции» утверждены «Наставления по организации формирования и ведения специализированных учётов федеральной специализированной территориально распределённой информационной системы Госавтоинспекции». В соответствии с п. 2.4 указанных наставлений специализированный федеральный учёт лиц, привлечённых к административной ответственности за нарушения правил дорожного движения (АИПС «Адмпрактика»), формируется на основе сведений, поступающих из подразделений Госавтоинспекции органов внутренних дел в районах, городах и иных муниципальных образованиях. Основанием для постановки на региональный учёт является оформление соответствующего протокола об административных правонарушениях в области обеспечения безопасности дорожного движения (п.9.1).

правоприменения. Так, по одному из дел суд отметил, что «…действия виновного по внесению заведомо ложных сведений об уплате штрафа, несоответствующих действительности, непосредственно связаны с осуществлением им своих прав и обязанностей, которые не вызывались служебной необходимостью и объективно противоречили как общим задачам и требованиям, предъявляемым к государственному аппарату, так и тем целям и задачам, для достижения которых виновный, как должностное лицо было наделено соответствующими должностными полномочиями»[1].

В другом решении суд, применив ч. 3 ст. 272 УК РФ, обоснованно указал, что наличие у виновного официального доступа к служебной базе данных само по себе не исключает возможности его осуждения по ст. 272 УК РФ, поскольку им совершены незаконные действия, связанные с неправомерным доступом к компьютерной информации, имевшие целью сокрытие ранее совершённого должностного преступления, а также направленные на избежание лицом, совершившим административное правонарушение, исполнения назначенного судебным решением наказания[2].

В отечественной теории уголовного права почти аксиоматичным является положение о материальной конструкции состава преступления, предусмотренного ст. 272 УК РФ. Отмечается, что преступление считается оконченным с момента наступления хотя бы одного из альтернативных общественно опасных последствий: уничтожения, блокирования, модификации либо копирования компьютерной информации[3].

Нетрадиционное видение на конструкцию неправомерного доступа к компьютерной информации демонстрирует О. М. Сафонов, указывая, что состав является формально-материальным, поскольку «для квалификации деяния по ст. 272 УК РФ необходимо наступление последствий в виде уничтожения, блокирования, модификации либо копирования компьютерной информации, либо угроза их наступления»[4].

Как представляется, с данным утверждением автора согласиться нельзя – современная редакция диспозиции ст. 272 УК РФ не содержит указания на «угрозу наступления» соответствующих последствий. Более того, такое

---

[1] Приговор Первомайского суда г. Кирова от 09 сентября 2016 года по делу № 1-222/2016.

[2] Приговор Катайского районного суда Курганской области от 18 апреля 2013 года по делу № 1-20/2013.

[3] Ефремова М. А. Уголовно-правовая охрана информационной безопасности: дис. …д-ра юрид. наук. М., 2018. С. 339.

[4] Сафонов О. М. Уголовно-правовая оценка использования компьютерных технологий при совершении преступлений: состояние законодательства и правоприменительной практики, перспективы совершенствования: дис. …канд. юрид. наук. М., 2015. С. 83.

расширительное толкование существенно влияет на пределы уголовной репрессии и грозит нарушением прав и законных интересов граждан, поскольку позволяет правоприменителю произвольно без прямого указания на то в законе решать вопрос об угрозе наступления негативных последствий для информации и, следовательно, наличии либо отсутствии признаков состава неправомерного доступа. Даже если допустить мысль о том, что О. М. Сафонов тем самым пытался обосновать возможность уголовного преследования за так называемое «чистое хакерство» – взлом компьютерной системы без последствий для самих данных, предложенная модель, связанная с «растягиванием» диспозиции ст. 272 УК РФ, является абсолютно неприемлемой в силу требований ст. 3 УК РФ.

В. В. Челноков отмечает, что указание в законе на несанкционированное уничтожение, блокирование, модификацию или копирование компьютерной информации является не совсем правильным. По мнению автора, таковыми следует считать значительный ущерб и (или) существенный вреда правам и законным интересам граждан или организаций либо охраняемым законом интересам общества или государства. В связи с этим автор предлагает внести соответствующие изменения в редакцию ст. 272 УК РФ[1].

Использование таких оценочных признаков для определения последствий неправомерного доступа к компьютерной информации вряд ли следует признать обоснованным. В отечественной доктрине уголовного права нет общепринятого толкования «существенности» нарушения или вреда, что закономерно порождает неоднозначную правоприменительную практику, когда тождественные по-сути деяния получают разную правовую оценку.

Уничтожение, как последствие неправомерного доступа к охраняемой законом компьютерной информацией, в отечественной науке уголовного права понимается по-разному. Так, А. Ю. Чупрова пишет, что необходимо разделять удаление информации и её уничтожение. При удалении происходит сокрытие информации, при котором применение специальных методов позволяет эти данные восстановить. В свою очередь при уничтожении информация восстановлению не подлежит[2]. Таким образом, для А. Ю. Чупровой уничтожением информации являются только такие последствия, когда компьютерные данные окончательно (бесповоротно) утрачены, то есть перестали существовать в какой-либо форме – ни потерпевший, ни провайдер, ни сам злоумышленник не обладает реальной возможностью по их восстановлению.

---

[1] Челноков В. В. Компьютерная информация как предмет преступления в отечественном уголовном праве: дис. …канд. юрид. наук. Екатеринбург, 2013. С. 11.

[2] Чупрова А. Ю. Проблемы квалификации мошенничества с использованием информационных технологий // Уголовное право. 2015. № 5. С. 133.

Принципиально другую позицию занимает М. А. Ефремова. Она пишет, что «уничтожением компьютерной информации следует считать её *удаление* (выделено мной – *Е. Р.*) из памяти компьютера или электронного носителя, когда доступ к ней законного пользователя или владельца невозможен, независимо от возможности её восстановления»[1].

Полагаем, что более предпочтительным является подход М. А. Ефремовой. Природа «уничтожения» компьютерной информации определяется отнюдь не возможностью/невозможностью её восстановления, а фактическим содержанием тех действий, которые были совершены виновным, – если злоумышленник задействовал команды по стиранию информации с электронного носителя, то налицо её уничтожение.

Следует дополнительно отметить, что позиция А. Ю. Чупровой несовершенна тем, что она допускает смешение «уничтожения» и «блокирования» информации. Если строго следовать её интерпретации, удаление информации злоумышленником с компьютера потерпевшего, связанное с предварительным сохранением её копии, необходимо оценивать как особую форму блокирования, что по ряду причин не выдерживает критики.

Развёрнутое определение блокированию компьютерной информации даёт Д. Г. Малышенко, определяя его как: «полную или частичную невозможность доступа и обработки компьютерной информации со стороны её легальных пользователей или владельца, явившуюся результатом несанкционированного воздействия на аппаратное или программное обеспечение вычислительной машины, независимо от продолжительности промежутка времени, в течение которого она отмечалась»[2].

Принципиальным признаком блокирования компьютерной информации, на наш взгляд, является то, что информация остаётся на исходном электронном носителе и сама по себе не подвергается деструктивному воздействию. При блокировании информации потерпевший теряет доступ к ней и не более того. В связи с этим правильнее было бы говорить о том, что при «блокировании» имеют место не деструктивные последствия для информации, а существенное нарушение нормального функционирования средств хранения, обработки или передачи компьютерной информации, в результате которого законный владелец информации теряет к ней доступ.

Закрытие доступа к информационным ресурсам (блокирование), как правило, наступает в результате изменения так называемых сетевых идентификаторов пользователя – логина и пароля. Так, например, М.,

---

[1] Ефремова М. А. Уголовно-правовая охрана информационной безопасности: дис. …д-ра юрид. наук. М., 2018. С. 339.

[2] Малышенко Д. Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации: дис. …канд. юрид. наук. М., 1998. С. 73.

действуя умышленно, из корыстной заинтересованности, используя свой персональный компьютер с установленной операционной системой, предоставляющей доступ в сеть Интернет, посредством интернет-соединения зашёл в сеть Интернет на сайт, после чего, продолжая свои преступные действия, ввёл учётные данные электронного почтового ящика: логин и неустановленный следствием пароль, ставшие известными М. от неустановленного следствием лица, и вошёл в личный кабинет пользователя Е. Продолжая реализовывать свои преступные намерения, действуя умышленно, из корыстных побуждений, М. изменил неустановленный следствием пароль в личном кабинете электронного почтового ящика, внесённый Е. и используемый им при работе в личном кабинете, на неустановленный следствием пароль, заблокировав таким образом доступ в личный кабинет электронного почтового ящика легального пользователя Е.[1]

Следующим альтернативным последствием неправомерного доступа к охраняемой законом компьютерной информацией является её модификация. Т. Л. Тропина под модификацией понимает «несанкционированное умышленное изменение компьютерной информации, а равно внесение в неё заведомо ложных данных при отсутствии признаков хищения чужого имущества или незаконного приобретения права на чужое имущество»[2]. Как нетрудно заметить, автор раскрывая модификацию компьютерной информации, включает в неё и признак субъективной стороны – умышленный характер воздействия на информацию.

В. В. Хилюта определяет модификацию компьютерной информации как внесение в компьютерную информацию любых изменений, которые обусловят ее отличие от ранее хранившейся в компьютерной сети, системе или на машинном носителе собственника информационного ресурса[3].

В целом с данным определением можно согласиться. Модификация, в отличие от уничтожения, предполагает некое реструктурирование информации, внесение или удаление записей, содержащихся в файлах и т.д.

Нельзя полностью согласиться с категоричным утверждением М. А. Ефремовой, что «масштабы модификации на квалификацию не влияют, поэтому для привлечения к ответственности формально достаточно

---

[1] Постановление Советского районного суда г. Нижнего Новгорода по делу № 1-112/2017.

[2] Тропина Т. Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: автореф. дис. …канд. юрид. наук. Владивосток, 2005. С. 12.

[3] Хилюта В. В. Вопросы квалификации преступлений против собственности не являющихся хищением: монография. Минск, 2013. С. 33.

изменения значения одного байта информации»[1]. Несанкционированная корректировка крайне небольших объёмов компьютерной информации требует рассмотрения вопроса о признании такого деяния малозначительным (ч. 2 ст. 14 УК РФ).

Копирование информации в теории уголовного права раскрывается как «изготовление одного или более (точных или относительно точных) дубликатов оригинала информации с переносом её на другой машинный носитель информации»[2]. При этом Д. Г. Малышенко подчёркивает, что способы копирования информации для квалификации значения не имеют[3].

С данной позицией соглашается М. А. Ефремова, указывая, что «копирование файла на дискету или чтение информации с экрана монитора с одновременной записью на бумагу могут наносить совершенно одинаковый вред собственнику информационных ресурсов»[4].

Такой подход находит своё подтверждение и в материалах судебно-следственной практики. Так, у А. после увольнения в июле 2015 года из корыстной заинтересованности возник умысел, направленный на осуществление неправомерного доступа к охраняемой законом компьютерной информации, находящейся в личном кабинете на сайте коммерческой организации. Реализуя задуманное, находясь в помещении офиса, применяя персональный компьютер, посредством сети Интернет, используя учётную запись и пароль, для доступа в систему, предоставленные ей ранее в период её работы в этой организации, осуществила неправомерный доступ к личному кабинету и находящейся в нём охраняемой законом компьютерной информации, содержащей данные о клиентах. Одновременно, путём создания изображения на своём персональном компьютере («скриншота») и печати на бумажный носитель, осуществила копирование данных о 1135 клиентах, заключивших кредитные договоры, договоры возмездного оказания услуг, купли-продажи, их паспортные данные, номера телефонов и др.[5]

---

[1] Ефремова М. А. Уголовная-ответственность за преступления, совершаемые с использованием информационно-телекоммуникационных технологий. М., 2015. С. 94.

[2] См.: Воробьев В. В. Особенности квалификации преступлений в сфере компьютерной информации // Российское право в период социальных реформ. Н. Новгород, 1998. С. 88.

[3] Малышенко Д. Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации: дис. …канд. юрид. наук. М., 1998. С. 78.

[4] Ефремова М. А. Уголовная-ответственность за преступления, совершаемые с использованием информационно-телекоммуникационных технологий. М., 2015. С. 96.

[5] Приговор Кировского районного суда г. Саратова от 10 февраля 2016 г. по делу № 1-39/2016.

Обязательным признаком объективной стороны преступления является и причинная связь между действиями лица, заключающимися в неправомерном доступе к компьютерной информации, и наступившими вредными последствиями, прямо указанными в диспозиции статьи. При этом отдельного пояснения требует позиция, согласно которой, если в силу настроек компьютерной программы при работе с ней, пусть даже и в результате неправомерного доступа, автоматически создаётся резервная копия компьютерной информации, то данное действие не будет иметь уголовно-правовых последствий, поскольку оно осуществляется независимо от волеизъявления лица и, соответственно, в прямой причинной связи с его действиями не состоит[1].

Сомнительно утверждать об отсутствии в такой ситуации причинно-следственной связи между действиями лица и наступившими общественно опасными последствиями в виде копирования охраняемой законом компьютерной информации. Думается, что такая связь объективно имеется. С другой стороны неосведомлённость лица об особенностях настроек программы фактически исключает вину по отношению к копированию информации. На наш взгляд, именно по этой причине и следует утверждать об отсутствии уголовно-правовых последствий за содеянное.

Субъектом основного состава преступления является физическое, вменяемое лицо, достигшее шестнадцатилетнего возраста и не наделённое в силу характера выполняемой работы полномочиями доступа к компьютерной информации.

Несмотря на то, что диспозиция рассматриваемой статьи не даёт прямых указаний относительно субъективной стороны преступления, можно с уверенностью говорить об умышленной форме вины в виде прямого или косвенного умысла. В связи с этим представляется дискуссионным мнение, что субъективная сторона рассматриваемого преступления характеризуется виной в форме умысла (прямого или косвенного) или неосторожности[2].

Мотивы и цели неправомерного доступа к компьютерной информации могут быть весьма разнообразными. Анализируемое преступление может совершаться из мести, зависти, хулиганства, «спортивного интереса», желания подорвать деловую репутацию конкурента и т.д. Обязательными признаками состава преступления они не являются и, следовательно, решающего значения для квалификации не имеют. Между тем их точное установление позволит не только выявить причины, побудившие лицо

---

[1] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации [Электронный ресурс] // Режим доступа: СПС «Консультант-Плюс».

[2] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации [Электронный ресурс] // Режим доступа: СПС «Консультант-Плюс».

совершить подобное преступление, но и назначить ему справедливое наказание.

Следует отметить, что проблема с установлением субъективной стороны преступления может возникнуть в случае доступа к компьютерной информации лицом, добросовестно полагающим, что владелец информации санкционировал либо не возражает против таких действий. Например, мать воспользовалась аккаунтом совершеннолетней дочери, которая ранее неоднократно разрешала ей пользоваться соответствующим интернет-ресурсом. Подобная извинительная ошибка при наличии на то объективных обстоятельств, конечно же, исключает вину и, следовательно, говорить о возможности привлечения лица к уголовной ответственности нельзя.

Непростым является вопрос относительно квалификации действий лица, выполнявшего незаконные манипуляции с компьютерной информацией по указанию (заданию) своего непосредственного руководителя (например, по распоряжению начальника рядовой системный администратор организации производит корректировку служебных баз данных). На наш взгляд, квалифицировать такие действия подчинённого необходимо с учётом разработанных в теории уголовного права правил квалификации преступлений при фактической ошибке относительно общественной опасности совершаемого деяния. В тех случаях, когда лицо добросовестно считало свои действия правомерными, не осознавая их общественной опасности, следует оценивать совершенное деяние как невиновное причинение вреда.

К квалифицирующим признакам, названным в ч. 2 ст. 272 УК РФ, относится совершение данного преступления с причинением крупного ущерба или из корыстной заинтересованности. В соответствии с примечанием к ст. 272 УК РФ ущерб признается крупным, если его сумма превышает один миллион рублей. С качественной стороны ущерб может выражаться как в прямых имущественных потерях обладателя информации (например, расходы, связанные с восстановлением уничтоженного или модифицированного программного обеспечения), так и в упущенной выгоде (например, недополученная прибыль в результате дезорганизации производственного процесса конкретного предприятия).

Корыстная заинтересованность при совершении данного преступления выражается в стремлении лица извлечь материальную выгоду из преступления для себя лично или других лиц. Так, например, сотрудниками управления «К» МВД России была пресечена деятельность группы, которая специализировалась на взломе аккаунтов в различных социальных сетях, почтовых серверах и web-сайтах. Необходимые для этих целей программы создавали как программисты из круга общения

злоумышленников, так и иные лица. За предоставление соответствующих сведений злоумышленники получали вознаграждение[1].

Часть 3 ст. 272 УК РФ предусматривает три особо квалифицирующих признака. Неправомерный доступ к охраняемой законом компьютерной информации, совершенный: группой лиц по предварительному сговору; организованной группой; лицом с использованием своего служебного положения.

Неправомерный доступ к компьютерной информации признается совершённым группой лиц по предварительному сговору, если в нем участвовали лица, заранее договорившиеся о совместном совершении этого преступления. Принципиальным следует считать положение о том, что каждый из образующих указанную группу лиц преступников должен сыграть роль соисполнителя. При наличии одного исполнителя и отсутствии иных квалифицирующих признаков этого преступления действия остальных его соучастников необходимо оценивать по ч. 1 ст. 272 УК РФ и соответствующей части ст. 33 УК РФ[2].

Современные информационные технологии все больше проникают в механизм государственного управления и деятельность хозяйствующих субъектов. Этот процесс обусловливает рост преступлений, связанных с различного рода злоупотреблениями при использовании служебных информационных ресурсов (программ, сетей, баз данных и т.п.). Анализ весьма противоречивой правоприменительной практики позволяет сделать вывод, что судебно-следственные органы испытывают определённые затруднения при толковании такого квалифицирующего признака ст. 272 УК РФ как совершение преступления «лицом с использованием своего служебного положения». Традиционное понимание данной категории лиц, как известно, отражено в п. 29 постановления Пленума Верховного Суда РФ от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», в соответствии с которым под ними следует понимать должностных лиц, обладающих признаками, предусмотренными п. 1 примечания к ст. 285 УК РФ, государственных или муниципальных служащих, не являющихся должностными лицами, а также иных лиц, отвечающих требованиям, предусмотренным п. 1 примечания к ст. 201 УК РФ (например, лицо, которое использует для совершения хищения чужого

---

[1] [Электронный ресурс] // Задержаны хакеры, взламывавшие по заказам страницы в соцсетях, почтовые ящики и занимавшиеся «прослушкой» // URL: https://мвд.рф/news/show_102385(дата обращения: 26.05.2018).

[2] Как известно, данная позиция нашла своё неоднократное подтверждение в решениях Верховного Суда Российской Федерации. См., например: постановление Президиума Верховного Суда РФ № 436п96 по делу Ткаченко В. П. и Хоперского В. В. // Бюллетень Верховного Суда РФ. 1997. № 4; постановление Президиума Верховного Суда РФ № 495п03 по делу Бычкало и других // Бюллетень Верховного Суда РФ. 2004. № 3 и др.

имущества свои служебные полномочия, включающие организационно-распорядительные или административно-хозяйственные обязанности в коммерческой организации)[1].

Вместе с тем, по другой категории дел Пленум Верховного Суда РФ демонстрирует более широкий взгляд на толкование «служебного положения» субъекта. Так, разъясняя положения п. «в» ч. 2 ст. 229 УК РФ, Пленум указывает, что такими субъектами являются не только должностные лица, но и другие, выполнение трудовых функций которых связано с работой с наркотическими средствами или психотропными веществами, а также растениями, содержащими наркотические средства или психотропные вещества, либо их частями, содержащими наркотические средства или психотропные вещества. Например, при изготовлении лекарственных препаратов таким лицом может являться провизор, лаборант, при отпуске и применении – работник аптеки, врач, медицинская сестра, при их охране – охранник, экспедитор[2].

В теории уголовного права высказываются предложения о переосмыслении подхода законодателя к определению круга лиц, использующих своё служебное положение для совершения преступных действий, путём расширения характеристик таких субъектов до пределов «иных служащих организаций независимо от формы собственности»[3].

Н. А. Лопашенко критически оценивает курс на включение в данную группу лиц наёмных работников организаций, не наделённых организационно-распорядительными или административно-хозяйственными функциями, отмечая, что нельзя расширять до бесконечности круг лиц, которые используют своё служебное положение[4].

Из этих же соображений П. С. Яни специально указывает, что возложенная на лицо обязанность производить перемещение имущества чисто технически (водитель – экспедитор – инкассатор, водитель бетономешалки, продавец) не означает наличия у него полномочий по распоряжению, управлению имуществом[5].

---

[1] Постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // СПС «Консультант-Плюс».

[2] Постановление Пленума Верховного Суда РФ от 15 июня 2006 г. № 14 «О судебной практике по делам о преступлениях, связанных с наркотическими средствами, психотропными, сильнодействующими и ядовитыми веществами» // СПС «Консультант-Плюс».

[3] Егорова Н. А. Ответственность за «служебные» мошенничества: необходимость новых подходов // Российская юстиция. 2014. № 8. С. 20.

[4] Лопашенко Н. А. Посягательства на собственность. М., 2012. С. 502.

[5] Яни П. С. Использование служебного положения при хищении вверенного имущества // Законность. 2010. № 3. С. 18.

Вместе с тем, в правоприменительной практике по делам о преступлениях в сфере компьютерной информации довольно распространённым является подход признания такими лицами рядовых специалистов по обслуживанию клиентов, имеющих доступ к охраняемой законом компьютерной информации в связи с осуществлением ими сугубо технических функций. Так, Р., являясь специалистом офиса обслуживания и продаж, используя индивидуальный и конфиденциальный логин и пароль, для работы в служебной компьютерной программе, содержащей данные клиентов компании и персональные данные их лицевых счетов, которые охраняются Федеральным законом РФ «Об информации, информационных технологиях и о защите информации», из корыстной заинтересованности, используя своё служебное положение, совершил неправомерный доступ к охраняемой законом компьютерной информации при следующих обстоятельствах. Р., используя своё служебное положение и возможность доступа к компьютерной информации, а именно персональным данным клиентов, реализуя преступный умысел, с целью незаконного обогащения, желая получить денежное вознаграждение от неустановленного лица за незаконные действия по замене сим-карты, посредством модуля по работе с клиентами (служебной программы), используя индивидуальный и конфиденциальный логин и пароль другого сотрудника, который в это время не находился на своём рабочем месте, не был осведомлён о его преступных намерениях и не разрешал последнему использовать его индивидуальный и конфиденциальный логин и пароль для работы в компьютерной программе, содержащей данные клиентов, достоверно зная, порядок и условия переоформления абонентских номеров, осуществил замену сим-карты, при этом неправомерно произвёл блокирование абонентского номера клиента[1].

По другому делу в качестве такого лица был признан дилер спутниковой компании, который осуществлял неправомерную модификацию смарт-карт организации. Согласно решению суда, З. незаконно модифицировал информацию на спутниковых смарт-картах, которые впоследствии продавал гражданам, желающим получать услуги спутникового телевидения. Суд апелляционной инстанции специально указал, что суд первой инстанции сделал правильный вывод, что З. совершил инкриминируемое преступления с использованием своего служебного положения. З. неправомерно модифицировал компьютерную информацию в связи с занимаемой должностью, поскольку, являясь дилером, имел специальный (авторизованный) доступ к служебной программе

[1] Приговор Ленинского районного суда г. Астрахани от 22 июня 2017 г. по делу № 1-334/2017.

спутниковой компании. Для этого ему не требовалось обладать признаками должностного лица[1].

В отдельных случаях обоснованность вменения использования лицом своего служебного положения по ч. 3 ст. 272 УК РФ становилась предметом самостоятельного разбирательства. Так, согласно приговору суда, И. признан виновным в неправомерном доступе к охраняемой законом компьютерной информации, повлёкшее копирование компьютерной информации, из корыстной заинтересованности, с использованием своего служебного положения. В апелляционном представлении прокурор просил изменить приговор в связи с неправильным применением уголовного закона, нарушением уголовно-процессуального закона, ссылаясь на то, что И., исходя из должностной инструкции, не был наделён организационно-распорядительными и административно-хозяйственными функциями в коммерческой организации, в связи с чем квалифицирующий признак «с использованием своего служебного положения» подлежит исключению из объёма обвинения. Суд, рассмотрев апелляционное представление, не согласился с мнением прокурора, указав, что под использованием служебного положения, предусмотренного в диспозиции ч. 3 ст. 272 УК РФ, понимается наличие у лица доступа к компьютерной информации в результате выполняемой работы (по трудовому, гражданско-правовому договору), то есть это лица, которые на законных основаниях используют компьютерную информацию и средства её обращения (программисты, администраторы баз данных, инженеры, специалисты). Таким образом, субъектом преступления, предусмотренного ч. 3 ст. 272 УК РФ по квалифицирующему признаку «с использованием служебного положения» не обязательно является только должностное лицо[2].

Однако, можно обнаружить примеры, когда судебно-следственные органы не признают наличие «служебного положения» при совершении компьютерного преступления работником организации. Так, например, Т. был осуждён по ч. 1 ст. 273 УК РФ. Согласно приговору суда, он, являясь системным администратором, имея доступ к компьютерной сети компании, находясь на своём рабочем месте, создал для последующего распространения компьютерную программу, заведомо предназначенную для несанкционированного уничтожения компьютерной программы – программного продукта «wget.bat», отвечающего за автоматический приём заявок от клиентов. После чего, Т., руководствуясь мотивом мести за

[1] Апелляционное постановление Судебной коллегии по уголовным делам Саратовского областного суда от 21 февраля 2017 года по делу № 22-527/2017.

[2] Апелляционное постановление Забайкальского краевого суда Читинской области от 23 марта 2015 года по делу № 1269-2015.

невыплату заработной платы работодателем, незаконно распространил ранее созданную им вредоносную компьютерную программу[1].

Как представляется, проблема более строгой ответственности лиц, обязанных в силу выполняемых ими трудовых функций, соблюдать и (или) обеспечивать информационную безопасность организации, требует отказа от классического (ограничительного) толкования лиц, использующих служебное положение, и отнесения к данной категории любых сотрудников, которые на законных основаниях используют компьютерную информацию компании или учреждения, а также средства ее обращения (системные инженеры, программисты, менеджеры, продавцы-консультанты и специалисты по обслуживанию клиентов, обладающие полномочиями по использованию баз данных и др.).

Данный подход по делам преступлениях, предусмотренных главой 28 УК РФ, находит всё большую поддержку на доктринальном уровне. Так, К. Н. Евдокимов, обосновывает, что «использование служебного положения» может быть как со стороны должностных лиц, государственных и муниципальных служащих, так и рядовых служащих коммерческой или некоммерческой организации, независимо от формы собственности, эксплуатирующих компьютерную технику и информационно-телекоммуникационные сети[2].

М. А. Ефремова считает такими лицами всех служащих, имеющих доступ к компьютеру на законных основаниях, отдельно подчёркивая, что ошибочным будет мнение о том, что подобными субъектами являются только должностные лица или лица, выполняющие управленческие функции в коммерческой или иной организации[3]. Наконец, нельзя не отметить, что данный подход нашёл своё отражение и в методических рекомендациях Генеральной прокуратуры Российской Федерации[4].

Непростым является вопрос об оценке неправомерной модификации информации, содержащейся в информационных базах данных государственных органов, совершаемой должностными лицами. В судебно-следственной практике подобного рода действия оцениваются по-разному.

В некоторых случаях, содеянное квалифицируется исключительно по ст. 285 УК РФ со ссылкой на то обстоятельство, что лицо в соответствии с

---

[1] Приговор Набережночелнинского городского суда Республики Татарстан от 24 октября 2013 года по делу № 1-1196/2013.

[2] Евдокимов К. Н. Противодействие компьютерной преступности в Российской Федерации: криминологические и уголовно-правовые аспекты: монография. Иркутск, 2016. С. 138.

[3] Ефремова М. А. Уголовно-правовая охрана информационной безопасности: монография. М., 2018. С . 270.

[4] Методические рекомендации Генеральной прокуратуры Российской Федерации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации. М., 2013. С. 9.

занимаемой должностью имело право доступа к информационным базам с присвоением соответствующих логина и пароля. Так, отмечается, что «…действия виновного по внесению заведомо ложных сведений об уплате штрафа, несоответствующих действительности, непосредственно связаны с осуществлением им своих прав и обязанностей, которые не вызывались служебной необходимостью и объективно противоречили как общим задачам и требованиям, предъявляемым к государственному аппарату, так и тем целям и задачам, для достижения которых виновный, как должностное лицо было наделено соответствующими должностными полномочиями»[1].

Однако, использование должностным лицом своих служебных полномочий отнюдь не исключает возможности признания доступа к компьютерной информации неправомерным. Это объясняется тем, что право должностного лица на доступ к информационной базе данных носит не общий характер, а возникает только в связи с строго определёнными (нормативно регламентированными) основаниями[2]. Так, в другом решении суд, применив ч. 3 ст. 272 УК РФ, обоснованно указал, что наличие у виновного официального доступа к служебной базе данных само по себе не исключает возможности его осуждения по ст. 272 УК РФ, поскольку им совершены незаконные действия, связанные с неправомерным доступом к компьютерной информации, имевшие целью сокрытие ранее совершённого должностного преступления, а также направленные на избежание лицом, совершившим административное правонарушение, исполнения назначенного судебным решением наказания[3].

Учитывая, что ч. 3 ст. 272 УК РФ точнее выражает направленность деяния, а также более полно описывает его признаки, следует, пожалуй,

---

[1] Приговор Первомайского суда г. Кирова от 09 сентября 2016 года по делу № 1-222/2016.

[2] Так, например, приказом МВД России № 1144 от 03.12.2007 г. «О системе информационного обеспечения Госавтоинспекции» утверждены «Наставления по организации формирования и ведения специализированных учётов федеральной специализированной территориально распределённой информационной системы Госавтоинспекции». В соответствии с п. 2.4 указанных наставлений специализированный федеральный учёт лиц, привлечённых к административной ответственности за нарушения правил дорожного движения (АИПС «Адмпрактика»), формируется на основе сведений, поступающих из подразделений Госавтоинспекции органов внутренних дел в районах, городах и иных муниципальных образованиях. Основанием для постановки на региональный учёт является оформление соответствующего протокола об административных правонарушениях в области обеспечения безопасности дорожного движения (п.9.1).

[3] Приговор Катайского районного суда Курганской области от 18 апреля 2013 года по делу № 1-20/2013.

поддержать последний подход. При этом, полагаем, что в силу ч. 1 ст. 17 УК РФ подобного рода действия должностных лиц полностью охватываются ч. 3 ст. 272 УК РФ и дополнительной квалификации по ст. 285 УК РФ или ст. 286 УК РФ не требуют. Исключением могут выступать лишь случаи, когда должностное лицо, используя свои служебные полномочия, наряду с неправомерным доступом к компьютерной информации, совершило другие незаконные действия, связанные со злоупотреблением или превышением должностных полномочий из корыстной или иной личной заинтересованности. При таких обстоятельствах содеянное надлежит квалифицировать по совокупности указанных преступлений. Данный подходит находит своё отражение и в материалах правоприменительной практики. Так, Н. признан виновным в получении от П. взятки в значительном размере за незаконные действия его, как должностного лица – оперуполномоченного ОУР отдела МВД России. Он же признан виновным в том, что, превышая свои должностные полномочия, обеспечил П. неправомерный доступ к охраняемой законом компьютерной информации – персональным данным граждан, хранящейся на веб-сайте ИЦ УМВД России в региональном интегрированном банке данных. Он же признан виновными в том, что, используя своё служебное положение, в различные дни, находясь в служебных помещениях отделов полиции, совершил неправомерный доступ к охраняемой законом компьютерной информации – персональным данным граждан, что повлекло ее копирование.

Оценив доказательства по делу, суд квалифицировал действия Н. по ч. 3 ст. 290 и ч. 3 ст. 272 УК РФ, а действия П.– по ч. 3 ст. 291 и ч. 3 ст. 272 УК РФ. Рассматривая вопрос о квалификации действий Н. по ч. 1 ст. 286 УК РФ, суд первой инстанции указал, что он превысил свои должностные полномочия, поскольку, не имея законных оснований, специального права, соответствующих пароля и логина, осуществил неправомерный допуск третьих лиц – П. к компьютерной информации, содержащей персональные данные граждан. Однако за совершение указанных действий Н. признан виновным по ч. 3 ст. 272 УК РФ, поэтому квалификация одних и тех же действий по двум составам преступлений является излишней. С учётом изложенного, суд апелляционной инстанции посчитал излишним дополнительное вменение Н. преступления, предусмотренного ч. 1 ст. 286 УК РФ[1].

Несмотря на то что информация, содержащаяся в информационных базах данных используется государственными органами при составлении официальных документов, внесение в них заведомо ложных сведений, на наш взгляд, нельзя квалифицировать как служебный подлог. Так, в одном случае, оценив внесение инспектором дорожно-патрульной службы заведомо ложных сведений об уплате лицом административных штрафов

[1] Апелляционное определение судебной коллегии по уголовным делам Костромского областного суда от 4 августа 2016 года по делу № 22-773/2016.

по ч. 3 ст. 272 УК РФ, суд обоснованно не согласился с необходимостью дополнительного вменения ст. 292 УК РФ. Аргументация принятого решения основывалась на том, что «…в качестве предмета данного преступления действующим законодательством признаются лишь официальные документы. В силу требований закона, официальный документ должен быть публичным, адресованным неопределённому кругу субъектов правоотношений, иметь соответствующие реквизиты и удостоверять факты, влекущие юридические последствия в виде предоставления или лишения прав, возложения или освобождения от обязанностей, изменения объёма прав и обязанностей. Вопреки доводам стороны обвинения, автоматизированная информационно-поисковая система данными признаками не обладает, является базой данных для внутреннего пользования органов полиции, тем самым, у суда отсутствуют основания утверждать, что Г., модифицировав компьютерную информацию в отношении Д., внесла тем самым и заведомо ложные сведения в официальный документ, совершив служебный подлог»[1].

В современной науке уголовного права проблемам электронного официального документа уделяется довольно серьёзное внимание[2], что объясняется прикладной значимостью соответствующих вопросов. Не углубляясь в известную полемику относительно признаков электронного официального документа как предмета преступления, отметим, что в силу положений ст. 2 Федерального закона № 149-ФЗ от 27 июля 2006 года «Об информации, информационных технологиях и о защите информации» информационные системы (информационно-поисковые системы, информационные базы данных и т.п.) следует предельно чётко отграничивать от электронных документов, в том числе официальных. Информационная система предназначена для накопления и обработки информации. При этом официальные электронные документы могут составлять содержание информационной системы, быть её частью. Совокупность преступлений, предусмотренных ч. 3 ст. 272 УК РФ и ст. 292 УК РФ может иметь место в том случае, если неправомерный доступ к

---

[1] Приговор Богдановичского городского суда Свердловской области от 27 августа 2015 года по делу № 1-30/2015.

[2] См.: Букалерова Л. А., Шагиева Р. В. О необходимости усиления правовой охраны оборота электронной подписи: современные проблемы теории и практики // Учёные труды Российской академии адвокатуры и нотариата. 2011. № 2 (21). С. 119-124; Ефремова М. А. Электронный документ как предмет преступления // Вестник Академии Генеральной прокуратуры Российской Федерации. 2015. № 5. С. 10- 15; Иванова Е. В. Официальный документ в электронной форме как предмет преступления, предусмотренного ст. 327 УК РФ // Уголовное право. 2012. № 3. С. 29-31; Лукьянова А. А. Электронный официальный документ как предмет преступления, предусмотренного ст. 327 УК РФ // Уголовное право. 2016. № 3. С. 57-62 и др.

компьютерной информации дополнительно был сопряжён с внесением соответствующим субъектом заведомо ложных сведений в электронные официальные документы.

Часть 4 ст. 272 УК РФ предусматривает два особо квалифицирующих признака. Неправомерный доступ к охраняемой законом компьютерной информации, если такие действия повлекли тяжкие последствия или создали угрозу их наступления.

Понятие «тяжкие последствия» является оценочным. На практике к ним относят: причинение смерти или тяжкого вреда здоровью человека; причинение средней тяжести вреда здоровью двум или более лицам; массовое причинение лёгкого вреда здоровью людей; наступление экологических катастроф, транспортных или производственных аварий, повлёкших длительную остановку транспорта или производственного процесса; дезорганизацию работы конкретного предприятия; причинение особо крупного ущерба и т.п. Как справедливо отмечает С. Д. Бражник, в оценке тяжких последствий применительно к компьютерным преступлениям сложились два подхода. Сторонники первого понимают под ним потерю исключительно незаменимой информации, наличие которой обеспечивает функционирование средств автоматизированной обработки компьютерной информации или необходима для функционирования физического или юридического лица. Большинство же учёных тяжкие последствия трактуют как «гибель людей, причинение вреда здоровью, дезорганизация производства на предприятии или в отрасли промышленности, осложнение дипломатических отношений с другим государством, возникновение вооружённого конфликта»[1].

Следует отметить, что преступление, предусмотренное ч. 4 ст. 272 УК РФ, будет иметь место не только при фактическом наступлении тяжких последствий, но и при создании угрозы их наступления. При этом угроза наступления тяжких последствий будет считаться созданной, если она была реальной, и тяжкие последствия не наступили, лишь вследствие обстоятельств, не зависящих от воли виновного, или благодаря вовремя принятым мерам.

1.2. СОЗДАНИЕ, ИСПОЛЬЗОВАНИЕ И РАСПРОСТРАНЕНИЕ ВРЕДОНОСНЫХ КОМПЬЮТЕРНЫХ ПРОГРАММ (СТ. 273 УК РФ)

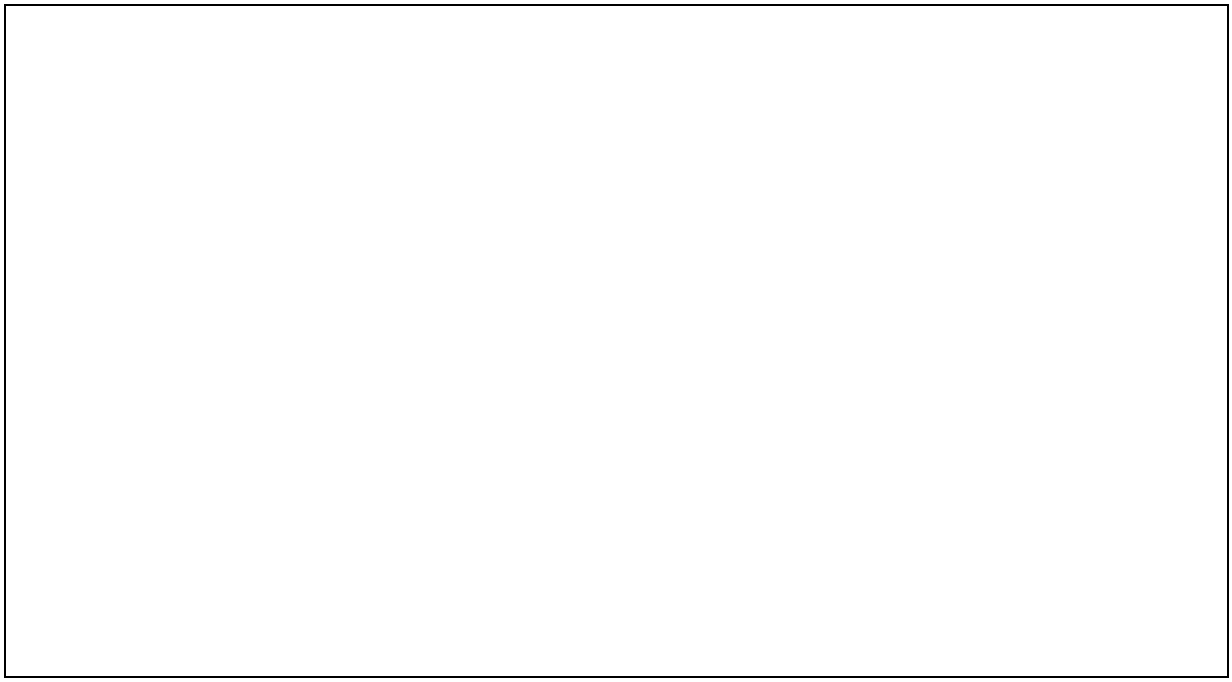
В наше время, пожалуй, трудно найти пользователя современными информационно-коммуникационными технологиями, который хотя бы раз не испытывал на себе негативное воздействие вредоносных компьютерных программ. Некоторые из них относительно безобидны, другие могут причинить непоправимый вред не только информационным активам, но и

[1] Бражник С. Д. Преступления в сфере компьютерной информации: проблемы законодательной техники: дис. …канд. юрид. наук. Ижевск, 2002. С. 140.

самому компьютерному оборудованию. В отношении наиболее опасных авторы предлагают и вовсе использовать термины «информационное оружие»[1] или «кибероружие»[2].

Совсем недавние атаки на информационную инфраструктуру ряда государств, в том числе России, вирусов-шифровальщиков «WannaCry» и «Petya» не позволяют признавать такие оценки надуманными либо преувеличенными. В общей сложности только от «WannaCry» пострадало более 500 тысяч компьютеров, принадлежащих частным лицам, коммерческим организациям и правительственным учреждениям, в более чем 150 странах мира[3].

Изучение статистических данных показывает, что в России ежегодно регистрируется сравнительно незначительное число случаев совершения преступления, предусмотренного ст. 273 УК РФ.



Объектом данного преступления выступают общественные отношения, связанные с обеспечением информационной безопасности от

[1] Фатьянов А. А. Правовое обеспечение безопасности информации в Российской Федерации: учебное пособие. М., 2001. С. 40.

[2] См.: Казарин О. В., Шаряпов Р. А. Вредоносные программы нового поколения – одна из существующих угроз международной информационной безопасности // Вестник РГГУ. Серия: Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность. 2015. № 12 (155). С. 9-23; Stefano Mele. Legal consideration on cyber-weapons and their definition // Journal of Law & Cyber Warfare, Volume 3, Issue 1, 2014. P.53.

[3] [Электронный ресурс] // URL: http://www.kommersant.ru/doc/3297338 (дата обращения - 20 ноября 2017).

деструктивного воздействия вредоносной компьютерной информации и вредоносных компьютерных программ.

Парадоксально, но несмотря на значимость проблемы противодействия деструктивным информационным объектам, в отечественной уголовно-правовой науке так и не сложилось единообразного понимания «вредоносной программы» как конструктивного признака ст. 273 УК РФ.

Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации определяет вредоносную программу как созданную или существующую программу со специально внесёнными изменениями, заведомо приводящую к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети[1].

В этом же ключе содержание вредоносной программы раскрывается в п. 2.6.5. и 2.6.6. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения», утверждённого Приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст[2]. Согласно государственному стандарту, вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы информационной системы. Несанкционированное воздействие на информацию – воздействие на защищаемую информацию с нарушением установленных прав и (или) правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Подобный подход, определяющий вредоносность программы её функциональным предназначением – оказывать неправомерное (несанкционированное) воздействие исключительно на компьютерные данные и системы – является наиболее распространённым и в доктрине уголовного права. Так, М. М. Малыковцев пишет, что «вредоносная программа – это программа, специально написанная на любом языке программирования, использование и распространение которой в информационной системе, либо в информационно-телекоммуникационной сети приводит к неправомерному воздействию на информацию и (или) на средства компьютерной техники и связи, выражающемуся в незаконном уничтожении, копировании, повреждении, блокировании, искажении информации, и (или) иному нарушению установленного законным

---

[1] Собрание законодательства Российской Федерации от 30 марта 2009 г. № 13 ст. 1460.

[2] ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. М.: Стандартинформ, 2008.

владельцем порядка работы указанных устройств»[1]. Похожим образом определяет вредоносность компьютерной программы Е. А. Маслакова, отмечая, что её сущностным свойством выступает способность вызывать несанкционированное собственником уничтожение, блокирование, модификацию либо копирование компьютерной информации[2].

В свою очередь М. А. Ефремова подчёркивает, что «основное отличие вредоносных программ от иных, которые также могут производить копирование, уничтожение, модификацию информации, определяется тем, что все действия производятся без уведомления пользователя, скрытно от него, а сам пользователь зачастую и не подозревает о наличии такой программы на его компьютере»[3].

А. П. Кузнецов также обосновывает, что «вредоносность или полезность соответствующих компьютерных программ определяется не в зависимости от их назначения, способности уничтожать, блокировать, модифицировать, копировать информацию (это может являться технической функцией лицензионных (разрешённых) компьютерных программ), а в связи с тем, предполагает ли их действие, во-первых, предварительное уведомление собственника компьютерной информации или другого добросовестного пользователя о характере действия программы, а во-вторых, получение его согласия (санкции) на реализацию программой своего назначения. Нарушение одного из этих требований делает компьютерную программу вредоносной»[4].

В. М. Быков, В. Н. Черкасов резюмируют, что для того, чтобы программа считалась вредоносной, она должна соответствовать следующим трём критериям: 1) направленность на уничтожение информации; 2) несанкционированный характер работы; и 3) целью создания программы является оказание неправомерного воздействия на информационные ресурсы[5].

---

[1] Малыковцев М. М. Уголовная ответственность за создание, использование и распространение вредоносных программ для ЭВМ: дис. ...канд. юрид. наук. М., 2007. С. 10.

[2] Маслакова Е. А. Незаконный оборот вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты: дис. ...канд. юрид. наук. Орёл, 2008. С. 68.

[3] Ефремова М. А. Уголовная ответственность за преступления, совершаемые с использованием информационно-коммуникационных технологий: монография. М., 2015. С. 101.

[4] См.: Кузнецов А. П. Полный курс уголовного права: в 5 т. / под ред. д. ю. н., проф., заслуженного деятеля науки РФ А. И. Коробеева. Т. IV: Преступления против общественной безопасности. СПб., 2008. С. 657.

[5] Быков В. М., Черкасов В. Н. Преступления в сфере компьютерной информации: криминологические, уголовно-правовые и криминалистические проблемы: монография. М., 2015. С. 126.

Нельзя не отметить спорный характер первого критерия, который неоправданно ограничивает вредоносность программы её нацеленностью именно на уничтожение компьютерных данных.

По мнению В. Б. Вехова, для того, чтобы признать компьютерную программу вредоносной, необходимо доказать наличие совокупности следующих обстоятельств: 1) программа способна уничтожать, блокировать, модифицировать либо копировать компьютерную информацию или нейтрализовать средства защиты компьютерной информации; 2) программа не предполагает предварительного уведомления собственника, владельца или пользователя (обладателя) компьютерной информации, компьютерного устройства, информационной системы или информационно-телекоммуникационной сети о характере своих действий; 3) программа не запрашивает согласия (санкции) у собственника, владельца или пользователя (обладателя) компьютерной информации, компьютерного устройства, информационной системы или информационно-телекоммуникационной сети на реализацию своего назначения (алгоритма)[1].

В судебно-следственной практике, пожалуй, наибольшее распространение получило признание вредоносными компьютерных программ, которые заведомо предназначены для генерации кода установки (серийного номера) и кода активации, запрашиваемых при установке лицензионных программных продуктов («KEYGEN.exe» и др.).Так, Р. был осуждён по ч. 2 ст. 146 УК РФ и ч. 1 ст. 273 УК РФ. Согласно приговору суда Р., находясь в помещении коммерческой организации, из корыстной заинтересованности выполнил несанкционированное копирование (установку) с неустановленного следствием носителя информации программного продукта на системный блок электронно-вычислительной машины, принадлежащей организации и для достижения работоспособности указанного программного продукта незаконно использовал вредоносную компьютерную программу с неустановленного следствием носителя информации. Таким образом Р. умышленно использовал вредоносную программу, чем заведомо исключил возможность штатной установки лицензионного ключа программы, и тем самым заведомо несанкционированно модифицировал (изменил) продукцию, обеспечив нейтрализацию средств защиты и нормальное функционирование работы программного продукта[2].

Сравнительно реже правоохранительные органы выявляют случаи использования «компьютерных вирусов», «троянов» и т.п. Так, например,

---

[1] Вехов В. Б. Вредоносные компьютерные программы как предмет и средство совершения преступления // Расследование преступлений: проблемы и пути их решения. 2015. № 2 (8). С. 45

[2] Приговор Александровского городского суда Владимирской области от 19 августа 2015 года по делу № 1-82/2015.

М. был осуждён по ч. 1 ст. 273 УК РФ. В соответствии с приговором суда М., обладая специальными познаниями в области работы с компьютерными программами, действуя умышленно, находясь по месту жительства приобрёл путем копирования с неустановленных интернет-ресурсов, компьютерные программы, заведомо предназначенные для несанкционированного копирования компьютерной информации, после чего посредством принадлежащего ему компьютерного оборудования, а также находящихся в его пользовании хостинговых сервисов (серверов для хранения информации в сети Интернет) использовал указанные вредоносные компьютерные программы для заражения 50 компьютеров неустановленных пользователей сети Интернет и построения из них контролируемой сети, в результате чего без ведома и согласия указанных пользователей скопировал хранящуюся в памяти заражённых устройств компьютерную информацию, содержащую сведения о логинах и паролях авторизации пользователей на различных интернет-ресурсах, которую планировал использовать в личных целях. Согласно заключению эксперта, на жёстком диске персонального компьютера М. обнаружены комплексы вредоносного программного обеспечения, предназначенного для построения «ботнетов» («бот-сетей»), то есть сетей из заражённых соответствующим вирусом компьютеров с возможностью уделённого копирования информации назначенным владельцем указанной сети без ведома пользователя и без получения его согласия на применение указанных программ. Работа обнаруженного на жёстком диске вредоносного программного обеспечения построена на использовании вирусов типа «троян» («троянская программа»)[1].

Господствующее толкование вредоносности компьютерной программы, к сожалению, имеет свои изъяны. Так, например, оно не позволяет отнести к таковым программы-шпионы (Spyware), целью которых является не причинение вреда информационным активам или инфраструктуре, а собирание сведений об активности пользователя в сети Интернет (о посещаемых сайтах, совершаемых покупках и т.п.), программы «злые

[1] Приговор Андроповского районного суда Ставропольского края от 6 апреля 2017 года по делу № 1-31/2017.

шутки» («Bad Jokes»)[1], так называемые «вирусные конструкторы» – программы, предназначенные не для осуществления атак на компьютерные ресурсы, а для генерирования новых вирусов. При общепринятом подходе нельзя отнести к вредоносным также программы, объективно приспособленные к совершению преступлений, но выполненные на основе легального программного обеспечения. В связи с этим обоснованно возникает вопрос, может ли вредоносность программы выражаться в её направленности на совершение посягательств в отношении иных охраняемых уголовным законом объектов? В. С. Комиссаров даёт утвердительный ответ на этот вопрос, поскольку считает, что вредоносность может быть обусловлена не только самим алгоритмом её действия, направленным на уничтожение, блокирование, модификацию или копирование информации, но и «специфическими свойствами, предназначенными для выполнения неправомерных или даже преступных действий (хищения денег с банковских счетов, укрытия средств от налогообложения, хулиганства и т.д.)»[2].

В. А. Голуб и М. В. Овчинникова также расширительно толкуют содержание вредоносной программы, определяя её как программу или фрагмент кода, специально созданную для выполнения или способствующую выполнению несанкционированных действий в информационной системе или информационно-телекоммуникационной сети, в результате которых возможно причинение вреда пользователям этой системы (сети) или другим лицам[3].

Пункт 2 «Правил оказания телематических услуг связи», утверждённых постановлением Правительства Российской Федерации от 10 сентября 2007 г. № 575, вредоносное программное обеспечение раскрывает как целенаправленно приводящее к нарушению законных прав абонента и (или) пользователя, в том числе к сбору, обработке или передаче с

---

[1] Такие программы не причиняют компьютеру прямого вреда, однако выводят сообщения о том, что такой вред уже причинён, либо будет причинён, предупреждают пользователя об опасности, которой на самом деле не существует. К «злым шуткам» относятся, например, программы, которые пугают пользователя сообщениями о форматировании диска (хотя никакого форматирования на самом деле не происходит), выводят сообщения, характерные для вирусов, и т.д. – в зависимости от «чувства юмора» автора такой программы. К этому классу также относятся программы, предназначенные для мошенничества, например путем распространения архивов с оплатой за смс // URL: https://threats.kaspersky.com/ru /threat/Hoax.JS.BadJoke/ (дата обращения: 22.04.2018 г.).

[2] Уголовное право: Особенная часть / под ред. А. И. Рарога. М., 2009. С. 532–533.

[3] Голуб В. А., Овчинникова М. В. Проблема корректного определения термина «вредоносная программа» // Вестник Воронежского государственного университета. Серия: Системный анализ и информационные технологии. 2008. № 1. С. 141.

абонентского терминала информации без согласия абонента и (или) пользователя, либо к ухудшению параметров функционирования абонентского терминала или сети связи[1].

Если исходить из подобного, более широкого, понимания вредоносности как предназначения программы к заведомо противоправной (преступной) деятельности в целом, то изготовление и распространение программ-шпионов, «Bad Jokes» и конструкторов вирусов может быть квалифицировано по ст. 273 УК РФ. На наш взгляд, современный процесс непрерывного роста использования информационно-коммуникационных технологий во всех сферах жизни общества, убедительно свидетельствует в пользу именно этого подхода. С течением времени вредоносные программные продукты всё больше будут направлены не на отношения информационной безопасности как таковые, а на иные социально значимые сферы – жизнь, здоровье, честь и достоинство личности, неприкосновенность частной жизни, отношения собственности, общественный порядок и др.

К. Н. Евдокимов делает вывод, что вредоносными программами могут быть и обычные лицензионные компьютерные программы в случае их использования при совершении преступного деяния и достижения вредных последствий, указанных в ст. 273 УК РФ[2]. Полагаем, что автор необоснованно смешивает вредоносные программы и легальное программное обеспечение, которое достаточно часто используется при совершении посягательств на объекты уголовно-правовой охраны. Известно, что многие разрешённые к обороту программные продукты применяются злоумышленниками для совершения преступлений. Так, например, программы для записи дисков (InfraRecoder, BurnAware, Nero и др.) используются злоумышленниками для изготовления контрафактной продукции (неправомерного копирования информации), программное обеспечение для удалённого администрирования (RDP, VNC, DameWare, TeamViewer, Remote Office Manager, Hamachi, и т.д.) довольно часто применяется при совершении хищений, связанных с неправомерным вмешательством в системы дистанционного банковского обслуживания. Вместе с тем, вредоносными их признавать нельзя, поскольку такие программы по факту остаются аутентичными, сохраняют стандартный набор настроек и возможностей, заложенный легальным разработчиком.

Другое дело, когда центральную часть программы (так называемый «движок») приспосабливают для совершения конкретных преступлений. Например, для незаконного пополнения баланса проездных билетов злоумышленник использует одну из многих компьютерных программ,

---

[1] Собрание законодательства РФ. 17.09.2007. № 38. ст. 4552.

[2] Евдокимов К. Н. Создание, использование и распространение вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты: монография. Иркутск, 2013. С. 60.

предназначенных для записи информации с одного носителя на другой, но меняет её интерфейс таким образом, чтобы можно было выбрать перевозчика, количество поездок, срок действия и т.п. В этом случае, на наш взгляд, можно говорить о наличии признаков изготовления вредоносной компьютерной программы, поскольку в окончательном виде полученное программное обеспечение обладает уже другими характеристиками, напрямую указывающими на её предназначение для осуществления противоправной деятельности.

Следует упомянуть об общепринятом в доктрине уголовного права положении – вредоносность программного обеспечения категория юридическая и находится в компетенции правоприменителя. Программно-техническая экспертиза должна решать свои задачи – раскрыть общий алгоритм и особенности действия программы, предоставить значимую для следствия информацию о её работе и т.п. Так или иначе выводы эксперта будут иметь лишь ориентирующий характер в разрешении вопроса о вредоносности программы. В свете современных угроз стремительно виртуализующегося общества полагаем, что единственно верным будет избрать в качестве основного критерия вредоносности программы её изначальное и основное предназначение – осуществление противоправной деятельности. В какой сфере такая деятельность будет осуществляться, будет ли работа программы носить несанкционированный пользователем или разрешённый характер (как с конструктором вирусов) имеет второстепенное значение. Таким образом, под вредоносной следует понимать компьютерную программу, созданную (в том числе путём модификации легальной программы) для осуществления противоправной деятельности.

Подобное толкование, на наш взгляд, позволит предупредить в будущем возможные проблемы применения такого оперативно-розыскного мероприятия как получение компьютерной информации (было внесено в Федеральный закон от 12.08.1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» в июле 2016 года). А. Л. Осипенко совершенно справедливо отмечает, что законодатель вряд ли связывает проведение данного оперативно-розыскного мероприятия с простейшими формами обращения к компьютерным ресурсам, находящимися в открытом доступе. Такие действия, осуществляемые, как правило, гласно и не подразумевающие необходимость преодоления определённых препятствий, следует оформлять как наведение справок, сбор образцов для сравнительного исследования и т.д. Основу же получения компьютерной информации как оперативно-розыскного мероприятия составляют достаточно сложные в техническом плане и требующие специальной подготовки действия по добыванию хранящейся в компьютерных системах или передаваемой по

техническим каналам связи информации о лицах и событиях, вызывающих оперативный интерес[1].

Представляется очевидным, что правоохранительными органами при получении компьютерной информации, как правило, будут использоваться «заблаговременно внедрённые программные продукты»[2] – практика, которая апробирована силовыми структурами многих зарубежных стран и уже получила освещение в печати[3]. Несмотря на то, что такие программные продукты обладают функционалом к преодолению средств защиты информации и её скрытой фиксации (несанкционированного пользователем копирования), их предназначение для правомерного использования при проведении оперативно-розыскных мероприятий не позволит признавать их вредоносными по смыслу ст. 273 УК РФ.

Некоторые авторы предлагают решить обозначенную проблему путём дополнения ст. 273 УК РФ соответствующим примечанием. Так, В. В. Челноков обосновывает необходимость указать в ст. 273 УК РФ на исключение из числа вредоносных компьютерных программам или иной компьютерной информации предназначенных для использования в оперативно-розыскной, разведывательной или контрразведывательной деятельности либо для осуществления производства по делу об административном правонарушении, производства дознания, предварительного следствия или осуществления правосудия, если они создаются, распространяются и используются лицами, наделёнными соответствующими законными полномочиями[4].

С учётом ранее сформулированного определения вредоносной компьютерной программы данная законотворческая инициатива нам представляется излишней. Полагаем, что подобный вопрос должен быть решён на уровне разъяснений Пленума Верховного Суда Российской Федерации.

С объективной стороны преступление проявляется в совершении хотя бы одного из следующих действий: 1) создание компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств

---

[1] Осипенко А. Л. Новое оперативно-розыскное мероприятие «получение компьютерной информации»: содержание и основы осуществления // Вестник Воронежского института МВД России. № 3. 2016. С. 86.

[2] Баженов С. В. Оперативно-розыскное мероприятие «Получение компьютерной информации» // Научный вестник Омской академии МВД России. № 2 (65). 2017. С. 32.

[3] Kaspersky E. What is wrong with «legal malware»? // Forbes. 22 dec. 2014.

[4] Челноков В. В. Компьютерная информация как предмет преступления в отечественном уголовном праве: дис. …канд. юрид. наук. Екатеринбург, 2013. С. 11.

защиты компьютерной информации; 2) использование таких компьютерных программ или такой компьютерной информации; 3) распространение таких компьютерных программ или такой компьютерной информации.

Создание вредоносной программы или вредоносной компьютерной информации представляет собой целенаправленную деятельность лица, результатом которой является возникновение программного продукта с заранее заданным деструктивным функционалом. При этом необходимо отметить, что в современных условиях создание вредоносного программного обеспечения отнюдь не предполагает, что лицо обладает профессиональными навыками программирования. Созданием также будет являться получение вредоносного программного продукта в результате использования так называемых «конструкторов вирусов». Так, например, Х. совершил создание вредоносной компьютерной программы, заведомо приводящей к несанкционированному уничтожению информации. Х., находясь по месту своего жительства, используя принадлежащий ему компьютер, обладая знаниями компьютерного программирования, знаниями команд и компилятора, умышленно, с целью последующего распространения машинного носителя с вредоносной программой, путем написания в текстовом файле перечня команд, удаляющих файлы с расширением «doc», «xls» самостоятельно создал вредоносную компьютерную программу, заведомо приводящую к несанкционированному удалению файлов с расширениями .zip, .rar, .xls, .doc, из корневого каталога диска и из всех каталогов и подкаталогов дисков компьютера, на который она была установлена и, тем самым приводящую к уничтожению информации, нарушению работы операционной системы семейства Microsoft Windows[1].

Под использованием вредоносной программы или вредоносной компьютерной информации следует понимать их непосредственный запуск, совершение действий по включению вредоносной программы. Использование вредоносной программы может осуществляться как в автономном режиме, так и в информационно-коммуникационной сети, в том числе сети Интернет. Так, например, А. с помощью своего компьютера, подключённого к информационно-телекоммуникационной сети Интернет через провайдера умышленно, с целью блокирования компьютерной информации, используя вредоносную компьютерную программу, заведомо предназначенную для несанкционированного блокирования компьютерной информации, осуществил компьютерную атаку типа «отказ в

[1] Приговор Смольнинского районного суда г. Санкт-Петербург от 02 февраля 2011 года по делу № 1-65/11

обслуживании» на сайт, принадлежащий официальному сайту Президента Российской Федерации[1].

Использованием вредоносной компьютерной программы также является широко распространённая практика установления пользователями контрафактного программного обеспечения (без активации ключа правообладателя) с последующим запуском патч-файла, устраняющим средство защиты компьютерной информации. Так, например, К. с целью обеспечения эксплуатации без ограничения по времени программного продукта «Microsoft Office Professional 2007 Russian», правообладателем которого является «Microsoft Corporation», без активационного ключа правообладателя, возник умысел, направленный на использование компьютерных программ, заведомо предназначенных для нейтрализации средств защиты компьютерной информации. Реализуя свой преступный умысел, К., не имея соответствующего разрешения от правообладателя, произвёл установку на жёсткий диск компьютера один экземпляр программного продукта «Microsoft Office Professional 2007 Russian». Затем К. во время установки вышеуказанного программного продукта, осознавая общественную опасность своих действий, предвидя наступление общественно опасных последствий и желая их наступления, с целью активации, регистрации и приведения контрафактного программного продукта «Microsoft Office Professional 2007 Russian» в работоспособное состояние и нейтрализации технических средств защиты авторского права указанного программного продукта, после нажатия клавиши запуска указанной программы, на предложение программы ввести лицензионный ключ, двойным нажатием на файл «Ключ.txt», ранее приобретённый им путем скачивания из сети Интернет и хранимый на USB-накопителе, открыл его и скопировал указанный там ключ в предложенное для ввода окно, чем активировал вышеуказанный программный продукт. Указанные действия К. повлекли нейтрализацию встроенной программной защиты от несанкционированного использования программного продукта «Microsoft Office Professional 2007 Russian», правообладателем которого является «Microsoft Corporation», а также снятие функциональных и временных ограничений, нейтрализацию встроенной программной защиты от несанкционированного использования, и нарушение их нормального функционирования[2].

Распространение вредоносной программы или вредоносной компьютерной информации заключается в сознательном предоставлении к ней доступа, в том числе сетевым способом. Так, например, М. распространил компьютерные программы и иную компьютерную

---

[1] Приговор Курганского городского суда от 21 сентября 2015 года по делу № 1-1388/15.

[2] Приговор Бийского городского суда от 26 марта 2015 года по делу № 1-250/2015.

информацию, заведомо предназначенные для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации и нейтрализации средств защиты компьютерной информации при следующих обстоятельствах. М. в целях извлечения для себя личной выгоды, выраженной в получении нематериальных благ и иных преимуществ в виде безвозмездного пользования компьютерной информацией, используя свои познания в области компьютерных технологий и специальную программу, путем копирования через сеть незаконно приобрёл у неустановленного лица и сохранил на жёстком диске своего системного блока программные продукты, содержащие две компьютерные программы, предназначенные для взлома программных продуктов, а также компьютерную информацию – один командный файл, блокирующий проверку подлинности лицензионных номеров, полученных способом генерации с помощью вышеуказанных программ, заведомо позволяющие осуществлять несанкционированное уничтожение, блокирование, модификацию, копирование, вносить изменения в существующие программные продукты и производить нейтрализацию средств защиты компьютерной информации. После этого М., имея преступный умысел, направленный на незаконное распространение вышеуказанных вредоносных компьютерных программ и компьютерной информации, используя компьютерную технику и специальную программу, незаконно выложил в Интернет вышеуказанные программные продукты, тем самым незаконно распространив их и предоставив неограниченному кругу пользователей данной сети возможность их копирования и использования по своему усмотрению[1].

В теории уголовного права считается практически общепринятым, что передача компьютерного вируса одному конкретному человеку также является его распространением[2]. В связи с этим нельзя не отметить, что Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» под распространением информации понимает исключительно действия, направленные на получение информации неопределённым кругом лиц или передачу информации неопределённому кругу лиц. Таким образом, по смыслу данного положения распространение прежде всего характеризуется тем, что информация передаётся не от лица к лицу, а размещается субъектом в свободном доступе, когда любой, изъявивший желание на её

[1] Приговор Октябрьского районного суда г. Ижевска от 23 июня 2014 года по делу № 1-186/14.

[2] См., например: Евдокимов К. Н. Создание, использование и распространение вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты: монография. Иркутск, 2013. С. 60; Ефремова М. А. Уголовная ответственность за преступления, совершаемые с использованием информационно-коммуникационных технологий: монография. М., 2015. С. 104 и др.

приобретение, может самостоятельно сохранить себе копию. Кроме того, путём толкования всё того же положения Закона об информации, распространением следует также считать массовую рассылку компьютерной информации, при котором количество получателей столь велико, что это деяние можно приравнять к размещению информации в свободном доступе.

Расширительное доктринальное толкование анализируемого признака, конечно же, в большей мере соответствует достижению цели обеспечения безопасности компьютерной информации и информационно-коммуникационной инфраструктуры. С другой стороны, нельзя игнорировать и тот очевидный факт, что системное толкование положений ст. 273 УК РФ в части признака распространения вредоносной компьютерной программы говорит не в пользу сложившегося правоприменения и обосновывающего его научного видения на проблему. Кроме того, оно закономерно влечёт ситуацию неопределённости на уровне восприятия права как профессиональным субъектом (судьёй, следователем и т.п.), так и простыми гражданами.

Создание, использование и распространение вредоносных компьютерных программ или вредоносной компьютерной информации, всегда предполагает активные действия со стороны лица, совершившего это преступление. Бездействием совершить рассматриваемое преступление не представляется возможным.

Следует согласиться с мнением, что использование вредоносной компьютерной программы для личных нужд (например, для уничтожения собственной компьютерной информации) ненаказуемо[1]. В продолжение следует лишь дополнить, что признаки преступления, предусмотренного ст. 273 УК РФ, будут также отсутствовать, когда вредоносная компьютерная программа используется в образовательных или исследовательских целях, для тестирования эффективности средств программно-технической защиты информации, а равно во всех случаях, когда вредоносная программа или информация не создаёт угрозы для автоматизированной обработки данных.

Состав преступления, предусмотренный ч. 1 ст. 273 УК РФ, сконструирован по типу формального, что прямо вытекает из буквы и смысла закона. Следовательно, для признания преступления оконченным не требуется наступления вредных последствий в виде уничтожения, блокирования, модификации копирования информации либо нейтрализации средств защиты компьютерной информации. Достаточно установить факт совершения хотя бы одного из альтернативно перечисленных в диспозиции статьи действий.

---

[1] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации [Электронный ресурс] // Режим доступа: СПС «Консультант-Плюс».

Субъектом создания, использования и распространения вредоносных компьютерных программ может являться любое физическое вменяемое лицо, достигшее шестнадцатилетнего возраста.

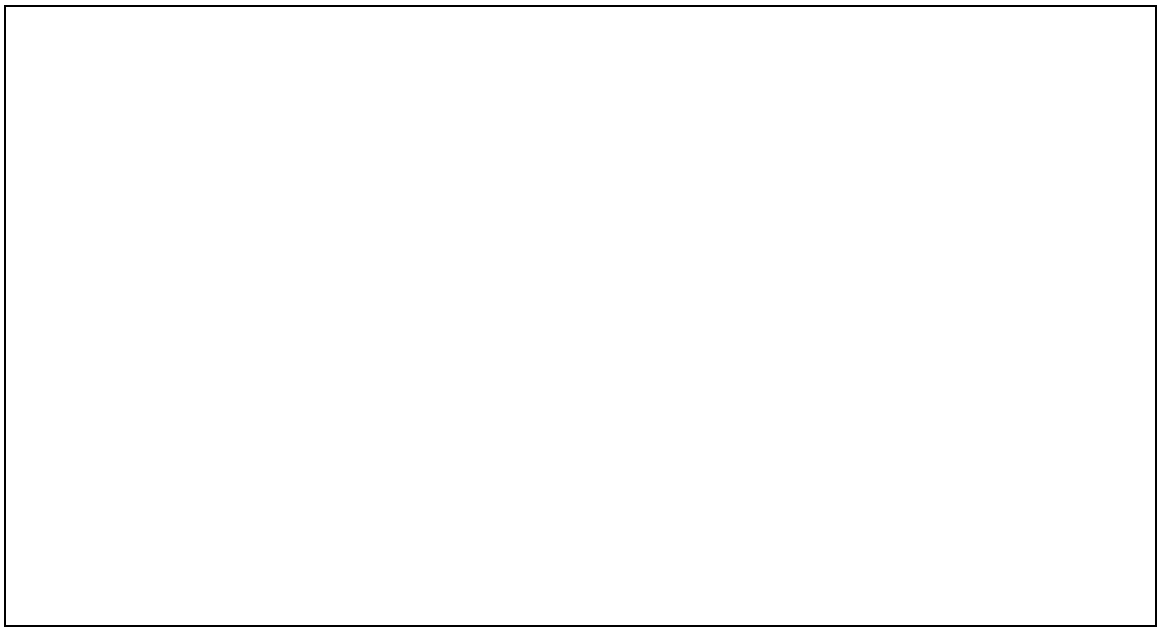
С субъективной стороны данное преступление совершается только с прямым умыслом. Виновный осознает, что создаёт такую программу либо компьютерную информацию, которая способна уничтожить, заблокировать, модифицировать либо копировать информацию, нейтрализовать средства защиты компьютерной информации, либо использует или распространяет вредоносную программу и желает эти действия совершить. Прежде всего, это подтверждается чётким указанием закона на заведомый характер деятельности виновного. Уже один этот факт исключает возможность совершения данного преступления по неосторожности либо с косвенным умыслом.

Мотивы анализируемого преступления и его цели (а они могут быть самыми разнообразными – месть, хулиганство, эксперимент и т.д.) – не являются обязательными признаками состава и учитываются лишь при назначении наказания.

1.3. НАРУШЕНИЕ ПРАВИЛ ЭКСПЛУАТАЦИИ СРЕДСТВ ХРАНЕНИЯ, ОБРАБОТКИ ИЛИ ПЕРЕДАЧИ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ ИЛИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ (СТ. 274 УК РФ)

Установление уголовной ответственности за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям имеет целью предупреждение невыполнения пользователями своих обязанностей, влияющих на сохранность хранимой и перерабатываемой компьютерной информации.

Как показывает изучение статистических данных, применение ст. 274 УК РФ стремится к нулевым показателям – год за годом регистрируются по-сути единичные случаи совершения данного преступления.



Столь невысокие показатели регистрации одного из преступлений в сфере компьютерной информации в условиях всеобщей цифровизации не могут не вызывать удивления и скептической оценки.

Объектом рассматриваемого преступления является совокупность общественных отношений в сфере соблюдения установленных правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям.

С точки зрения законодательного описания деяние, предусмотренное ст. 274 УК РФ, относится к весьма многочисленной группе преступлений, связанных с нарушением специальных правил, двойственная природа которых, по меткому определению Н.И. Пикурова, характеризуется сочетанием проступка и преступления (как бы формат «юридической матрешки»)[1]. Поэтому для уяснения признаков объективной стороны преступления необходимо, прежде всего, обратиться к тем конкретным положениям, закрепляющим правила эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правила доступа к информационно-телекоммуникационным сетям, которые были нарушены виновным.

По справедливому мнению Н. А. Лопашенко, не совсем ясно, что следует понимать под данными правилами. Имеются ли в виду технические правила обращения с компьютерной техникой (условно говоря – не бить, не ронять и т.п.), или же речь идёт о правилах обращения с компьютерной

[1] Проблемы квалификации преступлений : монография / под ред. К.В. Ображиева, Н.И. Пикурова. М., 2018. С. 74.

информацией. Отсутствие ответов на эти вопросы, отмечает автор, расширяет сферу преступного деяния, а границы криминализации делаются сверх подвижными, их наполняют реальным содержанием правоприменители, что недопустимо, поскольку противоречит принципу законности уголовного законодательства[1].

В Методических рекомендациях Генеральной прокуратуры Российской Федерации указано, что анализируемая норма является бланкетной и отсылает к конкретным инструкциям и правилам, устанавливающим порядок работы со средствами хранения, обработки или передачи охраняемой компьютерной информации, информационно-телекоммуникационными сетями и оконечным оборудованием в ведомстве или организации. Эти правила должны устанавливаться правомочным лицом. Общих правил эксплуатации, распространяющихся на неограниченный круг пользователей глобальной сети «Интернет» не существует[2].

В отличие от ряда иных специальных правил, сосредоточенных в конкретных нормативных актах, правила эксплуатации средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей не консолидированы и содержатся во множестве источников. В связи с этим возникает насущная потребность по-возможности чёткого определения их перечня.

Прежде всего, такие правила устанавливаются на уровне нормативных правовых актов. В качестве примера можно привести постановление Правительства РФ от 10 сентября 2007 г. № 575 «Об утверждении Правил оказания телематических услуг связи»[3], приказ Министерства связи и массовых коммуникаций РФ от 25 августа 2009 г. № 104 «Об утверждении Требований по обеспечению целостности, устойчивости, функционирования и безопасности информационных систем общего пользования»[4] и др. Последний классифицирует информационные системы общего пользования и регламентирует минимальные требования при их эксплуатации: использование сертифицированных антивирусных средств, наличие технических средств охраны помещений, в том числе систем

---

1 Лопашенко Н.А. Уголовно-правовая и криминологическая политика государства в области высоких технологий [Электронный ресурс] // URL:http://sartraccc.ru/i.php?filename=Pub%2Flopashenko%2830-06%29.htm&oper=read_file (дата обращения: 10.05.2018).

2 Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации // СПС «Консультант-Плюс».

3 Собрание законодательства Российской Федерации от 17 сентября 2007 г. № 38 ст. 4552.

4 Российская газета от 7 октября 2009 г. № 188.

видеонаблюдения, осуществление регистрации действий обслуживающего персонала и т.д.

В более конкретизированном виде правила пользования объектами информационно-телекоммуникационной инфраструктуры (оконечным оборудованием, терминалами оплаты, сайтами и т.п.) определяются на договорной основе (клиентским договором, договором на оказание услуг телематической связи, пользовательским соглашением и т.п.).

Так, по одному из дел суд обоснованно указал, что «…правила эксплуатации клиентом устройства самообслуживания определяется правилами пользования платёжной картой, внедряемой в банкомат в ходе его эксплуатации клиентом. В свою очередь правила пользования платёжной картой определяются условиями банковского договора, на основании которого клиент и получил в своё распоряжение указанную платёжную карту»[1].

Самостоятельным и значимым блоком следует признать правила, разработанные и утверждённые в конкретной организации (ведомстве) при определении обязанностей работников (служащих). В настоящее время специальными положениями или должностными инструкциями конкретных сотрудников, как правило, предусмотрены определённые ограничения по использованию компьютерной техники и сети Интернет. Типовыми правилами по эксплуатации являются запреты: загружать, самостоятельно устанавливать прикладное, операционное, сетевое и другие виды программного обеспечения, а также осуществлять обновления, если эта работа не входит в должностные обязанности лица; использовать ресурсы Интернет в не служебных целях; допускать к работе посторонних лиц; подключаться к ресурсам Интернет, используя компьютерную технику компании через не служебный канал доступа – сотовый телефон, модем и другие устройства; производить какие-либо действия с информацией, заражённой вирусом и т.п.

Так, прекращая уголовное дело в отношении А. в связи с истечением сроков давности, суд отдельно указал, что подсудимый был ознакомлен с должностной инструкцией по должности ведущий системный администратор, согласно которой ведущий системный администратор поддерживает в рабочем состоянии программное обеспечение рабочих станций с серверов (п.2.6), обеспечивает своевременное копирование, архивирование и резервирование данных (п.2.8), обеспечивает сетевую безопасность (п.2.18), сохраняет конфиденциальность служебной информации (п.2.26)[2].

---

[1] Приговор Кировградского городского суда Свердловской области от 5 августа 2016 года по делу № 1-105/2016.

[2] Постановление о прекращении уголовного дела Лефортовского районного суда г. Москвы от 13 января 2015 года по делу № 1-401/2014.

Бланкетные признаки ст. 274 УК РФ раскрываются и в правилах, установленных производителем компьютерного оборудования, то есть содержащихся в соответствующей технической документации. Таковыми, в частности, выступают общепринятые запреты на использование неоригинальных адаптеров переменного тока или батарей, осуществление работы в условиях перекрытия воздушного потока и др. Следует, однако, отметить, что при применении ст. 274 УК РФ необходимо установить, что лицо было ознакомлено (например, работодателем) с соответствующими техническими нормами или в силу фактических обстоятельств дела осознавало или должно было осознавать, что совершаемые им действия явно противоречат руководству по эксплуатации средств хранения, обработки ил передачи компьютерной информации.

А. Н. Ягудин делает вывод, что по смыслу ст. 274 УК РФ под «правилами эксплуатации» следует также понимать общепринятые нормы работы в сети Интернет, направленные на то, чтобы деятельность каждого пользователя сети не мешала работе других пользователей[1].

Полагаем, что такая позиция требует уточнения. Утверждение в общей форме о незаконности действий лица, противоправности избранного варианта поведения («в нарушение установленного порядка», «вопреки общепринятым нормам» и т.п.) без указания на источник правовой оценки и конкретизации конкретных пунктов нарушенных правил эксплуатации является недопустимым. Как справедливо пишет Н. И. Пикуров, отсутствие в постановлении о привлечении в качестве обвиняемого или в приговоре ссылки на нарушение предписаний конкретных пунктов и статей специальных правил означает незавершённость квалификации преступления[2].

Следует отдельно отметить, что примеры повседневной небрежности, повлёкшие уничтожение или повреждение компьютерного оборудования, уничтожение или модификацию данных и, как следствие, причинение имущественного ущерба потерпевшему, на наш взгляд, неправильно квалифицировать по ст. 274 УК РФ. При подобных обстоятельствах, когда лицо роняет компьютер, заливает его кофе или иным образом приводит в негодное для эксплуатации состояние, деяние не связано с нарушением специальных правил. Как представляется, содеянное не образует признаков какого-либо преступления и может выступать основанием для дисциплинарной и гражданско-правовой ответственности работника.

---

[1] Ягудин А. Н. Уголовная ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей: автореф. …дис. канд. юрид. наук. М., 2013. С. 14.

[2] Пикуров Н. И. Квалификация преступлений с бланкетными признаками состава: монография. М., 2009. С. 138.

Объективная сторона преступного нарушения правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, состоит из общественно опасного деяния в форме действия или бездействия, наступивших общественно опасных последствий и причинной связи между ними.

К действиям по смыслу ст. 274 УК РФ можно, например, отнести: нарушение запрета на подключение служебного оборудования к сети Интернет; предоставление посторонним лицам доступа к средствам хранения, обработки или передачи охраняемой компьютерной информации; несанкционированное разглашение логина или пароля законного пользователя; использование нелицензионного программного обеспечения; несанкционированная модификация программного обеспечения; несанкционированное изменение параметров настройки компьютера или информационно-телекоммуникационной сети; отключение средств противовирусной защиты и др. Преступное бездействие может проявляться в несоблюдении или прямом игнорировании соблюдения установленных правил, обеспечивающих должную работу средств хранения, обработки или передачи охраняемой компьютерной информации. Например, виновный не проверяет используемые средства хранения или передачи информации на наличие вредоносных программ, не включает систему защиты информации от несанкционированного доступа к ней, не выполняет обязательной процедуры резервного копирования компьютерной информации, оставляет без присмотра рабочее место и др.

Обязательным признаком объективной стороны этого преступления являются общественно опасные последствия. При этом необходимо отметить, что закон в ст. 274 УК РФ выделяет как бы два уровня последствий, каждый из которых является обязательным для признания состава преступления оконченным. В качестве последствий основного состава преступного нарушения правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, является уничтожение, блокирование, модификация либо копирование охраняемой законом компьютерной информации и причинение крупного ущерба (в соответствии с примечанием к ст. 272 УК РФ ущерб, сумма которого превышает один миллион рублей). Таким образом, формулировка закона исключает возможность привлечения лица к уголовной ответственности по ст. 274 УК РФ, если нарушение указанных правил хотя и повлекло уничтожение, блокирование, модификацию либо копирование информации, но объективно не причинило крупного ущерба.

Субъект преступления специальный – физическое, вменяемое лицо, достигшее к моменту совершения преступления шестнадцатилетнего возраста, которое, в силу характера выполняемой трудовой,

профессиональной или иной деятельности, имеет беспрепятственный доступ к средствам хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационным сетям и оконечному оборудованию и на которое, в силу закона или иного нормативного акта, возложено соблюдение соответствующих правил эксплуатации или доступа.

Отметим, что в теории уголовного права обосновывается позиция, согласно которой субъектом преступного деяния, предусмотренного ст. 274 УК РФ, будет являться любое физическое, вменяемое лицо, достигшее к моменту совершения преступления 16-летнего возраста, то есть общий субъект преступления[1].

Полагаем, что такой подход является дискуссионным и не позволяет провести четкое отграничение исследуемого преступного деяния от неправомерного доступа к компьютерной информации. Как совершенно справедливо резюмирует по данному поводу Р.Р. Гайфутдинов, по смыслу ст. 274 УК РФ у лица *имеется доступ* (выделено мной. – *Е.Р.*) к соответствующим объектам информационно-коммуникационной инфраструктуры[2]. Уточним лишь – доступ *правомерный*. Специализация субъекта здесь может определяться не только тем, что на лицо конкретными инструкциями или договорами возложены обязанности по соблюдению соответствующих правил, но и самим фактом использования лицом соответствующих ресурсов и (или) оборудования, то есть определяться фактической включенностью лица в специфическую группу общественных отношений. Присоединение к любому пользовательскому соглашению, которое, как известно, осуществляется лицом путем проставления соответствующей отметки при прохождении регистрации на том или ином ресурсе, автоматически включает его в такие отношения.

Здесь нужно прибегнуть к историческому толкованию действующей редакции ст. 274 УК РФ. Как известно, до внесения изменений Федеральным законом от 07 декабря 2011 г. № 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» диспозиция анализируемой нормы содержала оговорку о том, что нарушение правил эксплуатации должно быть допущено лицом, «имеющим доступ к ЭВМ, системе ЭВМ или их сети».

---

[1] Евдокимов К.Н. Проблемы квалификации и предупреждения нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ) : монография. Иркутск, 2018. С. 51.

[2] Гайфутдинов Р.Р. Понятие и квалификация преступлений против безопасности компьютерной информации : дис. … канд. юрид. наук. Казань, 2017. С. 142.

Справедливо отказываясь от архаизмов в тексте закона в пользу более универсальной категории средства хранения, обработки или передачи компьютерной информации, законодатель по какой-то причине (изучение паспорта законопроекта[1] ответа на этот вопрос не дает) исключает специальное указание на признаки специального субъекта в тексте нормы. Складывается представление, что оговорку о субъекте вычеркнули из ст. 274 УК РФ, что называется, походя. Можно, конечно же, предположить, что действующая редакция могла показаться законодателю в некотором смысле «перегруженной», тавтологичной, – нарушение правил эксплуатации предполагает, что лицо было к такой эксплуатации допущено. Однако верифицировать это предположение не представляется возможным.

Полагаем, что исключение специального указания о наличии у субъекта преступления, предусмотренного ст. 274 УК РФ, правомочий по доступу к соответствующим средствам хранения, обработки или передачи компьютерной информации, и без того усложнило понимание содержания данной уголовно-правовой нормы. Прежде всего это нашло свое проявление в отграничении нарушения правил эксплуатации от неправомерного доступа к компьютерной информации, совершенного лицом с использованием своего служебного положения (ч. 3 ст. 272 УК РФ). Как известно, в правоприменительной практике сложился подход, согласно которому неправомерность доступа к компьютерной информации определяется не только полномочиями субъекта по самому доступу, но и правомочиями по копированию, модификации, блокированию или уничтожению информации. Такое расширительное толкование неправомерного доступа к компьютерной информации, конечно же, не может не приводить к путанице в понимании, как самого неправомерного доступа к компьютерной информации, так и нарушения правил эксплуатации средств ее хранения, обработки или передачи. В качестве примера можно привести следующее судебное решение. Занимая должность менеджера по продажам дополнительного офиса банка, В., желая иметь статус эффективного работника, с целью исполнения возложенных на нее обязанностей по выполнению индивидуального плана, в нарушение Инструкции Центробанка РФ… а также внутренних нормативных и распорядительных документов, реализуя единый преступный умысел на неправомерный доступ к охраняемой законом компьютерной информации, используя возможность доступа к охраняемой законом компьютерной информации, в связи с исполнением

[1] Паспорт проекта Федерального закона № 559740-5 «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» (в части совершенствования законодательства Российской Федерации)».

должностных обязанностей и выполняемой работы, посредством служебного компьютера, осознавая, что не сможет исполнить возложенные на нее обязанности по выполнению индивидуального плана… неправомерно вошла в программу ФП Банковские карты АС Филиал, которая обеспечивает доступ к центральной базе данных филиала, *используя свои логин и пароль, предоставленные ей в силу служебных полномочий* (выделено мной. – *Е.Р.)*, тем самым преодолев средства защиты, в отсутствии реального обращения клиентов, выполнила операции по выдаче банковской карты категории «Momentum» на имя указанных лиц… далее была произведена активизация выпущенных карт и счетов на имя указанных лиц, что повлекло за собой модификацию компьютерной информации, с использованием своего служебного положения, в связи с чем были похищены денежные средства у указанных лиц и наступившие последствия причинили вред деловой репутации банка.

Далее в приговоре суд указывает на обстоятельства, которые вступают уже в прямое противоречие с самой квалификацией деяния по ст. 272 УК РФ: «…При этом доступ к центральной базе данных филиала В. был предоставлен работодателем при трудоустройстве последней, путем присвоения ей логина, создания пароля и предоставления электронной цифровой подписи, находящейся на ТМ-идентификаторе, которые В. использовала при исполнении ею своих служебных обязанностей, в связи с чем, в судебном заседании установлено наличие в действиях В. квалифицирующего признака с использованием своего служебного положения, предусмотренного ч. 3 ст. 272 УК РФ, ввиду того, что она при совершении инкриминируемых деяний, связанных с модификацией охраняемой законом компьютерной информации, содержащейся в центральной базе данных филиала, *имела к ней доступ* (выделено мной. – *Е.Р.*) в силу исполнения ею своих должностных обязанностей»[1].

Как представляется, работник кредитной организации, обладая *не аннулированным доступом* к служебной базе данных, имея соответствующие сетевые идентификаторы для работы, не может совершить неправомерный доступ к хранящейся в ней информации. Вместе с тем, такой работник может нарушить правила эксплуатации такой системы, как в приведенном решении – внести недостоверные сведения об обращениях клиентов банка за выдачей платежных карт.

Практика квалификации действий, связанных с уничтожением, модификацией или копированием охраняемой законом компьютерной ин-

[1] Приговор Ленинского районного суда г. Курска от 08 августа 2019 г. № 1-336/4-2019.

формации, совершенных лицами, которые на законных основаниях используют компьютерную информацию и средства ее обращения (программисты, системные администраторы, администраторы баз данных, специалисты по эксплуатации объектов информационно-телекоммуникационной инфраструктуры и др.), как неправомерного доступа по ч. 3 ст. 272 УК РФ, является широко распространенной[1] и, полагаем, вынужденной. Объективная необходимость каким-либо образом реагировать на подобные (согласимся, весьма опасные!) инциденты служебного злоупотребления со стороны лиц, которым были доверены соответствующие объекты информационно-телекоммуникационной инфраструктуры, вкупе с трудностями в установлении требуемого ст. 274 УК РФ крупного ущерба, обусловили искусственное расширение пределов действия уголовно-правового запрета об ответственности за неправомерный доступ.

Субъективная сторона преступного нарушения правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям характеризуется двумя формами вины. Нарушение правил эксплуатации и доступа, предусмотренное ч. 1 ст. 274 УК РФ, может совершаться как умышленно (при этом умысел должен быть направлен на нарушение правил эксплуатации и доступа), так и по неосторожности.

По мнению Р.Р. Гайфутдинова, субъективная сторона преступлений, предусмотренных ст. 274 и ч. 3 ст. 274[1] УК РФ, характеризуется исключительно неосторожной формой вины. Данный автор аргументирует это тем, что субъективная сторона деяния при нарушении правил характеризуется расчетом на предотвращение наступления последствий с надеждой на себя или другие объективные факторы, либо им они должны были и могли предвидеться (при должной внимательности и предусмотрительности), что характеризует уже небрежность[2].

Данная позиция представляется дискуссионной. Такое ограничительное толкование исследуемой нормы приводит к закономерному выводу, что умышленные действия работника организации, направленные на выведение из строя ее информационно-коммуникационной инфраструктуры, не могут быть квалифицированы не только по ст. 274 УК РФ, но и вообще в рамках отечественного уголовного законодательства.

---

[1] См.: Русскевич Е.А. О квалификации преступлений в сфере компьютерной информации, совершаемых с использованием служебного положения // Российское правосудие. – 2019. – № 2. – С. 35–41.

[2] Гайфутдинов Р.Р. Понятие и квалификация преступлений против безопасности компьютерной информации : дис. … канд. юрид. наук. Казань, 2017. С. 136.

При этом следует отметить, что подобное поведение и соответствующая оценка по ст. 274 УК РФ имеет место в правоприменительной практике. Так, например, А., имея умысел на нарушение правил эксплуатации средств хранения, передачи охраняемой компьютерной информации, повлекшее копирование компьютерной информации, находясь на своём рабочем месте, используя средства авторизации (логин и пароль), и имея, в силу исполняемых обязанностей, доступ к информационным носителям, на которых содержится охраняемая компьютерная информация, и действуя в нарушение Федерального закона «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года №149-ФЗ, ст.1225 ГК РФ «Охраняемые результаты интеллектуальной деятельности и средства индивидуализации», Указа Президента Российской Федерации от 06 марта 1997 года №188 «Перечень сведений конфиденциального характера», соглашения о сохранении служебной и коммерческой тайны, соглашения о конфиденциальности для сотрудников, а также должностной инструкции по должности ведущий системный администратор, скопировал на электронный носитель информацию из базы данных, а именно: не менее 40000 записей, содержащих не прошедших проверку имён, фамилий, никнеймов (имена, которые используется при регистрации на интернет сайтах), а так же адресов электронной почты. После чего А. передал вышеуказанную информацию В., который не был осведомлён о том, что полученная им информация охраняется действующим законодательством РФ. Вышеуказанные действия А. причинили ущерб, который выражается в следующих вынужденных действиях, которые были проведены сотрудниками юридического лица, а именно: 1) восстановление доступа к базе данных после смены всех паролей сотрудников, имеющих доступ к серверам, а так же смена паролей в учётных записях серверов и сервисов (общие затраты 388000 рублей); 2) проведения комплекса мероприятий, направленных на поиск лица (А.), которое копировало информацию из базы данных (общие затраты 153000 рублей); 3) средний простой 115 сотрудников, имеющих доступ к серверам, из-за необходимости их перенастройки составил 12 часов, то есть суммарно 920 часов на ожидание восстановления доступа к серверам, которые были оплачены организацией (общие затраты 414000 рублей); 4) покупка оборудования для сотрудников, взамен изъятого у А. по окончании служебной проверки (общие затраты 45330 рублей); 5) введение дополнительных средств учёта лиц, осуществляющих доступ к базе данных организации, а так же механизмов сохранения информации, направленных на недопущение копирования информации без согласования с руководством организации (общие затраты 155270 рублей).Таким образом, А. нарушил правила эксплуатации средств хранения и передачи охраняемой компьютерной информации, повлекшее

копирование компьютерной информации, чем причинил крупный вред юридическому лицу на общую сумму 1155600 рублей[1].

Мотивы преступления и его цели (если таковые имеются) не являются необходимыми признаками субъективной стороны анализируемого преступления и, следовательно, на квалификацию не влияют. Однако они должны учитываться в рамках общих начал назначения наказания.

Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей довольно часто может быть сопряжено с совершением других преступлений. Так, умышленное вмешательство в нормальное функционирование автоматизированных систем управления технологическим процессом (АСУ ТП) может быть обусловлено стремлением лица обеспечить осуществление другого преступления. Изучение материалов правоприменительной практики показывает, что, как правило, квалификация подобных деяний имеет неполный характер, оставляя без оценки действия лица, выразившиеся в нарушении правил эксплуатации объектов информационно-телекоммуникационной инфраструктуры. Так, С. был осужден п. «а» ч. 4 ст. 158 УК РФ. Согласно приговору суда, С., являясь оператором приемо-сдаточного пункта линейной производственно-диспетчерской станции, в чьи производственные обязанности входил отпуск нефтепродуктов на указанном пункте через автомобильную систему налива, заведомо зная функционал работы программного обеспечения «автоматизированная система оперативно-коммерческого учета движения нефтепродуктов» и прикладной программы к нему, из корыстных побуждений вступил в преступный сговор с Б., в ходе которого у данных лиц возник единый умысел, направленный на хищение дизельного топлива в особо крупном размере. С., реализуя преступный умысел, тайно в ходе исполнения своих производственных обязанностей по отпуску дизельного топлива посредством программного обеспечения «АРМ налива 3.0. вариант Воронеж» на приемо-сдаточном пункте похитил дизельное топливо объемом 219 820 литров общей стоимостью 7 529 167 рублей 65 копеек, путем размыкания в шкафу автоматики проводов, отвечающих за связь устройства съема сигнала с датчиком контроллера насоса, установленного на автомобильной системе налива, что позволило осуществлять налив дизельного топлива сверх установленного, согласно накладным объема от-

[1] Постановление Лефортовского районного суда г. Москвы от 13 января 2015 г. по делу № 1-401/2014 (дело было прекращено по основаниям, предусмотренным ст. 78 УК РФ).

пущенного нефтепродукта, без учета программным обеспечением «АРМ налива 3.0. вариант Воронеж»[1].

Учитывая, что практически все современные системы безопасности труда, охранно-пожарной сигнализации, контроля и управления доступа и др., разрабатываются и функционируют на основе использования компьютерной техники, нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, может быть сопряжено и с совершением преступлений, предусмотренных ст.ст. 143, 215–215.4, 216, 217, 217.1, 219 УК РФ. Полагаем, что при каждом подобном случае органы предварительного расследования должны рассматривать не только допущенные нарушения правил охраны труда или пожарной безопасности, но и оценивать действия (бездействие) системных администраторов, инженеров-программистов предприятия, отвечающих за нормальное функционирование автоматизированных систем охранно-пожарной сигнализации, управления технологическим процессом и т.п.

В отдельных случаях допущенные лицом нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей получают неверную юридическую оценку. Так, П. была оправдана в совершении преступления, предусмотренного ч. 3 ст. 159 УК РФ. Согласно приговору суда, П. работала в управляющей организации инженером-программистом, затем – начальником абонентского отдела, а в последующем – заместителем директора по экономическим вопросам. В силу возложенных на П. должностных обязанностей, а после назначения ее на должность заместителя директора по экономическим вопросам – в связи с фактическим исполнением ею обязанностей инженера-программиста и начальника абонентского отдела предприятия, П. имела доступ к банковским реестрам, а также к программе «1 С Квартплата». Имея высшее образование в области информатики и вычислительной техники, обладая специальными познаниями в сфере программного обеспечения, П., с учетом предоставленного ей допуска к банковским реестрам и программе «1 С Квартплата», путем корректировки лицевых счетов неоднократно вносила изменения в поступившие из банков реестры, а также в программу «1 С Квартплата». А именно: заменяла указанные в реестрах и данной программе номера лицевых счетов плательщиков на присвоенные ей и ее отцу управляющей организацией лицевые счета, предназначенные для оплаты за содержание,

[1] Приговор Новоусманского районного суда Воронежской области от 23 июля 2019 г. по делу № 1-231/2019.

текущий и капитальный ремонт жилого дома… Как следует из предъявленного П. обвинения, она, используя свое служебное положение, злоупотребляя доверием директора, сотрудников управляющей организации и плательщиков, путем замены в банковских реестрах и программе «1 С Квартплата» номеров лицевых счетов плательщиков на присвоенные ей и ее отцу управляющей организацией лицевые счета, похитила принадлежащие управляющей организации денежные средства на общую сумму 109 278 рублей 25 копеек, распорядившись ими по своему усмотрению. А именно, оставив на присвоенных ей и ее отцу лицевых счетах, с которых в последующем производилось списание в счет предоставленных П. услуг по содержанию, текущему и капитальному ремонту домов, причинив своими действиями материальный ущерб на указанную сумму. Между тем, в ходе судебного разбирательства в действиях П. не установлено ни физического изъятия чужого имущества, ни приобретения права на чужое имущество путем злоупотребления доверием. Денежные средства предприятия ни П., ни ее отец не получали, право на них не приобретали. Корректировка об оплате жилищно-коммунальных услуг по лицевым счетам, открытым на имя П. и ее отца, в программе «1 С Квартплата», банковских реестрах, о чем указывается в обвинении и установлено судом, не является по смыслу уголовного законодательства хищением, не лишает собственника, иное лицо, в пределах предоставленных ему полномочий, права владеть, пользоваться и распоряжаться находящимися у него денежными средствами, в том числе поступившими на его расчетный счет. Распорядиться деньгами управляющей организации путем оставления их на лицевых счетах, отрытых на имя подсудимой и на имя ее отца, как на то указывается в обвинении, П. не могла, поскольку денежные средства с расчетного счета предприятия на лицевые счета, отраженные в программе «1 С Квартплата», не перечисляются, на последних не аккумулируются. Указанная программа «1 С Квартплата» носит информационный характер, не имеет привязки к расчетному счету предприятия, а на лицевые счета, присвоенные абонентам, денежные средства ни с расчетного счета управляющей организации, ни с иных источников предприятия не корреспондируются. Следовательно, считать в данном случае предметом хищения безналичные либо электронные денежные средства, к чему фактически сводятся доводы стороны обвинения, оснований не имеется[1].

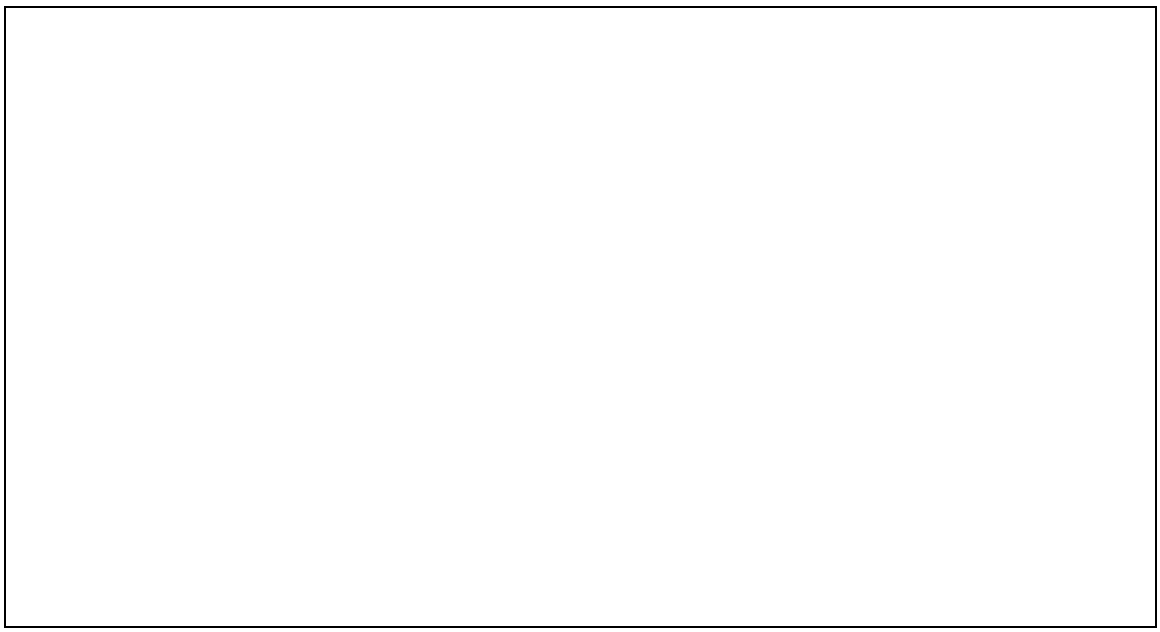
Как представляется, суд пришел к правильному выводу о том, что действиями подсудимой управляющей организации был причинен ущерб

[1] Приговор Бежецкого городского суда Тверской области от 27 марта 2018 г. по делу №1-3/2018.

в виде упущенной выгоды, то есть неполученных доходов, которые предприятие получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено. Однако, с учетом размера причиненного ущерба (109 278 рублей 25 копеек), в действиях П. не усматривается ни состава преступления, предусмотренного ст. 165 УК РФ, ни ст. 274 УК РФ.

1.4 НЕПРАВОМЕРНОЕ ВОЗДЕЙСТВИЕ НА ОБЪЕКТЫ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ (СТ. 274[1] УК РФ)

С 1 января 2018 г. вступил в силу Федеральный закон от 26 июля 2017 г. №194-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»[1], которым глава 28 УК РФ была дополнена специальной нормой об ответственности за неправомерное воздействие на объекты критической информационной инфраструктуры Российской Федерации (ст. 274[1]).



Специальная уголовно-правовая охрана информационно-коммуникационного комплекса, обеспечивающего нормальное функционирование особо важных для общества и государства объектов, не является изобретением российского законодателя и встречается во многих современных правовых режимах. Положения об уголовной ответственности за посягательства на публичные информационные

[1] Российская газета. №167. 31.07.2017 г.

ресурсы, обладающие исключительной значимостью, имеются в законодательстве Великобритании, Германии, Китая, Сингапура, США, Франции и др. В рамках СНГ использование категории «объект критической информационной инфраструктуры» пока ещё не получило широкого распространения. Так, в ряду квалифицирующих признаков совершения компьютерных преступлений УК Азербайджана содержится указание на «инфраструктурные объекты общественного значения». В соответствии с примечанием к ст. 271 УК Азербайджана, под такими объектами подразумеваются государственные учреждения, предприятия, организации, неправительственные организации (общественные объединения и фонды), кредитные организации, страховые компании, инвестиционные фонды, которые представляют большую значимость для государства и общества[1].

Новый Уголовный кодекс Республики Казахстан использует ограничительный подход и дифференцирует преступления в сфере компьютерной информации в зависимости от их направленности на «государственные электронные информационные ресурсы и информационные системы государственных органов», то есть только те электронные информационные ресурсы, которые были созданы или приобретены за счет бюджетных средств[2].

Всемирно известными примерами компьютерных атак на критическую инфраструктуру государства являются остановка центрифуг иранской атомной станции с помощью компьютерного вируса «StuxNet» в сентябре 2010 г. и выведение из строя нескольких крупных финансовых учреждений Южной Кореи в марте 2013 г. Отечественные объекты также подвергались неправомерным воздействиям со стороны киберпреступников. При этом назначенные наказания за их совершение нельзя назвать не то чтобы строгими, но хотя бы относительно адекватными содеянному. Так, в мае 2012 г. житель Красноярска, являясь последователем движения Anonymous, совершил хакерскую атаку на сайт Президента РФ. Суд приговорил его к одному году лишения свободы. Примерно через год практически идентичную атаку совершил житель Томска, вызвав блокировку

[1] [Электронный ресурс] // Уголовный кодекс Азербайджанской Республики от 30 декабря 1999 г. №787-IQ (с изм. и доп. по сост. на 31.05.2016 г.) // URL : http://online.zakon.kz/m/Document/?docid=30420353#sub_id=2710000 (дата обращения: 07.03.2018).

[2] [Электронный ресурс] // Уголовный кодекс Республики Казахстан от 3 июля 2014 г. №226-V (с изм. и доп. по сост. на 11.07.2017 г.) // URL : http://online.zakon.kz/m/Document/?doc_id=33885902 #sub_id=320200 (дата обращения: 07.03.2018).

указанного сайта. По данному делу суд назначил ещё более мягкое наказание – полтора года ограничения свободы[1].

Не впадая в бесплодный оптимизм, следует с сожалением констатировать, что в будущем инциденты подобного рода более чем вероятны. Меры информационной защиты, подобно всем мерам юридического противодействия криминальным явлениям, всегда имеют догоняющий характер. Стремительно развивающаяся архитектура виртуального пространства не только качественно улучшает нашу жизнь, но и параллельно с этим генерирует новые риски и угрозы. В докладе The Global Risks Report 2016, подготовленном по итогам Давосского экономического форума, выход из строя критически важной информационной инфраструктуры (critical information infrastructure breakdown) назван среди наиболее актуальных угроз мировой экономике[2]. В связи с чем информационные ресурсы стратегического значения, связанные с обеспечением общественной и государственной безопасности, должны быть действенно и эффективно защищены, в том числе с помощью системы дифференцированных мер уголовной ответственности за посягательства на их доступность и целостность.

Редакция ст. 274[1] УК РФ представляет собой объединение трёх традиционных для отечественного законодательства форм преступного посягательства на безопасность компьютерных данных и систем: 1) неправомерный доступ, 2) создание и распространение вредоносного контента и 3) нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации.

По смыслу ст. 274[1] УК РФ, все эти деяния должны быть направлены против объектов критической информационной инфраструктуры. Таким образом, анализируемая уголовно-правовая норма конкурирует сразу с тремя статьями (ст.ст. 272, 273 и 274 УК РФ) и является специальной по отношению к ним. В некотором смысле конструирование ст. 274[1] УК РФ противоречит сложившимся отечественным традициям криминализации и использования приёмов юридической техники при описании уголовно-правовых норм. Следуя им, установление более строгой уголовной ответственности за посягательства на объекты критической информационной инфраструктуры предпочтительнее было бы реализовать путем выделения соответствующих квалифицирующих и особо квалифицирующих признаков в ст.ст. 272, 273 и 274 УК РФ.

---

[1] См.: Осуждён томский хакер, взломавший сайт Президента РФ // РИА Новости. 2013. 23 декабря.

[2] The Global Risks Report 2016: Электронный ресурс: URL: http://www.mmc.com/content/dam/mmc-web/Global-Risk-Center/Files/world-economic-forum-global-risk-report-2016.pdf (дата обращения: 27.03.2018).

Анализируемая уголовно-правовая норма имеет бланкетный характер, что предполагает обязательное обращение к Федеральному закону от 26.07.2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[1].

Объектом преступлений, предусмотренных ст. 274[1] УК РФ, выступает безопасность критической информационной инфраструктуры Российской Федерации, то есть состояние ее защищенности от любого воздействия программными или программно-техническими средствами, которое способно привести к нарушению ее функционирования и (или) нарушению безопасности обрабатываемой ею информации.

Предметом преступления, предусмотренного частью 1 ст. 274[1] УК РФ, является компьютерная информация или компьютерные программы, заведомо предназначенные для совершения компьютерных атак на объекты критической информационной инфраструктуры. Нельзя не отметить, что установление данного признака на практике может вызвать значительные затруднения. Функциональная направленность вредоносной программы, то есть её предназначение именно для посягательств на соответствующие объекты, может быть установлена только в случае уникальности средств и технологий программной защиты объектов критической информационной инфраструктуры, что представляется маловероятным.

Специфическим предметом преступлений, предусмотренных частями 2 и 3 ст. 274[1] УК РФ, выступают объекты критической информационной инфраструктуры – информационные системы, информационно-телекоммуникационные сети государственных органов, а также информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления технологическими процессами, функционирующие в оборонной промышленности, области здравоохранения, транспорта, связи, кредитно-финансовой сфере, энергетике, топливной промышленности, атомной промышленности, ракетно-космической промышленности, горнодобывающей промышленности, металлургической промышленности и химической промышленности.

Относимость того или иного информационного ресурса к критическому определяется посредством его включения в Реестр значимых объектов критической информационной инфраструктуры (ст. 8 Федерального закона от 26.07.2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»).

Объективная сторона преступления, предусмотренного частью 1 ст. 274[1] УК РФ, предполагает совершение любого из трёх альтернативных действий: 1) создание, 2) использование или 3) распространение компьютерных программ или информации, заведомо предназначенных для

[1] Российская газета, №167, 31.07.2017 г.

совершения атак на объекты критической информационной инфраструктуры.

Состав по конструкции (по моменту описания в законе момента окончания преступления) является формальным. Если лицо одновременно разработало, использовало и распространило вредоносную компьютерную программу, заведомо предназначенную для совершения компьютерных атак на объекты критической информационной инфраструктуры, содеянное образует единое преступление.

Объективная сторона преступления, предусмотренного частью 2 ст. 274^1 УК РФ, заключается в неправомерном доступе к компьютерной информации, содержащейся в критической информационной инфраструктуре. Состав по конструкции является материальным. Преступление считается оконченным только в случае причинения вреда критической информационной инфраструктуре Российской Федерации. Таким образом, следует сделать вывод, что сам по себе неправомерный доступ (так называемое «чистое хакерство», осуществляемое из профессионального интереса без намерения причинить вред) по смыслу ч. 2 ст. 274^1 УК РФ не является преступлением. В свою очередь, если лицу, осуществившему неправомерный доступ к компьютерной информации, содержащейся в критической информационной инфраструктуре, по независящим от него обстоятельствам не удалось причинить вред критической информационной инфраструктуре Российской Федерации (например, в результате успешного срабатывания антивирусного программного обеспечения или действий сотрудников, отвечающих за информационную безопасность организации) содеянное следует квалифицировать как покушение на преступление по ч. 3 ст. 30, ч. 2 ст. 274^1 УК РФ.

Вред, как конструктивный признак состава преступления, предусмотренного ч. 2 ст. 274^1 УК РФ, не конкретизирован. Системное толкование отечественного уголовного законодательства позволяет сделать вывод, что таковым является уничтожение, блокирование, модификация, копирование информации, содержащейся в критической информационной инфраструктуре, нейтрализация средств защиты указанной информации или выведение из строя аппаратных и программных средств, обеспечивающих функционирование критической информационной инфраструктуры (за исключением случаев, когда это повлекло причинение смерти или тяжкого вреда здоровью человека, причинение средней тяжести вреда здоровью двум или более лицам, массовое причинение лёгкого вреда здоровью людей, наступление экологических катастроф, транспортных или производственных аварий, повлёкших длительную остановку транспорта или производственного процесса, дезорганизацию работы конкретного

предприятия, причинение особо крупного ущерба, то есть тяжких последствий[1], предусмотренных ч. 5 ст. 274[1] УК РФ).

Следует отметить, что подобное толкование последствий анализируемого состава преступления реализовано и на правоприменительном уровне. Так, О., Л.А. и Л.С. были осуждены по ч. 4 ст. 274[1] УК РФ. Согласно приговору суда, О., действуя по предварительному сговору с Л.А. и Л.С., используя вредоносную компьютерную программу в нарушение ч. 4 ст. 29 Конституции РФ, ч.ч. 1, 2 и п. 3 ч. 3 ст. 5, пунктов 1–3 ч. 1 ст. 16 и ст. 17 Федерального закона № 149-ФЗ «Об информации, информационных технологиях и о защите информации», с целью выявления уязвимых машин (персональных компьютеров различных организаций), осуществил нейтрализацию средств защиты компьютерной информации путем перебора логина и пароля (брутфорс), и произвел сканирование диапазона IP-адресов Российской Федерации в целях выявления открытых портов и дальнейшей проверки их на наличие возможности удаленного к ним доступа по RDP протоколу. Полученную информацию об IP-адресах, номерах портов подключения, логинах и паролях доступа к ЭВМ он передал Л.А. и Л.С. Те, в свою очередь, действуя совместно, согласно достигнутой ранее преступной договоренности, используя предоставленную О. информацию о выявленных IP-адресах, номерах портов подключения, логинах и паролях доступа к ЭВМ, используя компьютерную программу, получили удаленный доступ к ЭВМ АО «Восточная верфь», после чего, осуществили неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации путем ее *блокирования и модификации* (выделено мной. – *Е.Р.*), что повлекло причинение вреда критической информационной инфраструктуре АО «Восточная верфь», и причинение имущественного вреда указанной организации на сумму 655 034,52 рублей. Таким образом, Л.А., Л.С. и О., действуя совместно и по предварительному сговору, осуществили модификацию и блокирование охраняемой компьютерной информации, содержащейся в информационных системах и информационно-телекоммуникационных сетях, функционирующих в субъекте оборонной промышленности – АО «Восточная верфь»…, что *повлекло причинение вреда критической информационной инфраструктуре, выразившегося в модификации компьютерной информации и воздействиях на*

[1] См. подробнее: Гузеева О. С. Преступления, совершаемые в российском сегменте сети Интернет: монография. М.: Академия Генеральной прокуратуры Российской Федерации, 2015. С. 37; Русскевич Е. А. Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий: учебное пособие. М.: Научно-издательский центр ИНФРА-М, 2017. С. 44.

компьютерную информацию и технику, последствием которого невозможно осуществлять требуемые операции над компьютерной информацией (выделено мной. – *Е.Р.*) полностью или в требуемом режиме, совершив действия, приводящие к ограничению и закрытию доступа к компьютерному оборудованию и находящейся на нём информации[1].

Следует отдельно указать, что диспозиция ч. 2 ст. 274[1] УК РФ по сути содержит признаки составного преступления, поскольку указывает, что под неправомерным доступом следует также понимать доступ с использованием компьютерных программ либо иной компьютерной информации, которые заведомо предназначены для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, или иных вредоносных компьютерных программ. Таким образом, ч. 2 ст. 274[1] УК РФ охватывает и не требует квалифицировать по совокупности, неправомерный доступ к объектам критической информационной инфраструктуры, совершенный с использованием заведомо предназначенных для этого вредоносных программ (ч. 1 ст. 274[1] УК РФ) или иных вредоносных программ (ст. 273 УК РФ). При этом, если лицо, использовавшее программу, являлось и ее разработчиком, содеянное необходимо квалифицировать по совокупности преступлений. В данном случае вполне применимо известное правило квалификации, согласно которому действия по подготовке или исполнению деяния, не входящие в объективную сторону оконченного преступления (которые по сути не являются юридически значимым способом совершения этого преступления), должны получить самостоятельную уголовно-правовую оценку по другой статье закона[2].

Кроме того, совокупность преступлений, предусмотренных ст. 273 УК РФ и ч. 1 ст. 30 ч. 2 ст. 274[1] УК РФ, может иметь место и в том случае, когда лицо создаёт компьютерную программу либо иную компьютерную информацию, которые заведомо предназначены для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации. Однако в этом случае необходимо доказать умысел лица на их дальнейшее использование.

Практически значимым аспектом является оценка действий субъекта, который за вознаграждение изготавливает вредоносное программное обеспечение, предназначенное по своим характеристикам на осуществление атаки на объект критической информационной инфраструктуры, и сбывает его. При отсутствии осведомлённости о том,

---

[1] Приговор Первомайского районного суда г. Владивостока от 25 сентября 2019 г. по делу № 1-376/2019.

[2] См., подробнее: Решетников А. Ю. Квалификация неоконченных преступлений при наличии признаков совокупности преступлений // Вестник Академии Генеральной прокуратуры Российской Федерации. 2016. № 4. С. 85.

что с данным информационным орудием собирается делать заказчик, действия соответствующих лиц нельзя признать согласованными и совместными. Это исключает саму постановку вопроса о возможности соучастия в данном случае. При обратной ситуации, когда лицо понимает, для каких целей изготавливается данная программа, содеянное необходимо квалифицировать как пособничество в совершении неправомерного доступа, то есть по ч. 5 ст. 33 ч. 2 ст. 274^1 УК РФ.

Объективная сторона преступления, предусмотренного частью 3 ст. 274^1 УК РФ, заключается в нарушении:

1) правил эксплуатации: а) средств хранения, обработки или передачи охраняемой компьютерной информации, б) информационных систем, в) информационно-телекоммуникационных сетей, г) автоматизированных систем управления, д) сетей электросвязи, относящихся к критической информационной инфраструктуре Российской Федерации,

2) правил доступа к указанным средствам, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи.

Состав по конструкции является материальным; преступление считается оконченным только в случае причинения вреда критической информационной инфраструктуре Российской Федерации. В отличие от ст. 274 УК РФ, характеризующейся двумя уровнями взаимосвязанных общественно опасных последствий, ч. 3 ст. 274^1 УК РФ не предполагает установления признака крупного ущерба.

Учитывая специфику объектов посягательства, следует отметить, что совершение компьютерных атак на информационные ресурсы объектов транспорта, оборонной, атомной, ракетно-космической или химической промышленности, может содержать признаки и других преступлений, предусмотренных ст.ст. 205, 281, 275, 276 УК РФ и др.

Субъектом преступлений, предусмотренных частями 1 и 2 ст. 274^1 УК РФ, является физическое вменяемое лицо, достигшее возраста 16 лет. Субъектом ч. 3 ст. 274^1 УК РФ может быть как общий – в части правил доступа к ресурсам, так и специальный – в части соблюдения правил эксплуатации соответствующих средств, систем и сетей.

Субъективная сторона создания, использования и распространения компьютерных программ или информации, заведомо предназначенных для совершения атак на объекты критической информационной инфраструктуры, характеризуется прямым умыслом. Лицо, совершая те или иные действия, должно осознавать, что они направлены на публичные информационные ресурсы, обладающие исключительной важностью для общества и государства и включённые в соответствующий реестр.

При неправомерном доступе (ч. 2 ст. 274^1 УК РФ) умысел может быть как прямым, так и косвенным.

Субъективная сторона преступления, предусмотренного ч. 3 ст. 274^1 УК РФ характеризуется двумя формами вины. Нарушение правил

эксплуатации и доступа может совершаться как умышленно, так и по неосторожности. Следует поддержать точку зрения Н. Ш. Козаева, что неуказание на форму вины в составе нарушения правил эксплуатации средств хранения, обработки или передачи компьютерных данных (автор формулирует данный вывод применительно к ст. 274 УК РФ) является «упущением законодателя, поскольку сама конструкция состава логически требует признания возможности совершения деяния по неосторожности, но ч. 2 ст. 24 УК РФ позволяет признавать преступление совершённым по неосторожности, только если это предусмотрено соответствующей статьёй Особенной части УК РФ»[1].

Квалифицированные виды неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, предусмотренные ч. 4 и 5 ст. 274[1] УК РФ, являются традиционными для преступлений в сфере компьютерной информации и в целом хорошо освещены в современной литературе[2].

[1] Козаев Н. Ш. Современные технологии и проблемы уголовного права (анализ зарубежного и российского законодательства): монография. М.: Юрлитинформ, 2015. С. 172.

[2] См., например: Комментарий к Уголовному кодексу Российской Федерации (научно-практический, постатейный): 5-е издание, переработанное и дополненное // под ред. д-ра юрид. наук, профессора Дьякова С. В., д-ра юрид. наук, профессора Кадникова Н. Г. М.: ИД «Юриспруденция», 2017. С. 822 – 834.

ГЛАВА 2. ПРОБЛЕМЫ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

2.1 ПРОБЛЕМЫ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ (КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ)

Проблемные вопросы квалификации неоконченных преступлений в сфере компьютерной информации

Традиционной и одновременно непростой является проблематика юридической оценки неоконченной преступной деятельности. Момент окончания преступления, предусмотренного ст. 272 УК РФ, в теории уголовного права традиционно определяется наступлением последствий в виде уничтожения, блокирования, модификации или копирования охраняемой законом компьютерной информации[1]. Учитывая, что указанные последствия не взаимосвязаны между собой и являются альтернативными признаками анализируемого состава преступления, неправомерный доступ следует считать оконченным и тогда, когда фактически наступило лишь одно из них (например, копирование)[2]. Таким образом, сам по себе неправомерный доступ (так называемое «чистое хакерство», осуществляемое из профессионального интереса без намерения причинить вред), по смыслу ст. 272 УК РФ, не является преступлением.

Специалисты отмечают, что современные технические средства в ряде случаев позволяют восстановить утраченную информацию полностью или какую-то её часть. Однако, полагают исследователи, это не освобождает от уголовной ответственности по ч. 1 ст. 272 УК РФ такое лицо, которое совершило неправомерный доступ к охраняемой законом компьютерной

---

[1] См., например: Гузеева О. С. Преступления, совершаемые в российском сегменте сети Интернет: монография. М.: Академия Генеральной прокуратуры Российской Федерации, 2015; Козаев Н. Ш. Современные технологии и проблемы уголовного права (анализ зарубежного и российского законодательства): монография. М.: Юрлитинформ, 2015; Русскевич Е. А. Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий: учебное пособие. М.: Научно-издательский центр ИНФРА-М, 2017 и др.

[2] См.: Решетников А. Ю., Букалерова Л. А. Конструкция состава преступления и ее влияние на установление момента его окончания // Уголовное наказание в России и за рубежом: проблемы назначения и исполнения (к 10-летию принятия Европейский пенитенциарных правил). Сб. матер. междунар. науч.-практ. конференции. В 2-х частях / под общ. ред. П.В. Голодова. – Вологда, 2017. С. 249 – 251.

информации и затем попыталось её уничтожить, поскольку преступная цель оказалась не реализована по не зависящим от лица обстоятельствам. В связи с чем подобные действия следует оценивать как покушение на уничтожение охраняемой законом компьютерной информации по ч. 3 ст. 30 ч. 1 ст. 272 УК РФ[1].

Следует заметить, что наличие или отсутствие у потерпевшего системы архивного копирования и аварийного восстановления данных, вряд ли может однозначно предрешать вопрос об уголовной ответственности, единственным основанием наступления которой служит описанное в уголовном законе деяние, содержащее признаки состава преступления. А потому вывод о том, что предусмотренные ст. 272 УК РФ последствия не наступают, может быть оценен критически.

Как уже отмечалось ранее, юридический и фактический моменты окончания неправомерного доступа к компьютерной информации могут не совпадать. Копирование и модификация информации, как правило, не осуществляются одномоментно. При копировании значительных объёмов компьютерных данных процесс может потребовать несколько десятков минут, а иногда и часов. Вместе с тем, в случае, когда лицо, по независящим обстоятельствам не смогло скопировать или модифицировать заранее определённый объём информации (например, целиком заполучить интересующую его базу данных), содеянное всё равно образует оконченное преступление. Несмотря на то что умысел лица не был реализован в полном объёме, это свидетельствует лишь о фактической незавершённости деяния, в юридическом же смысле оно было окончено с момента копирования или модификации первого файла. Копирование (модификацию) информации в данном случае следует оценивать как процесс, ориентированный на определённый результат (получение полного объёма данных или их видоизменение). Однако этот результат (преступная цель) лежит за рамками состава преступления, предусмотренного ст. 272 УК РФ. А потому этот процесс, с учётом предписаний уголовного закона, следует оценивать как юридически завершённый преступный акт с момента его начала.

При этом как покушение на неправомерный доступ к охраняемой законом информации следует оценивать действия лица по установке специального оборудования, предназначенного для её скрытого копирования.

---

[1] См.: Быков В. М., Черкасов В. Н. Преступления в сфере компьютерной информации: криминологические, уголовно-правовые и криминалистические проблемы: монография. М., 2015. С. 116.

В правоприменительной практике подобная квалификация наиболее часто встречается по делам об установке так называемых «скиммеров»[1] на банкоматы.

Так, М. был осуждён по ч. 3 ст. 30 ч. 3 ст. 272 УК РФ – за покушение на неправомерный доступ к охраняемой законом компьютерной информации группой лиц по предварительному сговору. Согласно решению суда, движимый корыстными побуждениями М., находясь в неустановленном месте, вступил с неустановленным лицом в сговор, направленный на неправомерный доступ к охраняемой законом компьютерной информации, содержащейся на магнитных полосах пластиковых платёжных банковских карт неопределённого круга граждан путем ее копирования, с целью дальнейшей записи откопированной информации на магнитные полосы дубликатов платёжных карт, и последующего использования.

Реализуя задуманное, М. и неустановленное лицо, прибыли к банкомату, где М., осознавая противоправный характер своих действий, действуя из корыстных побуждений, согласно отведённой ему роли подошёл к вышеуказанному банкомату и установил «скимминговое» оборудование, а именно закрепил перед картоприёмником банкомата «скиммер», выполненный в виде накладной панели, закамуфлированной под конструктивный элемент картоприёмника банкомата, предназначенный для получения (копирования) информации, записанной на магнитную полосу пластиковых платёжных карт при их прохождении через картоприёмник банкомата, а также закрепил над клавиатурой банкомата видеорегистратор, выполненный в виде пластиковой планки, предназначенный для получения информации, вводимой пользователями посредством клавиатуры банкомата, в том числе PIN-кодов, таким образом привёл указанное нештатное оборудование в комплекте в работоспособное состояние, дающее возможность получения (копирования) вышеуказанной информации, которая согласно ФЗ №149 от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации» является охраняемой законом компьютерной информацией.

Довести свой преступный умысел, направленный на неправомерный доступ к охраняемой законом компьютерной информации путём её копирования, из корыстной заинтересованности, группой лиц по предварительному сговору, до конца М. и неустановленное лицо не смогли по независящим от них обстоятельствам, так как М. был задержан сотрудниками правоохранительных органов сразу после установки на

[1] Скиммер представляет собой устройство, скрытно устанавливаемое на картоприёмник банкомата, предназначенное для считывания данных магнитной полосы карты в целях их последующего воспроизведения на поддельной карте.

банкомат вышеуказанного внештатного оборудования, а неустановленное лицо успело скрыться с места преступления[1].

Неправомерный доступ к охраняемой законом компьютерной информации, осуществляемый под скрытым контролем сотрудников правоохранительных органов, следует квалифицировать как покушение на преступление, предусмотренное ст. 272 УК РФ.

Так, З. был осуждён по ч. 3 ст. 30, ч. 1 ст. 272 УК РФ – за покушение на неправомерный доступ к охраняемой законом компьютерной информации в целях её модификации. Согласно приговору, З., находясь на рабочем месте в мастерской по ремонту мобильных телефонов, с целью неправомерного доступа и модификации охраняемой законом информации, действуя умышленно, из корыстных побуждений, в рамках оперативно-розыскного мероприятия «проверочная закупка», за вознаграждение в размере 200 рублей, принял заказ от лица, выступавшего в роли закупщика, на смену международного идентификатора мобильного оборудования мобильного телефонного аппарата (IMEI), являющегося уникальным параметром, не подлежащим изменению, позволяющим операторам компаний сотовой связи обнаружить и идентифицировать аппарат в случае его утери, либо хищения. Реализуя преступный умысел и осознавая противоправность своих действий, З., используя имеющийся у него программатор, с помощью сервисного кабеля, подключил мобильный телефонный аппарат, переданный ему лицом, выступавшим в роли закупщика, к программатору, после чего подключил программатор к находящемуся в мастерской компьютеру. В продолжение реализации своих преступных намерений, используя находящуюся в пакете программного обеспечения программатора программу, получил неправомерный доступ к охраняемой законом информации об его IMEI-номере, а также возможность уничтожения и модификации указанной информации. После чего в нарушение требований ст.ст. 1225, 1261 части четвёртой Гражданского кодекса РФ произвёл модификацию (изменение) цифр IMEI-номера.

В результате преступных действий З. в мобильном телефонном аппарате, с использованием компьютерной программы, был изменён IMEI-номер. При решении вопроса о квалификации действий подсудимого суд учёл, что неправомерный доступ к охраняемой законом компьютерной информации, повлёкший модификацию такой информации, происходил под контролем правоохранительных органов в ходе оперативно-розыскного мероприятия «проверочная закупка», проводимой представителями правоохранительных органов в соответствии с Федеральным законом от 12 августа 1995 г. №144-ФЗ «Об оперативно-розыскной деятельности», в результате чего

[1] Приговор Пролетарского районного суда г. Твери от 2 декабря 2014 года по делу № 1-281/2014.

реального ущерба для компании не наступило, по независящим от З. обстоятельствам[1].

Обращает на себя внимание то обстоятельство, что суд, мотивируя принятое решение о квалификации деяния как неоконченного преступления, указывает на отсутствие «реального ущерба для компании». Вместе с тем данные последствия не предусмотрены законом. Не выражают они и сути видового объекта данной группы преступлений. Учитывая, что модификацию информации лицо осуществляло под непосредственным контролем правоохранительных органов в рамках оперативно-розыскного мероприятия, правильнее говорить об отсутствии признаков оконченного преступления ввиду изначально негодного объекта посягательства – изменение IMEI-кода на заранее определённом для этих целей мобильном устройстве не могло причинить вред отношениям информационной безопасности.

Недоведение преступления, предусмотренного ст. 272 УК РФ, до конца может быть обусловлено срабатыванием системы защиты охраняемой законом информации от неправомерного копирования, блокирования или уничтожения.

Так, Щ. был осуждён по ч. 3 ст. 30 ч. 1 ст. 272 УК РФ. С целью осуществления преступного умысла, Щ. прибыл в административное помещение юридического лица, где прошёл в служебный кабинет, расположенный на первом этаже. Воспользовавшись приятельскими отношениями с работником организации, находившемся в указанном кабинете, Щ. занял рабочее место за одним из столов, на котором находился компьютер, подключённый к локальной сети организации. Осуществляя задуманное, в указанное время Щ. неправомерно включил указанный компьютер, и, используя ранее имеющуюся у него учётную запись с логином и паролем, известным только ему, которые, несмотря на прекращение работы Щ. в организации, являлись действующими, вошёл в локальную компьютерную сеть организации, затем вошёл в ранее используемый им электронный почтовый ящик, создал электронное сообщение (письмо), к которому прикрепил файлы, находившиеся на сетевом ресурсе организации, содержащие охраняемую законом информацию о персональных данных. Указанное письмо и файлы он отправил на свой электронный почтовый ящик в сети Интернет… Этими действиями Щ. осуществил неправомерный доступ к охраняемой законом компьютерной информации, то есть совершил действия, непосредственно направленные на ее копирование, которое Щ. осуществить не удалось, поскольку в соответствии с настройками локальной сети организации

[1] Приговор Белгородского районного суда Белгородской области от 16 сентября 2010 года по делу № 1-43/2010.

отправка электронных писем на почтовый сервер запрещена, о чем Щ. осведомлён не был[1].

Хищение персонального компьютера либо носителя информации (внешнего жёсткого диска и т.п.) в целях последующего доступа к охраняемой законом компьютерной информации, следует рассматривать не только как соответствующее преступление против собственности, но и как приготовление к преступлению, предусмотренному ст. 272 УК РФ. Вместе с тем, в силу требований ч. 2 ст. 30 УК РФ, такая квалификация является возможной лишь при условии доказанности умысла виновного на наступление тяжких последствий (ч. 4 ст. 272 УК РФ).

Отдельного внимания заслуживает вопрос о добровольном отказе от совершения преступления, предусмотренного ст. 272 УК РФ. Добровольным отказом, безусловно, следует считать случаи, когда лицо самостоятельно прекращает действия, направленные на преодоление средств информационной защиты или прерывает процесс копирования либо модификации данных[2]. При этом добровольное восстановление уничтоженной информации или предоставление доступа к заблокированным данным по прошествии какого-то времени (пусть и незначительного) при наличии иных оснований следует рассматривать как деятельное раскаяние лица.

В теории уголовного права получила распространение позиция, согласно которой как оконченное преступление – создание вредоносной компьютерной программы – следует оценивать в том числе действия по её описанию в рукописном или машинописном виде. Так, М. Ю. Дворецкий пишет, что «…создание вредоносных программ – это целенаправленная деятельность, которая включает в себя: 1) постановку задачи, определение среды существования и цели программы; 2) выбор средств и языков реализации программы; 3) написание непосредственно текста программы; 4) отладку программы; 5) запуск и работу программы. Любое из перечисленных действий охватывается признаками создания вредоносной программы и может быть признано преступлением, предусмотренным ст. 273 УК РФ, даже в том случае, когда вредоносная программа ещё не создана, а находится, так сказать, ещё в стадии оформления. Рассматривать эти действия как подготовительные нельзя, так как термин «создание программы рассматривается законодателем как процесс, а не как

[1] Приговор Октябрьского районного суда г. Саратова от 23 января 2014 г. по делу № 1-27/2014.

[2] См. подробнее о признаках добровольного отказа. – Решетников А. Ю. Квалификация деяния исполнителя при добровольном отказе от доведения преступления до конца // Законность. 2017. №8. С. 41 – 45.

результат… состав преступления, предусмотренного ч. 1 ст. 273 УК РФ, можно считать усечённым»[1].

Данный подход нашёл своё отражение и в методических рекомендациях Генеральной прокуратуры Российской Федерации, где отмечается, что «…ст. 273 УК РФ устанавливает ответственность за незаконные действия с компьютерными программами, записанными не только на машинных, но и на иных носителях, в том числе на бумаге. Это обусловлено тем, что процесс создания компьютерной программы зачастую начинается с написания ее текста с последующим введением его в компьютер или без такового. С учётом этого наличие исходных текстов вредоносных компьютерных программ уже является основанием для привлечения к ответственности по ст. 273 УК РФ»[2].

Однако этот подход к квалификации подобного рода деятельности вызывает определённые сомнения. Прежде всего, как справедливо подчёркивает сам М. Ю. Дворецкий, описание алгоритма на естественном языке, а не на языке программирования, выступает лишь одним из этапов создания программы. В связи с этим напрашивается закономерный вывод, что сама по себе идея (концепция, проект и т.п.) вредоносной программы, выраженная на листе бумаге, не есть программа как таковая. Не станем же мы оценивать как оконченное изготовление оружия создание его сборочного чертежа с разнесёнными составными частями (взрыв-схемы)? Таким образом, определение целей компьютерного вируса, разработка его алгоритма и последующие действия по программированию правильнее оценивать как покушение на создание вредоносной программы. Создание вредоносной компьютерной программы следует считать оконченным с момента придания ей такого состояния, при котором она уже обладает соответствующим деструктивным функционалом (вредоносными свойствами) и пригодна для использования.

Самостоятельным и значимым вопросом является квалификация действий лица, которое осуществляет распространение вредоносной компьютерной программы (ст. 273 УК РФ) под контролем сотрудников оперативно-разыскных подразделений (при этом неважно, осуществлялась ли проверочная закупка в виртуальном или физическом пространстве). В разрешении данной проблемы нельзя оставить без внимания изменение правовой позиции Пленума Верховного Суда Российской Федерации в части юридической оценки сбыта наркотических средств. В соответствии с новым разъяснением, изъятие сотрудниками правоохранительных органов

---

[1] Дворецкий М. Ю. Преступления в сфере компьютерной информации: понятие, система, проблемы квалификации и наказания: монография. Тамбов, 2003. С. 78 – 79.

[2] Методические рекомендации Генеральной прокуратуры Российской Федерации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации. М., 2013. С. 9.

из незаконного оборота наркотиков при проведении проверочной закупки не влияет на квалификацию преступления как оконченного[1]. Ранее идея о том, что проведение оперативно-розыскного мероприятия не может и не должно оказывать влияние на признание сбыта наркотических средств оконченным, последовательно обосновывалась в доктрине уголовного права[2].

Вместе с тем, обобщение и анализ правоприменительной практики по делам о преступлениях в сфере компьютерной информации позволяет сделать вывод, что распространение вредоносного программного обеспечения под контролем правоохранительных органов обычно не признаётся оконченным преступлением.

Так, С., находясь по месту своего жительства, имея умысел на распространение вредоносных компьютерных программ, осознавая противоправный характер своих действий, скачал из сети Интернет программу-генератор ключей для программного обеспечения, заведомо приводящую к несанкционированной модификации информации, записал её на машинные носители – три лазерных оптических диска вместе с программным обеспечением. В тот же день С., находясь в указанной квартире, совершил распространение путем продажи другому лицу, участвовавшему в качестве покупателя при проведении сотрудниками ОРЧЭБ и ПК ОМВД России по г. Ноябрьску оперативно-розыскного мероприятия «Проверочная закупка», за денежное вознаграждение трёх лазерных оптических дисков с программным обеспечением, а также с программой-генератором ключей для указанного программного обеспечения, заведомо приводящей к несанкционированной модификации информации, программного продукта компании, путём подбора ключевой фразы, и, как следствие, являющуюся по отношению к данному программному обеспечению, вредоносной. Однако довести свой умысел С. до конца не смог по независящим от него обстоятельствам, так как его действия находились под контролем сотрудников правоохранительных органов – ОРЧЭБ и ПК ОМВД России, которые после получения закупщиком трёх лазерных оптических дисков, произвели их изъятие, в

---

[1] Постановление Пленума Верховного Суда РФ от 30 июня 2015 г. № 30 «О внесении изменений в постановление Пленума Верховного Суда Российской Федерации от 15 июня 2006 года № 14 «О судебной практике по делам о преступлениях, связанных с наркотическими средствами, психотропными, сильнодействующими и ядовитыми веществами» // Российская газета от 10 июля 2015 года № 150.

[2] См., например: Ролик А. И. Преступление, предусмотренное ст. 228[1] УК РФ: спорные вопросы характеристики // Lex Russia. 2014. № 9. С. 1079 – 1092.

связи с чем последний был лишён возможности владеть вредоносными программами[1].

По другому делу суд указал, что квалифицируя действия подсудимого по ч. 3 ст. 30 ч. 2ст. 273 УК РФ как покушение на распространение компьютерной программы, заведомо предназначенной для несанкционированной модификации компьютерной информации и нейтрализации средств защиты компьютерной информации, совершенное из корыстной заинтересованности, суд исходит из того, что продажа игровой консоли подсудимым была осуществлена в ходе проведённого оперативно-розыскного мероприятия – проверочная закупка и игровая консоль с установленной в ней на карте памяти программой, предназначенной для модификации компьютерной информации, в конечном итоге была изъята из незаконного оборота[2].

Полагаем, что подход к квалификации преступлений, связанных со сбытом запрещённых в свободном обороте объектов (наркотических средств, оружия, вредоносных компьютерных программ и т.д.) должен быть унифицированным. В связи с этим распространение вредоносного программного обеспечения при проведении проверочной закупки с учётом последних разъяснений Пленума ВС РФ, на наш взгляд, следует оценивать как оконченное преступление. Состав по своей конструкции (моменту описания его окончания) является формальным. Таким образом, законодатель запрещает сами действия, направленные на распространение соответствующих вредоносных программ.

Приобретение вредоносной компьютерной программы для последующего распространения или использования не образует состава преступления. Оно может быть оценено как приготовление к преступлению в случаях, когда будет установлено, что вредоносная программа предназначалась для использования в совершении тяжкого и особо тяжкого преступления и была способна по своим свойствам причинить тяжкие последствия.

Вопрос о предварительной преступной деятельности при совершении деяния, предусмотренного ст. 274 УК РФ, напрямую связан с определением субъективной стороны данного преступления. В отечественной доктрине уголовного права высказываются различные суждения на этот счёт. Как бы то ни было теория[3] и практика[1] придерживаются той известной позиции,

---

[1] Приговор Ноябрьского городского суда Ямало-Ненецкого автономного округа от 11 апреля 2012 г. по делу № 1-133/2012.

[2] Приговор Советского районного суда г. Тамбова от 25 апреля 2016 г. по делу № 1-106/2016.

[3] См., например: Рарог А. И. Проблемы квалификации преступлений по субъективным признакам: монография. М., 2015. С. 88; Кауфман М. А. Некоторые вопросы применения Общей части УК РФ // Государство и право. 2000. № 6. С. 59 и др.

что если непосредственно в тексте диспозиции уголовно-правовой нормы не указана форма вины, не упоминается специальная цель или мотив деяния, преступление (в том числе предусмотренное ст. 274 УК РФ) может быть совершено как умышленно, так и по неосторожности.

Преступление, предусмотренное ст. 274 УК РФ, как известно, характеризуется двухуровневыми последствиями – нарушение специальных правил использования компьютерных данных и систем является уголовно-наказуемым деянием только в случае, если это повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации и причинение крупного ущерба. Таким образом, причинение вреда информационным активам само по себе ещё не указывает на то, что данное преступление является оконченным.

Например, если служебные данные организации в нарушение установленного запрета были умышленно удалены одним из её работников (с кем работодатель, например, решил прекратить трудовые отношения), то содеянное будет содержать признаки преступления, предусмотренного ст. 274 УК РФ, только в случае причинения ущерба организации на сумму свыше одного миллиона рублей. Квалифицировать содеянное как покушение, на наш взгляд, возможно только в том случае, если характер совершённых лицом действий (какая по содержанию и объёму информация была уничтожена) явно указывает на то, что лицо стремилось к наступлению именно таких общественно опасных последствий. Например, по ст. 274 УК РФ со ссылкой на ч. 3 ст. 30 УК РФ необходимо квалифицировать действия лица, которое умышленно модифицировало программное обеспечение конвейерной сборки продукции на автомобильном заводе, однако крупный ущерб не наступил ввиду своевременного обнаружения вредоносного вмешательства службой информационной безопасности предприятия.

Понятно, что если само нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей было допущено по неосторожности или, хотя правила и нарушались сознательно, однако лицо самонадеянно рассчитывало, что негативные последствия не наступят (работник, используя служебный компьютер, в нарушение политики информационной безопасности предприятия, выходит в Интернет, что влечёт за собой заражение локальной сети организации вредоносной компьютерной программой «WannaCry» и шифрование всех служебных

---

[1] Например, Пленум Верховного Суда РФ в постановлении от 18 октября 2012 года № 21 «О применении судами законодательства об ответственности за нарушения в области охраны окружающей среды» разъяснил: «Исходя их положений ч. 2 ст. 24, если в диспозиции статьи главы 26 УК РФ форма вины не конкретизирована, то соответствующее экологическое преступление может быть совершено умышленно или по неосторожности…».

данных), говорить о возможности покушения на преступление, предусмотренное ст. 274 УК РФ, нельзя.

Объективная сторона преступления, предусмотренного частью 1 ст. 2741 УК РФ, предполагает совершение любого из трёх альтернативных действий: 1) создание, 2) использование или 3) распространение компьютерных программ или информации, заведомо предназначенных для совершения атак на объекты критической информационной инфраструктуры.

Состав по конструкции (по моменту описания в законе момента окончания преступления) является формальным. Совершение любого из указанных действий (равно как и их совокупности) образует оконченный состав преступления. Объёмы деяния применительно к этим альтернативным признакам состава преступления следует понимать подобно тому, как они трактуются применительно к составу преступления, предусмотренного ст. 273 УК РФ.

Объективная сторона преступления, предусмотренного частью 2 ст. 274^1 УК РФ, заключается в неправомерном доступе к компьютерной информации, содержащейся в критической информационной инфраструктуре. Состав по конструкции является материальным. Преступление считается оконченным только в случае причинения вреда критической информационной инфраструктуре Российской Федерации.

Если лицу, осуществившему неправомерный доступ к компьютерной информации, содержащейся в критической информационной инфраструктуре, по независящим от него обстоятельствам не удалось причинить вред критической информационной инфраструктуре Российской Федерации (например, в результате успешного срабатывания антивирусного программного обеспечения или действий сотрудников, отвечающих за информационную безопасность организации) содеянное следует квалифицировать как покушение на преступление по ч. 3 ст. 30, ч. 2 ст. 274^1 УК РФ.

Следует отдельно указать, что диспозиция ч. 2 ст. 274^1 УК РФ по сути содержит признаки составного преступления, поскольку указывает, что под неправомерным доступом следует также понимать доступ с использованием компьютерных программ либо иной компьютерной информации, которые заведомо предназначены для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, или иных вредоносных компьютерных программ. Таким образом, ч. 2 ст. 274^1 УК РФ охватывает и не требует квалифицировать по совокупности неправомерный доступ к объектам критической информационной инфраструктуры, совершенный с использованием заведомо предназначенных для этого вредоносных программ (ч. 1 ст. 274^1 УК РФ) или иных вредоносных программ (ст. 273 УК РФ).

При этом, если лицо, использовавшее программу, являлось и ее разработчиком, содеянное необходимо квалифицировать по совокупности преступлений. В данном случае вполне применимо известное правило квалификации, согласно которому действия по подготовке или исполнению деяния, не входящие в объективную сторону оконченного преступления (которые по сути не являются юридически значимым способом совершения этого преступления), должны получить самостоятельную уголовно-правовую оценку по другой статье закона.

Кроме того, совокупность преступлений, предусмотренных ч. 1 ст. 274^1 УК РФ и ч. 1 ст. 30 ч. 2 ст. 274^1 УК РФ, может иметь место и в том случае, когда лицо создаёт компьютерную программу либо иную компьютерную информацию, которые заведомо предназначены для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации. Однако в этом случае необходимо доказать умысел лица на их дальнейшее использование.

Дискуссионные вопросы соучастия в преступлениях в сфере компьютерной информации

Компьютерная преступность характеризуется специфической архитектурой криминальных связей. В абсолютном большинстве случаев лица не знают друг друга в реальной жизни и их взаимодействие реализуется посредством виртуальных средств идентификации. При этом площадками для построения и поддержания преступных связей, как правило, выступают специальные сайты, на которых осуществляется обмен сведениями о способах совершения компьютерных преступлений, предлагаются услуги по взлому электронной почты, распространяется вредоносное программное обеспечение, принимаются заказы и продаётся «ботнет», специальное оборудование, базы данных с реквизитами клиентов кредитных организаций и т.д. В данной связи можно сослаться на меткое наблюдение Н. Ш. Козаева: «Переход по первой же ссылке, – пишет он, – привёл на форум, где некое лицо предлагает оптом в 50 шт. приобрести карты оператора сотовой связи «Билайн» и беззастенчиво указывает цели: «если их пробивают, то показывают, что такого номера не существует, идеально подходит для создания киви, регистрации в соцсетях или для «мама срочно отправь на этот номер 500 руб., позже все объясню»[1].

В качестве отдельной проблемы следует также указать на получающие всё большую популярность онлайн-курсы для программистов («hacker schools»). Формально заявляя о реализации образовательных программ для тех, кто хочет приобрести знания и навыки в программировании,

[1] Козаев Н. Ш. Современные технологии и проблемы уголовного права (анализ зарубежного и российского законодательства). М., 2015. С. 187.

отдельные из них фактически являются площадками для подготовки к совершению компьютерных преступлений[1].

Масштабное распространение безадресного подстрекательства и предлагаемой по принципу «до востребования» помощи в совершении компьютерных преступлений позволило отдельным специалистам сделать вывод о необходимости переосмысления некоторых общетеоретических положений института соучастия. Так, по мнению А. Ю. Чупровой, особенностью подстрекательских действий в сети «Интернет» является то, что умысел лица не персонифицирован, его призыв к совершению преступления обращён к неопределённо большому кругу лиц. Кто найдёт предложение заслуживающим внимания и одобрения и реализует его на практике, автору прокламации неизвестно[2].

В свою очередь М. Д. Фролов уже напрямую пишет, что лицо, склоняющее к совершению преступления в сфере информационно-коммуникационных технологий, или оказывающее тому содействие неограниченному и не персонифицированному числу лиц, имеет не абстрактное, а вполне конкретное намерение. Абстрактность самого исполнителя не меняет общего вывода о наличии причинной обусловленности и реальной взаимосвязи таких действий, то есть о наличии признаков соучастия[3].

Вряд ли следует признать оправданным отказ от запрета на привлечение к ответственности за так называемое абстрактное соучастие. Подстрекательством может быть признано склонение другого лица к совершению конкретного преступления, а не пробуждение абстрактных преступных устремлений или интереса к противоправному поведению. Недостаточно дать кому-то совет заняться кражами: для признания лица подстрекателем необходимо, чтобы оно подстрекнуло совершить определённую кражу путем объяснения выгод от преступления, умаления трудностей и опасности, с которым сопряжено его выполнение[4]. В той же мере сказанное относится и к пособничеству.

Современная судебная практика демонстрирует строгую приверженность данной концепции. Так, оправдывая Ч. в совершении преступления, суд указал, что пособник осознает в совершении какого конкретного преступления он оказывает содействие, предвидит возможность наступления в результате действий исполнителя общественно опасных

---

[1] Qianyun Wang. A comparative study of cybercrime in criminal law of China, US, England, Singapore and the Council of Europe. Rotterdam, 2016. P. 46.

[2] Чупрова А. Ю. Уголовно-правовые механизмы регулирования отношений в сфере электронной коммерции: дисс. …д-ра юрид. наук. М., 2015. С. 259.

[3] Фролов М. Д. О некоторых проблемах квалификации мошенничества в сфере компьютерной информации // Адвокат. 2016. № 6. С. 57.

[4] Курс российского уголовного права. Общая часть / под ред. В. Н. Кудрявцева, А. В. Наумова. М., 2001. С. 359.

последствий и желает либо сознательно допускает наступление таких последствий …каких-либо фактов, свидетельствующих о том, что передавая С. и М. информацию о потерпевших, Ч. осознавал, что этим он способствует совершению преступлений в их отношении, не установлено[1].

По другому делу, соглашаясь с выводом об отсутствии в действиях Аджиева состава преступления, предусмотренного ч. 4 ст. 33 п. «б» ч. 2 ст. 105 УК РФ, суд указал, что призывы и пожелания общего характера, которые непосредственно не направлены на склонение лица к конкретному противоправному деянию, не являются подстрекательством. Отсутствует оно и в том случае, если лицо в общей форме выражает мысль о желательности совершения того или иного преступления, однако она не обращена к другому лицу как к избранному (предполагаемому) исполнителю этого преступления[2].

Согласимся, пожалуй, что попытки расширительного толкования подстрекательских и пособнических действий по делам о компьютерных преступлениях, имеют своё объяснение – публичное размещение информации, склоняющей или облегчающей их совершение, объективно является общественно опасным и требует надлежащей оценки. Вместе с тем, даже при решении самых злободневных проблем нельзя законность приносить в жертву «социальной необходимости», произвольно расширяя пределы действия уголовного закона. Пожалуй, отечественному законодателю необходимо обратить более пристальное внимание на опыт других государств, которые пошли по пути выделения специальных норм об ответственности за подобное поведение[3].

Другой значимой проблемой квалификации преступлений, совершаемых с использованием информационно-коммуникационных технологий, является возможность вменения соучастия в случаях, когда деяние совершено объективно групповым способом, однако между отдельными лицами не было прямого (реального или виртуального) взаимодействия.

Как известно, для квалификации соучастия недостаточно лишь внешнего единства деяния. Необходимым условием выступает также установление так называемого общего умысла и осознания факта участия в преступлении иных лиц. А. И. Рарог пишет, что из законодательного определения

---

[1] Апелляционное определение Верховного Суда РФ от 27.04.2017 г. по делу № 89-АПУ17-3сп.

[2] Апелляционное определение Верховного Суда РФ от 04.06.2015 г. по делу № 30-АПУ15-3.

[3] Например, с 2015 года ответственность за такие действия предусмотрена ст. 287 (Б) УК Китайской Народной Республики. См.: Qianyun Wang. A comparative study of cybercrime in criminal law of China, US, England, Singapore and the Council of Europe. Rotterdam, 2016. P. 42.

соучастия следует, что таковой признаётся только лишь умышленная совместная деятельность, то есть деятельность согласованная[1].

Вместе с тем, в теории уголовного права было обосновано, что соглашение между всеми участниками не является обязательным субъективным признаком соучастия[2]. Так, Г. А. Кригер отмечал, что отдельные соучастники «о подробностях деятельности каждого из участников могут не знать, их осведомлённость может быть ограничена знанием общего плана совершения хищения, то есть знанием того, что исполнителем должно быть похищено имущество, и они должны оказать то или иное содействие при подготовке хищения или при сокрытии и реализации похищенного»[3].

В современной литературе также справедливо обосновывается вывод, что «для преступных сообществ характерна ситуация, когда его участники ничего не знают о существовании друг друга. Это позволяет преступникам лучше конспирироваться, препятствует раскрытию всей цепочки в случае изобличения соучастников на каком-либо из звеньев, как правило низовом»[4]. В сложных организованных формах соучастия лица, участвующие в совершении преступления, могут не знать друг друга в целях конспирации, но они должны быть осведомлены о существовании иных соучастников[5].

Следует отметить, что подобный подход находит свою последовательную реализацию и в судебной практике. Так, по одному из дел суд отметил, что «довод о незнакомстве между собой некоторых членов преступной группы (Магомаева с Умаевым и Умархаджиевым) не опровергает выводов суда, поскольку для организованной группы не является обязательной связь каждого из её членов друг с другом»[6].

По другому делу суд напрямую указал: «…то обстоятельство, что некоторые члены группы не были знакомы между собой, и не знали друг друга в лицо, поддерживая связь только путем телефонных соединений, не

---

[1] Рарог А. И. Проблемы квалификации преступлений по субъективным признакам. М., 2015. С. 188.

[2] Гришаев П. И., Кригер Г. А. Соучастие по советскому уголовному праву. М., 1959. С. 44.

[3] Кригер Г. А. Ответственность за хищение государственного или общественного имущества по советскому уголовному праву. М., 1957. С. 157.

[4] Матейкович М. С. Об уголовной ответственности за преступления в сфере незаконного оборота наркотиков, совершенные организованными группами и преступными сообществами // Российская юстиция. 2015. № 12. С. 25 – 27.

[5] Комментарий к Уголовному кодексу Российской Федерации (постатейный) // отв. ред. В. И. Радченко, науч. ред. А. С. Михлин, В. А. Казакова. М., 2008. С. 247.

[6] Апелляционное определение Верховного Суда РФ от 23.09.2015 г. по делу № 5-АПУ15-76.

имеет правового значения и не может поставить под сомнение вывод суда о признании группы организованной»[1].

Таким образом, отдельный исполнитель компьютерного преступления может и не знать всех соучастников, а осведомлённость его может быть ограничена знакомством лишь с одним из них. При этом такой связи лица с одним из соучастников, на наш взгляд, вполне достаточно для признания соучастия, если при этом ему был известен хотя бы общий характер преступной деятельности группы.

Проблемой совершенно иного порядка является квалификация действий лица, которое для совершения преступления на постоянной основе привлекает других лиц, выполняющих строго определённые функции. Так, например, современное мошенничество, связанное с атаками на сервисы дистанционного банковского обслуживания, предполагает участие разработчиков вредоносного программного обеспечения, распространителей компьютерного вируса, лиц, контролирующих движение похищенных денежных средств («заливщиков») и, наконец, так называемых «обнальщиков» или «дропов», которые обналичивают похищенные денежные средства, используя поддельные платёжные карты.

Объективно действия указанных выше лиц дополняют друг друга, являются составной частью общей преступной деятельности – мошенничества в сфере компьютерной информации. Принципиальный момент заключается лишь в характере коммуникаций – единство действий достигается за счёт связующего звена. Таким звеном выступает лицо, которое изначально разработало план совершения преступления и подыскало необходимых участников. Только оно обладает полной информацией о действительной роли каждого из них.

Отдельно взятые субъекты не осознают, что они являются «винтиками» единого преступного механизма, входят в состав группы, организованной и управляемой одним лицом: разработчик вредоносного программного обеспечения сбывает его, не выясняя целей приобретателя; распространители вируса, получая вознаграждение, не интересуются последствиями его действия; «заливщики» не знают, кто изготовил и как распространялся компьютерный вирус; «дропы» не имеют ни малейшего представления о происхождении денежных средств. Каждый из них может лишь догадываться, предполагать, что его действия связаны с совершением преступления, но не более того.

Если взглянуть на описанную выше ситуацию с точки зрения положений действующего уголовного законодательства о совместной преступной деятельности, то следует признать, что соучастия нет. Имеет место всего лишь совершение разными лицами самостоятельных преступлений. Вместе с тем, при таком решении усматривается вполне очевидная

[1] Апелляционное определение Верховного Суда РФ от 04.04.2017 г. по делу № 35-АПУ17-3.

несправедливость – групповой характер посягательства никак не учитывается при оценке действий самого субъекта, который осуществляет его, вовлекая в процесс усилия иных лиц. Сложно не согласиться с тем, что в предлагаемом примере с компьютерным мошенничеством объединённые усилия нескольких лиц представляют большую общественную опасность по сравнению с действиями единичного преступника, поскольку повышают реальные возможности совершить задуманное в кратчайшие сроки и эффективно скрыть следы преступления.

В отечественной теории отмечалось, что, если лицо сознательно объединяет усилия группы лиц для достижения преступного результата, то есть применяет групповой способ посягательства, вполне правомерно привлечение его к ответственности за совершение группового преступления независимо от того, есть ещё в группе лица, подлежащие уголовной ответственности, или нет[1].

На этом основании дополнительно обосновывалось, что соучастие в преступлении и групповое причинение вреда (групповое посягательство) представляют собой разные явления, имеющие свой предмет и самостоятельное уголовно-правовое значение. Поэтому и в теории вопрос о них должен быть предметом самостоятельного научного исследования и решения[2].

Соглашаясь с последним тезисом, отметим, что теория уголовного права нуждается в поиске концепции, которая могла бы дать объяснение данному явлению, а в последующем и сформулировать рекомендации по его отражению в нормах уголовного права.

Проблемы квалификации сложных единичных преступлений в сфере компьютерной информации

Вопрос о квалификации сложных единичных преступлений в сфере компьютерной информации имеет свою специфику, обусловленную их «цифровой» природой. Как уже отмечалось ранее, преступлениям, совершаемым с использованием современных информационно-коммуникационных технологий, пожалуй, как никаким другим, свойственна нацеленность сразу на многих потерпевших и способность вызывать цепи многоуровневых общественно опасных последствий. При

---

[1] Сабиров Р. Д. Содержание признака насилия в групповых посягательствах на собственность // Проблемы совершенствования законодательства по укреплению правопорядка и усиление борьбы с правонарушениями. Межвузовский сборник научных трудов. Свердловск. 1982. С. 122.

[2] См.: Галиакбаров Р. Р. Нетрадиционные аспекты множественности в уголовном праве // Уголовно-правовые средства борьбы с преступностью. Межвузовский сборник научных трудов. Омск, 1983. С. 25; Малахов И. П. Соучастие и групповая организованная преступность // Правоведение. 1994. № 5-6. С. 126.

организованных криптовирусных атаках на кредитно-финансовый сектор и даже отдельных хозяйствующих субъектов или физических лиц количество потерпевших может измеряться сотнями и даже тысячами. Так, известным примером является инцидент с распространением вируса «ILoveYou» в мае 2000 года, который за короткий промежуток времени с территории Филиппин распространился по всему миру и поразил более 3 миллионов компьютеров, причинив ущерб в размере 10-15 миллиардов долларов США[1].

Подобные особенности компьютерной преступности закономерно вызывает некоторые затруднения у правоприменителей. Так, по одному из дел государственный обвинитель изменил предъявленное подсудимым обвинение в совершении 21 эпизода преступлений, предусмотренных ч. 2 ст. 272 УК РФ, на один состав ч. 2 ст. 272 УК РФ, мотивировав своё решение тем обстоятельством, что «…деяния совершались по одинаковой единожды согласованной схеме, совершены в короткий промежуток времени и во исполнение единого преступного умысла, направленного на совершение хищений денежных средств с банковских карт граждан… то есть умысел был сформирован на совершение хищений денежных средств с банковских карт неопределённого количества граждан, что свидетельствует о том, что все преступления, совершенные подсудимыми, охватывались единым умыслом, а преступление, квалифицируемое по ч. 2 ст. 272 УК РФ, носит продолжаемый характер»[2].

Таким образом, суть решения сводится к тому, что имело место продолжаемое преступление. В действительности, это не совсем так. Особенностью неправомерного доступа к компьютерной информации, совершаемого с использованием специального оборудования или вредоносных компьютерных программ, является его автоматизированный характер. В этом случае скрыто установленное устройство или компьютерный вирус без участия злоумышленника копирует, модифицирует или уничтожает охраняемую законом компьютерную информацию любого лица, решившего осуществить ту или иную финансовую операцию или посетить определённый интернет-ресурс. В течение суток банкоматный скиммер или фишинговый сайт могут накопить информацию о банковских картах сотен клиентов. Полагаем, что правила квалификации продолжаемого преступления[3] для таких случаев

---

[1] [Электронный ресурс] // URL: https://www.kaspersky.ru/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds (дата обращения: 08.06.2018).

[2] Постановление Октябрьского районного суда г. Иркутска от 04 сентября 2015 года по делу № 1-461/2015.

[3] Например, сформулированных в абз. 2 п. 16 постановления Пленума Верховного Суда Российской Федерации от 27.12.2002 года № 29 «О судебной практике по делам о краже, грабеже и разбое».

неприменимы, поскольку для продолжаемого преступления характерна неоднократность тождественных противоправных действий. Неправильным будет оценивать подобный «автоматизированный» неправомерный доступ и как идеальную совокупность преступлений. Такой вывод подтверждается судебной практикой, в которой представлен другой подход к оценке преступных деяний, одновременно посягающих на двух или более потерпевших[1].

Представляется, что верной квалификацией неправомерного доступа к компьютерной информации, совершаемого с использованием специального оборудования и (или) вредоносного компьютерного обеспечения будет вменение сложного единичного преступления с множественностью потерпевших[2], характеризующегося следующими отличительными чертами: 1) направленностью посягательства на двух или более лиц; 2) причинением вреда нескольким потерпевшим в результате одного преступного деяния; 3) причинной связью нескольких последствий (в виде копирования, блокирования или уничтожения охраняемой законом компьютерной информации) с одним преступным деянием; 4) единством умысла виновного, направленного на неправомерный доступ к охраняемой законом компьютерной информации в отношении двух или более лиц.

Важно подчеркнуть, что в случае сложного единичного неправомерного доступа к охраняемой законом компьютерной информации с множественной потерпевших (100 человек и более) деяние необходимо квалифицировать по ч. 4 ст. 272 УК РФ, как повлекшее тяжкие последствия.

Если неправомерный доступ к компьютерной информации носил не автоматизированный, а, что называется, «ручной» характер, о признаках продолжаемого преступления следует говорить лишь в случае, когда лицо неоднократно осуществляет действия по преодолению средств программно-технической защиты информационного ресурса одного и того же потерпевшего с незначительном разрывом во времени и при обстоятельствах, указывающих на единство умысла. Например,

---

[1] См.: Определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 21.01.2014 № 72-АПУ13-63 // Бюллетень Верховного Суда российской Федерации. 2014. № 8; пункт 9 постановления Пленума Верховного Суда Российской Федерации от 09.12.2008 г. № 25 «О судебной практике по делам о преступлениях, связанных с нарушением правил дорожного движения и эксплуатации транспортных средств, а также с их неправомерным завладением без цели хищения» // СПС «КонсультантПлюс»; постановление Президиума Верховного Суда Российской Федерации № 323-П08ПР / Обзор законодательства и судебной практики Верховного Суда Российской Федерации за четвёртый квартал 2008 года // СПС «КонсультантПлюс».

[2] См.: Актуальные проблемы уголовного права: курс лекций / под ред. О. С. Капинус; рук. авт. кол. К. В. Ображиев. М., 2015. С. 201.

злоумышленник, выполняя заказ, ежедневно в течение недели взламывает аккаунт пользователя в социальной сети, копирует переписку и отправляет заказчику.

Если такие действия совершались в интересах одного и того же заказчика, но в отношении разных пользователей сети Интернет, каждый неправомерный доступ следует квалифицировать самостоятельно по числу потерпевших.

Современные технологии позволяют пользователю синхронизировать принадлежащие ему различные устройства: смартфон, планшет, домашний и рабочий компьютеры – и обрабатывать одну и ту же информацию на любом из них. В случае неправомерного доступа и уничтожения данных множественность устройств, имевших к ним доступ, не обусловливает возможность вменения совокупности преступлений. Так, А., имея доступ к сети Интернет, из корыстных побуждений совершал неправомерный доступ к принадлежащим потерпевшим учётным записям интернет-сервиса «iCloud», после чего изменял пароли к ним. В продолжение своего умысла А., используя учётные записи, стирал и (или) блокировал всю имеющуюся на мобильных телефонах потерпевших информацию и выводил на экране устройств текст примерно следующего содержания: «Это устройство было утеряно и стёрто. Для возврата напишите письмо на… Укажите в письме этот код устройства:…». После получения электронного письма от потерпевшего А. направлял в ответ инструкцию в виде текста, согласно которой он требовал для разблокировки устройства перечисления денежных средств. Потерпевшие, выполняя условия А., переводили указанные им суммы[1].

Как следует из решения, действия по неправомерному доступу к учётной записи пользователей и последующие доступ и блокировка компьютерной информации на нескольких устройствах потерпевших обоснованно квалифицированы судом как единое преступление.

А. А. Энгельгардт обращается к смежной проблеме и анализирует судебное решение об осуждении виновного по восьми эпизодам неправомерного доступа к компьютерной информации, связанного с нейтрализацией средств защиты программного обеспечения от несанкционированной установки. Суд признал в действиях подсудимого совокупность преступлений, ссылаясь на то обстоятельство, что при «проверочной закупке» он выполнил незаконную установку нескольких программ. Как справедливо отмечает автор, по данному делу неправомерное поведение виновного воспринимается как единое событийное явление, поскольку: 1) эпизоды являются тождественными; 2) охраняемое правовое благо было нарушено действиями, тесно связанными

[1] Приговор Ленинского районного суда г. Махачкалы от 07 сентября 2015 года по делу № 1-357/2015.

во времени; 3) несколько действий было осуществлено на основе единой мотивации, непрерывно определяющей поведение исполнителя[1].

Другим значимым вопросом квалификации неправомерного доступа к компьютерной информации является возможность признания его длящимся преступлением. М. А. Ефремова пишет, что «неправомерный доступ следует понимать и как процесс, так и результат, выражающийся в определённом состоянии, вызванном действием или действиями»[2]. С одной стороны, мысль автора понятна и одновременно примечательна – злоумышленник, взломав чужой аккаунт в сети «Интернет», как бы находится в «состоянии» неправомерного доступа к компьютерной информации. Однако с точки зрения отечественной доктрины уголовного права это указывает не на состояние, а на признаки непрерывного выполнения объективной стороны преступления, предусмотренного ст. 272 УК РФ. Это в свою очередь позволяет обосновать вывод, что юридический и фактический моменты окончания неправомерного доступа к компьютерной информации могут не совпадать. В ситуации завладения чужим аккаунтом в социальной сети, юридически оконченным неправомерный доступ будет с момента смены злоумышленником пароля к странице, что повлечёт за собой блокирование компьютерной информации для потерпевшего. Фактический же момент окончания преступления находится в будущем и может быть связан с различными обстоятельствами: возвратом аккаунта законному владельцу самим виновным (за деньги, например), вмешательством администрации интернет-ресурса и пресечением действий злоумышленника с восстановлением доступа потерпевшего, удалением аккаунта самим виновным и др.

Некоторую сложность представляет решение вопроса о том, следует ли квалифицировать по совокупности действия лица, которое осуществляет изготовление вредоносной компьютерной программы и спустя определённый период времени распространяет или использует её. В теории уголовного права отмечается, что подобная ситуация являет собой пример сложного единичного преступления с альтернативными действиями, для которого достаточно совершения лицом любого из указанных в статье уголовного закона действий (бездействий). При этом совершение лицом нескольких или всех поименованных в диспозиции статьи Особенной части УК РФ альтернативных деяний не образует реальной совокупности[3].

---

[1] Энгельгардт А. А. Оценка преступлений как продолжаемого деяния или множественности (на примере преступлений в сфере компьютерной информации) // Право и политика. 2014. № 12 (180). С. 1863.

[2] Ефремова М. А. Уголовно-правовая охрана информационной безопасности: дис. …д-ра юрид. наук. М., 2018. С. 338.

[3] Совокупность преступлений: проблемы теории и практики квалификации. Монография / Под ред. Ю. Е. Пудовочкина. М., 2016. С. 115.

Данный подход, как известно, нашёл своё отражение и в практике Верховного Суда Российской Федерации[1].

Вместе с тем, указанное правило о квалификации сложного единичного преступления с альтернативными действиями нельзя абсолютизировать, игнорируя содержание субъективной стороны виновного, поскольку при определённых обстоятельствах это будет препятствовать справедливой юридической оценке содеянного. Так, если преступник изготовил вредоносную компьютерную программу и, разместив объявление в так называемом «даркнете», неоднократно осуществляет её распространение за плату, то, на наш взгляд, правильно квалифицировать его действия по совокупности, самостоятельно оценивая каждый эпизод сбыта компьютерного вируса. На множественность преступлений здесь главным образом указывает отсутствие единства умысла у виновного на совершение сразу нескольких деяний, описанных в диспозиции статьи Особенной части УК РФ.

Смежным вопросом является оценка действий лица, которое изготавливает вредоносную компьютерную программу, а затем в течение определённого времени периодически дорабатывает её, изменяя таким образом, чтобы антивирусное программное обеспечение перестало обнаруживать такую программу, и она снова могла быть пригодна для использования в преступной деятельности. Изучение судебно-следственной практики показывает, что правоприменители квалифицируют исключительно факт первичного изготовления и распространения компьютерного вируса. Так, Р. в июне 2014 года в сервисе мгновенного обмена сообщениями познакомился с Х. и сообщил ему о своём намерении приобрести вредоносную компьютерную программу, которая способна без уведомления пользователя мобильного телефона, работающего на операционной системе «Android», осуществлять перехват входящих и исходящих смс-сообщений, блокировать входящие смс-сообщения, удалять исходящие смс-сообщения, с целью получения доступа к потенциальным возможностям, предоставленными банком и компаниями сотовой связи, а также к данным абонента (в том числе к данным о наличии денежных средств на балансе банковской карты), на мобильный телефон которого установлена указанная программа. Х., имеющий специальные познания в сфере высоких технологий и компьютерной информации, осознавая, что компьютерная программа, обладающая указанными функциональными возможностями является вредоносной, желая получить материальное вознаграждение, изготовил её и впоследствии передал Р.

Позднее в сентябре 2014 года Р. предложил Х. на протяжении всего периода осуществления преступной деятельности поддерживать функционирование и использование созданной им программы путем её

[1] См., например: Дело № 23 АПУ 14-11. Апелляционное определение от 13 ноября 2014 г.

постоянного обновления, на что Х. согласился. За поддержание функционирования, модернизацию и устранение ошибок при работе программного комплекса Х. через виртуальные кошельки получал от Р.денежные средства.

Суд квалифицировал действия Х. по ст. 273 ч. 2 УК РФ – создание, распространение и использование компьютерных программ, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации, совершённые из корыстной заинтересованности; по ч. 5 ст. 33 ч. 4 ст. 159[6] УК РФ – пособничество в совершении мошенничества в сфере компьютерной информации, то есть хищении чужого имущества путем ввода, удаления, блокирования, модификации компьютерной информации, совершенное организованной группой, с причинением значительного ущерба гражданину[1]. Таким образом, сам факт первичного изготовления и последующие «обновления» вредоносной компьютерной программы были оценены судом как продолжаемое преступление.

Полагаем, что представленный подход к квалификации таких действий является дискуссионным. Камнем преткновения здесь выступает то обстоятельство, что при подобных обстоятельствах сугубо технически нельзя говорить об одной и той же вредоносной компьютерной программе. Модернизированный компьютерный вирус представляет собой уже новую вредоносную компьютерную программу, которая обладает определённым сходством, но не совпадает с прототипом. Следовательно, каждое «обновление» компьютерного вируса есть не что иное как самостоятельное выполнение объективной стороны преступления, предусмотренного ст. 273 УК РФ.

Сложным вопросом является квалификация посягательств на информацию ограниченного доступа (личную, семейную, коммерческую, банковскую тайны и др.), хранящуюся в электронной форме. В теории отмечается, что такие деяния необходимо квалифицировать по совокупности со ст. 272 УК РФ, если они совершены путём незаконного доступа именно к компьютерной информации[2]. Этот подход находит своё отражение и в правоприменительной практике.

Так, М. осуждена по ч. 1 ст. 138 УК РФ и ч. 1 ст. 272 УК РФ. Согласно материалам дела М. на почве ревности позвонила в абонентскую службу оператора сотовой связи и получила сведения о коде абонентского номера потерпевшей. В продолжение своих преступных действий М., используя сеть Интернет, изменила пароль для входа в «Личный кабинет» клиента,

---

[1] Приговор Канавинского районного суда г. Нижний Новгород от 29 января 2018 года по делу 1-70/2018.

[2] См., например: Шарков А. Е. Неправомерный доступ к компьютерной информации: преступность деяния и проблемы квалификации: дис. …канд. юрид. наук. Ставрополь, 2004. С. 8.

где модифицировала личные атрибуты абонента, указав свои адреса электронной почты. Позднее вопреки воле потерпевшего и без его согласия не менее четырёх раз путём подачи электронных заявок получала информацию о соединениях потерпевшего, их времени и продолжительности[1].

Вместе с тем практика по данной категории дел неоднообразна. В отдельных случаях квалификация ограничивается исключительно применением ст. 272 УК РФ несмотря на то что уничтожение, модификация и копирование были осуществлены в отношении информации ограниченного доступа. В качестве подобного примера можно привести дело А., который осуждён по ч. 1 ст. 272 УК РФ за совершение неправомерного доступа к охраняемой законом компьютерной информации юридического лица – «…сведениям о персональных данных сотрудников, о налогах, расчётных банковских счетах и движении денежных средств по ним, что составляет налоговую и банковскую тайну»[2].

Учитывая, что положения уголовно-правовых норм об ответственности за посягательства на информацию, в отношении которой установлен специальный режим правовой защиты, не содержат специальных указаний на их совершение путём неправомерного доступа к компьютерной информации, содеянное необходимо квалифицировать по совокупности преступлений.

2.2. ПРОБЛЕМЫ КВАЛИФИКАЦИИ КОМПЬЮТЕРИЗИРОВАННЫХ ПРЕСТУПЛЕНИЙ

В структуре отечественного уголовного закона можно выделить 32 нормы об ответственности за компьютеризированные преступления. К их числу относятся: п. «д» ч. 2 ст. 110 УК РФ «Доведение до самоубийства», п. «д» ч. 3 ст. 110^1 УК РФ «Склонение к совершению самоубийства или содействие совершению самоубийства», ч. 2 ст. 110^2 УК РФ «Организация деятельности, направленной на побуждение к совершению самоубийства», ст. 128^1 УК РФ «Клевета», ст. 137 УК РФ «Нарушение неприкосновенности частной жизни», ст. 138 УК РФ «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений», ст. 138^1 УК РФ «Незаконный оборот специальных технических средств, предназначенных для негласного получения информации», ч. 3 ст. 141 УК РФ «Воспрепятствование осуществлению избирательных прав или работе избирательных комиссий», ст. 146 УК РФ «Нарушение авторских и смеж-

[1] Приговор Московского районного суда г. Твери от 21 ноября 2016 года по делу № 1-308/2016.

[2] Апелляционное постановление Верховного Суда Республики Татарстан от 13 декабря 2016 года по делу № 22-8753.

ных прав», п. «в» ч. 2 ст. 151^2 УК РФ «Вовлечение несовершеннолетнего в совершение действий, представляющих опасность для жизни несовершеннолетнего», п. «г» ч. 3 ст. 158 УК РФ «Кража», ст. 159^3 УК РФ «Мошенничество с использованием электронных средств платежа», ст. 159^6 УК РФ «Мошенничество в сфере компьютерной информации», ст. 171^2 УК РФ «Незаконные организация и проведение азартных игр», ст. 185^3 УК РФ «Манипулирование рынком», ст. 187 УК РФ «Неправомерный оборот средств платежей», ч. 2 ст. 205^2 УК РФ «Публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма», п. «в» ч. 3 ст. 222 УК РФ «Незаконные приобретение, передача, сбыт, хранение, перевозка, пересылка или ношение оружия основных частей огнестрельного оружия, боеприпасов», п. «в» ч. 3 ст. 222^1 Незаконные приобретение, передача, сбыт, хранение, перевозка, пересылка или ношение взрывчатых веществ или взрывных устройств», п. «в» ч. 3 ст. 222^2 УК РФ «Незаконные приобретение, передача, сбыт, хранение, перевозка, пересылка или ношение крупнокалиберного огнестрельного оружия, его основных частей и боеприпасов к нему», п. «б» ч. 2 ст. 228^1 УК РФ «Незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества», п. «д» ч. 2 ст. 230 УК РФ «Склонение к потреблению наркотических средств, психотропных веществ или их аналогов», ч. 1^1 ст. 238^1 УК РФ «Обращение фальсифицированных, недоброкачественных и незарегистрированных лекарственных средств, медицинских изделий и оборот фальсифицированных биологически активных добавок», п. «б» ч. 3 ст. 242 УК РФ «Незаконные изготовление и оборот порнографических материалов или предметов», п. «г» ч. 2 ст. 242^1 УК РФ «Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних», п. «г» ч. 2 ст. 242^2 УК РФ «Использование несовершеннолетнего в целях изготовления порнографических материалов или предметов», п. «г» ч. 2 ст. 245 УК РФ «Жестокое обращение с животными», п. «б» ч. 2 ст. 258^1 УК РФ «Незаконные добыча и оборот особо ценных диких животных и водных биологических ресурсов, принадлежащих к видам, занесенным в Красную книгу Российской Федерации и (или) охраняемых международными договорами Российской Федерации», ч. 2 ст. 280 УК РФ «Публичные призывы к осуществлению экстремистской деятельности», ч. 2 ст. 280^1 УК РФ «Публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации», ч. 1 ст. 282 УК РФ «Возбуждение

ненависти либо вражды, а равно унижение человеческого достоинства», ст. 354[1] «Реабилитация нацизма».

Многие из указанных уголовно-наказуемых деяний получили самостоятельную и достаточно подробную проработку в отечественной доктрине уголовного права, однако до настоящего времени ни одно из них еще не рассматривалось в рамках единого смыслового образования – компьютеризированной преступности. Между тем такие деяния представляют собой новые «цифровые» формы посягательств на традиционно охраняемые уголовным законом общественные отношения и в этом качестве, на наш взгляд, могут рассматриваться юридической наукой в принципиально новом смысловом ключе. Как следствие, в рамках настоящей работы нами не будут анализироваться все имеющиеся проблемы квалификации указанных выше преступлений. Предмет исследования составят преимущественно те из них, которые непосредственно затрагивают цифровую сущность таких посягательств.

Нельзя не отметить, что в ряде уголовно-правовых норм (ст. 185[3] УК РФ, ст. 205[2] УК РФ, ст. 228[1] УК РФ, ст. 258[1] УК РФ, ст. 280[1] УК РФ) имеется указание на совершение соответствующих общественно опасных деяний с использованием «*электронных сетей*». Следует отметить, что понятие электронной сети не только не раскрывается, но и не используется Федеральным законом Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Проведенное исследование судебно-следственной практики не позволило выявить и случаев применения данного признака при квалификации конкретных преступлений. В современной литературе авторы, как правило, обосновывают вывод, что электронная сеть и информационно-телекоммуникационная сеть являются попросту синонимами[1].

На наш взгляд, специальное указание на электронную сеть в ряду квалифицирующих признаков статей Особенной части УК РФ явилось следствием ситуативного и необдуманного законотворчества. Здесь лишь следует обратиться к истории проблемы и более пристально рассмотреть генезис уголовно-правовой нормы о публичных призывах к нарушению территориальной целостности Российской Федерации, где оговорка о совершении данного преступления с использованием электронной сети по-

[1] См., например: Ковлагина Д.А. Понятие «электронные сети» в контексте некоторых составов преступлений, предусмотренных УК РФ // Молодой ученый. – 2016. – № 16. – С. 249–251; Мальков С., Винокуров В. Квалификация сбыта наркотических средств, психотропных веществ или их аналогов с использованием электронных или информационно-телекоммуникационных сетей // Уголовное право. – 2014. – № 4. – С. 51–53.

явилась в результате несовершенства первоначальной редакции ч. 2 ст. 280[1] УК РФ, которая устанавливала повышенную ответственность за подобного рода деяния с использованием средств массовой информации, а равно ресурсов сети «Интернет», *имеющих статус средства массовой информации*. Принимая во внимание объемы криминогенной пропаганды в интернет-пространстве, законодатель попытался спешно исправить ситуацию путем специального указания на электронную сеть (Федеральный закон от 21.07.2014 № 274-ФЗ). В официальном отзыве Правительства Российской Федерации от 28 апреля 2014 г. № 2577п-П4 «На проект Федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации» отмечалось, что «предусмотренный в предлагаемой законопроектом редакции части второй статьи 280[1] УК термин "электронные сети" в законодательстве Российской Федерации и в законопроекте не определен, что повлечет в правоприменительной практике его неоднозначное толкование»[1]. Позднее аналогичным образом была скорректирована и ч. 2 ст. 205[2] УК РФ (Федеральный закон от 06.07.2016 № 375-ФЗ).

Получив первичное отражение в ст. 185[3] УК РФ «Манипулирование рынком» (при этом в отсутствие какого-либо обоснования при подготовке законопроекта), признак начал время от времени воспроизводиться в других статьях, но не системно, а ситуативно, чему достаточно сложно найти объяснение с опорой на научную аргументацию. В качестве общего вывода, полагаем, что в целях чистоты уголовного закона и его универсализации законодателю необходимо отказаться как от признака «*электронной сети*», так и от признака «*информационно-телекоммуникационной сети*»[2], заменив их более общей, признанной на международном уровне конструкцией: «*информационно-коммуникационная технология*».

Законодатель признал использование информационно-коммуникационных технологий квалифицирующим признаком всех преступлений, обуслfвливающих суицидальное поведение человека (п. «д» ч. 2 ст. 110; п. «д» ч. 3 ст. 110[1]; ч. 2 ст. 110[2] УК РФ). Данное решение во многом было обусловлено общественным резонансом по поводу участившихся случаев самоубийств несовершеннолетних, связанных с деятельностью так называемых «групп смерти» в сети «Интернет».

---

[1] [Электронный ресурс] // URL:http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=PRJ&n=119058&rnd=EB9410B1A6F9F6D3DF0B9B5130A3F184#013540789066660963 (дата обращения: 05.07.2019).

[2] Смена парадигмы от канальной телекоммуникационной идеологии к информационно-коммуникационной обстоятельно доказана в работе: Концепция Информационного кодекса Российской Федерации / под ред. И.Л. Бачило. М., 2014.

Здесь необходимо обратить внимание на то важное обстоятельство, что информационно-коммуникационный способ не всегда предопределяет повышение степени общественной опасности доведения до самоубийства или склонения (содействия) к таковому. Так, доведение до самоубийства путем систематического унижения человеческого достоинства с использованием обыкновенной электронной почты либо аккаунта в социальной сети мало отличается от аналогичных действий, совершаемых виновным в процессе личного общения с потерпевшим. В отдельных случаях лицо может и сочетать способы психологического давления – оскорбляя потерпевшего лично, отправляя ему сообщения в популярных мессенджерах, социальных сетях и даже оставляя записки с угрозами у автомобиля или жилища. Как бы то ни было, ключевым аспектом выступает не форма коммуникации – было ли информационное воздействие на потерпевшего вербальным, либо реализовывалось посредством обыкновенных или электронных писем, а то обстоятельство – обеспечивала ли она анонимность злоумышленника, тем самым существенно затрудняя раскрытие и расследование преступления.

В связи с этим полагаем, что в составах преступлений, предусмотренных п. «д» ч. 2 ст. 110 УК РФ и п. «д» ч. 3 ст. 110^1 УК РФ, законодателю следовало бы установить повышенную ответственность не просто за использование информационно-телекоммуникационных сетей, а за соответствующие действия, сопряженные «*с неправомерным сокрытием либо изменением идентификаторов оконечного оборудования пользователя информационно-коммуникационных технологий*».

Как нетрудно заметить, предлагаемое нами решение не затрагивает конструкцию ст. 110^2 УК РФ, где деятельность виновного обращена к индивидуально-неопределенному кругу лиц и заключается в публичном распространении запрещенной информации. Здесь использование информационно-коммуникационных технологий всегда выступает фактором, качественно меняющим общественную опасность деяния.

Нарушение неприкосновенности частной жизни (ст. 137 УК РФ) и нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (ст. 138 УК РФ) уже на протяжении довольно длительного времени демонстрируют тенденцию все большей «миграции» в киберпространство. Объяснение тому, что называется, «лежит на поверхности», учитывая стремительное замещение привычных средств коммуникации (телефонной связи и традиционного почтового сообщения) новыми информационными формами: электронной почтой, мессенджерами, социальными интернет-сетями и т.п.

До настоящего времени конструкции анализируемых уголовно-правовых норм практически не отражают этой «цифровой трансформации». В декабре 2013 г. ст. 137 УК РФ была дополнена частью 3, в которой законодатель сделал акцент лишь на распространении с использованием информационно-телекоммуникационных сетей строго определенной информации о малолетнем.

При этом, как уже отмечалось ранее, правоприменительная практика не демонстрирует единого подхода к квалификации указанных посягательств, совершенных посредством преодоления программно-технических средств защиты информации. Преодоление проблем прикладного характера и отражение процесса масштабной цифровизации нарушения неприкосновенности частной жизни и тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, на наш взгляд, может быть достигнуто путем совершенствования системы квалифицирующих признаков данных преступлений путем дополнения частей вторых ст.ст. 137, 138 УК РФ указанием на совершение преступления «*путем неправомерного доступа к компьютерной информации».*

В отечественной теории уголовного права практически не разрабатывался вопрос об ответственности за распространение сведений об активности другого человека в сети «Интернет». Проведенное нами исследование позволило прийти к выводу, что посещение лицом определенных информационных ресурсов, интернет-магазинов, аккаунтов других пользователей в социальных сетях и т.п. в полной мере подпадает под категорию личной тайны, охраняемой в рамках ст. 137 УК РФ. Таким образом, полагаем, что как нарушение неприкосновенности частной жизни по ст. 137 УК РФ следует квалифицировать действия лица, которое осуществило распространение сведений об активности другого пользователя в сети «Интернет» без его согласия (например, распространило скриншоты истории браузера)[1].

Уголовно-правовая норма об ответственности за незаконный оборот специальных технических средств, предназначенных для негласного получения информации (ст. 138^1 УК РФ), отнесена нами к числу компьютеризированных преступлений сразу по двум причинам. Прежде всего предмет данного преступления практически всегда составляют устройства, предполагающие автоматизированную обработку данных, в том числе их последующую передачу по каналам связи. Кроме того, незаконный оборот подобных устройств по большей части осуществляется посредством специализированных ресурсов в сети «Интернет» (преимуществен-

[1] Данный вывод нашел поддержку у 62 % опрошенных респондентов.

но в его «теневом» сегменте). В современной судебно-следственной практике можно найти многочисленные примеры приобретения или сбыта специальных технических средств, предназначенных для негласного получения информации, именно через глобальную сеть «Интернет». Так, З. был осужден по ст. 138[1] УК РФ. Согласно материалам дела, у З. возник умысел, направленный на незаконный сбыт специальных технических средств, предназначенных для негласного получения информации – камеры видеонаблюдения, вмонтированной в корпус датчика движения. Реализуя задуманное, З. разместил объявление о продаже данного технического средства на специализированном интернет-ресурсе. Позднее он, преследуя корыстные цели, не зная о том, что в отношении него сотрудниками правоохранительных органов проводятся оперативно-розыскные мероприятия, направленные на недопущение его преступной деятельности, находясь на автомобильной стоянке магазина, осуществил незаконный сбыт вышеуказанной портативной видеокамеры, получив денежное вознаграждение в размере 1 000 рублей[1].

На уровне правоприменения нет однозначного подхода к пониманию содержания ст. 138[1] УК РФ относительно оборота так называемых «код-грабберов» – специальных технических средств, предназначенных для эмулирования радиокоманд передатчика (пульта управления) автомобильной системы охранной сигнализации. Проведенное исследование показывает, что по делам о кражах транспортных средств с использованием «код-грабберов» органы предварительного следствия ограничиваются исключительно вменением ст. 158 УК РФ. Типичным примером может выступать следующее судебное решение в отношении К., осужденного по п. «в» ч. 3 ст. 158 УК РФ. Согласно решению суда, К., имея умысел, направленный на тайное хищение чужого имущества в крупном размере, используя заранее приобретенный брелок, являющийся, согласно заключению эксперта, «код-граббером», выбрал в качестве предмета преступного посягательства автомобиль, принадлежащий потерпевшему З. При помощи вышеуказанного брелока перехватил сигнал охранной сигнализации вышеуказанного автомобиля, после чего подошел к данному автомобилю, где убедившись, что за его действиями никто не наблюдает, то есть его действия являются тайными для окружающих, используя вышеуказанный брелок дистанционно отключил режим «охрана» автомобильной системы охранной сигнализации, что позволило ему беспрепятственно и тайно от окружающих проникнуть в салон автомобиля, а также разблокировать

[1] Приговор Ленинского районного суда г. Тамбова от 19 июня 2018 г. по делу № 1-91/2018.

электронный блок управления двигателем, где, используя имеющийся при нем неустановленный предмет, вставив его в ключевую скважину цилиндра замка зажигания, путем поворота цилиндра в патроне, и осуществив замыкание соответствующих электрических цепей запуска двигателя, разрушив и провернув цилиндр замка зажигания, запустил двигатель автомобиля. После чего похитил вышеуказанный автомобиль, распорядившись им впоследствии по своему усмотрению[1].

Вместе с тем, в ситуациях, связанных исключительно с оборотом (приобретением или сбытом) таких устройств, судебно-следственные органы последовательно исходят из возможности применения ст. 138[1] УК РФ[2].

Сложно найти объяснение тому, почему при квалификации хищений транспортных средств с использованием «код-грабберов» правоприменитель «забывает» дополнительно квалифицировать действия злоумышленника по незаконному приобретению специального технического средства, предназначенного для негласного получения информации. При этом надо отметить, что в конкретных ситуациях одной из причин является отсутствие возможности обнаружения и изъятия самого устройства, а, следовательно, и проведения необходимой экспертизы по нему.

Как представляется, хищения автотранспортных средств с использованием «код-грабберов» должны квалифицироваться по совокупности со ст. 138[1] УК РФ. Такое решение, впрочем, не является идеальным, поскольку оценка подобного деяния в рамках ст. 138[1] УК РФ некоторым образом противоречит содержанию видового объекта данного преступления – «код-грабберы», по сути, не затрагивают основные конституционные права и свободы человека и гражданина.

Уголовно-правовая норма об ответственности за неправомерное вмешательство в работу Государственной автоматизированной системы Российской Федерации «Выборы» (ч. 3 ст. 141 УК РФ) имеет очевидные пересечения с положениями ч. 2 ст. 274[1] УК РФ. Преодоление данной конкуренции в сложившихся условиях представляется довольно проблематичным, поскольку, сопоставление санкций указанных норм позволяет сделать вывод, что общая норма об ответственности за вмешательство в работу объектов критической информационной инфраструктуры Российской Федерации должна быть замещена специальной нормой об ответственности за вмешательство в функционирование ГАС РФ «Выборы»,

[1] Приговор Люблинского районного суда г. Москвы от 16 мая 2018 г. по делу № 01-0289/2018.

[2] Постановление Новосибирского областного суда от 29 марта 2017 г. по делу № 22-1701/2017.

хотя последняя предусматривает более мягкое наказание и не содержит каких-либо привилегирующих признаков. С другой стороны, правила разрешения конкуренции между общей и специальной нормой предельно четко закреплены в ч. 3 ст. 17 УК РФ. Пренебрежение требованием о преимуществе специальной нормы и квалификация содеянного как идеальной совокупности объективно породит ситуацию двойного вменения, что, как известно, не допускается положениями ч. 2 ст. 6 УК РФ. Полагаем, что именно так и должна строиться практика по делам о совершении компьютерных атак на ГАС РФ «Выборы»[1]. Вопрос о наличии явного противоречия в справедливости санкции за данное преступление имеет характер научной дискуссии и предметно должен рассматриваться законодателем.

С недавнего времени признаки компьютеризированного преступления приобрела кража. Федеральным законом от 23 апреля 2018 г. № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» ч. 3 ст. 158 УК РФ была дополнена новым особо квалифицирующим обстоятельством совершения кражи – с банковского счета, а равно в отношении электронных денежных средств. Ранее нами уже обращалось внимание на те негативные последствия, к которым привело включение данного признака в состав уголовно-правовой нормы об ответственности за мошенничество в сфере компьютерной информации (ст. 159^6 УК РФ). Ошибочным, на наш взгляд, было и выделение п. «г» ч. 3 ст. 158 УК РФ. Следствием данного законотворческого решения является то, что кража денежных средств с банковского счета или электронных денежных средств оказалась механически приравнена к краже, совершенной в крупном размере. Таким образом, традиционная модель дифференциации ответственности за преступления против собственности на основе размера похищенного имущества была фактически нарушена. Разработчики законопроекта указывали на то, что хищение денежных средств в электронной форме либо с банковского счета клиента, как правило, сопряжено с профессионализмом преступников, их оснащенностью и, как следствие, повышенной общественной опасностью[2]. Однако, даже поверхностный анализ правоприменительной практики позволяет сделать вывод, что данный довод весьма далек от реального положения дел. В этой связи уместен следующий пример хищения денежных средств с банковского счета клиента на примитивно-бытовом уровне. В., находясь в квартире Ш., увидел

---

[1] Данный вывод нашел поддержку у 82 % опрошенных респондентов.

[2] [Электронный ресурс] // URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=PRJ&n=159733&rnd=4C4C85B84AD6F5C60364116A6485AEF6#006814073483298333 (дата обращения: 05.07.2018).

на полке мебельной стенки сим-карту потерпевшей. Осознавая, что данная сим-карта ему не принадлежит, В. вставил ее в мобильный телефон и получил смс-сообщение от «Мобильного банка» о том, что на расчетном счету банковской карты Ш. находятся денежные средства в размере 5900 рублей. Реализуя умысел на хищение чужого имущества, В., осознавая, что его действия никем не замечены и носят тайный характер, используя мобильный телефон, с помощью услуги «Мобильный банк» осуществил операцию по переводу денежных средств в размере 5900 рублей, принадлежащих Ш., на расчетный счет своей банковской карты[1].

Следует лишь дополнительно отметить, что подобная практика носит массовый характер. Полагаем, что единственно приемлемым выходом из сложившейся ситуации является исключение анализируемого особо квалифицирующего признака из уголовно-правовой нормы об ответственности за кражу.

Данным законом также скорректированы название и диспозиция ст. 159^3 УК РФ путем указания на «электронные средства платежа». Понятие таких средств раскрывается в ст. 3 Федерального закона от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе». В целом указанная категория является более универсальной и охватывает не только платежные карты, но и иные современные средства безналичных расчетов с использованием информационно-коммуникационных технологий.

Введение игорных зон, запрет деятельности казино и игровых клубов на подавляющей части территории России предсказуемо спровоцировало виртуализацию игорной индустрии – игорный бизнес ушел в сеть. Произошло закономерное замещение, когда бывшие владельцы игорных заведений, не желая продолжать свою деятельность в создаваемых государством игорных зонах, инвестировали свободные средства в открытие и развитие интернет-казино[2]. Это и неудивительно, в отличие от подпольных казино и залов игровых автоматов виртуальная организация игорного бизнеса имеет ряд преимуществ: она не связана с необходимостью аренды помещения; не требуется содержать обслуживающий персонал игорного заведения; доступность информационно-коммуникационных технологий позволяет иметь значительную клиентскую базу; сеть позволяет осу-

---

[1] Приговор Октябрьского районного суда г. Красноярска от 11 января 2018 г. по делу № 1-108/2018.

[2] Степашина М.С. Комментарий к Федеральному закону от 29 декабря 2006 г. №244-ФЗ «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации» (постатейный) // Подготовлен для СПС «КонсультантПлюс», 2009.

ществлять деятельность по организации и проведению азартных игр на территории Российской Федерации анонимно и практически из любой точки мира, что существенно снижает риск ответственности.

Наиболее спорным и болезненным вопросом виртуализации игорной индустрии является возможность применения отечественного законодательства об азартных играх к регулированию деятельности нерезидентов Российской Федерации. Следует сразу отметить, что в теории уголовного права нет общепринятого мнения на этот счет. Одни авторы полагают, что осуществляя организацию азартных игр в сети «Интернет» с территории государства, где игорная деятельность разрешена, предприниматели не нарушают требований действующего российского законодательства[1].

Отмечается также, даже если владельцем кипрской или мальтийской компании окажется россиянин, проживающий в Санкт-Петербурге, никаких нарушений ему вменить будет невозможно – на территории России он не организовывал игорных мероприятий, а законодательство того же Кипра или Мальты не запрещает создание казино[2]. Если согласиться с таким подходом, то необходимо будет признать, что уголовно-правовой запрет на проведение азартных игр с использованием сети «Интернет», предусмотренный ст. 171[2] УК РФ, имеет почти декларативный характер.

Как представляется, в этом вопросе принципиально важным является определение места проведения азартных игр. Предыдущие авторы исходят из того, что таким местом является территория иностранного государства, где зарегистрирована соответствующая организация или находится игровой сервер. Вместе с тем, следует согласиться с О.П. Науменко, отмечающей, что хотя ставка и осуществляется в так называемом интернет-пространстве, но фактически ее делает лицо, находящееся на территории Российской Федерации[3]. Следовательно, в таких случаях местом проведения азартных игр необходимо признавать территорию России. То есть, такую деятельность можно будет признавать противоречащей требованиям Федерального закона от 29 декабря 2006 г. №244-ФЗ «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты

---

[1] Изюмова Е.С. Проблемы организации азартных игр в сети «Интернет» // Вопросы права в современном мире : материалы международной заочной научно-практической конференции (07 мая 2013 г.). Новосибирск, 2013. С. 12–19.

[2] Нетупский П. Азартных россиян и валютных трейдеров выгоняют из «Интернета» / [Электронный ресурс] // URL: http: // www.kadis.ru/daily/? Id=57598. (дата обращения: 18.08.2017).

[3] Науменко О.П. Уголовная ответственность за незаконные организацию и проведение азартных игр : дис. … канд. юрид. наук. М., 2016. С. 95.

Российской Федерации»[1], и, соответственно, подпадающей под признаки состава преступления, предусмотренного ст. 171[2] УК РФ[2].

Широко известной проблемой уголовно-правового противодействия незаконному игорному бизнесу в виртуальном пространстве является квалификация действий владельцев интернет-кафе, в которых фактически предоставляются услуги, связанные с проведением азартных игр. В периодической печати открыто обсуждались преимущества и безопасность такого вида деятельности: «…Самым важным преимуществом создатели системы игровых терминалов считают то, что деятельность их партнеров-посредников, предоставляющих терминалы игрокам, (внимание!) не является игорным бизнесом, и абсолютно не играет роли, что игровая система подключена к Интернету, запрещенному «азартным» законодательством… Субагентский договор составляется таким образом, чтобы не допустить ни одного основания признать деятельность оператора терминалов (субагентов) «азартной» … в договоре не говорится ни слова об азартных играх…»[3].

М.С. Степашина напрямую указывает, что запрет на проведение азартных игр с использованием сети «Интернет» российское юридическое лицо или индивидуальный предприниматель легко могут обойти, если они предоставляют только возможность пользования всемирной компьютерной сетью, то есть фактически осуществляют лишь трансляцию азартной игры, а непосредственно организатор азартной игры расположен за пределами Российской Федерации, в стране, где такая деятельность не находится под запретом[4].

Представители правоохранительных органов справедливо ссылаются на то, что недобросовестные хозяйствующие субъекты под видом компьютерного клуба осуществляют проведение азартных игр с использованием

---

[1] Далее по тексту Федеральный закон от 29 декабря 2006 г. №244-ФЗ.

[2] В 1998 году аналогичный подход был применен в США по делу Джея Коэна, осужденного по обвинению в незаконном проведения азартных игр на территории США через принадлежащую ему букмекерскую контору, зарегистрированную на Антигуа и Барбуда.

[3] Локтева Ю.А. Оцениваем возможности системы игровых терминалов // Игорный бизнес: бухгалтерский учет и налогообложение. – 2007. – № 6 // [Электронный ресурс] URL: http: //www.lawmix.ru/bux/58057/ (дата обращения: 20.07.2017).

[4] Степашина М.С. Комментарий к Федеральному закону от 29 декабря 2006 г. №244-ФЗ «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации» (постатейный) // Подготовлен для СПС «КонсультантПлюс», 2009.

сети «Интернет». Основополагающим тезисом выступает система расчетов между администрацией интернет-клуба и посетителями, которая связана не просто с оплатой времени за пользование сетью «Интернет», а напрямую зависит от проигрыша (выигрыша) посетителя – лицо с целью получения возможности сыграть в азартную игру, размещенную на соответствующем онлайн-ресурсе, передает денежные средства работнику клуба. В случае выигрыша, денежные средства выплачиваются игроку из кассы интернет-клуба.

Однако суды не всегда признают такие доводы достаточными. Так, в одном из судебных решений была представлена следующая аргументация: «…При этом С. лишен возможности каким-либо образом воздействовать на состояние баланса, поскольку его функции (субагента), по-существу, ограничиваются функциями оператора, обеспечивающего с помощью принадлежащего ему стандартного компьютерного оборудования доступ пользователей в систему, а также ввод наличных денег в систему и выплату денег из системы при их наличии на балансе. Расходование электронных денег осуществляется пользователями платежно-расчетной системы по их собственному усмотрению на различные нужды.

Таким образом, С. осуществляется субагентская деятельность по приёму-выдаче платежей клиентам системы расчетов с помощью оборудования, подключенного к сети «Интернет». Данный вид деятельности регулируется главой 52 Гражданского кодекса Российской Федерации.

Указанная деятельность осуществляется посредством стандартного компьютерного оборудования. Никаких соглашений о выигрыше в арендованном С. помещении не происходит. С. не принимает ставок, никаких правил об азартных играх не устанавливает. Никакого игрового программного продукта в эксплуатируемом оборудовании не содержит. При доступе клиента к ресурсу, предоставляемому иностранным Принципалом, никаких азартных игр на платежном терминале самообслуживания не происходит…»[1].

Согласно ст. 1005 ГК РФ по агентскому договору одна сторона (агент) обязуется за вознаграждение совершать по поручению другой стороны (принципала) юридические и иные действия от своего имени, но за счет принципала либо от имени и за счет принципала. По сделке, совершенной агентом с третьим лицом от имени и за счет принципала, права и обязанности возникают непосредственно у принципала.

[1] Решение Ленинского районного суда г. Ростова-на-Дону от 09 апреля 2011 г. по делу № 2-613/11 // ГАС «Правосудие».

В связи с этим Е.И. Спектор делает вывод: фактически агент выступает в качестве расчетной системы, и его взаимоотношения с физическими лицами – клиентами ограничиваются лишь приёмом и выдачей денег, суть и природа которых имеет принципиальное отличие от приёма ставок и заключения пари, легальные определения которых содержатся в пунктах 2 и 3 ст. 4 Закона №244-ФЗ[1].

Получается, что агент, являясь резидентом Российской Федерации, организацией и проведением азартных игр как бы не занимается, поскольку является лишь посредником между организатором (иностранной компанией) и игроком (клиентом).

Вместе с тем, Е.С. Изюмова справедливо отмечает, что фактически все обстоит с точностью до наоборот, агент организует игорную деятельность: арендует помещение, платит заработную плату персоналу, принимает ставки, выдает выигрыш, а принципал – получает прибыль и обеспечивает видимую законность и безнаказанность всего мероприятия одним своим существованием[2].

Несмотря на это, А.В. Иванчин полагает, что квалифицировать подобные действия по ст. 171^2 УК РФ всё же нельзя. Деятельность общества по предоставлению посетителям интернет-клуба (кафе и т.д.) доступа к конкретному сайту азартных игр не является деятельностью по организации и проведению азартных игр в смысле, придаваемом этой деятельности Федеральным законом №244. Организация, оказывающая клиентам услуги доступа к сети «Интернет», в том числе оплаты услуг с помощью «электронного кошелька», не может нести ответственность за действия клиента, решившего воспользоваться услугами интернет-казино и использующего при этом электронные средства оплаты, предварительно принятые от него этой организацией и зачисленные на его счет[3].

О.П. Науменко пишет, что, если с мнением А.В. Иванчина и можно согласиться, то только частично. По ее мнению, если хозяйствующий

---

[1] Спектор Е.И. О правомерности осуществления агентом в интересах и от имени принципала (лицензиата) услуги по приему платежей и осуществлению им выплат клиентам без получения лицензии на осуществление деятельности по организации и проведению азартных игр в букмекерских конторах и тотализаторах // Законодательство и экономика. – 2012.– № 5. – С. 53.

[2] Изюмова Е.С. Проблемы организации азартных игр в сети «Интернет» // Вопросы права в современном мире : материалы международной заочной научно-практической конференции (07 мая 2013 г.). Новосибирск, 2013. С. С. 12–19.

[3] Иванчин А.В. О совершенствовании уголовно-правовых и иноотраслевых средств борьбы с незаконной организацией азартных игр в России // Вестник Ярославского государственного университета. – 2013. – № 1 (23). – С. 43.

субъект сознательно предоставляет доступ к конкретному сайту азартных игр и участвует в проведении расчетов с игроками, то фактически такая деятельность является проведением азартных игр. Субагентский договор, равно как и имеющееся разрешение на оказание услуг связи не меняют, а лишь прикрывают действительное содержание осуществляемой деятельности. В этой связи, на наш взгляд, юридическая оценка подобного рода действий как незаконных организации и проведения азартных игр, является возможной только при условии признания, что заключенный между сторонами субагентский договор обладает признаками притворной сделки, которая хотя формально и не нарушает закон, но на самом деле прикрывает собой сделку, совершаемую с целью, противной основам правопорядка и нравственности, – проведения азартных игр с использованием сети «Интернет». Как известно, в силу ст. 169 ГК РФ такая сделка является недействительной независимо от ее признания таковой судом[1].

Действительно, владелец такого заведения не просто предоставляет доступ в глобальную сеть, он сознательно участвует в заключении соглашений о выигрыше между его посетителями и компанией-владельцем интернет-казино.

Таким образом, умышленное создание на территории Российской Федерации необходимых условий для заключения соглашений о выигрыше между гражданами и субъектами (организациями), осуществляющими проведение азартных игр в информационно-телекоммуникационной сети «Интернет», необходимо квалифицировать по ст. 171[2] УК РФ. Юридическая оценка подобного рода действий как незаконных организации и проведения азартных игр, является возможной только при условии признания, что заключенный между сторонами субагентский договор обладает признаками притворной сделки, которая хотя формально и не нарушает закон, но на самом деле прикрывает собой сделку, совершаемую с целью, противной основам правопорядка и нравственности, – проведения азартных игр с использованием сети «Интернет»[2].

Проблемы уголовно-правового противодействия распространению порнографических материалов достаточно хорошо освещены в отечественной науке. Специалисты неоднократно обращались к социально-правовой обусловленности криминализации подобного рода деятельно-

---

[1] Науменко О.П. Уголовная ответственность за незаконные организацию и проведение азартных игр : дис. … канд. юрид. наук. М., 2016. С. 100.

[2] См., например: Науменко О.П. Уголовная ответственность за незаконные организацию и проведение азартных игр : дис. … канд. юрид. наук. М., 2016. С. 12.

сти[1], неопределенности самого предмета – порнографии[2], особенностям содержания объективной стороны соответствующих составов преступлений[3] и т.д.

Учитывая, что незаконный оборот порнографических материалов является по своей природе информационным преступлением, неудивительно, что в современных условиях всеобщей виртуализации он преимущественно сместился в пространство информационно-телекоммуникационной сети «Интернет». Доступность, дистанционность, анонимность, наличие удобных платежных сервисов (web-money, яндекс-деньги и т.п.) делают интерактивный способ распространения порнографии крайне привлекательным для преступников. В свою очередь, это заставляет правоохранителей и ученых-криминалистов сфокусировать свое внимание именно на проблемах противодействия распространению порнографии в web-зоне.

Необходимость научного осмысления специфики виртуального оборота порнографических материалов обусловлена высоким уровнем риска привлечения к уголовной ответственности невиновных лиц. Современная обвинительная практика строится на основе выявления IP-адреса, фигурирующего в обороте порнографии[4]. Вместе с тем, известно, что сам по себе IP-адрес идентифицирует устройство, а не его оператора. Таким образом, следствию необходимо еще доказать, кто конкретно осуществлял те или иные манипуляции с порнографическими материалами. При этом неправомерный контроль третьего лица над компьютером с соответствующим IP-адресом может быть не только физическим, но и интерактивным – посредством использования программного обеспечения для удаленного

---

[1] См., например: Супонина Е.А. К вопросу о возможности установления административной ответственности за незаконные изготовление и оборот порнографических материалов и предметов // Инновационная наука. – 2015. – № 9.

[2] См., например: Осокин Р.Б. Порнография: опыт легального, доктринального и судебного толкования // Вестник Нижегородской академии МВД России. – 2014. – № 1 (25).

[3] См., например: Гунарис Р.Г. О некоторых вопросах терминологии статьи 242 Уголовного кодекса Российской Федерации // Правовая реформа: пути совершенствования : материалы научно-практической конференции (Ставрополь, 15–16 марта 1999 г.) Ставрополь, 1999. С. 107; Денисенко М.В., Осокин Р.Б. Уголовно-правовая характеристика незаконного распространения порнографических материалов или предметов. М., 2005; Узденов Р.М. Актуальные вопросы квалификации деяний, предусмотренных статьями 242 и 242.1 УК РФ // Проблемы современной науки и практики. – 2008. – № 2 и др.

[4] См., например: Гончар В.В. Теоретические и правовые аспекты розыскной деятельности следователя : монография. М., 2017.

управления. Копирование той или иной информации на компьютер может быть также осуществлено и незаметно для самого пользователя в результате работы вредоносных компьютерных программ.

Вместе с тем, обобщение судебных решений позволяет сделать вывод, что суды весьма скептически относятся к такому техническому обоснованию подсудимым своей невиновности. При этом, как правило, отказывая в удовлетворении поданных жалоб, суды никак не комментируют очевидную неполноту проведенного следствия, ограничиваясь стандартным – выводы суда о виновности осужденного в совершенном им преступлении основаны на доказательствах, полученных в установленном законом порядке, всесторонне, полно и объективно исследованных в судебном заседании и получивших оценку суда в соответствии с требованиями ст. 88 УПК РФ.

Так, например, Р. был осужден по ст. 242 УК РФ за незаконное распространение порнографических материалов. Не согласившись с приговором, он обжаловал его, просил приговор отменить и вынести в отношении него оправдательный приговор. В обоснование своей просьбы указал, что судом не было доказано, что именно он с неустановленного дознанием источника скопировал на жесткий магнитный диск своего персонального компьютера файл, содержащий признаки порнографической продукции, а также тот факт, что он распространил и публично продемонстрировал порнографическую видеозапись неопределенному кругу лиц, разместив его на странице сайта, поскольку невозможно определить, кто находился в указанное время за компьютером, что в судебном заседании подтвердили свидетели, имеющие высшее техническое образование и квалификацию инженера по специальности «Автоматизированные системы обработки информации и управление», пояснившие, что компьютером мог управлять удаленный пользователь, используя вредоносные программы, при этом не оставляя никаких следов взлома компьютера[1].

Как представляется, чтобы устранить сомнения в совершении распространения порнографических материалов конкретным лицом на стадии предварительного расследования в обязательном порядке должны проводиться компьютерно-технические экспертизы изъятого оборудования. Это позволит не только выявить следы либо подтвердить факт хранения запрещенного контента, но и определить: 1) заражен ли компьютер вредоносными программами; 2) характер деятельности имеющихся вирусов; 3) имеется ли программное обеспечение, позволяющее управлять компьюте-

[1] Кассационное определение судебной коллегии по уголовным делам Волгоградского областного суда от 07 марта 2013 г. по делу № 22-853/13.

ром дистанционно и т.п. Признавая неоспоримую значимость получения ответов на указанные выше вопросы, представляется очевидным, что в сложившихся условиях бремя установления подобного рода обстоятельств во многом будет лежать на стороне защиты.

Изучение современной судебно-следственной практики показывает, что типичной ситуацией совершения одного из преступлений, предусмотренных ст.ст. 242, 242[1] УК РФ, является копирование лицом аудиовизуального файла с использованием torrent-клиента (специальной программы для файлообмена). Установление признака специальной цели – распространение, по данной категории дел зачастую сводится к утверждению, что лицо знало или должно было знать, что torrent-клиент работает по принципу «скачивая-раздаешь». Иными словами, копируя материалы порнографического содержания, лицо как бы осознает, что создает техническую возможность их получения другими пользователями файлообменника. Приведенная формулировка довольно часто встречается в уголовных делах, расследуемых по факту совершения преступления, предусмотренного ст. 242[1] УК РФ. Так, например, А., имея умысел на хранение в целях распространения материалов с порнографическими изображениями лиц, достигших восемнадцатилетнего возраста, содержащие изображение и описание сексуальных действий с участием указанных лиц, изображение и описание нестандартных форм сексуальной активности, детализированное изображение крупного плана этапов полового акта, и реализуя задуманное, из неустановленного источника информации, посредством сети «Интернет» и пиринговой сети передачи данных, скопировал в ранее им созданную папку «Закачка» видеофайлы порнографического содержания. Продолжая свои преступные действия, направленные на распространение материалов с порнографическими изображениями лиц, достигших восемнадцатилетнего возраста, А., находясь по месту жительства, используя доступ к файлообменной пиринговой сети, дающей возможность обмена файлами между ее абонентами, предоставил указанные видеофайлы, хранящиеся в памяти его персонального компьютера посредством файлообменного сервера, доступного неограниченному кругу пользователей файлообменной сети, заведомо осознавая, что перечисленные выше видеофайлы становятся доступными для просмотра и копирования неограниченному кругу пользователей указанной сети, то есть являются общедоступными[1].

Вместе с тем, довольно часто привлекаемые к ответственности лица

[1] Приговор Норильского городского суда Красноярского края от 20 октября 2011 г. по делу № 1-165/2011.

в своих показаниях указывают, что после копирования интересующего файла на свой компьютер, они блокировали «раздачу», чтобы не участвовать в процессе файлообмена запрещенным контентом. Однако даже при таких обстоятельствах можно утверждать, что в процессе самого копирования лицо пусть и весьма непродолжительное время, но все же участвовало в файлообмене. По-настоящему же проблемным является вопрос о том, что конкретно передает такое лицо? Как известно, программа-файлообменник работает по принципу пиринговой сети, когда между пользователями посредством сети «Интернет» происходит взаимный обмен данными (компьютерной информацией). При этом необходимо учитывать, что получаемые файлы передаются рассеянно, от конкретного пользователя к конкретному пользователю копируется лишь фрагмент запрашиваемого файла. В таких условиях вероятность получения компьютерного файла в полном объеме от одного пользователя к другому без участия третьего, четвертого, пятого стремится к нулю. Следовательно, конкретный пользователь torrent-клиента, получив необходимый ему файл и технически предотвратив его последующую «раздачу», в процессе копирования осуществил передачу некого количества компьютерных данных иным пользователям torrent-клиентов, но не самого файла в полном объеме. Таким образом, переданный программой пакет данных не является завершенным продуктом и не может быть воспроизведен стандартным программным обеспечением как видео, фото, аудио произведение. Подобная компьютерная информация в виде отдельных сегментов конкретных файлов, которая недоступна слуховому и визуальному восприятию человеком, объективно еще не может расцениваться как предмет преступлений, предусмотренных ст.ст. 242, 242[1] УК РФ.

Дискуссионным является вопрос о квалификации онлайн-показа посредством веб-камер (и сервиса Skype, например) различных действий сексуального характера (от стриптиза до реального полового акта). М.М. Зазирная полагает, что подобные случаи не могут быть квалифицированы по ст. 242 УК РФ, однако не в связи с отсутствием предмета, а ввиду отсутствия таких признаков объективной стороны указанного состава преступления, как публичная демонстрация, рекламирование либо распространение порнографических материалов или предметов[1].

Соглашаясь с окончательным выводом автора, нельзя не отметить спорность предложенной аргументации. Совершение лицом определен-

[1] Зазирная М.М. Квалификация распространения порнографических материалов в режиме реального времени с использованием сети «Интернет» // Уголовное право. – 2015. – № 6. – С. 22.

ных действий перед веб-камерой вряд ли следует оценивать как демонстрацию либо распространение порнографического материала по смыслу ст. 242 УК РФ. Природа данной статьи предполагает наличие овеществленного объекта с определенным содержанием – порнографией, которого как раз и нет. Совершение подобного рода действий в отношении совершеннолетних лиц, пожалуй, не подпадает под действие уголовного закона. В случае, когда зрителем такого онлайн-показа выступает лицо, не достигшее возраста 16 лет, имеются признаки преступления, предусмотренного ст. 135 УК РФ.

Следует, однако, отметить, что запись такого стриптиза или иных действий сексуального характера, транслируемых посредством сети «Интернет», в целях последующего распространения, публичной демонстрации или рекламирования будет уже являться незаконным изготовлением порнографических материалов в соответствии со ст. 242 УК РФ.

Относительно дискуссионным является вопрос квалификации распространения порнографического анимационного материала, то есть продукта (файла), который не изображает реальных людей. По справедливому мнению М.В. Гусаровой, незаконные действия с виртуальной порнографией (3D-порнографией), безусловно, должны охватываться действием ст.ст. 242, 242[1] УК РФ, так как вред общественной нравственности наступает вне зависимости от способа создания указанной продукции[1]. Как представляется, такой подход в целом соответствует статье 1 Международной конвенции о пресечении обращения порнографических изданий и торговли ими (Женева, 12 сентября 1923 г.), согласно которой к порнографическим предметам относятся рисунки, гравюры, картины, афиши и т.д.

Наличие существенных проблем в законодательном определении компьютеризированных преступлений, пожалуй, наиболее ярко может быть представлено на примере уголовно-правовой нормы об ответственности за незаконную добычу и оборот особо ценных диких животных и водных биологических ресурсов, принадлежащих к видам, занесенным в Красную книгу Российской Федерации и (или) охраняемым международными договорами Российской Федерации (ст. 258[1] УК РФ).

С момента появления в июле 2013 года данная норма подвергалась двум значимым изменениям. Так, в декабре 2017 года часть вторая была дополнена указанием на специфический способ совершения незаконных

[1] Гусарова М.В. Уголовно-правовые меры противодействия незаконному обороту порнографических материалов и предметов // Вестник экономии, права и социологии. – 2015. – №3. – С. 131.

действий с особо ценными дикими животными и водными биологическими ресурсами – «с публичной демонстрацией, в том числе в средствах массовой информации либо информационно-телекоммуникационных сетях (включая сеть «Интернет»)».

Однако уже в июне 2018 года законодатель продолжил «оцифровку» ст. 258^1 УК РФ, включив в нее по-сути самостоятельный состав преступления, установив в ч. 1^1 ответственность за незаконные приобретение или продажу особо ценных диких животных либо водных биологических ресурсов «с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет».

Как нетрудно заметить, разница между действующими редакциями частей 1^1 и 2 ст. 258^1 УК РФ заключается собственно в том, что в первом случае речь идет об использовании информационно-телекоммуникационных сетей при приобретении или продаже особо ценных диких животных и водных биологических ресурсов вообще, а во втором – о публичной демонстрации таких животных и ресурсов, в том числе с использованием информационно-телекоммуникационных сетей. Таким образом, с формально-логической точки зрения использование информационно-телекоммуникационной сети является более объемным понятием и охватывает таковое, совершаемое в целях публичной демонстрации соответствующих объектов. В этой части положения пункта «б» части 2 ст. 258^1 УК РФ являются специальной нормой по отношению к ч. 1^1 ст. 258^1 УК РФ.

Вместе с тем, понятно, что договоренность о сбыте особо ценных диких животных или водных биологических ресурсов не может быть достигнута исключительно посредством демонстрации реализуемой особи животного или птицы в сети «Интернет». Так или иначе, но сторонам необходимо оговаривать такие значимые условия, как цена незаконной сделки, порядок расчетов, условия и сроки доставки животного и т.п. Означает ли это, что ч. 2 ст. 258^1 УК РФ фактически теряет какое-либо прикладное значение? Полагаем, что ответ на поставленный вопрос должен быть отрицательным. Объясняется это тем, что наказание по ч. 2 ст. 258^1 УК РФ является более строгим чем в ч. 1^1 этой же статьи. Следовательно, в случае, когда лицо использует информационно-телекоммуникационные сети для приобретения или продажи особо ценных диких животных без их визуальной демонстрации, применению подлежит ч. 1^1. В том же случае, когда потенциальному приобретателю предоставлялись визуальные материалы, содеянное необходимо квалифицировать уже по ч. 2 ст. 258^1 УК РФ.

Н.В. Летёлкин обращает внимание на юридико-техническое несовершенство конструкции квалифицирующего признака, предусмотренного п. «г» ч. 2 ст. 245 УК РФ. Автор указывает, что смысл данного отягчающего обстоятельства заключается в «публичной демонстративности» жестокого обращения с животными, то есть действия должны совершаться либо в присутствии индивидуально-неопределенного круга лиц, либо транслироваться в режиме реального времени в средствах массовой информации или информационно-телекоммуникационных сетях[1].

Вместе с тем, как известно, целью законодателя было повысить ответственность не только за публичное жестокое обращение с животными, но и за жестокое обращение, сопряженное с последующим распространением аудиовизуальных материалов об этом посредством информационно-коммуникационных сетей.

Так, в пояснительной записке к Федеральному закону от 20 декабря 2017 г. № 412-ФЗ «О внесении изменений в статьи 245 и 258[1] Уголовного кодекса Российской Федерации и статьи 150 и 151 Уголовно-процессуального кодекса Российской Федерации» разработки ссылаются на то, что общественная опасность подобных преступлений существенно повышается за счет доступа к таким материалам индивидуально неопределенной аудитории, имеющей реальную возможность в любой удобный момент осуществить их просмотр. Сама демонстрация этих материалов наносит дополнительный вред общественным отношениям, отнесенным к объекту уголовно-правовой охраны[2].

Практика, как известно, пошла по пути именного такого толкования анализируемого квалифицирующего признака[3]. Мнение Н.В. Летёлкина о

---

[1] Летёлкин Н.В. Об очередном примере расширения системы преступлений, совершаемых с использованием информационно-телекоммуникационных сетей // Обеспечение национальной безопасности – приоритетное направление уголовно-правовой, криминологической и уголовно-исполнительной политики : материалы XI Российского Конгресса уголовного права, посвященного памяти доктора юридических наук, профессора Владимира Сергеевича Комиссарова. М., 2018. С. 157. С. 160–161.

[2] [Электронный ресурс] // URL:http://www.consultant.ru/cons/cgi/online.cgi?req=doc&cacheid=6908ADC4E95D7C163C4F1BFD2D2D48CC&mode=backrefs&div=LAW&dirRefFld=65532&opt=1&BASENODE=27-3&ts=16950153349780423084&base=PRJ&n=165398&rnd= 0.4391729140295988#06627350361694648 (дата обращения: 05.07.2018).

[3] Приговор «хабаровским живодеркам»: реальные сроки и обязательный работы // [Электронный ресурс] // URL: https://ria.ru/incidents/20170825/1501074099.html (дата обращения: 05.07.2018).

том, что это вступает в противоречие с конструкцией состава преступления, предусмотренного ст. 245 УК РФ, и как бы выходит за пределы его объективной стороны, уязвимо в том отношении, что автор концентрирует свое внимание на моменте окончания именно основного состава. Вместе с тем, применительно к п. «г» ч. 2 ст. 245 УК РФ необходимо говорить о моменте окончания квалифицированного состава жестокого обращения с животными, который альтернативен и может быть связан с моментом публичной демонстрации соответствующих действий в информационно-коммуникационной сети «Интернет».

Обобщение современной судебно-следственной практики позволяет сделать вывод о все большем преобладании террористической и экстремистской пропаганды, а равно действий, связанных с возбуждением ненависти либо вражды, именно в глобальной сети «Интернет». Еще в докладе о результатах и основных направлениях деятельности Министерства внутренних дел Российской Федерации за 2013 год отмечалось, что особую роль в распространении деструктивной идеологии в последние годы стал играть Интернет, служащий для лидеров радикальных структур средством коммуникации и организации экстремистских и террористических акций[1].

Несмотря на то, что традиционные формы распространения экстремистских и террористических убеждений не потеряли своей актуальности – правоохранительные органы периодически изымают экземпляры запрещенной литературы, пресекают деятельность лиц, занимающихся криминальной пропагандой под прикрытием религиозной деятельности, – центром борьбы за нормальное «духовно-нравственное» состояние населения все в большей степени становится виртуальная среда.

Отметим, что в отдельных случаях совершение преступлений экстремистской направленности, связанных с распространением запрещенной информации, может быть сопряжено с посягательством на безопасность компьютерных данных и систем. Так, Ц. был признан виновным в совершении преступлений, предусмотренных ч. 1 ст. 272 УК РФ, ч. 1 ст. 282 УК РФ и ч. 3 ст. 212 УК РФ. Согласно приговору суда, Ц. взламывал электронные почтовые ящики физических и юридических лиц, получая тем самым неправомерный доступ к ним. В последующем с указанных почтовых ящиков он осуществлял массовую рассылку электронных писем с угрозами и подстрекательством к насилию в отношении лиц различных

[1] Официальный сайт Министерства внутренних дел Российской Федерации // [Электронный ресурс] // URL: https://мвд.рф/Deljatelnost/results/annual_reports (дата обращения: 02.11.2017).

национальностей, представителям власти, промышленной и бизнес-элит, Русской православной церкви и лиц, исповедующих православие. В письмах также содержались призывы к совершению массовых беспорядков[1].

При квалификации компьютеризированных преступлений, связанных с распространением криминогенной информации, довольно часто возникает вопрос о применении сроков давности к действиям лица, которое разместило тот или иной аудиовизуальный материал в общем доступе в сети «Интернет». Так, например, по одному из дел суд пришел к выводу, что поскольку представленными материалами уголовного дела достоверно не установлено время размещения подсудимым Б. видеороликов экстремистской направленности в социальной сети, а сам он настаивает на том, что добавил их практически сразу после регистрации, о точной дате которой суд имеет неопровержимые сведения, имеются основания для применения ст. 78 УК РФ[2].

На наш взгляд, является неверным подход, связанный с исчислением сроков давности с момента размещения соответствующего экстремистского или террористического контента в сети «Интернет». При сохранении такого файла (файлов) в общем доступе в течение продолжительного периода времени необходимо вести речь о наличии признаков длящегося преступления и отсчитывать сроки давности с момента, когда лицо по тем или иным причинам прекратило свои действия, то есть, например, соответствующий материал был удален самим виновным либо администратором интернет-ресурса. Полагаем, что предлагаемое решение не только точнее выявляет содержание преступной интернет-пропаганды, но и избавит судебно-следственные органы от необходимости изыскания информации о времени непосредственной «загрузки» запрещенных данных, что в отдельных случаях представляет собой попросту невыполнимую задачу.

2.3. ПРОБЛЕМЫ КВАЛИФИКАЦИИ МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ (СТ. 159[6] УК РФ)

Вопрос о законодательном определении ответственности за хищение, совершаемое посредством вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или инфор-

[1] В Ухте осужден хакер-экстремист / Официальный сайт прокуратуры Республики Коми. 2014. 23 октября // [Электронный ресурс] // URL: http://procrf.ru/news/252749-v-uhte-osujden-haker-ekstremist.html (дата обращения: 20.06.2018).

[2] Приговор Ленинского районного суда г. Новосибирска от 31 марта 2014 г. по делу № 1-43/2014.

мационно-коммуникационных сетей, обладает совершенно особым теоретико-прикладным значением. Как известно, современная цифровая преступность в основной своей части – преступность корыстная. Так, согласно данным Positive Technologies, в 2017 году 70 % от всех компьютерных атак были совершены с целью получения прямой финансовой выгоды (прежде всего посредством вывода денег с банковских счетов потерпевшего), 23 % в качестве главной цели предполагали неправомерное получение данных, остальные 7 % составляют деяния, которые специалисты относят к категории так называемого «хактивизма», то есть совершения атаки ради самой атаки, с целью демонстрации или проверки собственных навыков или тестирования нового вредоносного программного обеспечения и т.п.[1]

В связи с этим познание особенностей конструкции ст. 159[6] УК РФ, а также специфики проблем и противоречий, возникающих при ее практической реализации, составляет самостоятельную и крайне важную исследовательскую задачу.

Как известно, появление в 2012 году специальной нормы о мошенничестве в сфере компьютерной информации (ст. 159[6] УК РФ) вызвало немало дискуссий в научном сообществе и породило неоднообразную правоприменительную практику. Теоретики преимущественно расходились по двум вопросам: 1) предполагает ли компьютерное мошенничество воздействие на психику человека с целью введения его в заблуждение, то есть обман или злоупотребление доверием[2] и 2) является ли преступление, предусмотренное ст. 159[6] УК РФ, двуобъектным, одновременно посягающим и на отношения собственности, и на отношения информационной безопасности[3].

Неудивительно, что при такой неопределенности на уровне толкования практики по-разному оценивали хищения денежных средств граждан,

---

[1] Сборник исследований по практической безопасности АО «Позитив Текнолоджиз». М., 2018. С. 13.

[2] См., например: Комментарий к Уголовному кодексу Российской Федерации (постатейный). Т. 1. – 2-е изд., перераб. и доп. / под ред. засл. юриста Российской Федерации, д-ра юрид. наук, проф. А.В. Бриллиантова // СПС «КонсультантПлюс»; Лопатина Т.М. Проблемы уголовно-правовой защиты сфер компьютерной информации: современный взгляд на мошенничество // Право и безопасность. – 2013. – № 3-4 (45). – С. 91; Хилюта В.В. Хищение с использованием компьютерной техники или компьютерное мошенничество? // Библиотека криминалиста. – 2013. – № 5 (10). – С. 62; Шумихин В.Г. Седьмая форма хищения чужого имущества // Вестник Пермского университета. – 2014. – № 2 (24). – С. 229 и др.

[3] См.: Третьяк М.И. Проблемы квалификации новых способов мошенничества // Уголовное право. – 2015. – № 2. – С. 95.

совершенные с использованием современных информационно-коммуникационных технологий. Пожалуй, наиболее наглядно это проявлялось при квалификации хищений денежных средств со счетов граждан посредством использования сервиса «мобильный банк» – в опубликованной судебной практике без труда можно найти примеры квалификации таких деяний и по ст. 158 УК РФ, и по ст. 159^6 УК РФ, и по совокупности ст. 159^6 и ст. 272 УК РФ.

В связи с этим представляется востребованным и своевременным принятие Пленумом Верховного Суда Российской Федерации постановления от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате»[1]. В п. 1 постановления Пленум, по сути, поставил точку в дискуссии относительно способа совершения преступления, предусмотренного ст. 159^6 УК РФ. Интерпретировав разъяснение высшей судебной инстанции, следует сделать вывод, что обман или злоупотребление доверием не являются способами мошенничества в сфере компьютерной информации.

Таким образом, получил поддержку подход, согласно которому преступление, предусмотренное ст. 159^6 УК РФ, характеризуется своим специфическим способом, не вписывающимся ни в одну из традиционно выделяемых форм хищения. В первоначальной редакции п. 1 постановления Пленума состоял из двух абзацев и содержал специальное указание на то, что мошенничество в сфере компьютерной информации совершается не путем обмана или злоупотребления доверия, а иным способом – путем вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации. Исключение данного разъяснения редакционной коллегией было мотивировано тем, что в теории уголовного права нет общепринятой позиции относительно того, является ли такое вмешательство разновидностью обмана или самостоятельным способом мошенничества[2].

Как представляется, проблема оценки манипуляций с компьютерной информацией как особого рода обмана имеет искусственный характер и обусловлена изначально неудачной редакцией ст. 159^6 УК РФ. Название данной нормы, к сожалению, представляет собой не адаптированный к российской правовой системе, почти автоматизированный перевод ст. 8

---

[1] Официальный сайт Верховного Суда Российской Федерации // [Электронный ресурс]: URL: http://www.vsrf.ru/documents/own/26108/ (дата обращения: 05.12.2017).

[2] Заседание Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. // [Электронный ресурс] // URL: http://www.vsrf.ru/press_center/news/26093/ (дата обращения: 06.12.2017).

«Компьютерное мошенничество» (Computer fraud) Конвенции «О преступности в сфере компьютерной информации» (Будапешт, 23 ноября 2001 г.)[1]. Учитывая многовековую отечественную традицию толкования природы мошенничества и обмана как способа его совершения, изначально правильнее было бы предусмотреть ответственность за «хищение в сфере компьютерной информации», как это реализовано, например, в ст. 212 УК Республики Беларусь[2]. В сложившихся же условиях в ст. 159[6] УК РФ мы имеем новую форму хищения в сфере информационных технологий, которая мошенничеством не является, но называется таковым.

Принимая во внимание расположение уголовно-правовой нормы о мошенничестве в сфере компьютерной информации, представляется очевидным, что непосредственным объектом этого преступления выступают общественные отношения в сфере собственности. В современной литературе такое понимание содержания объекта преступления, предусмотренного ст. 159[6] УК РФ, является наиболее распространенным[3].

Вместе с тем, имеются и другие точки зрения. Так, В.И. Гладких отмечает, что чрезвычайно трудно сформулировать объект и предмет деяния, указанного в ст. 159[6] УК РФ, поскольку, как поясняет автор, общеизвестное представление о непосредственном объекте мошенничества как конкретной форме собственности вступает в противоречие с действующей редакцией компьютерного мошенничества, поскольку сфера компьютерной информации относится совершенно к другой области общественных отношений, а именно к тем отношениям, которые подвергаются воздействию со стороны преступлений, предусмотренных гл. 28 УК РФ «Преступления в сфере компьютерной информации»[4]. В целом В.И. Гладких делает вывод, что расположение в структуре Особенной части УК РФ нормы о мошенничестве в сфере компьютерной информации является ошибочным.

---

[1] Конвенция о преступности в сфере компьютерной информации (EST № 185) от 23 ноября 2001 г. // СПС «КонсультантПлюс».

[2] Уголовный кодекс Республики Беларусь: с изм. и доп. на 05 января 2015 г. Минск : Нац. центр правовой информ. Респ. Беларусь, 2015. С. 98.

[3] См., например: Комментарий к Уголовному кодексу Российской Федерации (научно-практический, постатейный). – 3-е изд., перераб. и доп. / под ред. д-ра юрид. наук, проф. С.В. Дьякова, д-ра юрид. наук, проф. Н.Г. Кадникова. М., 2015. С. 406; Комментарий к Уголовному кодексу Российской Федерации (постатейный). Т. 1. – 2-е изд., перераб. и доп. / под ред. засл. юриста РФ, д-ра юрид. наук, проф. А.В. Бриллиантова // СПС «КонсультантПлюс» и др.

[4] Гладких В.И. Компьютерное мошенничество: а были ли основания его криминализации? // Российский следователь. – 2014. – № 22. – С. 25–31.

Согласно обоснованному в науке уголовного права подходу, основной объект преступления лишь в большей степени определяет социальную направленность преступления, структуру соответствующего состава и его место в системе Особенной части УК РФ[1]. В связи с этим следует констатировать, что мошенничество в сфере компьютерной информации по своей направленности справедливо причислено к числу противоправных посягательств именно на отношения собственности.

А.Г. Безверхов пишет, что в условиях поступательного движения современной России к постиндустриальному обществу, постепенного перехода нашей страны к использованию высоких технологий повышается опасность «компьютерного мошенничества». Такое деяние характеризуется дополнительным объектом. Им выступает общественная безопасность[2].

В свете последних разъяснений Пленума Верховного Суда Российской Федерации следует согласиться с мнением А.Г. Безверхова – в качестве дополнительного объекта мошенничества в сфере компьютерной информации выступают общественные отношения, обеспечивающие информационную безопасность.

По мнению Т.М. Лопатиной, предметом компьютерного мошенничества, как и традиционного мошенничества, является чужое имущество или право на него. Но в компьютерах и компьютерных сетях хранятся не деньги или имущество, а информация о них или об их движении. Информация – это не имущество, она не обладает экономическим, социальным и юридическим признаками, характеризующими чужое имущество как предмет хищения, который выступает обязательным признаком состава мошенничества. Это всего лишь сведения, представленные в специфической форме. Законодателем акцент сделан на форму существования информации как сведений о лицах, явлениях и процессах, содержащихся в информационных системах (банках данных) именно в компилированном виде[3].

В свою очередь М.Ю. Дворецкий пишет, что предметом преступного посягательства по ст. 159[6] УК РФ являются: 1) компьютерная информация, под которой в уголовно-правовом аспекте понимаются сведения (или сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи, согласно по-

---

[1] Российское уголовное право. В 2-х т. Т. 1. Общая часть / под ред. А.И. Рарога. М., 2008. С. 111.

[2] Безверхов А.Г. Мошенничество и его виды: вопросы законодательной регламентации и квалификации // Уголовное право. – 2015. – №5. – С.13.

[3] Лопатина Т.М. Проблемы уголовно-правовой защиты сфер компьютерной информации: современный взгляд на мошенничество // Право и безопасность. – 2013. – №3-4 (45). – С. 93.

ложениям примечания к ст. 272 УК РФ; 2) имущество, то есть совокупность вещей, которые находятся в собственности лица, в том числе включая деньги и ценные бумаги, а также имущественные права на получение вещей или имущественное удовлетворение от других лиц[1].

Представляется, что в качестве предмета компьютерного мошенничества, как и любого другого хищения, справедливо рассматривать имущество. Однако специфика рассматриваемого преступления такова, что вещи, как и наличные денежные средства, обладающие вещно-правовой природой, хотя и могут выступать предметом[2], но не типичны для данного вида мошенничества. Практика показывает, что предметом посягательства при компьютерном мошенничестве, как правило, выступают безналичные и электронные деньги.

Нематериальный характер безналичных и электронных денег, как представляется, не может выступать веским аргументом в пользу отрицания возможности их рассмотрения в качестве предмета мошенничества в сфере компьютерной информации. Ю.Е. Пудовочкин совершенно прав, когда отмечает, что потребности сегодняшнего дня настоятельно требуют отказаться от ставшего догмой понимания предмета только и исключительно как вещи (предмета материального мира)[3].

Проведенное исследование показало, что предметом компьютерного мошенничества на практике также признаются бездокументарные ценные бумаги, которые представляют собой ни что иное, как электронную запись на носителе[4]. Вместе с тем, бездокументарная ценная бумага имеет все данные, характерные для документарной (бумажной) ценной бумаги.

Дискуссионным является вопрос о возможности отнесения к предмету мошенничества в сфере компьютерной информации премиальных денежных суррогатов, возникающих в связи с реализацией разнообразных программ потребительской лояльности (бонусы, баллы, подарочные мили и т.п.). По мнению Г.А. Есакова, реализация премиальных денежных сур-

---

[1] Дворецкий М.Ю. Уголовная ответственность за мошенничество в сфере компьютерной информации: проблемы теории и правоприменительной практики // Вестник ТГУ. – 2013. – № 8 (124). – С. 407.

[2] См., например: Приговор Лефортовского районного суда г. Москвы от 29 апреля 2014 г. по делу № 1-72/2014. Согласно материалам дела предметом мошенничества в сфере компьютерной информации выступила продукция (оргтехника), принадлежащая ООО «Самсунг Электроникс Рус Компани».

[3] Пудовочкин Ю.Е. Учение о составе преступления : учебное пособие. М., 2009. С. 61.

[4] Приговор Железнодорожного районного суда г. Красноярска от 2 декабря 2015 г. по уголовному делу № 1-12/2014.

рогатов лицом, незаконно завладевшим ими, очевидно, причиняет ущерб их законному владельцу, лишая его полагающейся ему премии[1].

Обозначенная проблема интересна не только в теоретическом плане, но и обусловлена прикладными потребностями. В судебно-следственной практике можно встретить решения, связанные с оценкой подобных противоправных действий с премиальными денежными суррогатами. Так, М., являясь оператором телефонного центра ООО «Директ Стар», которое выполняет для ОАО «Аэрофлот» функции контакт-центра по обслуживанию пассажиров, используя доступ к информационной системе «Аэрофлот Бонус», создал более 10 фиктивных счетов на имя вымышленных лиц, посредством чего неправомерно накапливал бонусные мили за счет полетов пассажиров, не являющихся участниками программы. В дальнейшем М. через сеть «Интернет» предложил тридцати одному клиенту за значительно меньшую оплату возможность приобретения бонусных авиабилетов ОАО «Аэрофлот». В результате действий М. по незаконному накоплению бонусных миль и приобретению за их счет премиальных авиабилетов ОАО «Аэрофлот» был причинен имущественный ущерб на сумму 1 345 675 рублей 35 копеек. Решением суда М. признан виновным по п. «б» ч. 2 ст. 165 УК РФ[2].

На наш взгляд, суд совершенно обоснованно квалифицировал действия виновного как причинение имущественного ущерба путем обмана. У компании-перевозчика не изымали имущество путем совершения обманных действий, а используя правила бонусной программы потребительской лояльности не доплатили за оказанные услуги, то есть реальный ущерб выразился в неполучении должного дохода. Непростым является вопрос о возможности признания предметом компьютерного мошенничества виртуальных объектов, приобретаемых пользователями информационных ресурсов за реальные деньги[3]. По справедливому мнению В.М. Елина, вопрос о возможности рассмотрения информационной вещи в качестве предмета мошенничества в настоящее время не может решаться однозначно и нуждается в дальнейшей проработке[4].

---

[1] Есаков Г.А. Денежные суррогаты и ответственность за хищение // СПС «Консультант Плюс».

[2] Уголовное дело №1-35 // Архив Ленинского районного суда г. Владимира за 2013 г.

[3] См., например: Савельев А.И. Правовая природа виртуальных объектов, приобретаемых за реальные деньги в многопользовательских играх // Вестник гражданского права. – 2014. – №1 ; СПС «КонсультантПлюс».

[4] Елин В.М. Мошенничество в сфере компьютерной информации как новый состав преступления // Бизнес-информатика. – 2013. – №2 (24). – С. 74.

Как справедливо отмечает А.Г. Безверхов, в современном экономическом мире все большее число отношений складывается с лишенными вещественного содержания благами. С учетом этих реалий предметом «преступлений против собственности» может быть любое экономическое благо, имеющее как материальный, так и нематериальный характер. Главное, чтобы это благо имело действительную или потенциальную экономическую ценность, признавалось возможным объектом экономического оборота, принимало товарную форму и получало стоимостное выражение[1].

В ст. 159^6 УК РФ способами совершения мошенничества в сфере компьютерной информации названы: 1) ввод компьютерной информации; 2) удаление компьютерной информации; 3) блокирование компьютерной информации; 4) модификация компьютерной информации; 5) вмешательство в функционирование средств хранения компьютерной информации; 6) вмешательство в функционирование средств обработки компьютерной информации; 7) вмешательство в функционирование средств передачи компьютерной информации; 8) вмешательство в функционирование информационно-телекоммуникационной сети.

В самом обобщенном виде под вводом понимается добавление новой информации в компьютерную систему. М.И. Третьяк дает более конкретизированное понятие, определяя ввод компьютерной информации как определенный алгоритм действий по набору данных об адресате (номера его лицевого счета, мобильного телефона, данных мобильного кошелька и др.), сведений о сумме денежных средств (данные о ценной бумаге) и непосредственному переводу их по указанному адресату (операции «перевести», «отправить», «исполнить»)[2].

Изучение судебно-следственной практики по делам о мошенничестве в сфере компьютерной информации показывает, что подавляющее большинство таких преступлений связано именно со вводом компьютерной информации. Так, Д. был осужден по ч. 3 ст. 159^6 УК РФ, то есть за мошенничество в сфере компьютерной информации, совершенное в крупном размере. Д., имея умысел на хищение чужого имущества, получил неправомерный доступ к моноблочному персональному компьютеру и путем

---

[1] Безверхов А.Г. Уголовно-правовая охрана собственности в условиях рыночной экономики // Уголовное право в эпоху финансово-экономических перемен : материалы IX Российского Конгресса уголовного права, состоявшегося 29–30 мая 2014 г. / отв. ред. д-р юрид. наук, проф. В.С. Комиссаров. М. : Юрлитинформ, 2014. С. 117.

[2] Третьяк М.И. Проблемы понимания способа компьютерного мошенничества в судебной практике // Уголовное право. – 2015. – № 5. – С. 109.

ввода компьютерной информации в программу «Парус 1С Продавец», осуществил три перевода денежных средств, принадлежащих юридическому лицу, на счет принадлежащей ему банковской карты, получив реальную возможность распорядиться похищенными денежными средствами[1].

В современной теории уголовного права удаление компьютерной информации раскрывается как привидение информации или ее части в непригодное для использования состояние, при котором исключается ее получение с соответствующего раздела памяти компьютера, иного устройства, съемного носителя или интернет-сайта, независимо от возможности восстановления данной информации[2]. В современной правоприменительной практике совершение компьютерного мошенничества только лишь путем удаления информации не встречается. Наиболее часто такие действия сопряжены с вводом информации.

Блокирование представляет собой действия, направленные на прекращение доступа к информации для лиц, которые имеют право на такой доступ. Закрытие доступа к информационным ресурсам (блокирование), как правило, осуществляется путем изменения учетных данных пользователя – логина и (или) пароля. Совершение мошеннических действий, связанных с блокированием компьютерной информации, может выражаться в оказании «услуг» по ремонту неисправного оборудования (компьютера или компьютерной системы), когда сами лица предварительно совершают действия, направленные на выведение таких объектов из строя. Следует, конечно же, отметить, что само по себе блокирование здесь будет выступать промежуточным этапом, позволяющим виновным позднее ввести в заблуждение потерпевшего и обманным путем получить имущество в качестве вознаграждения за «работу» по восстановлению доступа к заблокированной информации.

Модификация представляет собой внесение изменений в содержащуюся в системе информацию. В.В. Хилюта определяет модификацию компьютерной информации как внесение в неё любых изменений, которые обусловят ее отличие от ранее хранившейся в компьютерной сети, системе или на машинном носителе собственника информационного ресурса, в результате чего потерпевшему будет причинен имущественный

---

[1] Приговор Симоновского районного суда г. Москвы от 14 февраля 2013 г. по делу №1-79/2013.

[2] Ответы кафедры уголовного права и криминалистики факультета права Национального исследовательского университета «Высшая школа экономики» на вопросы, представленные для обсуждения в ходе конференции 23 апреля 2015 г. // Уголовное право. – 2015. – № 5. – С. 43.

ущерб, а виновное лицо извлечет из этого выгоду[1]. Как представляется, принципиальное отличие модификации от ввода заключается в том, что в последнем случае лицо не изменяет какой-то информационный объект (блок), а создает новый.

По мнению М.И. Третьяк, существенным признаком совершения мошенничества путем модификации компьютерной информации является то, что у виновного лица имеется законный доступ к компьютерной информации[2]. На наш взгляд, такое толкование термина «модификация» применительно к компьютерной информации является спорным. Согласно букве закона, обладало ли лицо правом на доступ к информации или нет – никак не влияет на содержание самого деяния. Модификацию от ввода необходимо отграничивать по содержанию самих манипуляций с компьютерной информацией. Примером компьютерного мошенничества, совершаемого анализируемым способом, является изменение виновным банковских реквизитов, указанных, например, на сайте по оплате штрафов.

К способам совершения преступления, ответственность за которое предусмотрена ст. 159[6] УК РФ, законодатель также отнес иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Подобное вмешательство описывается в литературе как осуществление неправомерных действий, нарушающих установленный процесс обработки, хранения, использования, передачи и иного реального обращения с компьютерной информацией[3].

Так, Л. и Б. признаны виновными в мошенничестве в сфере компьютерной информации, то есть хищении чужого имущества путем иного вмешательства в функционирование средств хранения, обработки и передачи компьютерной информации, совершенное организованной группой. Из описательно-мотивировочной части приговора следует, что Л., Б. и неустановленные следствием лица, из корыстных побуждений, получив через Б., оформленную на имя Л. платежную банковскую карту ОАО «Б» со счетом и со всеми документами, во исполнение своей преступной роли,

---

[1] Хилюта В.В. Вопросы квалификации преступлений против собственности не являющихся хищением : монография. Минск, 2013. С. 33.

[2] См.: Третьяк М.И. Проблемы понимания способа компьютерного мошенничества в судебной практике // Уголовное право. – 2015. – № 5. – С. 109; Третьяк М. И. Модификация компьютерной информации и ее соотношение с другими способами компьютерного мошенничества // Уголовное право. – 2016. – № 6. – С. 101.

[3] Дворецкий М.Ю. Уголовная ответственность за мошенничество в сфере компьютерной информации: проблемы теории и правоприменительной практики // Вестник ТГУ. – 2013. – № 8 (124). – С. 407.

используя компьютерную технику и программы, технические познания в сфере работы с компьютерной информацией, удаленно, неправомерно, через сеть «Интернет», осуществили вмешательство в функционирование компьютера ООО «Б», вследствие чего, получили удаленный несанкционированный доступ к управлению расчетным счетом ООО «Б», открытым в ДО «Ж» «М» (ОАО); при помощи неустановленного программного обеспечения, произвели копирование электронных документов, содержащих информацию в электронной цифровой форме об ООО «Б», а также копирование пароля, логина и электронного аналога собственноручной подписи, после чего похитили с расчетного счета ООО «Б» денежные средства на общую сумму 438 000 рублей[1].

Пленум Верховного Суда Российской Федерации скорректировал традиционный подход к определению момента окончания хищения, если его предметом выступали безналичные денежные средства, в том числе электронные денежные средства. Согласно новой позиции такое хищение следует считать оконченным не с момента зачисления денежных средств на счет виновного или третьих лиц, а с момента их изъятия у владельца (пункт 5). Данное решение Пленума было продиктовано двумя обстоятельствами: 1) редакционная коллегия отметила, что высокий уровень развития товарно-денежных отношений, информационных технологий и банковских услуг позволяет за считанные минуты осуществлять перевод и зачисление денежных средств, оплату товаров и др. В связи с этим с момента списания денежных средств со счета потерпевшего у виновного появляется реальная возможность по их беспрепятственному распоряжению и 2) в отдельных случаях у правоохранительных органов не всегда имеется возможность достоверно установить, куда были перечислены похищенные денежные средства потерпевшего, что само по себе не должно влиять на квалификацию мошенничества как оконченного преступления[2].

Указанное разъяснение высшей судебной инстанции в целом следует оценить положительно. Как известно, случаи неверного толкования момента окончания компьютерного мошенничества на практике встречались. Например, как покушение на компьютерное мошенничество были квалифицированы действия лиц, которые были задержаны в отделении банка уже при попытке получения похищенных денежных средств с расчетного счета фирмы-однодневки, куда были перечислены похищенные

---

[1] Приговор Хамовнического районного суда г. Москвы от 1 августа 2013 г. в отношении Б. и Л.

[2] Заседание Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. // [Электронный ресурс] // URL: http://www.vsrf.ru/press_center/news/26093/ (дата обращения: 06.12.2017).

денежные средства юридического лица в результате заражения вредоносным программным обеспечением служебного компьютера организации с установленной системой «Банк-Клиент»[1]. Вместе с тем, ошибочно полагать, что данное разъяснение не может иметь исключений. На наш взгляд, несмотря на положения пункта 5 нового постановления Пленума, как покушение на мошенничество в сфере компьютерной информации следует оценивать ситуации, когда в рамках оперативно-розыскных мероприятий по запросу правоохранительных органов финансовая организация заранее приостановила любые расходные операции по счету, на который впоследствии были зачислены похищенные злоумышленниками денежные средства.

В целом по конструкции объективной стороны состав мошенничества в сфере компьютерной информации является материальным и считается оконченным с момента причинения имущественного ущерба потерпевшему.

По мнению отдельных авторов, программы, локальные и глобальные компьютерные сети являются средствами совершения преступления, а компьютер и иные устройства (принтер, сканер, модем, мобильный телефон), применявшиеся с целью посягательства на объект уголовно-правовой охраны, должны рассматриваться как орудия преступления[2].

Поддерживая в целом такое разграничение, необходимо отметить, что орудиями совершения мошенничества в сфере компьютерной информации может также выступать компьютерное оборудование (компьютерные сети) других граждан и организаций, заражённое вредоносными программами. То обстоятельство, что виновный никогда фактически не владел такими объектами, а лишь дистанционно установил противоправный контроль над ними, как представляется, не препятствует выводу о возможности признания их орудиями совершения компьютерного мошенничества.

Пленум Верховного Суда Российской Федерации также сделал вывод, что мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа или создания, использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по ст.ст. 272, 273, 274[1] УК РФ. Соглашаясь с этим разъяснением по существу, необходимо отметить следующее. Рас-

---

[1] Приговор Пресненского районного суда г. Москвы от 23 января 2014 г. по делу № 1-43/2014.

[2] Иванченко Р.Б., Малышев А.Н. Проблемы квалификации мошенничества в сфере компьютерной информации // Вестник Воронежского института МВД России. – 2014. – № 1. – С. 196.

крывая в п. 20 содержание вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации, Пленум указывает, что оно «нарушает установленный процесс обработки, хранения, передачи компьютерной информации». Так или иначе, в данной части речь идет о причинении вреда отношениям по обеспечению безопасности компьютерных данных и систем, то есть налицо двуобъектность мошенничества в сфере компьютерной информации, которая по правилам квалификации преступлений должна была бы исключать совокупность. Вместе с тем, она ее не исключает ввиду того, что нормы гл. 28 УК РФ содержат более строгие санкции. Как справедливо отмечает П.С. Яни, даже если рассматривать преступление, предусмотренное ст. 272 УК РФ, в качестве способа совершения мошенничества в сфере компьютерной информации, содеянное должно квалифицироваться по совокупности ст. 159^6 УК РФ и названной нормы[1].

Пожалуй, наиболее востребованным на правоприменительном уровне будет разъяснение Пленума Верховного Суда Российской Федерации, сформулированное в п. 21, согласно которому в тех случаях, когда хищение совершается путем использования учетных данных собственника или иного владельца имущества независимо от способа получения доступа к таким данным (тайно либо путем обмана воспользовался телефоном потерпевшего, подключенным к услуге «мобильный банк», авторизовался в системе интернет-платежей под известными ему данными другого лица и т.п.), такие действия подлежат квалификации как кража, если виновным не было оказано незаконного воздействия на программное обеспечение серверов, компьютеров или на сами информационно-телекоммуникационные сети. Таким образом, новые формы посягательства преимущественно на электронные денежные средства граждан Пленум Верховного Суда Российской Федерации предложил квалифицировать по-старинке – как тайное хищение чужого имущества.

Подобный подход вызывает ряд вопросов и требует некоторых замечаний. Прежде всего, объективно не всякое хищение, совершенное с использованием учетных данных, можно будет квалифицировать как кражу. Так, если соответствующая команда на списание денежных средств была отправлена открыто, в присутствии третьих лиц, не являющихся близкими виновному и осознававшими противоправный характер совершаемых действий, содеянное необходимо будет квалифицировать как грабеж. Более того, если возможность воспользоваться телефоном потерпевшего воз-

[1] Яни П.С. Специальные виды мошенничества // Законность. – 2015. – № 8. – С. 40.

никла в результате нападения, сопряженного с применением насилия опасного для жизни или здоровья потерпевшего либо с угрозой его применения, и манипуляции с «мобильным банком» были осуществлены непосредственно в процессе нападения, содеянное будет охватываться составом разбоя. Полагаем, что как кражу можно будет квалифицировать действия лица, которое отправило команду на перевод денежных средств позднее, после нападения и завладения телефоном потерпевшего.

В некотором смысле анализируемое разъяснение Пленума Верховного Суда Российской Федерации нивелирует смысл и значение самостоятельного определения ст. 159^6 УК РФ. Оно распространяет действие ст. 158 УК РФ на такие часто встречающиеся в сети «Интернет» посягательства на электронные денежные средства граждан, как совершенные в результате завладения учетными данными потерпевшего путем обмана («социальная инженерия»), создания сайтов-двойников («фишинг»), незаконной замены сим-карт и использования вредоносного программного обеспечения.

С учетом последних разъяснений Пленума Верховного Суда Российской Федерации как мошенничество в сфере компьютерной информации следует оценивать хищения денежных средств граждан и организаций в результате использования вредоносных компьютерных программ. Так, например, Б. был осужден за совершение преступлений, предусмотренных ч. 2 ст. 273 УК РФ, ч. 2 ст. 272 УК РФ, ч. 2 ст. 159^6 УК РФ. В соответствии с приговором суда, Б., обладая достаточными познаниями в области компьютерной техники и навыками работы в сети «Интернет», приобрел путем копирования на накопитель своего персонального компьютера, программы, заведомо приводящие к несанкционированному доступу, уничтожению, блокированию, модификации, либо копированию информации. Функционально указанные программы были предназначены для управления удаленным компьютером по сети. После этого, Б. отправил на адрес электронной почты, используемого индивидуальным предпринимателем в своей финансовой деятельности, письмо свободного содержания, в которое под видом документа вложил указанные вредоносные программы. Продавец-консультант индивидуального предпринимателя, не подозревая о вредоносном содержании письма, используя служебный компьютер, открыл данное письмо, тем самым автоматически установив на компьютер вредоносную программу. Далее Б., незаконно используя вредоносные программы, без согласия и без ведома легального обладателя информации (индивидуального предпринимателя), из корыстной заинтересованности осуществил неправомерный доступ к компьютеру последнего, что вызвало блокирование компьютерной информации и сделало невозможным ис-

пользование информации законным владельцем. После этого, продолжая свои преступные действия, направленные на мошенничество в сфере компьютерной информации, используя вредоносные свойства программ, посредством которых получил возможность ознакомиться с информацией о банковским счете и находящимися на нем денежными средствами, принадлежащими индивидуальному предпринимателю, Б. осуществил перевод денежных средств потерпевшего на счет своего абонентского номера телефона, причинив значительный материальный ущерб[1].

Теоретически обоснованным и практически значимым следует признать разъяснение Пленума Верховного Суда Российской Федерации об оценке мошеннических действий в сети «Интернет» с использованием так называемой «социальной инженерии». В соответствии со вторым абзацем п. 21 постановления, если хищение чужого имущества или приобретение права на чужое имущество осуществляется путем распространения заведомо ложных сведений в информационно-телекоммуникационных сетях, включая сеть «Интернет» (например, создание поддельных сайтов благотворительных организаций, интернет-магазинов, использование электронной почты), то такое мошенничество следует квалифицировать по статье 159, а не 159^6 УК РФ. Таким образом, принципиальным отличием общеуголовного мошенничества от компьютерного выступает наличие обмана или злоупотребления доверием потерпевшего, в результате чего он лично или через третьих лиц передает денежные средства или иное имущество злоумышленнику. Следует отметить, что введение в заблуждение потерпевшего может быть следствием работы вредоносного программного обеспечения, что само по себе не исключает необходимость квалификации содеянного по ст. 159 УК РФ. Так, спорным представляется решение суда по следующему делу. Братья С. были осуждены по ч. 2 ст. 159^6 УК РФ и ч. 2 ст. 273 УК РФ. Согласно материалам дела, виновные создали в сети «Интернет» сайты, в стартовый файл которых были заранее интегрированы вредоносные программы, заведомо предназначенные для блокирования функций операционной системы персональных компьютеров. Одновременно с блокированием пользователям приходили сообщения якобы от правоохранительных органов (МВД России, Управления «К» МВД России и др.), содержащие сведения о необходимости перечисления денежных средств по соответствующим реквизитам в качестве оплаты наложенного на пользователя сети «Интернет» административного штрафа за просмотр и копирование материалов порнографического содержания. Полученные

[1] Приговор Советского районного суда г. Улан-Удэ Республика Бурятия от 22 сентября 2015 г. по делу № 1-715/2015.

от потерпевших денежные средства С. в дальнейшем тратили на собственные нужды[1]. Учитывая, что денежные средства списывались вредоносной программой не автоматически, а перечислялись потерпевшими самостоятельно в качестве оплаты несуществующих административных штрафов за просмотр порнографических материалов, содеянное, на наш взгляд, подпадает под действие общей нормы о мошенничестве.

Крайне дискуссионным и в определенном смысле противоречащим теоретико-правовым основам дифференциации уголовной ответственности явилось решение законодателя о включении в ч. 3 ст. 159[6] УК РФ особо квалифицирующего признака, связанного с совершением компьютерного мошенничества в отношении электронных денежных средств и средств, которые находятся на банковском счете потерпевшего. С учетом специфического способа мошенничество в сфере компьютерной информации изначально не предполагало возможности его осуществления в отношении обычных (бумажных) денежных средств. Это наглядно подтверждается и материалами довольно многочисленной судебно-следственной практики, где анализируемое преступление так или иначе всегда посягает на безналичные или электронные деньги. Таким образом, изменив редакцию ст. 159[6] УК РФ, законодатель фактически аннулировал действие ее первой и второй частей[2].

Нельзя не отметить, что принятие Федерального закона от 23 апреля 2018 г. № 111-ФЗ некоторым образом нивелировало значимость официальных рекомендаций Пленума Верховного Суда Российской Федерации о квалификации специальных видов мошенничества, в которых, по справедливому мнению А.Г. Кибальника, заключалась его главная правоприменительная ценность[3]. После апрельских изменений отечественного уголовного закона правоприменитель опять оказался в ситуации частичной неопределенности и, прежде всего, в вопросе разделения посягательств на электронные денежные средства граждан и денежные средства, хранимые на банковских счетах.

Полагаем, что для решения вопроса об отграничении «электронной кражи» от вышеуказанных составов преступлений следует исходить из того, какую роль играл тот или иной способ в механизме совершения посягательства.

---

[1] Приговор Первомайского районного суда Оренбургской области от 8 июля 2016 г. по делу № 1-58/2016.

[2] Данный вывод нашел поддержку у 72 % опрошенных респондентов.

[3] Кибальник А.Г. Квалификация мошенничества в новом постановлении Пленума Верховного Суда Российской Федерации // Уголовное право. – 2018. – № 1. – С. 61.

Следует согласиться с А.А. Лебедевой, что в случаях, когда лицо похитило денежные средства, воспользовавшись необходимой для получения доступа к ним конфиденциальной информацией держателя платежной карты (например, персональными данными владельца, данными платежной карты, контрольной информацией, паролями), переданной злоумышленнику самим держателем платежной карты под воздействием обмана или злоупотребления доверием, действия виновного следует квалифицировать как кража[1].

Анализ судебной практики показывает, что по п. «г» ч. 3 ст. 158 УК РФ оцениваются действия лица, которое завладело платежной картой потерпевшего и осуществило изъятие денежных средств в наличной форме через устройство самообслуживания клиентов. Так, М. был осужден по п. «г» ч. 3 ст. 158 УК РФ. В соответствии с приговором суда М., используя предварительно изъятую у потерпевшей банковскую карту, а также информацию о пин-коде, которую потерпевшая сообщила М. ранее, через банкомат осуществил четыре операции по обналичиванию денежных средств с банковского счета в размере 33 864 рубля, чем причинил потрепевшей значительный материальный ущерб[2].

Компьютеризация состава кражи заставляет несколько переосмыслить обоснованный в теории уголовного права подход, согласно которому «статья 159^6 УК РФ должна применяться в случаях, когда использование способов: ввода, удаления, блокирования компьютерной информации и т.д. – приводит к переводу денежных средств с одного счета на другой, контролируемый виновным счет»[3]. В современной редакции ст. 158 УК РФ такое толкование является обоснованным только в том случае, если манипуляции с компьютерной информацией (ввод, модификация и т.д.) привели не просто к перемещению денежных средств, но и повлекли нарушение нормальной работы объектов информационно-коммуникационной инфраструктуры (например, блокировке личного кабинета потерпевшего в системе дистанционного банковского обслуживания). При отсутствии таких последствий, содеянное необходимо квалифицировать по п. «г» ч. 3 ст. 158 УК РФ. Подобный подход находит свое отражение и в правоприменительной практике. Так, в решении суда по уголовному делу в отношении Д., квалифицировавшем содеянное по п. «г» ч.

---

[1] Лебедева А.А. Актуальные вопросы квалификации мошенничества в сфере компьютерной информации // Безопасность бизнеса. – 2018. – № 5. – С. 47.

[2] Приговор Ленинского районного суда г. Смоленска от 20 сентября 2018 г. по делу № 1-275/2018.

[3] Тюнин В. Мошенничество в сфере компьютерной информации: сложности квалификации // Уголовное право. – 2017. – № 5. – С. 95.

3 ст. 158 УК РФ, виновный, получив во временное пользование телефон потерпевшего, в котором было установлено приложение дистанционного банковского обслуживания и убедившись, что потерпевший отвлечен и за его преступными действиями не наблюдает, осуществил перевод денежных средств в сумме 17 000 рублей, принадлежащих потерпевшему[1].

Изучение имеющейся судебно-следственной практики показывает, что действия, связанные с оплатой товаров и услуг, довольно часто квалифицируются как кража с банковского счета. Так, по п. «г» ч. 3 ст. 158 УК РФ были квалифицированы действия лица, которое, воспользовавшись отсутствием потерпевшего, изъяло принадлежащую ему банковскую карту. После чего в продолжение своего преступного умысла, находясь в магазине, трижды осуществило оплату приобретенного товара банковской картой на суммы: 591 рубль 06 копеек, 354 рубля, 970 рублей 82 копейки. Примерно в это же время, находясь уже в другом магазине, дважды осуществило оплату приобретенного товара банковской картой потерпевшего на суммы: 151 рубль 80 копеек, 105 рублей[2].

Изменив диспозицию ст. 159^3 УК РФ, законодатель по каким-то причинам исключил оговорку о том, что соответствующие действия должны быть сопряжены с обманом уполномоченного работника кредитной или иной организации. Если согласиться с тем, что такой способ уже не является обязательным, то данный состав преступления станет абсолютно неотличимым от кражи с банковского счета, а равно в отношении электронных денежных средств (п. «г» ч. 3 ст. 158 УК РФ). В связи с этим полагаем, что толкование данного преступления по-прежнему должно основываться на разъяснениях, сформулированных в п. 17 постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», согласно которым признаки ст. 159^3 УК РФ имеют место только в случаях, когда хищение имущества осуществлялось путем сообщения уполномоченному работнику кредитной, торговой или иной организации заведомо ложных сведений о принадлежности лицу карты (с учетом изменений – электронного средства платежа) на законных основаниях либо путем умолчания о незаконном владении им такой картой (с учетом изменений – электронным средством платежа).

Так, осуществляя переквалификацию с п. «г» ч. 3 ст. 158 УК РФ на ст. 159^3 УК РФ, суд, ссылаясь на указанное выше разъяснение Пленума,

---

[1] Приговор Центрального районного суда г. Воронежа от 25 октября 2018 г. по делу № 1-312/2018.

[2] Приговор Домодедовского городского суда Московской области от 6 ноября 2018 г. по делу № 1-399/2018.

обосновывает вывод, что поскольку А., реализуя свой преступный умысел, совершил хищение денежных средств потерпевшего путем умолчания перед продавцом о незаконном владении им платежной картой, оплатив ряд покупок безналичным путем, используя систему «ПайПасс», содеянное является мошенничеством с использованием электронных средств платежа, а не кражей с банковского счета[1].

По другому делу суд согласился с позицией обвинения о наличии в действиях виновного совокупности преступлений, предусмотренных п. «г» ч. 3 ст. 158 УК РФ и ч. 2 ст. 159^3 УК РФ, ссылаясь на то, что лицо совершило как изъятие денежных средств потерпевшего посредством банкомата, так и, «выдавая себя за собственника банковской карты, обманывая работника торговой организации» произвело оплату купленных товаров[2].

По мнению З.И. Хисамовой, имеющаяся в законе оговорка «при отсутствии признаков преступления, предусмотренного статьей 159^3» выражается в том, что неправомерный доступ к счету или электронному кошельку был получен и осуществлен без применения специальных информационно-телекоммуникационных технологий (скиммеров, банковских троянов и др.)[3]. При этом в обоснование собственного подхода автор отдельно оговаривает, что основное отличие кражи от мошенничества с использованием электронных средств платежа заключается именно в способе хищения. Для квалификации деяния как мошенничества с использованием электронного средства платежа необходимо целенаправленное воздействие на программное обеспечение, приложение, устройство, позволяющее получить неправомерный доступ к счету владельца[4].

Как представляется, данная точка зрения является дискуссионной. Подобное видение объективной стороны мошенничества с использованием электронных средств платежа делает его неотличимым от мошенничества в сфере компьютерной информации. Как уже отмечалось ранее, в отличие от кражи с банковского счета и мошенничества с использованием электронных средств платежа компьютерное мошенничество, предусмотренное ст. 159^6 УК РФ, предполагает неправомерное вмешательство в

---

[1] Приговор Ново-Савинского районного суда г. Казани от 16 ноября 2018 г. по делу № 1-525/2018.

[2] Приговор Муромского городского суда Владимирской области от 30 ноября 2018 г. по делу № 1-297/2018.

[3] Хисамова З.И. Об уголовной ответственности за хищения, совершенные с использованием IT-технологий: анализ изменений законодательства и правоприменительной практики // Российский следователь. – 2018. – № 9. – С. 46.

[4] Там же.

процесс нормального функционирования объектов информационно-коммуникационной инфраструктуры (п. 20 постановления Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате»).

Типичным примером мошенничества в сфере компьютерной информации может выступать следующее решение суда по уголовному делу. Так, Ж., выполняя свою роль в преступной группе, установил на терминал по приему платежей от населения программу удаленного администрирования, а также вредоносную компьютерную программу. После чего Ж., убедившись в том, что при помощи установленной им программы можно осуществить удаленный доступ к терминалу, покинул торговое помещение. В этот же день, находясь по месту своего проживания, Ж. в сервисе мгновенного обмена сообщениями отправил неустановленный идентификационный номер А., который, выполняя свою роль в преступной группе, произвел подключение к программе удаленного администрирования, установил в память терминала: программное обеспечение, позволяющее подтвердить принятие денежной купюры в устройстве, предназначенном для проверки купюр (валидаторе), при ее действительном отсутствии, а также другие программы, обеспечивающие настройку и корректную работу программного обеспечения, позволяющего подтвердить принятие денежной купюры в устройстве, предназначенном для проверки купюр (валидаторе), при ее действительном отсутствии, то есть осуществил модификацию компьютерной информации. После чего А., имея возможность удаленно управлять программными продуктами, установленными им в терминал по приему платежей от населения, незаконно, путем ввода и модификации компьютерной информации, осуществил 8 переводов денежных средств на общую сумму 35 300 рублей со специального счета терминала по приему платежей от населения на счет в одной из электронных платежных систем[1].

Как мошенничество в сфере компьютерной информации, на наш взгляд, также следует оценивать действия злоумышленника, который изымает в наличной форме денежные средства из устройства самообслуживания клиентов банка (банкомата, терминала оплаты и др.) посредством неправомерного вмешательства в его функционирование с использованием вредоносных компьютерных программ (так называемые атаки типа «blackbox», при которых лицо просверливает отверстие в банкомате, подключается через USB-порт и использует вредоносное программное обес-

[1] Приговор Советского районного суда г. Орска Оренбургской области от 17 августа 2018 г. по делу № 1-240/2018.

печение, чтобы дать команду на выдачу денежных средств). Здесь изъятие денежных средств имеет не примитивно-бытовой характер, а реализуется способом, который напрямую описан в диспозиции ст. 159[6] УК РФ – путем ввода и модификации компьютерной информации в программном обеспечении банкомата. При этом следует, конечно же, оговориться, что простое изъятие купюроприемника с сейфом в результате повреждения банкомата должно оцениваться как кража (однако без применения п. «г» ч. 3), либо в зависимости от обстоятельств содеянного как грабеж либо разбой.

Следует отметить, что введение в заблуждение потерпевшего может быть следствием работы вредоносного программного обеспечения, что само по себе не обосновывает необходимость квалификации содеянного по ст. 159[6] УК РФ. В этой связи спорным представляется решение суда по следующему делу. Так, Братья С. были осуждены по ч. 2 ст. 159[6] и ч. 2 ст. 273 УК РФ. Согласно материалам дела, виновные создали в сети «Интернет» сайты, в стартовые файлы которых были заранее интегрированы вредоносные программы. Эти программы заведомо предназначались для блокирования функций операционной системы персональных компьютеров. Одновременно с блокированием пользователям приходили сообщения якобы от правоохранительных органов (МВД России, Управления «К» МВД России и др.) с требованием перечислить денежные средства по соответствующим реквизитам в качестве оплаты наложенного на интернет-пользователя административного штрафа за просмотр и копирование материалов порнографического содержания. Полученные от потерпевших денежные средства братья С. в дальнейшем тратили на собственные нужды[1].

Принимая во внимание, что денежные средства списывались вредоносной программой не автоматически, а перечислялись потерпевшими самостоятельно в качестве оплаты несуществующих административных штрафов за просмотр порнографических материалов, содеянное, на наш взгляд, подпадает под действие общей нормы о мошенничестве.

Сложности в оценке деяний имеют место в случаях отграничения кражи с банковского счета от общеуголовного мошенничества, в результате которого потерпевший самостоятельно перечисляет денежные средства, используя сервисы дистанционного банковского обслуживания. Так, Н. была осуждена по ч. 2 ст. 159 УК РФ. В соответствии с приговором суда, Н., имея умысел на хищение чужого имущества, принадлежащего Ш.,

[1] Приговор Первомайского районного суда Оренбургской области от 8 июля 2016 г. по делу № 1-58/2016.

под надуманным предлогом продажи товара, заведомо осознавая, что товар не предоставит, а полученные в качестве оплаты денежные средства обратит в свою пользу, путем обмана получила со счета, зарегистрированной на Ш. банковской карты, принадлежащие не ей и предназначавшиеся в качестве оплаты за товар денежные средства Ш. в размере 15 500 рублей, после чего распорядилась её деньгами по своему усмотрению, причинив Ш. значительный материальный ущерб[1].

Принципиальным отличием общеуголовного мошенничества с использованием методов так называемой «социальной инженерии» от кражи с банковского счета потерпевшего выступает наличие обмана или злоупотребления доверием потерпевшего, в результате чего он лично или через третьих лиц передает денежные средства или иное имущество злоумышленнику. Следовательно, в распространенных случаях введения клиентов банков в заблуждение по телефону, когда виновный представляется работником службы безопасности финансовой организации либо социальным работником, необходимо установить в результате каких действий денежные средства были списаны со счета. Если виновный стремился к тому, чтобы клиент совершил соответствующие манипуляции с платежной картой и тем самым самостоятельно перевел денежные средства на счет злоумышленника, содеянное образует признаки общеуголовного мошенничества. В тех же случаях, когда лицо обманным путем лишь получает сведения о платежной карте либо другую критически значимую информацию, касающуюся работы сервисов дистанционного банковского обслуживания (например, одноразовый код-пароль для входа в систему), и, как это бывает на практике, не прерывая разговора с потерпевшим, параллельно совершает операции по изъятию денежных средств с банковского счета, содеянное необходимо квалифицировать по п. «г» ч. 3 ст. 158 УК РФ.

Решение законодателя, реализованное в Федеральном законе от 23 апреля 2018 г. № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации», еще раз подтверждает наш тезис о «дизрупции уголовного права» – неспособности выполнять свои базовые функции ввиду перманентного и динамичного внешнесредового воздействия, связанного с состоянием эпизодического и бессистемного изменения, угрожающего разрушением субстанциональных признаков отрасли. Решением данной проблемы является комплексное доктринальное осмысление явле-

[1] Приговор Солнцевского районного суда г. Москвы от 6 ноября 2018 г. по делу № 1-318/18.

ния, а также ориентированное на науку законотворчество и правоприменение.

Более перспективным направлением, на наш взгляд, является установление повышенной ответственности за совершение мошенничества в сфере компьютерной информации *«с неправомерным сокрытием либо изменением идентификаторов оконечного оборудования пользователя информационно-коммуникационной сети (в том числе сети «Интернет»)».*

Как справедливо отмечает В.Х. Каримов, системы шифрования и сокрытия данных пользователей Интернета активно используются преступным миром, вследствие чего у заинтересованных структур, в том числе правоохранительных, возникают сложности в расшифровке сведений и установлении лиц, их использующих[1].

Таким образом, с учетом высказанных замечаний и обоснованных выводов уголовно-правовую норму об ответственности за мошенничество в сфере компьютерной информации следует изложить в следующей редакции:

«Статья 159⁶. Хищение в сфере компьютерной информации

1. Хищение чужого имущества или приобретение права на чужое имущество путем вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-коммуникационных сетей, –

наказывается штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо арестом на срок до четырех месяцев.

2. То же деяние, совершенное группой лиц по предварительному сговору, а равно с причинением значительного ущерба гражданину, –

наказывается штрафом в размере до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до двух лет, либо обязательными работами на срок до четырехсот восьмидесяти часов, либо исправительными работами на срок до двух лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до одного года или без такового, либо лишением свободы на срок

[1] Каримов В.Х. Актуальные вопросы борьбы с преступлениями, совершаемыми с использованием систем анонимизации пользователей в сети «Интернет» // Российский следователь. – 2018. – № 6. – С. 52.

до пяти лет с ограничением свободы на срок до одного года или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные:

а) лицом с использованием своего служебного положения;

б) в крупном размере;

в) с неправомерным сокрытием либо изменением идентификаторов оконечного оборудования пользователя информационно-коммуникационной сети (в том числе сети «Интернет»), –

наказываются штрафом в размере от ста тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до двух лет или без такового, либо лишением свободы на срок до шести лет со штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев либо без такового и с ограничением свободы на срок до полутора лет либо без такового.

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, совершенные организованной группой либо в особо крупном размере, – наказываются лишением свободы на срок до десяти лет со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до трех лет либо без такового и с ограничением свободы на срок до двух лет либо без такового».

2.4. ПРОБЛЕМЫ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ, В ОТНОШЕНИИ И ПО ПОВОДУ ЦИФРОВЫХ ФИНАНСОВЫХ АКТИВОВ (КРИПТОВАЛЮТ)

Квалификация преступлений, совершаемых с использованием криптовалют, в целом основывается на общих руководящих началах (принципах) и правилах уголовно-правовой оценки деяния. Несмотря на наличие

известного правового вакуума[1], следует согласиться с мнением А.Н. Ляскало, что «расширение сферы обращения и повышенный криминальный интерес к использованию криптовалюты все чаще вынуждают правоприменителя признавать ее предметом или средством преступления»[2].

Изучение доктринальных источников и материалов отечественной судебно-следственной практики позволяет выделить следующие основные группы преступлений, сопряженных с использованием в той или иной форме цифровых финансовых активов (криптовалют):

1) преступления, в которых криптовалюта выступает средством их совершения;

2) преступления, в которых криптовалюта выступает предметом посягательства;

3) преступления, совершаемые в целях генерации (майнинга) криптовалюты.

По меткому замечанию М.И. Немовой, «попытка осмысления возможности применения УК РФ к преступным посягательствам, совершаемым посредством или в отношении криптовалют, – это попытка помещения динамично развивающихся экономических отношений в прокрустово ложе консервативного по своей сути уголовного закона»[3]. Согласимся с автором. Во многом это действительно так. Однако зададимся вопросом – что же остается доктрине в условиях задумавшегося (надолго ли?) над проблемой законодателя? Ответ представляется очевидным – на основе скрупулезного обобщения и анализа отдельных казусов, используя допустимую интерпретационную ёмкость уголовного закона, готовить рекомендации для правоприменительной практики, которая вынуждена уже сейчас в реальном времени реагировать на новые вызовы и угрозы, связанные с блокчейн-революцией.

---

[1] В нашей стране оборот криптовалюты до настоящего времени не урегулирован. Статус криптовалюты оговаривается в предостережении Центробанка России от 27 января 2014 г. «Об использовании при совершении сделок «виртуальных валют», в письмах ФНС от 3 октября 2016 г. № ОА-18-17/1027 и 13 октября 2017 г. № 03-04-05/66994, информационном письме Федеральной службы по финансовому мониторингу от 6 января 2014 г. «Об использовании криптовалют», где она определяется как денежный суррогат.

[2] Ляскало А.Н. Криптовалюта как предмет и средство преступления // Уголовное право: стратегия развития в XXI веке : материалы XVI Международной научно-практической конференции. М., 2019. С. 89.

[3] Немова М.И. Уголовный закон и криптовалюта: вызовы и перспективы // Уголовное право: стратегия развития в XXI веке : материалы XV Международной научно-практической конференции. М., 2018. С. 585.

Первую группу преступлений, с каждым днем получающих все большее распространение, составляют деяния, связанные с оборотом предметов, ограниченных или запрещенных в гражданском обороте, в которых криптовалюта выступает платежным инструментом. К таковым, прежде всего, относятся преступления, связанные с незаконным оборотом наркотических средств и психотропных веществ, оружия, а также порнографических материалов. Так, по одному из дел суд указал, что подсудимый примерно в январе 2019 года посредством сети «Интернет» заплатил 25 000 рублей, переведя указанные денежные средства в не отслеживаемую криптовалюту «Биткоин», перечислил указанные платежные средства на интернет-сайт «Рутор», осуществив заказ оружия. Затем, действуя умышленно и незаконно, приобрел путем подбора «тайника-закладки» в неустановленном месте возле станции метро «Нагатинская» в городе Москве пистолет, который был переделан самодельным способом из сигнального пистолета «МР-371». Также, имея на то преступный умысел, в неустановленное время, но не позднее 07 марта 2019 года, в неустановленном месте в городе Москве приобрел боеприпасы: 66 патронов калибра 9 мм. Не имея лицензии на приобретение оружия, его основных частей и боеприпасов, действуя в нарушение Федерального закона Российской Федерации № 150 ФЗ «Об оружии» от 13 декабря 1996 г., и зная, что установлена уголовная ответственность за незаконный оборот оружия, его основных частей и боеприпасов, он обратил пистолет и патроны в свое противоправное владение, поместив их в своей квартире[1].

С использованием виртуальной валюты приобретаются также поддельные официальные и другие важные личные документы. Так, К. был осужден по ч. 3 ст. 327 УК РФ. Согласно приговору суда, К. приобрел поддельное водительское удостоверение на право управления транспортными средствами категории «В» через сеть «Интернет». Сумма заказа составила 40 000 рублей. С исполнителем все общение проходило посредством текстовых сообщений. К. оплатил всю сумму путем списания денежных средств с электронного кошелька. Предварительно данную сумму он перевел в электронную валюту «Биткоин». Также через сеть «Интернет» он переслал свою фотографию. Через две недели курьерской службой ему домой привезли конверт, в котором находилось водительское удостоверение на имя Б. с его фотографией[2].

---

[1] Приговор Перовского районного суда г. Москвы от 17 июня 2019 г. по делу № 01-0603/2019.

[2] Приговор Сормовского районного суда города Нижнего Новгорода от 7 сентября 2018 г. по делу № 1-212/2018.

Следует сделать вывод, что в судебно-следственной практике, как правило, не возникает сложностей в квалификации таких преступлений. Само по себе использование криптовалюты для приобретения соответствующих предметов не оказывает значимого влияния на оценку содеянного по ст.ст. 222, 228, 228[1] УК РФ и др., а относится в большей мере к криминологической и криминалистической характеристике содеянного.

Равным образом специалисты сходятся во мнении, что использование цифровых финансовых активов не создает каких-либо значимых проблем при юридической оценке финансирования преступной деятельности по ст.ст. 205[1], 208, 282[3], 359 УК РФ[1].

Использование криптовалюты является распространенным средством совершения легализации денежных средств, приобретенных преступным путем. Квалификация транзакций с цифровыми финансовыми активами по ст.ст. 174 и 174[1] УК РФ основывается на правовой позиции, сформулированной в п. 1 постановления Пленума Верховного Суда Российской Федерации от 7 июля 2015 г. № 32 «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем». Пленум Верховного суда Российской Федерации разъяснил, что, исходя из положений статьи 1 Конвенции Совета Европы об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности и о финансировании терроризма от 16 мая 2005 г., и с учетом Рекомендации 15 ФАТФ предметом преступлений, предусмотренных статьями 174 и 174[1] УК РФ, могут выступать, в том числе, и денежные средства, преобразованные из виртуальных активов (криптовалюты), приобретенных в результате совершения преступления.

Так, Ш. был осужден за совершение преступлений, предусмотренных п. «а» ч. 3 ст. 228[1], ч. 3 ст. 30, п. «г» ч. 4 ст. 228[1], п. «а» ч. 3 ст. 174[1], ч. 2 ст. 228 УК РФ. Согласно приговору суда, Ш. и неустановленные лица разработали план легализации денежных средств, полученных в результате совершаемых преступлений, – незаконного сбыта наркотических средств неопределенному кругу лиц. Согласно данного плана, Ш., получая

---

[1] См., например: Кунев Д.А. Современные угрозы использования криптовалют в преступных целях // Финансовая безопасность. – 2018. – № 20. – С. 60–63; Сидоренко Э.Л. Криминальное использование криптовалюты: международные оценки // Международное уголовное правосудие и международная юстиция. – 2016. – № 6. – С. 8–10; Сидоренко Э.Л. Криминологические риски оборота криптовалюты и проблемы ее правовой идентификации // Библиотека криминалиста. Научный журнал. – 2016. – № 3. – С. 148–154 и др.

денежные средства от неопределенного круга лиц в качестве оплаты за приобретаемые наркотические средства на различные номера виртуальных счетов/кошельков системы электронных платежей «Киви», должен был на обменном сервисе «ЛокалБиткойнс» в целях придания правомерного вида владению, пользованию и распоряжению указанными денежными средствами, систематически, ежедневно, совершать сделки купли-продажи виртуальной валюты «Биткойн». После совершения сделки купли-продажи виртуальной валюты Ш. должен был, используя известную ему учетную запись на обменном сервисе «ЛокалБиткойнс», переводить приобретенную виртуальную валюту на «Биткойн-кошелек» неустановленным лицам. В свою очередь, неустановленные лица должны были переводить полученную от Ш. виртуальную валюту «Биткойн» на «Биткойн-кошелек», связанный с иной известной неустановленным лицам и Ш. учетной записью на обменном сервисе «ЛокалБиткойнс», доступ к ресурсам которой имелся у Ш. Получив от неустановленных лиц на указанный «Биткойн-кошелек» виртуальную валюту, Ш. должен был вновь совершать сделки по ее продаже на указанном выше обменном сервисе с неопределенным кругом лиц, получая от тех в качестве оплаты за продаваемую виртуальную валюту российские рубли. Впоследствии, снимая денежные средства с различных номеров виртуальных счетов/кошельков системы электронных платежей «Киви», и придавая при этом указанным денежным средствам правомерный вид владению, пользованию и распоряжению указанными денежными средствами, Ш. распоряжался ими по своему усмотрению[1].

Как нетрудно заметить, совершение транзакций (как правило, не имеющих экономического смысла) с криптовалютой направлено к одной единственной цели – скрыть реальных выгодоприобретателей того или иного вида преступной деятельности, разорвать прямой финансовый след между ними. Здесь следует лишь упомянуть о таком известном свойстве отдельных криптовалют (Monero, BlackCoin и др.), как их полная анонимность при осуществлении расчетов, когда установить информацию об отправителе/получателе цифровых финансовых активов попросту невозможно.

Следует, однако, указать, что такие транзакции с криптовалютой сами по себе не «отмывают» их происхождение. В конечном итоге виновный добивается лишь того, чтобы установить связь между капиталом, цифровыми финансовыми активами и конкретной преступной деятельностью правоохранительным органам было крайне сложно. Финансовый

[1] Приговор Волжского городского суда от 06 марта 2018 г. по делу № 1-277/2018.

след попросту теряется в цепочке сделок с цифровыми финансовыми активами, совершаемыми множеством участников на разных торговых площадках. Такое расширительное понимание легализации (признание таковой любых сделок с денежными средствами либо имуществом, добытыми преступным путем, в целях сокрытия их истинного происхождения) в целом основано на рекомендациях ФАТФ и, пожалуй, является, целесообразным в современных условиях[1].

Обращаясь к обсуждаемой проблеме, М.И. Немова делает оговорку о том, что сама по себе конвертация криптовалюты в национальную или иностранную валюту не означает обязательного наличия цели придания правомерного вида владению, пользованию и распоряжению преступным доходом, если конвертация была совершена в связи с необходимостью расходования полученного имущества для личных нужд. Автор делает акцент на том, что о наличии цели придания правомерного вида преступным доходам свидетельствуют дополнительные транзакции по переводу конвертированных денежных средств на электронные кошельки, дробление сумм, переводы на счета третьих лиц и т.п.[2]

Полагаем, что с указанным мнением М.И. Немовой необходимо согласиться, использование лицом криптовалюты не должно априорно свидетельствовать о том, что имела место легализация. При простом распоряжении виртуальной валютой, например, в целях оплаты товаров или услуг без намерения придания правомерного вида преступным доходам говорить о наличии признаков состава преступления, предусмотренного ст. 174[1] УК РФ, нельзя.

Как представляется, в первой группе преступлений следует также выделить посягательства на денежные средства граждан, которые хотя и совершаются без непосредственного использования виртуальной валюты, однако под предлогом совершения каких-либо операций с нею (обмена, инвестирования и т.д.). В целом указанные деяния образуют признаки общеуголовного мошенничества (ст. 159 УК РФ). Здесь следует отметить, что при подобных обстоятельствах злоумышленники используют низкую осведомленность граждан, делают упор на сверхдоходность криптовалютного рынка, его свободу от государственного регулирования и налогооб-

---

[1] Подробнее см.: Ализаде В.А., Волеводз А.Г. Неприменение ст. 174.1 УК РФ по делам о наркопреступлениях, совершенных с использованием криптовалюты, как следствие непонимания сущности легализации (отмывания) нового вида преступных активов // Наркоконтроль. – 2018. – № 1 (50). – С. 5–13.

[2] Немова М.И. Использование криптовалюты при легализации (отмывании) денежных средств или иного имущества: приобретенных преступным путем: анализ судебной практики // Уголовное право. – 2019. – № 4. – С. 63–68.

ложения. Так, О., руководствуясь корыстными побуждениями, провела встречу с жителями города Бийска, партнерами компании «OneCoin». На данной встрече О. с целью введения присутствующих граждан в заблуждение, создавая видимость правомерности своих действий, сообщила заведомо ложные сведения о том, что она желает открыть общий «пул» (личный кабинет) на сайте «www.onelife.eu» компании «OneCoin» на сумму 3 100 000 рублей, для последующего приобретения криптовалюты по выгодной цене. В ходе данной встречи О. сообщила присутствующим о том, что для реализации данного бизнес-плана необходимо передать ей по 31 000 рублей (по одной сотой стоимости всего пула) для приобретения криптовалюты «OneCoin». При этом О. пояснила, что принесенные с собой на встречу денежные средства необходимо передать ей лично. После чего введенные в заблуждение потерпевшие, не догадываясь о преступных намерениях О., не предполагая обмана с ее стороны, поверив в достоверность слов последней, согласились на данное предложение О. Своими продолжаемыми преступными действиями О. путем обмана и злоупотребления доверием похитила 124 000 рублей[1].

Как мошенничество по ст. 159 УК РФ следует также квалифицировать случаи хищения денежных средств граждан под предлогом привлечения финансирования через ICO (Initial Coin Offering – форма привлечения инвестиций граждан в виде выпуска и продажи инвесторам новых криптовалют / токенов), когда субъекты реально не намеревались осуществлять подобного рода деятельность. Здесь можно привести известный пример из международного опыта. В октябре 2017 года в газете Ведомости была опубликована статья о возбуждении в США уголовного преследования в отношении Максима Заславского, который предлагал инвесторам несуществующие токены и криптовалюту, обещая при этом солидные дивиденды от вложений[2].

В теории уголовного права нет однозначного ответа на вопрос, следует ли квалифицировать как незаконное предпринимательство по ст. 171 УК РФ деятельность субъектов, которые занимаются обменными операциями с криптовалютой и извлекли при этом доход в крупном размере. Одним из главных аргументов против такой юридической оценки является

---

[1] Постановление Бийского городского суда Алтайского края от 24 января 2018 г. по делу № 1-88/2018 в отношении О., обвиняемой в совершении преступления, предусмотренного ч. 2 ст. 159 УК РФ (дело прекращено по основаниям, предусмотренным ст. 76 УК РФ).

[2] В США возбудили первое в истории дело о мошенничестве при ICO // [Электронный адрес]: https://www.vedomosti.ru/technology/articles/2017/10/03/736241-ssha-delo-ico (дата обращения: 04.06.2020).

неопределенный статус криптовалюты, который не позволяет говорить о том, что подобного рода деятельность могла быть зарегистрирована в принципе.

В свою очередь Ю.В. Трунцевский и А.Н. Сухаренко отстаивают позицию, согласно которой деятельность по обмену фиатных денег на криптовалюты на территории России соответствует всем признакам незаконного предпринимательства[1]. Подобный подход нашел свое отражение и в материалах правоприменительной практики. Так, Д.Е.А., Д.Е.Н. и Е. признаны виновными в совершении преступления, предусмотренного п. «а» ч. 2 ст. 171 УК РФ. Согласно приговору суда, в составе организованной группы как самостоятельно, так и с привлечением неосведомлённых о преступном характере их деятельности иных лиц, без регистрации и без лицензии осуществляли сопряженную с извлечением дохода в крупном размере (свыше 2,6 млн рублей) предпринимательскую деятельность по предоставлению посредством сети «Интернет» неопределенному кругу заинтересованных лиц возмездных (в размере не менее 0,5% от суммы поступивших денежных средств) услуг по переводу с использованием платежного сервиса «Visa QIWI Wallet» электронных денежных средств и купле-продаже так называемых «титульных знаков» электронных платежных систем расчетов и бирж: «Perfect Money», «WebMoney», «Payeer», «BTC-E».

В апелляционной жалобе адвокат поставил вопрос об отмене приговора в связи с тем, что инкриминированная Д.Е.А. деятельность в принципе не могла быть зарегистрирована в качестве предпринимательской. Гражданское законодательство не содержит понятия криптовалюты. Имеющая существенное значение для квалификации содеянного сумма полученного Д.Е.А. дохода от деятельности обменных сервисов в ходе производства по делу не установлена. Результаты проведенных банковских экспертиз относительно суммы полученного дохода носят вероятностный (предположительный) характер, основанный на произвольном предположении следствия о взимании осужденными вознаграждения (теневой комиссии) в размере 0,5% от поступившей суммы.

Суд, не согласившись с доводами защиты, в своем решении указал, что деятельность по оказанию через сайты «Freshobmen.ru» и «Cashservise.com» услуг по переводу денежных средств и купле-продаже так называемых «титульных знаков» являлась предпринимательской дея-

[1] Трунцевский Ю.В., Сухаренко А.Н. Противодействие использованию криптовалюты в незаконных целях: состояние и перспективы // Международное публичное и частное право. – 2019. – № 1. – С. 45.

тельностью, осуществляемой без регистрации. Доводы стороны защиты о том, что инкриминированная осужденным деятельность в принципе не могла быть зарегистрирована в качестве предпринимательской, были оценены судом как не состоятельные, поскольку деятельность «обменного сервиса» фактически сводилась к оказанию услуг по посредничеству в денежно-кредитной сфере, входящих в Общероссийский классификатор продукции по видам экономической деятельности[1].

Нельзя не отметить, что первоначально участникам данной преступной группы были предъявлены обвинения по ч. 2 ст. 172 УК РФ, однако в ходе производства по делу их действия переквалифицировали на ст. 171 УК РФ по той причине, что криптовалюта не считается официально признанным в России денежным средством, поэтому операции с ней не могут быть квалифицированы как банковские.

По мнению М.М. Долгиевой, в приведенном примере квалификация по ст. 171 УК РФ является вынужденной в свете отсутствия норм, которые бы предусматривали ответственность за такие действия. Автор также ссылается на то, что услуги по обмену криптовалюты на рубли не являются законными на территории Российской Федерации, соответственно и регистрация в таком качестве или получение лицензии на оказание таких услуг невозможны по действующему законодательству[2].

Полагаем, что ответственность за незаконное предпринимательство в ситуации осуществления деятельности, связанной с обменом криптовалюты на фиатные денежные средства и наоборот, направленной на систематическое получения прибыли за счет взимания комиссии по каждой операции, все-таки возможна. Учитывая, что получение лицензии на оказание таких услуг является невозможным по действующему законодательству, лицо будет нести ответственность за незаконное предпринимательство при условии, если оно осуществляло указанную деятельность без регистрации.

В отечественной науке уголовного права также обсуждается проблема использования криптовалюты для совершения преступлений, связанных с процедурой банкротства (ст.ст. 195, 196, 197 УК РФ). Действительно, в силу известных свойств виртуальные валюты выступают весьма удобным средством для оперативного и надежного вывода активов хозяйствующего субъекта с целью последующего уклонения от исполнения

---

[1] Апелляционное определение Костромского областного суда от 18 октября 2018 г. по делу № 22-827/2018.

[2] Долгиева М.М. Противодействие легализации преступных доходов при использовании криптовалюты // Вестник Томского государственного университета. – 2019. – № 449. – С. 216.

обязательств перед контрагентами. В связи с этим Е.Г. Быкова и А.А. Казаков делают справедливый вывод, что, если вложение денежных средств гражданина в криптовалюту привело к возникновению признаков банкротства, не усматривается препятствий для юридической оценки содеянного по ст. 196 УК РФ при наличии к тому оснований[1].

Полагаем, что при квалификации подобных действий традиционно основной проблемой будет выступать установление того обстоятельства, что лицо, совершая соответствующие транзакции, осознавало их заведомо убыточный характер и тем самым стремилось к банкротству. Вряд ли следует оспаривать, что в отдельных случаях поведение лица может быть обусловлено добросовестным стремлением к получению прибыли на волатильности курсов цифровых финансовых активов. В любом случае указанные обстоятельства должны оцениваться в обязательном порядке, в том числе с учетом мнения представителей экспертного сообщества. При этом, на наш взгляд, непозволительным будет выступать формирование на уровне правоприменения некой презумпции, согласно которой сам факт инвестирования в еще не получившие официальный статус криптовалюты является признаком совершения заведомо убыточных, ведущих к банкротству действий.

Проблемой совершенно другого порядка является квалификация действий руководителя организации, совершившего реализацию цифровых финансовых активов (в размере эквивалентном 2 250 000 рублей) при наличии признаков банкротства. Применение ст. 195 УК РФ в подобной ситуации наталкивается на невозможность установление юридически значимой связи между криптовалютой и конкретным хозяйствующим субъектом. Как справедливо отмечают по этому поводу Е.Г. Быкова и А.А. Казаков, юридическое лицо не может владеть, пользоваться и распоряжаться криптовалютой ввиду отсутствия у последней законодательно закрепленного правового статуса[2].

В отечественной теории уголовного права нет однозначной точки зрения относительно вопроса о том, может ли криптовалюта выступать предметом хищения. М.А. Простосердов отстаивает позицию, что криптовалюта, как цифровой информационный продукт, то есть совокупность уникальных компьютерных данных, объединенных в виртуальный носитель, обладающих всеми признаками товара, собственной стоимостью и принадлежащих на праве собственности другому лицу, может выступать

---

[1] Быкова Е.Г., Казаков А.А. Проблемы квалификации криминальных банкротств с использованием криптовалюты // Уголовное право. – 2018. – № 6. – С. 14.

[2] Быкова Е.Г., Казаков А.А. Проблемы квалификации криминальных банкротств с использованием криптовалюты // Уголовное право. – 2018. – № 6. – С. 14.

предметом хищения в преступлениях, предусмотренных ст.ст. 159, 159[6] и 160 УК РФ[1].

М.М. Долгиева также отмечает, что в силу своих специфических свойств, ценности и возможности являться предметом гражданского оборота криптовалюта должна быть отнесена к видам иного имущества в рамках ст. 128 Гражданского кодекса Российской Федерации[2]. Эта позиция получает все большую поддержку в отечественной науке уголовного права. Ю.В. Грачева, С.В. Маликов и А.И. Чучаев напрямую указывают, что статьи 128 и 141[1] ГК РФ позволяют криптовалюту относить к имуществу и тем самым снимают проблему квалификации деяний, в которых она выступает предметом преступления[3]. В данной связи нельзя не упомянуть, что в отечественной судебной практике уже создан прецедент, в рамках которого криптовалюта фактически признана иным имуществом. В своем решении Девятый арбитражный апелляционный суд выразил позицию, что «согласно ст. 128 ГК РФ к объектам гражданских прав относятся вещи, включая наличные деньги и документарные ценные бумаги, иное имущество, в том числе безналичные денежные средства, бездокументарные ценные бумаги, имущественные права; результаты работ и оказание услуг; охраняемые результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации (интеллектуальная собственность); нематериальные блага. В силу диспозитивности норм гражданского права в ГК РФ отсутствует закрытый перечень объектов гражданских прав. Поскольку ... действующее гражданское законодательство не содержит понятия “иное имущество” упомянутое в статье 128 ГК РФ, с учетом современных экономических реалий и уровня развития информационных технологий допустимо максимально широкое его толкование»[4].

В свою очередь, Э.Л. Сидоренко отмечает, что из-за отсутствия легальной дефиниции криптовалюты в российском законодательстве ее нельзя признать объектом гражданских прав и, следовательно, любые формы ее присвоения априори не могут быть признаны хищением, по-

---

[1] Простосердов М.А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им : автореф. дис. … канд. юрид. наук. М., 2016. С. 18.

[2] Долгиева М.М. Конфискация криптовалюты // Законность. – 2018. – № 11. – С. 45.

[3] Грачева Ю.В., Маликов С.В., Чучаев А.И. Предупреждение девиаций в цифровом мире уголовно-правовыми средствами // Право. Журнал Высшей школы экономики. – 2020. – № 1. – С. 207.

[4] Постановление Девятого арбитражного апелляционного суда г. Москвы от 15 мая 2018 г. № 09АП-16416/2018 по делу № А40-124668/2017.

скольку криптовалюта не обладает свойственными для предмета хищения определенными экономическими и материальными параметрами[1].

Изучение материалов современной судебно-следственной практики позволяет сделать вывод, что функционирование современных криптовалютных площадок, к сожалению, сопряжено с деятельностью лиц, которые, используя свои знания в области информационных технологий, осуществляют действия, направленные на изъятие цифровых финансовых активов пользователей.

Одной из распространенных преступных схем является завладение криптовалютой пользователей под предлогом ее обмена на российские рубли или иную валюту. Так, суд согласился с квалификацией действий виновного по ч. 2 ст. 159 УК РФ, который из корыстных побуждений с целью хищения чужого имущества, путем обмана и злоупотребления доверием, под никнеймом «polya2218» на сайте «www.LocalBitcoins.com» вступил в переписку с потерпевшим, в ходе которой договорился о покупке у данного пользователя криптовалюты в размере 0.03875392 «BTC-e», заранее не намереваясь выполнять свои обязательства по ее оплате. В ходе переписки потерпевший оценил данную сделку на сумму 20 000 рублей. Продолжая реализовывать свой преступный умысел, направленный на хищение чужого имущества путем обмана и злоупотребления доверием, не намереваясь выполнять взятые на себя обязательства по оплате криптовалюты, злоумышленник отправил потерпевшему смс-сообщение, полностью повторяющее по своему содержанию смс-сообщение от сервиса мобильный банк. Будучи введенным в заблуждение, полагая, что смс-сообщение получено от сервиса мобильный банк, потерпевший подумал, что виновный свои обязательства по оплате криптовалюты исполнил и перевел на биткоин-кошелек под никнеймом «polya2218» на сайте «www.LocalBitcoins.com» криптовалюту на сумму 0,03875392 «BTC-e», стоимостью 20 000 рублей[2].

Следует отметить, что такие действия довольно часто сопряжены с неправомерным доступом к охраняемой законом компьютерной информации, а именно к личным кабинетам других пользователей. Так, например, Ш. и О. были осуждены по ч. 3 ст. 159 и ч. 3 ст. 272 УК РФ. Согласно приговору суда, указанные лица в неустановленное следствием время вступили в предварительный сговор с целью хищения чужого имущества, а именно «BTC-e» кодов, посредством сети «Интернет», путем незаконного

---

[1] Сидоренко Э.Л. Криминологические риски оборота криптовалюты // Экономика. Налоги. Право. – 2017. – № 6. – С. 147.

[2] Приговор Октябрьского районного суда г. Тамбова от 15 февраля 2019 г. по делу № 1-134/19.

получения доступа к учетным записям пользователей и под предлогом обмена «BTC-e» кодов. Продолжая совместные преступные действия, Ш. и О. осуществили неправомерный доступ к учетным записям пользователей «wmalliance» и «Djin37», после чего изменили их учетную информацию, добавив свой уникальный идентификационный номер для общения в реальном времени, а также от имени пользователей «wmalliance» и «Djin37» создали тему «Вывод «BTC-e» / Биткоинов. +7%», и положительные комментарии к ней от имени других неустановленных пользователей сайта. После чего Ш. и О., имея умысел на хищение у ранее незнакомого лица, использующего программу «ICQ» для работы в протоколе OSCAR и имя «Gambit», ввели его в заблуждение, пообещав ему обменять «BTC-e» код на российские рубли, чего заведомо не намеревались делать. Потерпевший, будучи введенным в заблуждение относительно преступных намерений Ш. и О., используя свою учетную запись «ser198», с целью обмена, принадлежащего ему «BTC-e» кода на 10 000 долларов США на российские рубли, в личном сообщении передал пользователю «wmalliance», доступ к которому имели Ш. и О., «BTC-e» код на 10 000 долларов США, рыночная стоимость которого, по состоянию на дату отправки сообщения, согласно заключению эксперта, составляла 821 100 рублей 00 копеек. Далее Ш. и О. зачислили полученный BTC-e код, принадлежащий потерпевшему, на счет своей учетной записи, тем самым похитили его и в дальнейшем распорядились им по своему усмотрению[1].

Тайное хищение цифровых финансовых активов граждан, как правило, сопряжено с неправомерным доступом к личному кабинету клиента торговой площадки. При этом, пытаясь получить неправомерный доступ к аккаунту клиента, злоумышленники предварительно взламывают электронную почту потерпевшего. Нельзя не отметить, что в правоприменительной практике такие действия довольно часто получают неполную квалификацию. Следственные органы, возбуждая уголовные дела по ст. 158 УК РФ, оставляют без внимания, что на стадии приготовления к совершению хищения злоумышленник совершил самостоятельное преступление, предусмотренное ч. 2 ст. 272 УК РФ. Так, например, судебно-следственные органы квалифицировали действия неустановленного лица, похитившего криптовалюту, принадлежащую потерпевшему Ш., на сумму не менее 400 000 рублей, по п. «в, г» ч. 3 ст. 158 УК РФ. Согласно материалам дела, неустановленное лицо посредством несанкционированного доступа к электронному почтовому ящику потерпевшего, зарегистрирован-

[1] Приговор Сургутского городского суда Ханты-Мансийского автономного округа от 13 ноября 2017 г. по делу № 1-762/2017.

ного на коммуникационном портале «mail.ru», и его личному кабинету на сайте «bittrex.com», осуществило транзакцию (вывод) криптовалюты[1]. С учетом приведенных фактических обстоятельств содеянного, полагаем, что окончательная квалификация действий виновного должна быть осуществлена по совокупности ч. 1 ст. 138, п. «в, г» ч. 3 ст. 158, ч. 2 ст. 272 УК РФ.

Посягательства на цифровые финансовые активы граждан могут носить и открытый характер. В зависимости от конкретных фактических обстоятельств содеянного (прежде всего, характера применяемого насилия к потерпевшему) противоправное изъятие криптовалюты может быть квалифицировано как грабеж или разбой. Так, П., С., С-ва и М., узнав, что у Е. в специальном цифровом кошельке, созданном на онлайн-площадке «Blockchain.info», имеются в наличии криптовалюта «Биткойн», которые последний желает реализовать, вступили в предварительный преступный сговор на совершение открытого хищения криптовалюты «Биткойн» у Е., при этом заранее разработали план совершения преступления и распределили между собой преступные роли. Согласно разработанному преступному плану и распределенным ролям: С-ва должна была под вымышленным именем при помощи мессенджера выйти на связь с Е. и, выступая в роли покупателя криптовалюты, назначить ему встречу; М. и П. должны были прибыть на встречу и, представившись сотрудниками полиции, вывезти Е. на заранее приисканной для этого автомашине, в свободное от посторонних глаз место с целью совершения в отношении Е. открытого хищения имущества, а также завладеть мобильным телефоном Е., с установленной в нем программой «Blockchain» с целью хищения криптовалюты «Биткойн». С. должен был приискать средства и орудия для совершения преступления, а именно наручники и приобрести бланк удостоверения внешне похожий на удостоверения сотрудников органов внутренних дел для их использования в ходе совершения преступления в отношении Е. с целью оказания психологического давления и физического насилия в отношении него, а также, имея необходимые познания в сфере транзакций криптовалюты в системе «Blockchain», после завладения мобильным телефоном Е., должен был перевести криптовалюту со специального электронного кошелька, используемого Е., на специальный электронный кошелек, подконтрольной указанным участникам преступной группы. Преступление было осуществлено согласно разработанному плану. Потерпевший Е., будучи психически и физически подавлен, после высказанных

[1] Сведения приведены по информационной справке СУ МВД России по Республике Коми.

в отношении него угроз применения насилия, не опасного для жизни и здоровья, а также примененного в отношении него насилия, не опасного для жизни и здоровья, согласился осуществить перевод принадлежащей ему криптовалюты «Биткойн», после чего разблокировал свой мобильный телефон, находившийся в руках М., и осуществил вход в личный кабинет в системе «Blockchain». Далее, С., действуя в группе лиц по предварительному сговору, согласно отведенной себе преступной роли, имея доступ к специальному электронному кошельку, используемому Е. на онлайн-площадке «Blockchain.info», осуществил перевод с указанного электронного кошелька криптовалюты «Биткойн», принадлежащих Е., на заранее созданный специальный электронный кошелек на онлайн-площадке «Blockchain.info», подконтрольный участникам преступной группы, в количестве 2,8 единицы, получив реальную возможность распорядиться ими по своему усмотрению. Согласно бирже криптовалют «EXMO» курс 1 «Bitcoin» по состоянию на 28 февраля 2018 года составил 11 002 доллара 38 центов США, всего на сумму 30 806 долларов 664 цента США, стоимостью по курсу Центрального банка России на 28 февраля 2018 года 55, 6717 рублей за 1 доллар США, а всего на общую сумму 1 715 059 рублей 36 копеек, что является особо крупным размером.

Действия П., С., С-ва и М. были квалифицированы по п. «б» ч. 3 ст. 161 УК РФ – грабеж, то есть открытое хищение чужого имущества, совершенный группой лиц по предварительному сговору, с применением насилия, не опасного для жизни и здоровья, и с угрозой применения такого насилия, в особо крупном размере[1].

Требования о передаче цифровых финансовых активов, соединенные с угрозой применения насилия к потерпевшему, уничтожения или повреждения его имущества, а равно под угрозой распространения сведений, позорящих потерпевшего или его близких, образуют признаки вымогательства. Так, СУ УМВД России по Южно-Сахалинску было возбуждено уголовное дело по признакам преступления, предусмотренного п. «б» ч. 3 ст. 163 УК РФ. Согласно материалам дела неустановленное лицо выдвинуло требование о передаче ему 100 «BTC-е» кодов, что по курсу на момент совершения преступного деяния составляло 45 373 769 рублей 22 копеек под угрозой уничтожения имущества, принадлежащего юридическому лицу[2].

---

[1] Сведения приведены по данным, предоставленным ИЦ МВД по Республике Татарстан.

[2] Сведения приведены по информационной справке СУ УМВД России по Сахалинской области.

Правоприменительные органы в качестве системной проблемы, возникающей при расследовании подобной категории дел, отмечают отсутствие на территории Российской Федерации органа, уполномоченного дать оценку стоимости криптовалюты на конкретную дату. В настоящее время при расследовании уголовных дел установление размера причиненного ущерба потерпевшему основывается либо на заключении специалиста, либо посредством получения информации о курсе криптовалюты на время совершения преступления непосредственно через данные торговой площадки (криптобиржи).

Последнюю группу составляют преступные посягательства, которые совершаются в целях генерации (майнинга) криптовалюты. Анализ современной правоприменительной практики показывает, что к таковым относятся все посягательства, ответственность за которые предусмотрена гл. 28 УК РФ «Преступления в сфере компьютерной информации». Прежде всего здесь следует выделить неправомерный доступ к охраняемой законом компьютерной информации (ст. 272 УК РФ). Так, Б. признан виновным в неправомерном доступе к охраняемой законом компьютерной информации, содержащейся в административной части сайта «regionorel.ru» ГУП ОО «Орловский издательский дом», повлекшем ее модификацию путем внедрения кода скрипта с индивидуальным ключом для получения криптовалюты «Monero» в личное пользование, а также уничтожение компьютерной информации, содержащей сведения обо всех посещениях сайта пользователями и изменениях компьютерной информации сайта (журналы истории посещений и истории команд) объемом 45 Гб, совершенных из корыстной заинтересованности.

Согласно решению суда, Б. состоял в трудовых отношения с ГУП ОО «Орловский издательский дом», в должности ведущего специалиста разработал сайт, который к 2012 году обрел свой вид и был размещен на домене «epressa.su» на сервере, распложенном в редакции газета «Орловская правда». В 2014 году редакцией было принято решение о переименовании сайта и смены доменного имени, и вместо «epressa.su» был приобретен домен «regionorel.ru». В июне 2015 года Б. уволился, после чего никакого отношения к сайту «regionorel.ru» не имел.

Прекратив трудовые отношения с ГУП ОО «Орловский издательский дом» с 17.06.2015, перестав иметь законные основания на доступ к серверу и к административной части сайта «regionorel.ru», Б. со своего рабочего компьютера осуществил неправомерный доступ к информации, содержащейся на административной части сайта «regionorel.ru», владельцем которого является ГУП ОО «Орловский издательский дом», путем создания новой учетной записи с правами администратора на любые изменения, ре-

гистрации нового пользователя сайта и введения кода скрипта с индивидуальным ключом для получения криптовалюты «Monero» в личное пользование.

Сторона защиты, не согласившись с решением суда первой инстанции в апелляции указывала на то, что файлы, в которые вносились изменения, являлись общедоступными, автором сайта «regionorel.ru» является Б., а ГУП ОО «Орловский издательский дом» принадлежит только адрес. Сторона защиты не согласилась также с вменением квалифицирующего признака «корыстная заинтересованность», поскольку доказательств возможности получения денежных средств из криптовалюты, их ценность и возможность конвертации, обвинением не было представлено.

Несмотря на то что контент сайта не был приведен в непригодное состояние, суд апелляционной инстанции также признал, что это само по себе не влияет на квалификацию действий осужденного, поскольку приведенными выше доказательствами достоверно установлено, что скрипт, внедренный Б. в тело файлов «header.php» и «footer.php», модифицировал сайт «regionorel.ru» в целях получения криптовалюты «Monero» в его личное пользование путем использования вычислительных ресурсов неограниченного круга посетителей пользовательской части сайта «regionorel.ru».

Наличие в действиях Б. квалифицирующего признака «корыстной заинтересованности» суд подлежал установленным, сославшись на то, что в личном кабинете Б. на сайте «Coinhive» имеется информация о том, что сайт, используемый для майнинга – «regionorel.ru», сумма «монет», заработанная за весь период, составила 0,03225 XMR. Доводы защиты о необходимости представления доказательств получения денежных средств из криптовалюты, суд посчитал также необоснованными, поскольку «сведения о криптовалютах, как о платежных средствах в сети «Интернет», являются общеизвестными и общедоступными, содержащимися в сети «Интернет», где также приводятся и их списки и курс»[1].

Использование вредоносных компьютерных программ (ст. 273 УК РФ), как правило, осуществляется лицами для обеспечения неправомерного доступа к вычислительным ресурсам потерпевших и последующего майнинга криптовалюты.

Так, согласно приговору суда, у Ш. возник преступный умысел, направленный на использование из корыстных побуждений аппаратной мощности серверов различных организаций, расположенных на террито-

[1] Апелляционное постановление Орловского областного суда от 23 августа 2019 г. по делу № 22-1120/2019.

рии Российской Федерации, для генерации криптовалюты (майнинга) путем установки на него своего программного обеспечения и получения таким способом денежных средств. В период с 28 ноября 2017 г. по 9 января 2018 г. Ш., получив с помощью компьютерной программы IP-адрес сервера с открытым портом, принадлежащего местной муниципальной организации, Ш. с целью реализации своего преступного умысла, находясь по месту своего жительства, умышленно, из корыстной заинтересованности, ввел IP-адрес организации во вредоносную компьютерную программу, и с помощью своего персонального компьютера, подключенного к сети «Интернет», запустил ее, тем самым предпринял попытку получения удаленного доступа к интернет-ресурсам организации, размещенным на сервере, осуществляя повторяющиеся однотипные TCP-сессии с последующей передачей аутентификационной информации. Через некоторое время вредоносная компьютерная программа подобрала логин и пароль к серверу организации. После чего Ш. с помощью незаконно полученных логина и пароля осуществил доступ к серверу и установил на нем свое программное обеспечение (не являющееся вредоносным) для генерации криптовалюты (процесса майнинга)[1].

В приведенном примере квалификация содеянного только по ст. 273 УК РФ, на наш взгляд, является неверной. Исходя из фабулы дела, виновный не только подобрал сетевые идентификаторы к серверу, но и установил программное обеспечение для майнинга криптовалюты, что позволяет утверждать о модификации компьютерной информации. Таким образом, полная юридическая оценка содеянного должна была также включать квалификацию самого неправомерного доступа к серверу с последующей модификацией информации по ст. 272 УК РФ.

По ст. 274 УК РФ как преступное нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей следует оценивать действия работников организации, использовавших ее вычислительные мощности для вычисления (майнинга) криптовалюты. Подобный подход нашел свое отражение и в правоприменительной практике. Так, Б. был признан виновным в совершении преступления, предусмотренного ч. 1 ст. 274 УК РФ. Согласно приговору суда, Б., совместно с другими лицами, находясь в Институте теоретической и математической физики (ИТМФ), действуя умышленно, из корыстной заинтересованности, обладая специальными познаниями в сфере компьютерной техники, заведомо зная о

[1] Приговор Курганского городского суда Курганской области от 29 ноября 2018 г. по делу № 1-1186/18.

действующих в Федеральном государственном унитарном предприятии «Российский федеральный ядерный центр – Всероссийский научно-исследовательский институт экспериментальной физики» (ФГУП «РФЯЦ-ВНИИЭФ») правилах эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, в том числе о запретах на подключение служебной вычислительной сети к сети «Интернет», а также использование на автоматизированных рабочих местах программного обеспечения, не разрешенного к применению соответствующей комиссией института, договорились об использовании вычислительных мощностей находящегося в Институте неиспользуемого компьютерного оборудования и возможностей служебной вычислительной сети, предназначенной для обработки конфиденциальной информации уровня конфиденциальности «для служебного пользования», «персональные данные» и «коммерческая тайна», для вычисления (майнинга) криптовалюты и ее последующего обращения в свою пользу, вопреки служебным интересам ФГУП «РФЯЦ-ВНИИЭФ». Реализуя совместный преступный умысел, Б. проследовал в комнату 104 здания ФГУП «РФЯЦ-ВНИИЭФ», где действуя умышленно, из корыстной заинтересованности, выполняя свою роль в совершаемом преступлении, под непосредственным личным контролем со стороны других соучастников, действуя с ними группой лиц по предварительному сговору, путем соединения предоставленных вычислительных систем (серверов) посредством предоставленного коммутатора осуществил сборку вычислителя, необходимого для вычислений (майнинга) криптовалюты. Для обеспечения соединения собранного вычислителя с сетью «Интернет», подключил к нему GSM-модем, после чего, по согласованию с другими соучастниками и под их контролем, загрузил из сети «Интернет» программное обеспечение, предназначенное для майнинга криптовалюты, а также программное обеспечение «eth-proxy», предназначенное для получения через сеть «Интернет» задач на вычисление (майнинг) криптовалюты, сбора результатов вычислений и их отправки в сеть «Интернет» на «Pool» (сервер, который связан со всеми участниками майнинга криптовалют). После этого в период с 1 мая по 31 июля 2017 года Б., действуя умышленно, из корыстной заинтересованности, в составе группы лиц по предварительному сговору, находясь в здании ИТМФ в течение нескольких недель преимущественно в ночное время запускали процесс майнинга криптовалют на вышеназванной «ферме».

Вышеуказанные действия по нарушению установленных в ИТМФ правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации привели к нарушению условий действия аттестата соответствия на объект информатизации Автоматизированные

системы в защищенном исполнении «Служебная вычислительная сеть РФЯЦ-ВНИИЭФ» № от 29 июля 2016 г., что, в соответствии с п. 7.3 ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения» повлекло необходимость в проведении внеочередной повторной аттестации Автоматизированные системы в защищенном исполнении «Служебная вычислительная сеть РФЯЦ-ВНИИЭФ», сегментом которой является служебная локальная вычислительная сеть ИТМФ, стоимость которой составила 1 140 157 рублей 10 копеек. Таким образом, нарушение правил эксплуатации средств хранения, обработки и передачи охраняемой компьютерной информации, совершенное Б., повлекло причинение ФГУП «РФЯЦ-ВНИИЭФ» крупного материального ущерба, составляющего 1 140 157 рублей 10 копеек[1].

Развитие и внедрение блокчейн-технологий связаны с высоким уровнем неопределенности. Равным образом этот вывод можно распространить на будущее виртуальных валют. Это означает, что мы не имеем четкого представления, как будет трансформироваться новая (криптовалютная) преступность. Однако сама сложность процесса цифровизации уголовно-правовой сферы предполагает повышенную ответственность научного сообщества, которое должно обеспечить надлежащий уровень осмысления формирующихся тенденций. Предпринятая в настоящей работе попытка обобщить и проанализировать особенности правоприменения в части квалификации преступлений, совершаемых с использованием, в отношении и по поводу цифровых финансовых активов, конечно же, не претендует на абсолютность, носит субъективно-несовершенный, а значит и незавершенный характер. Вместе с тем, не вызывает сомнений, что совместные усилия экспертного сообщества в сфере высоких технологий и юристов в ближайшей перспективе внесут определенность в понимание правового статуса криптовалюты, а, следовательно, и правовой оценки действий, совершаемых с нею.

[1] Приговор Саровского городского суда Нижегородской области от 17 сентября 2019 г. по делу № 1-149/2019.

ЗАКЛЮЧЕНИЕ

Невозможно точно предсказать, каким окажется будущее. Вместе с тем, одно представляется очевидным – технологии будут гораздо глубже и прочнее вплетены в нашу повседневную жизнь. В гиперподключённом мире уголовно-правовые риски возрастут многократно. За многочисленные устройства и приложения, существенно облегчающие жизнь, человечеству придётся заплатить появлением «цифровой преступности», которая будет активно эксплуатировать достижения четвертой промышленной революции.

Цифровизация завораживает. Прогнозируемое появление автономных транспортных средств и концепция возможного будущего – запрограммированного безаварийного и бесконфликтного дорожного движения – формирует оптимистичную картину всеобщей безопасности. Но в то же время, достаточно ясно просматриваются и те потенциальные катастрофические последствия, которые могут наступить в случае, если кто-либо неправомерно получит доступ к такой системе и изменит её настройки хотя бы на несколько минут.

Интернет и цифровые технологии, цифровизация преступности, уже сейчас оказывают влияние на отечественное уголовное право. Однако, можно сказать определённо – это только начало. Следующие годы принесут гораздо большие практические сложности реализации механизма уголовно-правовой охраны. Так, лишь в стадии своего становления находится национальное законодательство об искусственном интеллекте. Можно выделить лишь отдельные нормативные акты, которые регулируют частные вопросы разработки либо использования искусственного интеллекта. В своей совокупности они еще не составляют замкнутого контура необходимой нормативной правовой основы.

Примеры непосредственного использования искусственного интеллекта для совершения общественно опасного посягательства на охраняемые уголовным законом общественные отношения до настоящего времени в российской правоприменительной практике отсутствуют. Вместе с тем, в российской науке уже активно обсуждаются вопросы достаточности механизма уголовно-правовой охраны для реагирования на перспективные угрозы развития AI-технологий [1]. Ссылаясь на то, что деятельность по созданию робота для целей совершения преступлений в настоящее время не охватывается составами преступлений, предусмотренными действующим УК РФ, предлагается криминализовать создание и (или) распространение роботов, предназначенных для целей совершения преступления. При этом И.Р. Бегишев не без оснований отмечает, что

[1] См.: Бегишев И.Р., Хисамова З.И. Искусственный интеллект и уголовный закон: монография. – М.: Проспект, 2021. – 192 с.

совершение аналогичных действий по отношению к *автономному* роботу обладает повышенной общественной опасностью и должно наказываться строже в рамках самостоятельной уголовно-правовой нормы[1]. В дополнение следует отметить, что по мере расширения регулирования технологий искусственного интеллекта и робототехники с высокой вероятностью возникнет потребность в уголовно-правовом обеспечении соответствующего правопорядка, в том числе посредством криминализации незаконного оборота систем искусственного интеллекта и роботов, обладающих функциональными особенностями, нарушающими установленные технические стандарты и требования (например, AI-систем и роботов с отсутствующими (отключенными) возможностями потребителя прекратить деятельность искусственного интеллекта в критической ситуации («красная кнопка») или обеспечить фиксацию фактов, позволяющих установить обстоятельства причинения вреда («черный ящик»).

Изобретение некоего «цифрового уголовного права» является утопической задачей. По мере того как формируется глобальный и взаимоподключённый мир, конечно же, потребуется проанализировать и пересмотреть отдельные подходы к противодействию преступности. Вместе с тем, крайне важным является то, чтобы «оцифровка» отечественного уголовного права не привела к разрушению субстанциональных признаков отрасли.

Значимым направлением приспосабливания уголовно-правового механизма к противодействию преступлениям, совершаемым с использованием информационно-коммуникационных технологий, на наш взгляд, является преодоление «традиционного», «не цифрового», восприятия уголовного права. Это довольно сложная и многоаспектная проблема, которая касается не только подготовки кадров в образовательных учреждениях и повышения квалификации действующих сотрудников правоохранительных органов. В данном аспекте насущно необходимым представляется активизация Пленумом Верховного Суда Российской Федерации работы по разработке постановления о судебной практике по делам о преступлениях в сфере компьютерной информации, в рамках которого необходимо разрешить не только наиболее обсуждаемые вопросы применения норм, предусмотренных главой 28 УК РФ, но и целый ряд смежных проблем, возникающих при квалификации посягательств на конституционные права граждан, отношения собственности, общественную безопасность и др.

Цифровая трансформация преступности не завершена, как и не завершено осмысление этого процесса. И это содержит большой методологический

---

[1] Бегишев И.Р. Уголовная ответственность за создание и (или) распространение роботов, предназначенных для целей совершения преступлений // Северо-Кавказский юридический вестник. 2021. № 2. С. 146 – 147.

потенциал для юриспруденции, в том числе в аспекте науки уголовного права.

БЛАГОДАРНОСТИ

Эта книга не появилась бы на свет без активной поддержки и участия этих прекрасных людей. Я хотел бы поблагодарить:

Любовь Русскевич, мою любимую жену, которая терпела мое физическое и умственное отсутствие в период работы над монографией, и поддерживала меня на всем пути.

Андрея Петровича Дмитренко, доктора юридических наук, профессора, моего научного консультанта – за помощь в работе и поддержку.

Николая Григорьевича Кадникова, доктора юридических наук, профессора – за структурные правки и общие советы.

Олега Валентиновича Зиборова, заместителя начальника Московского университета МВД России имения В.Я. Кикотя, доктора юридических наук, доцента – за поддержку на всех этапах проведения исследования и написания книги.

Игоря Геннадьевича Чекунова, заместителя генерального директора компании «Лаборатория Касперского», кандидата юридических наук – за исключительные знания и опыт, переданные как в режиме онлайн, так и при личном общении.

Михаила Михайловича Дайшутова, начальника кафедры уголовного права Московского университета МВД России имения В.Я. Кикотя, кандидата юридических наук, доцента – за поддержку на всех этапах проведения исследования и написания книги.

Владимира Владимировича Гончара, кандидата юридических наук, доцента – за его дружбу и поддержку.

Александра Юрьевича Решетникова, кандидата юридических наук, доцента – за его дружбу и честный отзыв.

Команду издательства «Инфра-М» – за их энтузиазм, скрупулезный и творческий подход к работе.

Всех участников «Кибергруппы» Московского университета МВД России имени В.Я. Кикотя – за обмен знаниями, творческую атмосферу и сотрудничество.

Выражаю глубокую благодарность **Ильдару Рустамовичу Бегишеву**, **Сергею Викторовичу Борисову, Людмиле Александровне Букалеровой, Валерию Александровичу Жабскому, Марине Александровне Ефремовой, Виктору Ивановичу Динеке, Нодару Шотаевичу Козаеву, Станиславу Львовичу Нуделю, Александру Михайловичу Плешакову, Юрию Евгеньевичу Пудовочкину, Павлу Сергеевичу Яни, Борису Викторовичу Яцеленко** за поддержку, критику, сотрудничество и обмен знаниями.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Нормативно-правовые акты:

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 №6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ).
2. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ // СПС «Консультант-Плюс».
3. Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (Заключено в г. Минске 01.06.2001) // Собрание законодательства РФ. 30 марта 2009 г. № 13. Ст. 1460.
4. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 29.06.2018) «Об информации, информационных технологиях и о защите информации».
5. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Учебная и научная литература:

1. Архипов В. В. Виртуальное право: основные проблемы нового направления юридических исследований [Текст] / В.В. Архипов // Известия высших учебных заведений. Правоведение. – 2013. – № 2. – С. 93 – 114.
2. Асланян Р. Г. Информация как предмет и средство совершения преступлений в сфере экономической деятельности [Текст]: дис. …канд.юрид.наук / Р. Г. Асланян – Краснодар, 2016. – 21 с.
3. Бабаев М. М. Проблемы российской уголовной политики [Текст] / М. М. Бабаев, Ю. Е. Пудовочкин. – М.: Проспект, 2014. – 296 с.
4. Бегишев И.Р., Хисамова З.И. Искусственный интеллект и уголовный закон: монография. – М.: Проспект, 2021. – 192 с.
5. Букалерова Л. А. Информационные преступления в сфере государственного и муниципального управления: законотворческие и правоприменительные проблемы [Текст]: дис. …д-ра юрид. наук / Л. А. Букалерова. – М., 2007. – 574 с.
5. Гончар В. В. Теоретические и правовые аспекты розыскной деятельности следователя: монография [Текст] / В. В. Гончар. – М.: ИНФРА-М, 2017. – 162 с.
6. Гилинский Я. И. Криминологические основы уголовного права в эпоху постмодерна [Текст] / Я. И. Гилинский // Криминологические основы уголовного права // Материалы X Российского конгресса уголовного права, состоявшегося 26-27 мая 2016 г. / отв. ред., докт. юрид. наук, проф. В. С. Комиссаров. – М.: Юрлитинформ, 2016. – С. 294 – 298.

7. Гузеева О. С. Преступления, совершаемые в российском сегменте сети Интернет: монография [Текст] / О. С. Гузеева. – М.: Академия Генеральной прокуратуры Российской Федерации, 2015. – 136 с.
8. Дюранске Б. Т. Виртуальные миры, реальные проблемы [Текст] / Б.Т. Дюранске, Ш. Ф. Кейн // Известия высших учебных заведений. Правоведение. – 2013. – № 2. – С. 115 – 134.
9. Елин В. М. Мошенничество в сфере компьютерной информации как новый состав преступления [Текст] / В. М. Елин // Бизнес-информатика. – 2013. – № 2 (24). – С. 70 – 76.
10. Ефремова М. А. Уголовно-правовая охрана информационной безопасности [Текст]: дис. …д-ра юрид. наук / М. А. Ефремова. – М., 2018. – 427 с.
11. Зазирная М. М. Квалификация распространения порнографических материалов в режиме реального времени с использованием сети Интернет [Текст] / М. М. Зазирная // Уголовное право. – 2015. – № 6. – С. 16 – 22.
12. Кауфман М. А. Пробельность, неопределенность, избыточность уголовного законодательства как криминогенные факторы [Текст] / М. А. Кауфман // Материалы X Российского конгресса уголовного права, состоявшегося 26-27 мая 2016 г. / отв. ред., докт. юрид. наук, проф. В.С. Комиссаров. – М., 2016. – С. 100 – 105.
13. Козаев Н. Ш. Современные технологии и проблемы уголовного права (анализ зарубежного и российского законодательства): монография. [Текст] / Н.Ш. Козаев. – М.: Юрлитинформ, 2015. – 224 с.
14. Комментарий к Уголовному кодексу Российской Федерации (научно-практический, постатейный): 5-е издание, переработанное и дополненное [Текст] / под ред. д.ю.н., профессора С.Ф. Дьякова, д.ю.н., профессора Н. Г. Кадникова. – М.: ИД «Юриспруденция», 2017. – 1072 с.
15. Комментарий к Уголовному кодексу Российской Федерации (постатейный). Том 1. 2-е изд., перераб. и доп. [Текст] / под ред. засл. юриста РФ, д.ю.н., профессора А. В. Бриллиантова // Режим доступа: СПС «Консультант-Плюс».
16. Кругликов Л. Л. Сбои в конструировании санкций в уголовном законодательстве [Текст] / Л. Л. Кругликов // Юридическая техника. – 2008. – № 2. – С. 110 – 113.
17. Крылов В. В. Информационные компьютерные преступления. [Текст] / В. В. Крылов. – М.: Инфра-М - Норма, 1997. – 285 с.
18. Кудрявцев В. Н. Объективная сторона преступления [Текст] / В.Н. Кудрявцев. – М.: Госюриздат, 1960. – 244 с.
19. Кулезин М. А. Реальные проблемы виртуальных объектов [Текст] / М. А. Кулезин // Евразийская адвокатура. – 2015. – № 5 (18). – С. 51 – 53.
20. Лисаченко А. В. Право виртуальных миров: новые объекты гражданских прав [Текст] / А. В. Лисаченко // Российский юридический журнал. – 2014. – № 2. – С. 104 – 110.

21. Лопатина Т. М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности [Текст]: автореф. дис. …д-ра юрид. наук / Т. М. Лопатина – М., 2006. – 60 с.
22. Лопатина Т. М. Проблемы уголовно-правовой защиты сфер компьютерной информации: современный взгляд на мошенничество [Текст] / Т. М. Лопатина // Право и безопасность. – 2013. – № 3-4 (45). – С. 89 – 95.
23. Лопашенко Н. А. Законодательная реформа мошенничества: вынужденные вопросы и вынужденные ответы [Текст] / Н. А. Лопашенко // Криминологический журнал Байкальского государственного университета экономики и права. – 2015. – № 3. – С. 504 – 513.
24. Овчинский В. С. Криминология цифрового мира: учебник для магистратуры [Текст] / В. С. Овчинский. – М.: Норма: ИНФРА-М, 2018. – 352 с.
25. Побегайло А. Э. Киберпреступность: учеб. пособие (для бакалавров) / А. Э. Побегайло. – М.: Академия Генеральной прокуратуры Российской Федерации. 2014. – 96 с.
26. Потапкин С. Н. Вопросы объективной стороны мошенничества в сфере компьютерной информации в судебно-следственной практике [Текст] / С. Н. Потапкин, А. В. Солдатов, Т. Т. Утешева, Д. А. Данилов // Библиотека научных публикаций Электронного юридического справочника Система Гарант. – 2015. – №1 (5).
27. Пудовочкин Ю. Е. Учение о составе преступления. Учебное пособие. [Текст] / Ю. Е. Пудовочкин. – М.: Юрлитинформ, 2009. – 248 с.
28. Решняк М. Г. О некоторых вопросах современного уголовно-правового законотворчества [Текст] / М. Г. Решняк // Российский следователь. – 2014. – № 3. – С. 25 – 28.
29. Рогова Е. В. Учение о дифференциации уголовной ответственности: дисс. …д-ра. юрид. наук. [Текст] / Е. В. Рогова. – М., 2014. – 596 с.
30. Русскевич Е. А. Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий: учебное пособие [Текст] / Е. А. Русскевич. – М.: ИНФРА-М, 2017. – 115 с.
31. Савельев А. И. Правовая природа виртуальных объектов, приобретаемых за реальные деньги в многопользовательских играх [Текст] / А. И. Савельев // Вестник гражданского права. – 2014. – № 1. – С. 127 – 152.
32. Сафонов О. М. Уголовно-правовая оценка использования компьютерных технологий при совершении преступлений: состояние законодательства и правоприменительной практики, перспективы совершенствования [Текст]: дис. …канд.юрид.наук. / О. М. Сафонов. – М., 2015. – 222 с.
33. Семенюта Б. Онлайн-игры: правовая природа отношений [Текст] / Б. Семенюта // Интеллектуальная собственность. Авторское право и смежные права. – 2014. – № 8. – С. 38 – 45.

34. Третьяк М. И. Проблемы понимания способа компьютерного мошенничества в судебной практике [Текст] / М. И. Третьяк // Уголовное право. – 2015. – № 5. – С. 109 – 112.
35. Третьяк М. И. Проблемы квалификации новых способов мошенничества [Текст] / М. И. Третьяк // Уголовное право. – 2015. – № 2. – С. 94 – 98.
36. Тропина Т. Л. Борьба с киберпреступностью: возможна ли разработка универсального механизма? [Текст] / Т. Л. Тропина // Международное правосудие. – 2012. – № 3. – С. 86 – 95.
37. Тропина Т. Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: понятие, состояние, уголовно-правовые меры борьбы [Текст]: дис. …канд. юрид. наук / Т. Л. Тропина. – Владивосток, 2005. – 235 с.
38. Тюнин В. Реструктуризация уголовного законодательства об ответственности за мошенничество [Текст] / В. Тюнин // Уголовное право. – 2013. – № 2. – С. 35 – 41.
39. Чекунов И. Г. Криминологическое и уголовно-правовое обеспечение предупреждения киберпреступности [Текст]: автореф. дис. …канд. юрид. наук / И. Г. Чекунов. – М., 2013. – 23 с.
40. Чупрова А. Ю. Уголовно-правовые механизмы регулирования отношений в сфере электронной коммерции [Текст]: дис. …д-ра юрид. наук / А. Ю. Чупрова – М., 2015. – 608 с.
41. Чупрова А. Ю. Проблемы квалификации мошенничества с использованием информационных технологий [Текст] / А. Ю. Чупрова // Уголовное право. – 2015. – № 5. – С. 131 – 134.
42. Хабриева Т. Я. Право в условиях цифровой реальности [Текст] / Т. Я. Хабриева, Н. Н. Черногор // Журнал российского права. – 2018. – № 1. – С. 85 – 102.
43. Хилюта В. В. Хищение с использованием компьютерной техники или компьютерное мошенничество? [Текст] / В. В. Хилюта // Библиотека криминалиста. – 2013. – № 5 (10). – С. 55 – 65.
44. Шваб К. Четвёртая промышленная революция: перевод с английского [Текст] / К. Шваб. – М.: Издательство «Э», 2018. – 208 с.
45. Шумихин В. Г. Седьмая форма хищения чужого имущества [Текст] / В. Г. Шумихин // Вестник Пермского университета. – 2014. – № 2 (24). – С. 229 – 233.
46. Breivik P. S. Education for the information age // D.W. Farmer and T.F. Mech, eds. New Directions for Higher Education. № 78. 1992.
47. Dana L. Bazelon, Yun Jung Choi and Jason F. Conaty. Computer crimes. Am. Crim. L. Rev. 2006.
48. Douglas H. Hancock. To what extent should computer related crimes be the subject of specific legislative attention? Alb. L.J. Sci. & Tech. 2001.

49. Portela, Irene Maria. Information Communication Technology Law, Protection and Access Rights: Global Approaches and Issues // Idea Group Inc (IGI), 2010 . P.103.
50. Stephen P. Heymann, Legislating computer crime. Harv. J. On Legis. 1997.

ПРИЛОЖЕНИЕ

ПОСТАНОВЛЕНИЕ ПЛЕНУМА ВЕРХОВНОГО СУДА РОССИЙСКОЙ ФЕДЕРАЦИИ «О СУДЕБНОЙ ПРАКТИКЕ ПО ДЕЛАМ О ПРЕСТУПЛЕНИЯХ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ» (ПРОЕКТ)

В XXI веке информационные технологии являются не только основной движущей силой экономического и технологического развития, но и центральным фактором, преображающим материальную и духовную жизнь отдельного индивидуума и социума. Расширение телекоммуникационной инфраструктуры и информационного пространства на качественно новом уровне актуализирует проблему информационной безопасности человека, общества и государства.

В Российской Федерации правовую основу противодействия преступлениям в сфере компьютерной информации составляют Конституция Российской Федерации, общепризнанные принципы и нормы международного права, международные договоры Российской Федерации, Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и другие нормативные правовые акты, направленные на противодействие преступлениям в сфере компьютерной информации.

В целях уголовно-правового обеспечения противодействия преступлениям в сфере компьютерной информации и в интересах выполнения международных обязательств Уголовный кодекс Российской Федерации устанавливает ответственность за совершение преступлений, предусмотренных статьями 272, 273, 274 и 274^1.

В связи с вопросами, возникающими у судов при рассмотрении уголовных дел по преступлениям в сфере компьютерной информации, и в целях обеспечения единства судебной практики Пленум Верховного Суда Российской Федерации, руководствуясь статьей 126 Конституции Российской Федерации, постановляет дать судам следующие разъяснения:

1. Обратить внимание судов, что преступления в сфере компьютерной информации посягают на общественные отношения, складывающиеся в связи с безопасным созданием, хранением, обработкой и передачей компьютерной информации, а также функционированием информационно-

телекоммуникационных сетей, оконечного оборудования и объектов критической информационной инфраструктуры Российской Федерации.

2. Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи (примечание 1 к статье 272 УК РФ).

3. Разъяснить судам, что предметом преступления, предусмотренного статьей 272 УК РФ, является как конфиденциальная компьютерная информация, так и открытая информация, в отношении которой правообладателем установлены программно-технические средства защиты, направленные на обеспечение ее целостности и доступности.

4. Неправомерный доступ к компьютерной информации, содержащей сведения, составляющие охраняемую законом тайну, в зависимости от обстоятельств дела следует дополнительно квалифицировать по статьям 137, 138, 183, 275, 276 и др.

5. Под неправомерным доступом следует понимать совершение любых (как высокотехнологичных, так и примитивно-бытовых) действий, предоставляющих лицу возможность распоряжения информацией (ее уничтожение, модификация, блокирование, копирование) по собственному усмотрению без согласия на то законного владельца.

6. При рассмотрении судами уголовных дел о преступлениях, предусмотренных статьей 272 УК РФ, под уничтожением компьютерной информации следует понимать ее удаление из памяти компьютера или любого другого электронного носителя, когда доступ к ней законного владельца невозможен, независимо от возможности восстановления.

Под блокированием компьютерной информации следует понимать прекращение доступа к компьютерной информации для лиц, которые имеют право на такой доступ.

Модификация компьютерной информации представляет собой искажение первоначальных данных, приводящее к невозможности их использования законным владельцем или иными лицами.

Под копированием охраняемой законом компьютерной информации следует понимать ее воспроизведение на другом носителе независимо от способа (переноса на другой электронный носитель, выполнения рукописной или машинописной копии, фотографирования и т.д.). По смыслу закона уголовно-наказуемым является только неправомерный доступ, повлекший копирование конфиденциальной информации.

7. Судам следует учитывать, что лицо, осуществившее доступ в информационно-телекоммуникационную сеть «Интернет» с использованием учетно-регистрационных данных другого пользователя без

его согласия, не подлежит уголовной ответственности по статье 272 УК РФ. При наличии достаточных на то оснований содеянное может быть квалифицировано по статье 165 УК РФ.

8. Обратить внимание судов на то, что незаконное завладение техническими средствами, предназначенными для хранения, обработки или передачи компьютерной информации, следует дополнительно квалифицировать по статье 272 УК РФ в случаях, когда обстоятельства содеянного указывают на то, что умысел лица был заведомо направлен на незаконное уничтожение, модификацию либо копирование охраняемой законом компьютерной информации.

9. В каждом случае, когда действия лица привели к уничтожению, модификации либо копированию незначительных объемов компьютерной информации, а равно когда блокирование компьютерной информации имело непродолжительный характер судам необходимо рассматривать вопрос о признании деяния малозначительным по смыслу статьи 14 УК РФ.

10. Субъектом преступления, предусмотренного статьей 272 УК РФ, является физическое, вменяемое лицо, достигшее к моменту совершения преступления 16-летнего возраста и не имеющее права доступа к компьютерной информации.

11. По смыслу закона неправомерный доступ к охраняемой законом компьютерной информации может быть только умышленным. При этом умысел может быть как прямым, так и косвенным.

12. Неправомерный доступ к охраняемой законом компьютерной информации, причинивший крупный ущерб или совершенный из корыстной заинтересованности, следует квалифицировать по части 2 статьи 272 УК РФ.

13. Под ущербом следует понимать негативные имущественные последствия для владельца компьютерной информации, которые могут состоять в прямых материальных убытках (например, вред, возникший в результате ненадлежащей работы программного обеспечения производственного оборудования и получения значительного количества испорченной продукции; расходы, связанные с ошибками в комплектовании грузов либо их доставке; траты на восстановление нормального функционирования программного обеспечения и т.п.).

При расчете ущерба по смыслу части 2 статьи 272 УК РФ судами также должна учитываться упущенная выгода (например, недополученная торговой организацией прибыль в результате нарушения нормального функционирования контрольно-кассового оборудования).

14. Под корыстной заинтересованностью следует понимать стремление виновного получить выгоду имущественного характера для

себя лично или других лиц путем неправомерного доступа к охраняемой законом компьютерной информации.

Неправомерный доступ к компьютерной информации, связанный с хищением чужого имущества, требует дополнительной квалификации по статье 159^6 УК РФ.

15. Неправомерный доступ к компьютерной информации признается совершенным группой лиц по предварительному сговору, если в нем участвовали лица, заранее договорившиеся о совместном совершении этого преступления. При этом судам следует иметь в виду, что уголовная ответственность по части 3 статьи 272 УК РФ наступает и в тех случаях, когда согласно предварительной договоренности между соучастниками непосредственный доступ к охраняемой законом компьютерной информации осуществляет один из них.

Неправомерный доступ к компьютерной информации признается совершенным организованной группой, если он совершен устойчивой группой лиц, заранее объединившихся для совершения одного или нескольких преступлений.

16. При квалификации неправомерного доступа к охраняемой законом компьютерной информации, совершенного лицом с использованием служебного положения, по части 3 статьи 272 УК РФ, судам следует иметь в виду, что к таким лицам, прежде всего, относятся должностные лица, обладающие признаками, предусмотренными примечанием 1 к статье 285 УК РФ, государственные или муниципальные служащие, не являющиеся должностными лицами, а также иные лица, отвечающие требованиям, предусмотренным примечанием 1 к статье 201 УК РФ.

Под использованием служебного положения, предусмотренного в диспозиции части 3 статьи 272 УК РФ, понимается также наличие у лица доступа к компьютерной информации в результате выполняемой работы по трудовому, или гражданско-правовому договору (программисты, администраторы баз данных, инженеры, специалисты и др.).

17. Разъяснить судам, что под вредоносной следует понимать компьютерную программу либо информацию, созданную (в том числе путем модификации существующей компьютерной программы, не обладающей признаками вредоносности) для осуществления противоправной деятельности.

18. Под использованием вредоносной компьютерной программы или вредоносной компьютерной информации следует понимать их непосредственный запуск и задействование функциональных возможностей вредоносной программы. При этом использование

вредоносной программы может осуществляться как в автономном режиме, так и в информационно-телекоммуникационной сети, в том числе сети «Интернет».

Распространение вредоносной программы или вредоносной компьютерной информации заключается в умышленном их предоставлении как конкретному лицу, так и размещение таких материалов в общем доступе для неограниченного круга лиц, в том числе с использованием информационно-телекоммуникационных сетей.

Распространение вредоносных компьютерных программ либо вредоносной компьютерной информации при проведении проверочной закупки образует признаки оконченного преступления, предусмотренного статьей 273 УК РФ.

19. Судам следует учитывать, что не образует преступления, предусмотренного статьей 273 УК РФ, создание и использование вредоносной компьютерной программы либо вредоносной компьютерной информации для личных нужд (например, для тестирования эффективности средств программно-технической защиты собственной информации), их использование в образовательных или исследовательских целях, а равно во всех случаях, когда вредоносная компьютерная программа или информация не создают угрозы для автоматизированной обработки данных, нормального функционирования информационно-телекоммуникационных сетей и оконечного оборудования.

20. Субъектом преступления, предусмотренного статьей 273 УК РФ, является любое физическое, вменяемое лицо, достигшее к моменту совершения преступления 16-летнего возраста.

21. Преступление, предусмотренное статьей 273 УК РФ, совершается только с прямым умыслом. Решая вопрос о виновности, судам необходимо установить осведомленность подсудимого о вредоносности использованной и (или) распространенной им компьютерной программы (информации).

22. Разъяснить судам, что нарушением правил эксплуатации по смыслу статьи 274 УК РФ является несоблюдение либо ненадлежащее соблюдение установленных правил, обеспечивающих безопасность функционирования средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (например, нарушение запрета на подключение служебного оборудования к сети «Интернет»; предоставление посторонним лицам доступа к средствам хранения, обработки или передачи охраняемой компьютерной информации; несанкционированное разглашение логина или пароля законного пользователя; использование нелицензионного программного обеспечения; несанкционирован-

ная модификация программного обеспечения; несанкционированное изменение параметров настройки компьютера или информационно-телекоммуникационной сети; отключение средств противовирусной защиты; несоблюдение или прямое игнорирование требования об обязательной проверке используемых средств хранения или передачи информации на наличие вредоносных программ; невыполнение обязательной процедуры резервного копирования компьютерной информации и др.).

23. Обратить внимание судов на то, что правила эксплуатации средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей не консолидированы и в современных условиях содержатся в отдельных нормативных правовых актах, определяются на договорной основе (клиентским договором, договором на оказание услуг телематической связи, пользовательским соглашением и т.п.), регламентируются в конкретной организации (ведомстве) при определении обязанностей работников (служащих), а также раскрываются в технической документации производителя компьютерного оборудования.

24. При рассмотрении дел о преступлениях, предусмотренных статьей 274 УК РФ и частью 3 статьи 274^1 УК РФ, судам следует указывать в приговоре нарушение каких правил эксплуатации повлекло наступление соответствующих общественно опасных последствий, и в чем конкретно выразилось это нарушение.

25. Разъяснить судам, что уничтожение или повреждение компьютерного оборудования, уничтожение или модификация компьютерной информации и, как следствие, причинение имущественного ущерба потерпевшему, ставшие следствием бытовой небрежности (например, когда лицо роняет компьютер, утрачивает электронный носитель компьютерной информации и т.п.), содеянное не образует признаков преступления, предусмотренного статьей 274 УК РФ, и может выступать основанием для дисциплинарной и гражданско-правовой ответственности работника.

26. Обратить внимание судов на то, что для признания преступления, предусмотренного статьей 274 УК РФ, оконченным необходимо установить наступление общественно опасных последствий в виде уничтожения, блокирования, модификации либо копирования охраняемой законом компьютерной информации и причинения крупного ущерба (в соответствии с примечанием к статье 272 УК РФ, это ущерб, сумма которого превышает один миллион рублей). Таким образом, если нарушение соответствующих правил хотя и повлекло уничтожение, блокирование, модификацию либо копирование информации, но не причинило крупного ущерба, привлече-

ние лица к уголовной ответственности по статье 274 УК РФ является невозможным.

27. Субъектом преступления, предусмотренного статьей 274 УК РФ, является физическое, вменяемое лицо, достигшее к моменту совершения преступления 16-летнего возраста, на которое в силу закона, иного нормативного акта либо характера выполняемой профессиональной, трудовой или иной деятельности возложена обязанность по соблюдению соответствующих правил эксплуатации или доступа.

28. Преступление, предусмотренное статьей 274 УК РФ, может быть совершено как умышленно, так и по неосторожности.

29. Диспозиция статьи 274^1 УК РФ имеет бланкетный характер и предполагает обращение к Федеральному закону от 26 июля 2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

30. Предметом преступления, предусмотренного частью 1 статьи 274^1 УК РФ, является компьютерная информация или компьютерные программы, заведомо предназначенные для совершения компьютерных атак на объекты критической информационной инфраструктуры.

Предметом преступлений, предусмотренных частями 2 и 3 статьи 274^1 УК РФ, выступают объекты критической информационной инфраструктуры – информационные системы, информационно-телекоммуникационные сети государственных органов, а также информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления технологическими процессами, функционирующие в области здравоохранения, транспорта, связи, кредитно-финансовой сфере, энергетике, оборонной, топливной, атомной, ракетно-космической, горнодобывающей, металлургической и химической промышленностях.

Относимость того или иного информационного ресурса к критическому определяется посредством его включения в Реестр значимых объектов критической информационной инфраструктуры (ст. 8 Федерального закона от 26 июля 2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»).

31. Объективная сторона преступления, предусмотренного частью 2 статьи 274^1 УК РФ, заключается в неправомерном доступе к компьютерной информации, содержащейся в критической информационной инфраструктуре. Вред, как конструктивный признак состава преступления, предусмотренного частью 2 статьи 274^1 УК РФ, может заключаться в уничтожении, блокировании, модификации, копировании информации, содержащейся в критической информационной инфраструктуре, нейтрали-

зации средств защиты указанной информации или выведении из строя аппаратных и программных средств, обеспечивающих функционирование критической информационной инфраструктуры (за исключением случаев, когда это повлекло причинение смерти или тяжкого вреда здоровью человека, причинение средней тяжести вреда здоровью двум или более лицам, массовое причинение легкого вреда здоровью людей, наступление экологических катастроф, транспортных или производственных аварий, повлекших длительную остановку транспорта или производственного процесса, дезорганизацию работы конкретного предприятия, причинение особо крупного ущерба, то есть тяжких последствий, предусмотренных частью 5 статьи 274^1 УК РФ).

32. Обратить внимание судов на то, что часть 2 статьи 274^1 УК РФ охватывает неправомерный доступ к объектам критической информационной инфраструктуры, совершенный с использованием заведомо предназначенных для этого вредоносных программ (ч. 1 ст. 274^1 УК РФ) или иных вредоносных программ (ст. 273 УК РФ). При этом, если лицо, использовавшее программу, являлось и ее разработчиком, содеянное необходимо квалифицировать по совокупности преступлений.

33. Разъяснить судам, что совершение компьютерных атак на информационные ресурсы объектов транспорта, оборонной, атомной, ракетно-космической или химической промышленности, в зависимости от обстоятельств дела может содержать признаки преступлений, предусмотренных статьями 205, 281, 275, 276 УК РФ и др.

34. Субъектом преступлений, предусмотренных частями 1 и 2 статьи 274^1 УК РФ, является физическое, вменяемое лицо, достигшее возраста 16 лет. Субъектом преступления, предусмотренного частью 3 статьи 274^1 УК РФ, выступает физическое, вменяемое лицо, достигшее к моменту совершения преступления 16-летнего возраста, на которое в силу закона, иного нормативного акта, либо характера выполняемой профессиональной, трудовой или иной деятельности возложена обязанность по соблюдению соответствующих правил эксплуатации или доступа.

35. Субъективная сторона создания, использования и распространения компьютерных программ или информации, заведомо предназначенных для совершения атак на объекты критической информационной инфраструктуры, характеризуется прямым умыслом. Лицо, совершая те или иные действия, должно осознавать, что они направлены на публичные информационные ресурсы, обладающие исключительной важностью для общества и государства и включенные в соответствующий реестр.

При неправомерном доступе (ч. 2 ст. 274^1 УК РФ) умысел может быть как прямым, так и косвенным.

Субъективная сторона преступления, предусмотренного частью 3 статьи 274^1 УК РФ, характеризуется двумя формами вины.

36. При рассмотрении уголовных дел о преступлениях в сфере компьютерной информации, а также иных преступлений, совершенных с использованием информационно-телекоммуникационных технологий, судам следует выявлять обстоятельства, способствовавшие совершению указанных преступлений, нарушения прав и свобод граждан, а также другие нарушения закона, допущенные при производстве предварительного следствия или при рассмотрении уголовного дела нижестоящим судом. Согласно части 4 статьи 29 УПК РФ, необходимо обращать внимание соответствующих организаций и должностных лиц на выявленные факты нарушений закона путем вынесения частных определений или постановлений».

СОДЕРЖАНИЕ