Министерство образования и науки Российской Федерации
ФГБОУ ВПО «Алтайский государственный университет»
Физико-технический факультет
Юридический факультет
Научное студенческое общество АлтГУ

ПРОБЛЕМЫ ПРАВОВОЙ И ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ – 2014

Материалы междисциплинарной межвузовской конференции студентов, магистрантов и аспирантов

Барнаул 2014

ББК 67.401.114+32.81
П 781

П 781 Проблемы правовой и технической защиты информации – 2014 / Материалы междисциплинарной межвузовской конференции студентов, магистрантов и аспирантов. – Барнаул: ИП Колмогоров И.А., 2014. – 144 с.

ISBN 978-5-91556-085-6

В сборник включены статьи участников междисциплинарной межвузовской конференции студентов, магистрантов и аспирантов «Проблемы правовой и технической защиты информации – 2014» (Барнаул, Алтайский государственный университет, 20 мая 2014 года). Рассматриваются актуальные проблемы обеспечения комплексной информационной безопасности на различных уровнях.

Сборник издан в рамках Молодежного форума «Барнаул.pro».

Оглавление

ПРОБЛЕМЫ ТЕХНИЧЕСКОГО ОБЕСПЕЧЕНИЯ КОМПЛЕКСНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ПРАВОВЫЕ, КРИМИНОЛОГИЧЕСКИЕ И КРИМИНАЛИСТИЧЕСКИЕ ПРОБЛЕМЫ ПРЕСТУПНОСТИ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

П.Н. Алпеев, АлтГУ, юридический факультет, 4 к.
Научный руководитель – ***В.В. Поляков*****,** к.ю.н., доцент.

Научно-техническая революция XX в. полностью изменила представления человечества об окружающем мире. Процесс внедрения высоких технологий в повседневную жизнь сказывался на качественном изменении отношений в обществе, информация приобретала все большую значимость. Негативным последствием информатизации общества стало появление так называемой компьютерной преступности. Сложность решения вопроса заключается в том, что диапазон противоправных действий, совершаемых с использованием средств компьютерной техники, чрезвычайно широк – от преступлений традиционного типа до чисто компьютерных преступлений.

Появление на рынке в 1974 году компактных и сравнительно недорогих персональных компьютеров дало возможность подключаться к мощным информационным потокам неограниченному кругу лиц. Встал вопрос о контроле доступа к информации, ее сохранности и целостности. Проблема защиты информации и информационных систем сейчас является одной из самых актуальных во всем мире.

К разряду компьютерных следует отнести те преступления, у которых объектом преступного посягательства является информация, обрабатываемая и хранящаяся в компьютерных системах, а средством совершения преступлений служит компьютер [1].

Компьютерная информация, особенно в виде баз данных, содержащих различного рода сведения конфиденциального характера, обладает, с одной стороны, высокой стоимостью, а с другой - ее использование лицами, не уполномоченными для этого. В последнее десятилетие картотеки и базы данных многих государственных и иных структур преобразованы в электронную форму. В

силу встречающейся недобросовестности их держателей, а также иных причин, значительное число таких баз данных стало достоянием различных структур, которые занимаются их продажей. Это влечет за собой неконтролируемое использование такой информации. Речь ведется о базах данных ГИБДД, телефонных служб, таможенных органов и т.д. [2]. В последние годы в мире уделяется повышенное внимание проблемам борьбы с распространением детской порнографии в сети Интернет.

Сточки зрения криминологии можно выделить следующие проблемы:

1. устойчивый рост преступности;
2. рост количества преступлений, совершаемых организованными преступными группировками и сообществами, кибертерроризм;
3. качественное изменение в связи со стремительным ростом научно-технического прогресса, применения новейших технологий;
4. высокий уровень латентности;
5. транснациональный характер.

Как следует из интервью Алексея Мошкова, начальника Бюро специальных технических мероприятий, генерал-майора полиции, на протяжении последних 5 лет количественные показатели IT-преступности колебались от 8 тысяч до 17,5 тысяч. За последние 3 года количество обращений граждан непосредственно в Управление «К» МВД России резко увеличилось. Латентность данного вида преступлений остается довольно высокой и по некоторым данным достигает 90 – 95 % [3].

Что касается кибертерроризма, то киберпреступники приняли на вооружение и активно используют тактику «точечных ударов», целенаправленно атакуя определенные компании с целью хищения конфиденциальных данных и финансовой информации.

Страны, где больше всего жертв киберпреступлений среди пользователей: Россия – 85%, Китаи – 77%, Южная Африка – 73%, США – 63%, Канада – 68%, Бразилия – 60%, Мексика – 71%, Объединенное Королевство – 58%, Франция – 45%, Германия – 53%, Италия – 56%, Швеция – 56%, Польша – 60%, Нидерланды – 50%, Австралия – 60%, Индия – 65%, Япония – 19%, Сингапур – 61%, Новая Зеландия – 69%, Турция – 63%, Дания – 50%, Саудовская

Аравия – 62%, ОАЭ – 71%, Колумбия – 64%. Во всех случаях учитывались те, кто оказывался жертвой хотя бы раз в жизни [4].

Несмотря на то, что в последние годы в криминалистической литературе уделяется повышенное внимание методике расследования компьютерных преступлений, в этой области еще остается ряд нерешенных вопросов. Дискуссионными вопросами являются формулировки базовых понятия в области компьютерных преступлений [5].

Следует отметить, что разработка теоретических основ расследования преступлений в сфере компьютерной информации сложна и имеет много аспектов на стыке права, теории информатики, производства и эксплуатации аппаратных средств компьютерных систем, сетей и иного сопряженного оборудования. Однако до сих пор в криминалистике не существует разработанной комплексной методики расследования компьютерных преступлений, отвечающей практическим нуждам их расследования.

В процессе формирования криминалистической методики расследования преступлений в сфере компьютерной информации возникают ряд проблемных вопросов и сложностей, связанных в основном следующими факторами:

1. высокая латентность, достигающая по разным оценкам порядка 90%;
2. сложность сбора доказательств и процесса доказывания в суде ввиду отсутствия достаточной следственной практики;
3. широкий спектр криминалистически значимых признаков этих преступлений;
4. несовпадение места совершения противоправных действий и места наступления общественно опасных последствий [6];
5. механизм совершения скрыт от правоохранительных органов;
6. общественным мнением данный вид преступлений не рассматривается как серьезная угроза;
7. отсутствие четкой программы борьбы с компьютерными преступлениями;
8. сложность раскрытия компьютерных преступлений;
9. отсутствие достаточной следственной практики по расследованию компьютерных преступлений.

Специфика среды, а также способов совершения преступлений в сфере компьютерной информации, привели к тому, что сложившаяся система частных криминалистических теорий оказалась не способной удовлетворить потребности практики борьбы с преступлениями в новой сфере человеческой деятельности. В связи с этим, в последнее время весьма остро встал вопрос о разработке самостоятельной частной криминалистической теории расследования преступлений в сфере компьютерной информации.

В качестве основных проблем, препятствующих успешному решению вопросов выявления и расследования компьютерных преступлений, можно отметить:

1. возможность оперативного сокрытия преступником следов своей преступной деятельности по некоторым видам компьютерных преступлений [7];
2. сложность классификации деструктивных событий, происходящих в компьютерной системе;
3. проблемы организационного характера;
4. проблемы организационно-технического характера;
5. отсутствие единого подхода к описанию имевших место событий;
6. отсутствие действенной методики проведения первоначального этапа расследования по данному виду преступлений; проблемы международных (трансграничных) компьютерных преступлений [8].

В вопросах обеспечения информационной безопасности до сих пор существует широкий спектр проблем, требующих решения. Необходима работа, целью которой является формирование эффективного механизма реализации государственной политики в области обеспечения информационной безопасности в целом и борьбы с преступлениями в сфере компьютерной информации в частности.

Список литературы

1. Батурин Ю.М. Проблемы компьютерного права. – Москва: Юрид лит., 1991. – С. 35.
2. Викторов А.Ю. Секретные материалы оптом и в розницу // Независимая газета. 2008. № 65. С. 7.

3. Чудненко Ю.В. Обзор: ИТ в органах государственной власти 2013 (Алексей Мошков: «Ни одно преступление в сфере ИТ не останется безнаказанным») // CNews: Аналитика. 2014. №187. С. 12.
4. Осипенко К.Ю. Жертвы и последствия киберпреступлений NORTON REPORT 2013 // Information Security/ Информационная безопасность. 2013. №5. С. 25.
5. Поляков В.В. Об использовании новых понятий при доказывании преступлений в сфере компьютерной информации // Российская юридическая наука: состояние, проблемы, перспективы: матер. Всеросс. науч.-практ. конф., посвященной 45-летию юридического образования на Алтае, 19-20 сентября 2008. – Барнаул: Изд-во АлтГУ, 2008. С 427 - 431.
6. Поляков В.В. Особенности расследования неправомерного удаленного доступа к компьютерной информации: дис. канд. юрид. наук: 12.00.09. Омск, 2008. 247 с.
7. Поляков В.В. Программное обеспечение, используемое для совершения компьютерных преступлений // Ломоносовские чтения на Алтае–2013: матер. Междунар. молодежной школы-семинара (Барнаул, 5-8 ноября 2013 г.). – Барнаул: Изд-во Алт. ун-та, 2013. Ч. 2 . С. 15-17.
8. Мамедов Н.А. Криминалистические проблемы расследования преступлений в сфере компьютерной информации // Юрист. 2008. №9. С. 32.

АУТЕНТИФИКАЦИЯ КАК СРЕДСТВО ОБЕСПЕЧЕНИИЯ БЕЗОПАСНОСТИ СЕРВЕРОВ НА ОСНОВЕ ClearOS

А.А. Егораев, АлтГТУ, факультет информационных технологий, 4к.
Научный руководитель – ***Е.В. Шарлаев*****,** к.т.н., доцент.

В условиях современной реальности уже трудно представить какую-нибудь крупную компанию без сосредоточенного информационного управляющего ресурса – сервера, так как с каждым днем человек все более и более стремиться автоматизировать весь процесс своей работы. В офисах появляются множество компьютеров, нормальное функционирование которых без сервера представить сложно – растут вычислительные мощности, объемы

информации растут еще быстрее и обходиться без файлового сервера или же просто интернет шлюза очень сложно и зачастую просто неудобно.

На серверах храниться множество информации, цену которой порой невозможно рассчитать, поэтому деятельность по обеспечению безопасности сервера выходит на первое место, ведь чем дороже на серверах информация, тем больше находиться желающих, которые хотят ею обладать. На сегодняшний день используются множество серверов, которые исполняют глобальное количество сервисов и процессов и далеко не секрет что практически каждый сервис имеет ту или иную уязвимость и найти ее дело времени. Уязвимости находят даже в тех сервисах, где их совсем и не ждешь. Без своевременного реагирования и устранения проблем, являющихся следствием ошибочно порождаемого программного продукта, о безопасности системы можно забыть.

Сложно представить какие страшные последствия понесет компания, если на ресурсы ее сервера проникнет злоумышленник. К наиболее вероятностным способам для проникновения злоумышленника на вычислительные ресурсы относиться выполнение задач, которые являются следствием не декларированных возможностей различного ПО, присутствия программных закладок или результатом действия вирусного программного обеспечения. Одним из возможных решений в обеспечении безопасности сервера является применение собственных менеджеров процессов, которые позволяют разграничить их между пользователями, контролировать действия, назначать привилегии и права. Однако использование менеджера процессов без связки с двухфакторной аутентификацией [3] лишь немного затруднит и замедлит злоумышленника ведь количество эксплоитов и «дыр» растет и быть уверенным в том, что злоумышленник не сможет получить права суперпользователя, используя ту или иную «дыру» нельзя.

На сегодняшний день двухфакторная аутентификация используется довольно часто в WEB сфере, но при удаленном доступе к данным сервера этот механизм защиты до сих пор является редкостью и, как правило, ограничивается лишь использованием электронных замков и Е-токенов.

Целью настоящего исследования является поиск наиболее безопасного соединения с удаленным сервером. В качестве объекта исследования выбрана вычислительная сеть на основе сервер на

базе ClearOS с внешним подключением по SSH протоколу[1], т.е. использующее в качестве подключения клиента к серверу 22-ой программный порт.

Для начала необходимо сделать так, чтобы сервер при попытке подключения к нему клиента выглядел как обычный сервер, это поможет завести злоумышленника в заблуждение. Так же необходимо настроить подключение по SSH на контроль количества попыток ввода пароля, предпочтительно три раза, после чего отбрасываются все попытки соединения с сервером, при этом необходимость занести ip-адресс устройства клиента, который пытался инициировать соединение в так называемый «бан лист» (черный список) на один час, что обезопасит от использования «брут перебора» неопытных атакующих и замедлит опытных, так как вызовет у них необходимость в использовании дополнительных промежуточных узлов составной сети, например прокси-серверов, для автоматизации и анализа каким образом сервер-цель сбрасывает соединение. Для усиления защитных механизмов также необходимо установить ограничение на количества одновременно подключенных клиентов. После применения данных настроек можно оставить конфигурирование SSH-параметров и перейти ко второй стадии защиты.

Вторым фактором усиленной аутоинтефикации[2] является применение генерации случайных символов, а именно 6 символов. Программа реализована на языке C# с применением Mono. Это позволило реализовать универсальное приложение, которое можно использовать как на Unix платформах, так и на других. Приложение основано на клиент-серверной технологии. Серверная часть располагается непосредственно на самом сервере и работает как сервис, при ее запуске в конфигурационный файл записываются все запущенные приложения и закрывается к ним доступ ровно до того момента как сервис не пропустит к ним. Это позволяет оградить злоумышленника от интересующих файлов и ввести в легкое недоумение - ведь только что у него появилось окно приветствия подключения по SSH, а вслед за ним окно с 6 символами и окном ввода информации.

Рассмотрим работу серверной части поподробнее. Когда клиент подключается к серверу и проходит аутентификацию SSH, происходит генерация случайных символов, с комбинацией различных алгоритмов. Желательно использование не одного алго-

ритма генерации, а нескольких, в зависимости от времени или дня недели, например. День недели на мой взгляд намного лучше нежели время, так как его можно использовать как еще один символ, то есть у нас высвечивается на сервере окно с 6 символами плюс один скрытый который мы будем вводить после третьего видимого символа на нашем клиенте, при генерации кода на сервере это пройдет автоматически.

Обратим внимание на использование клиентского модуля. Клиентская часть используется как на Unix, так на Windows, но есть необходимость иногда подключиться к серверу моментально, используя, например, смартфон, поэтому клиентская часть адаптируется под андроид. Алгоритм работы клиентской части очень прост. Запускаем клиентскую часть, видим окно ввода, вводим в поля символы, которые представил нам сервер и не забываем, что после третьего символа должен идти символ, отвечающий за день недели, после чего клиентская часть выдает нам с генерированный по этим данным ключ для подключения. Вводим его в окно на сервере и получаем после этого доступ ко всем функциям системы. Подобрать такой с генерированный пароль довольно сложно, но все же лучше сделать следующее: ограничить количество попыток ввода двумя, после второй, неправильной попытки, будет происходить разрыв соединения с сервером и клиенту придется заново осуществлять подключение и аутентификацию по SSH, при этом вновь произведётся генерация пароля уже нового, что сделает перебор невозможным

Данный способ прохождения аутентификации не делает сервер полностью безопасным, но он усложняет действия злоумышленников. А так как используется помимо двухфакторной аутентификации еще и менеджер процессов, то злоумышленнику придется потратить много времени и сил, чтобы проникнуть и получить нужные ему файлы.

Список литературы

1. Настройка сервера SSH (теория и практика). [Электронный ресурс]. – Режим доступа: http://www.nixp.ru/articles/Настройка-сервера-SSH-(теория-и-практика).html
2. Контроль доступа (информатика) / Материал из Википедии – свободной энциклопедии, [Электронный ресурс]. – Режим до-

ступа: http://ru.wikipedia.org/wiki/Контроль_доступа (информатика)/
3. Что такое двухфакторная аутентификация. Юрий Медяков 14.01.2014 / [Электронный ресурс]. – Режим доступа: https://cryptostore.ru/article/obzory/chto_takoe_dvukhfaktornaya_autentifikatsiya/

ПРИМЕНЕНИЕ DATA LOSS PREVENTION ТЕХНОЛОГИЙ ДЛЯ ЗАЩИТЫ ОТ ИНСАЙДЕРСКИХ УГРОЗ

И.А. Красников, АлтГТУ, факультет информационных технологий, 5 к.
Научный руководитель – ***Е.В. Шарлаев***, к.т.н., доцент.

Распространение информационных технологий и тенденция подключения государственных информационных систем (ГИС) к информационно-телекомуникационным сетям общего пользования являются порождающим фактором увеличения риска реализации инсайдерских угроз информационной безопасности организаций. Согласно нормативно-правовым актам (НПА) в области обеспечения защиты информации в ГИС, таких как ФЗ №152 «О персональных данных», Постановление правительства 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Указ Президента РФ от 17.03.2008 N 351 "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена", Приказ ФТЭК от 13.02.2013 №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», Приказ ФСТЭК 18.02.13 №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и Руководящие документы ФСТЭК, необходимо использование сертифицированных по требованиям безопасности средств защиты информации. Делая акцент на увеличение количества утечек конфиденциальной информации в сеть, следует предпринимать своевременные меры по нейтрализации

данного типа угроз посредством разработки, внедрения и эксплуатации DLP – систем. Использование данной технологии в совокупности с профессиональной настройкой системы, опираясь на перечень сведений конфиденциального характера, выполненной по требованиям НПА, позволяет сократить уровень риска утечки КИ до приемлемого уровня и существенно упростить технические мероприятия по расследованию возможных инцидентов.

Предотвращение утечек (Data Loss Prevention, DLP) – технологии предотвращения утечек конфиденциальной информации из информационной системы вовне, а также технические устройства (программные или программно-аппаратные) для такого предотвращения утечек [4]. DLP-системы строятся на анализе потоков данных, пересекающих периметр защищаемой информационной системы. При детектировании в этом потоке конфиденциальной информации срабатывает активная компонента системы, и передача сообщения (пакета, потока, сессии) блокируется. Распознавание конфиденциальной информации в DLP-системах производится двумя способами: анализом формальных признаков (например, грифа документа, специально введённых меток, сравнением хэш-функции) и анализом контента.

К основным задачам DLP – систем относятся следующие:

1. предотвращение передачи конфиденциальной информации за пределы информационной системы;
2. архивирование пересылаемых сообщений на случай возможных в будущем расследований инцидентов;
3. выявление инсайдеров внутри компании;
4. повышение эффективности работы отдела по защите информации;
5. предотвращение передачи нежелательной информации не только изнутри наружу, но и снаружи внутрь информационной системы;
6. оптимизация загрузки каналов, экономия трафика;
7. контроль присутствия работников на рабочем месте;
8. отслеживание благонадёжности сотрудников.

Основными методами детектирования конфиденциальной информации являются:

1. Сигнатуры – поиск в потоке данных некоторой последовательности символов. Достоинство: простота пополнения

словаря запрещённых терминов. Недостаток: лингвистическое разнообразие словесных форм.

2. Цифровые отпечатки – детектирование на основе хэшей шаблонов. Достоинство: простота добавления новых шаблонов, высокую степень детектирования и прозрачность алгоритма технологии для сотрудников подразделений по защите информации. Недостаток: необходимость постоянного обновления базы данных «цифровых отпечатков».
3. Метки – расстановка специальных «меток» внутри файлов. Достоинство: высокое качество детектирования. Недостаток: значительная перестройка инфраструктуры внутри сети и введение множества новых правил и форматов файлов для пользователей.
4. Регулярные выражения – нахождение совпадения по форме данных. Достоинства: позволяют детектировать специфичный для каждой организации тип контента. Недостаток: ограниченная сфера применения в рамках DLP – систем и невозможность применения независимо от других технологий.
5. Лингвистические методы – основаны на лингвистическом анализе текста. Достоинства: высокая степень эффективности при намного меньших трудозатратах на внедрение и поддержку. Недостаток: зависимость от языка.
6. Ручное детектирование – фильтрация контента специалистом по защите информации. Достоинства: высокое качество детектирования. Недостаток: ограниченный объём контента.

Современные DLP – системы имеют следующие функции:

1. Контроль доступа к устройствам и интерфейсам. Обеспечение контроля доступа пользователей и групп к портам ввода-вывода, адаптерам WiFi и Bluetooth, любым типам принтеров, мобильным устройствам и дисководам.
2. Контроль сетевых коммуникаций. Обеспечение детектирования коммуникационных приложений и их селективную блокировку.
3. Мониторинг и фильтрация трафика. Информация анализируется на предмет соответствия корпоративным политикам безопасности.

4. Централизованное управление. Полная интеграция централизованного управления в групповые политики Windows.
5. Контроль по типу файлов. Разрешение и запрет доступа к определенным типам файлов.
6. Контроль буфера обмена. Предотвращение утечки данных при намеренном или случайном копировании между различными приложениями и документами через встроенный в ОС Windows буфер обмена.
7. Межсетевое экранирование.
8. Белый список носителей и сетевых протоколов. Для каждого пользователя или группы можно задать свой "белый" список, доступ к которым будет всегда разрешен.
9. Аудит. Протоколирование всех действий пользователей с устройствами и файлами.
10. Централизованное хранение журналов аудита и теневого копирования.

В качестве объектов сравнительного анализа были взяты три DLP - системы российских разработчиков: DeviceLock, InfoWatch Traffic Monitor Enterprise и Дозор Джет.

Для проведения сравнительного анализа DLP - систем были выбраны следующие критерии: [5]

1. Позиционирование системы на рынке.
2. Системные требования.
3. Используемые технологии детектирования.
4. Контролируемые каналы передачи данных.
5. Возможности контроля подключаемых внешних устройств.
6. Мониторинг агентов и их защита.
7. Управление системой и обработка инцидентов.
8. Отчетность.
9. Интеграция с решениями сторонних производителей.

Рассмотренные DLP – системы полностью удовлетворяют требованиям российского законодательства и имеют идентичные функциональные возможности по основным критериям анализа. Ключевым фактором выбора средства защиты информации является наличие свободно распространяемой полнофункциональной демонстрационной версии, так как разработка и внедрение проекта системы защиты от утечки конфиденциальной информации будет реализовано в виртуальной среде. Услуга по предоставлению де-

мо-версий доступна только для продуктовой линейки DeviceLock 7 Endpoint DLP Suite. При последующем внедрении проекта в автоматизированную информационную систему важным элементом является стоимость DLP – системы. Очевидное преимущество комплекса DeviceLock заключается в возможности активации лицензий только на необходимые компоненты в зависимости от потребностей организации.

Методика внедрения и эксплуатации DLP – системы имеет следующие этапы:

1. определение целей и задач DLP;
2. классификация данных;
3. определение рисков и каналов утечки данных;
4. разработка политик безопасности;
5. определение компонентов необходимых для построения DLP;
6. определение областей реорганизации существующей структуры сети;
7. техническое внедрение системы;
8. определение необходимых настроек DLP;
9. тестирование;
10. осуществление управления и отчётности.

Проанализировав функционал DLP – систем, можно сделать вывод о том, что данная технология обладает высокой эффективностью и имеет перспективы развития. Становится очевидно, что блокирование доступа в интернет является нерациональным способом ограждения информационных систем от существующих угроз, так как это влечёт за собой усложнение или полный отказ информационного взаимодействия посредством телекоммуникационных сетей общего пользования. Поэтому DLP – системы становятся необходимым элементом в системе защиты информационных систем и используются в совокупности с СЗИ от НСД, МЭ и антивирусными средствами.

Список литературы

1. INFOWATCH TRAFFIC MONITOR ENTERPRISE «Естественное и искусственное освещение» [Электронный ресурс]. – Режим доступа: http://www.infowatch.ru/products/ traffic_ monitor_enterprise/

2. Комплекс защиты от утечек информации Дозор Джет [Электронный ресурс]. – Режим доступа: http://www.dozor-jet.ru/
3. DeviceLock защита от инсайдеров [Электронный ресурс]. – Режим доступа: http://www.devicelock.com/ru/
4. DLP – Википедия [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org/wiki/DLP
5. Сравнение систем защиты от утечек [Электронный ресурс]. – Режим доступа: http://www.anti-malware.ru/comparisons/data_leak_protection_2014_part1

ОСОБЕННОСТИ ПОСТРОЕНИЯ СЕЛЕКТИВНЫХ МЕТАЛЛОДЕТЕКТОРОВ НА ОСНОВЕ МИКРОКОНТРОЛЛЕРА

А.Ю. Лаптев, АлтГУ, физико-технический факультет, 5 к.
Научный руководитель – ***А.В. Егоров,*** к.ф.-м.н., доцент.

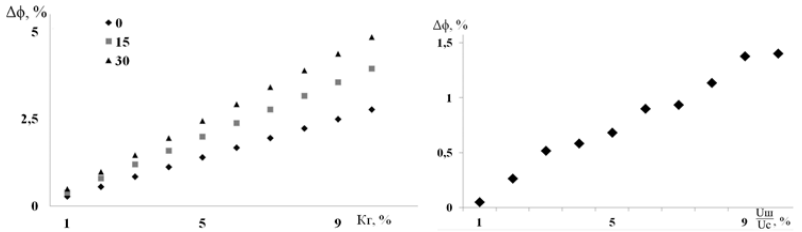
Рост числа объектов информатизации, обрабатывающих и хранящих конфиденциальные данные, ставит жесткие требования к комплексному подходу обеспечения информационной безопасности. Важную роль в решении этой задачи играют различные технические средства, позволяющие выявлять несанкционированные устройства для съема информации [1]. Эффективность такого обнаружения зависит не только от методов измерений, но и от алгоритмов обработки сигналов, регистрируемых измерительными датчиками. В селективных поисковых системах, как правило, приходится определять параметры гармонических сигналов. При этом полезную информацию, как правило, несут не абсолютные значения сигнала, а их небольшие изменения. Из существующих методов обработки широкое применение нашли цифровые методы, использующие аппроксимацию мгновенных значений сигнала исходной модельной функцией. При реализации данного подхода приходится накапливать сумму произведений мгновенных значений сигнала на значения тригонометрических функций, что предъявляет повышенные требования к производительности микроконтроллеров. В настоящей работе для определения комплексной амплитуды гармонического сигнала использовали функции Уолша [2], что позволило существенно снизить вычислительную нагрузку на микроконтроллер без ухудшения точности измерений.

Мгновенные значения сигнала аппроксимировали линейной комбинацией трех первых функций Уолша (1):

$$y(x) = b0\,\mathrm{wal}(0,x) + b1\,\mathrm{wal}(1,x) + b2\,\mathrm{wal}(2,x), \quad (1)$$

где $x=t/T$ – относительное время, T – период сигнала. Такой ряд очень грубо описывает гармонический сигнал [3], но его коэффициенты содержат всю необходимую информацию об определяемых параметрах. При расчетах функции Уолша принимали значения либо +1, либо -1, благодаря чему операция умножения свелась к смене знака при сложении.

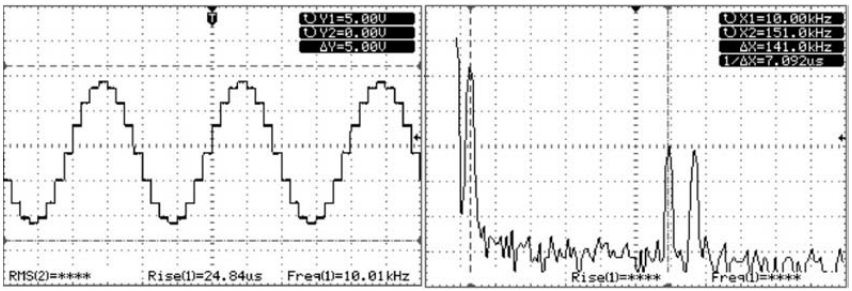
Для оценки влияния коэффициента гармоник с различной начальной фазой (рис1. а) и белого шума (Рис1. б) на точность определения фазы, был создан виртуальный прибор в среде графического программирования LabView. По результатам эксперимента было установлено, что основную погрешность вносит третья гармоника.



а) *б)*

Рис. 1. Влияние различных факторов на погрешность определения начальной фазы.
а) Влияние третьей гармоники б) Влияние уровня белого шума

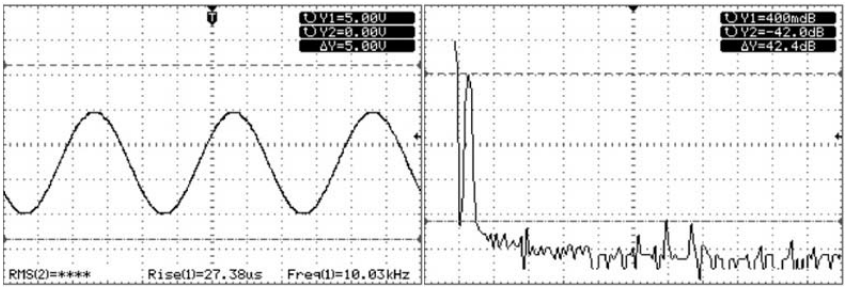
Для генерации синусоидального сигнала создан генератор на делителе напряжения с переменными плечами. Такое решение позволяет генерировать сигнал в широком диапазоне частот без использования расчетных таблиц и дополнительных расчетов в реальном времени, но получаемый сигнал имеет высокий коэффициент гармоник, что демонстрирует рис 2.



а) *б)*

Рис. 2. а) Генерируемый сигнал; б) Спектр сигнала

Для уменьшения уровня высших гармоник необходимо применить фильтр низких частот. Для обеспечения работы генератора в широком диапазоне частот был использован переключаемый фильтр низких частот на мультиплексоре, позволяющий коммутировать сигнал между несколькими фильтрами низкой частоты с различной частотой среза. Коэффициент 15 и 17 гармоник после прохождения фильтра становится меньше 1% (Рис 3), что удовлетворяет требованиям, предъявляемым к генератору сигнала.



а) *б)*

Рис. 3. а) Сигнал после фильтра низких частот б) Спектр сигнала

Используя полученное оборудование и программное обеспечение для микроконтроллера и персонального компьютера, было создано устройство, измеряющее индуктивность и активное сопротивление датчика на разных частотах. Результат работы прибора можно отобразить на годографе (рис.4). По оси абсцисс откла-

дывается отношение внесенного активного сопротивления к реактивному сопротивлению датчика без образца (X_0), по оси ординат откладывается отношение внесенного реактивного сопротивления к X_0.

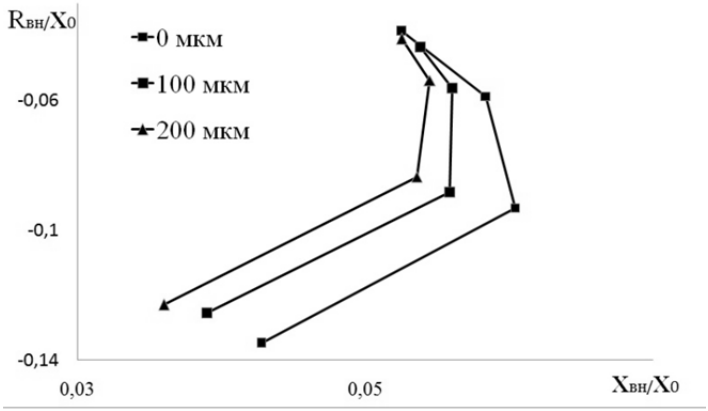


Рис. 4. Результат работы прибора с различным расстоянием до образца.

Измерения проводились на частоте 300, 500, 1000 и 3000 герц. Конструктивные особенности прибора позволяют увеличить количество используемых частот. Полученные прибором данные ОВ могут быть классифицированы при помощи методов многомерного анализа данных [4] и для определения магнитной и электрической проводимости [5]. Результаты работы могут быть использованы при создании портативных селективных поисковых систем на основе микроконтроллеров, анализирующих параметры синусоидальных сигналов при наличии помех.

Список литературы

1. Зайцев, А.П. Технические средства и методы защиты информации: Учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: Машиностроение, 2009.

2. Залманзон Л.А. Преобразования Фурье, Уолша, Хаара и их применение в управлении, связи и других областях. / Л.А. Залманзон. – М.: Наука, 1989. – 496 с.
3. Егоров А.В., Поляков В.В., Лаптев А.Ю., Игнатов А.В., Метод обработки сигналов в детекторах обнаружения устройств несанкционированного съема информации // Доклады V Пленума СибРОУМО по образованию в области информационной безопасности и XIII конференции: Томск – Новосибирск, 5–9 июня 2012г. – Томск: В – Спектр, 2012. – с.102-102.
4. Егоров А.В., Парфенова А.В., Применение методов многомерного анализа для интерпретации результатов вихретокового контроля пористых металлических предметов //Известия АлтГУ. – 2011. – №1
5. Поляков В.В., Егоров А.В., Вихретоковой контроль удельной электрической проводимости и магнитной проницаемости изделий из магнитомягких материалов //Дефектоскопия. -1992. – №12

ОПЕРАТИВНО-РОЗЫСКНАЯ ДЕЯТЕЛЬНОСТЬ В СЕТИ ИНТЕРНЕТ КАК СРЕДСТВО ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ПРЕДУПРЕЖДЕНИЯ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

А.С. Мананников, АлтГУ, юридический факультет, 4 к.
Научные руководители **– *В.А. Мазуров*,** к.ю.н., доцент,
***В.В. Поляков*,** к.ю.н., доцент.

XXI век - век информационных технологий, которые динамично развиваются и способствуют улучшению жизнедеятельности общества.

Несмотря на многочисленные преимущества современных компьютерных технологий, они создали новые условия, которые содействуют совершению преступлений на национальном и международном уровнях. [1] Доходы преступников, связанные с незаконным использованием новейших технологий, занимают третье место в мире после доходов от торговли наркотиками и оружием.

В настоящее время усматривается неуклонный рост числа компьютерных преступлений. По данным статистики, за первое

полугодие 2012 года в России было зафиксировано 5696 киберпреступлений, что почти на 11 % больше, чем в аналогичном периоде 2011 года. [2] Стоит отметить, что на сегодняшний день тенденция роста сохраняется.

При этом очевидно, что данная статистика отражает лишь зарегистрированные преступления, но с учетом высокого уровня латентности рассматриваемой категории преступлений, их может быть в разы больше.

По оценкам экспертов, латентность компьютерных преступлений в США достигает 80%, в Великобритании – 85%, в ФРГ – 75%, в России – более 90%. [3]

Отмечается, усиление организованности криминальных структур, использующих возможности Интернета для осуществления преступной деятельности. Такие структуры все чаще применяют методы конспирации, совершенствуют способы сокрытия следов преступлений, пытаются получить доступ к информационным системам правоохранительных органов, спецслужб, органов государственной власти. [4] Тем самым подрывается информационная безопасность государства.

Учитывая неуклонный рост компьютерных преступлений и возможные тяжкие последствия от их совершения, необходимо искать новые пути развития, способные обеспечить более эффективную борьбу с рассматриваемыми общественно-опасными деяниями и лицами, их совершающими.

В этой связи, считаем, что наиболее действенным и первостепенным средством правового обеспечения информационной безопасности и предупреждения компьютерных преступлений является оперативно-розыскная деятельность (далее – ОРД).

Объективная необходимость ОРД изначально предопределена самим существованием преступности, что с неизбежностью подтверждается многовековым историческим и современным опытом развития правоохранительной системы. Ее роль и социальная значимость обусловливается широкими потенциальными возможностями использования результатов в решении различных задач, в том числе и задач уголовного судопроизводства. [5]

В настоящее время Интернет необходимо позиционировать не только как систему телекоммуникаций, допускающую снятие информации с технических каналов связи, но и как место осу-

ществление ОРД. Борьба с преступностью в сети Интернет уже невозможна без применения оперативно-розыскных сил, средств и методов.

Эффективное осуществление оперативно-розыскных мероприятий (далее - ОРМ), в сетевом пространстве невозможно без корректировки методов ОРД. Необходимость модернизации ОРД в данном случае, вызвана уникальностью сетевого пространства, которая заключается в том, что преступления в сети, могут совершаться различными нетипичными способами, в том числе:

1. удаленно (совершение действий, при которых воздействие осуществляется на информационный объект, находящийся на значительном расстоянии или не имеющий физической привязки к конкретному месту); [6]
2. динамически (выполнение действий с помощью мобильных устройств, при перемещении их оператора в физическом пространстве);
3. трансгранично (преступное действие выполняется в одном государстве, общественно-опасные последствия наступают в другом, при этом физического пересечения преступником границ государства не происходит).

При осуществлении определенных ОРМ в сети Интернет (опрос, оперативное внедрение, оперативный эксперимент и др.) для оперативного сотрудника важным является понимание субкультуры хакерского сообщества, включающей взгляды его участников, их привычки, стереотипы поведения, нормы общения. Получение необходимых знаний возможно в процессе наблюдения за местами сетевого общения хакеров, где происходит взаимное согласование мнений, вырабатываются суждения о моральных ценностях, осуществляется обмен криминальным опытом и сведениями о потенциальных жертвах, обсуждаются способы противодействия правоохранительным органам. [7]

На наш взгляд, наблюдение за местами сетевого общения хакеров может осуществляться самим оперативным работником или же путем привлечения к данной деятельности конфидентов. В случае если наблюдение дает положительные результаты, то необходимо незамедлительно брать под контроль выявленные хакерские сайты и форумы для дальнейшего получения ценной оперативной информации (интернет адреса посетителей; характер и сте-

пень их активности; сведения о совершенных или готовящихся преступлениях).

Помимо этого, для обеспечения информационной безопасности и предупреждения преступлений в сфере высоких технологий оперативным сотрудникам надлежит в рамках реализации главы IV ФЗ об ОРД [8] привлекать граждан к содействию ОРД. При этом стоит отметить, что особенности сетевого пространства предполагают специфичные формы привлечения граждан к содействию ОРД. Используя сеть Интернет, граждане могут содействовать ОРД путем заполнения на специализированных сайтах форм сообщений о совершенных или готовящихся преступлениях, о потенциальных преступниках, их связях и т.п. (аналог телефона доверия).

Вместе с тем, считаем, что повысить эффективность ОРД в рассматриваемом направлении может проведение опроса в электронной форме.

Из тактических соображений предпочтение стоит отдавать легендированной форме опроса, при которой оперативный сотрудник скрывает свои истинные цели и профессиональную принадлежность. При осуществлении указанных ОРМ возможно выявление лиц, готовых оказывать содействие оперативно-розыскным органам (далее – ОРО) на конфиденциальной основе. При наличии признаков достаточной осведомленности таких лиц важным становится укрепление доверительных отношений с ними и выход на непосредственное общение. Привлечение граждан к содействию ОРО позволяет не только получать достоверную информацию о состоянии оперативной обстановки на контролируемых сетевых объектах, но и изучать способы совершения и сокрытия следов сетевых компьютерных преступлений, ранее не встречавшихся в оперативно-розыскной практике. [9]

Вместе с тем, в ОРД в области расследования компьютерных преступлений целесообразно применять криминологическое прогнозирование индивидуального и группового преступного поведения. Определенную информацию можно извлечь, анализируя сетевой трафик локальных и региональных компьютерных сетей. Прогнозирование может успешно осуществляться в основе первичных материалов оперативного учета, так как его банки информации создаются на основе прогноза вероятности преступного по-

ведения определенных криминогенных контингентов. Именно прошлое (судимость, правонарушения, антиобщественные поступки, большие успехи в области программирования), настоящее (поддержание криминальных связей, склонность к антиобщественным занятиям) дают основания для прогностических выводов о вероятном противоправном поведении в будущем. Принимаются во внимание социальные оценки, даваемые лицу, представляющему оперативный интерес, роль для него мнения представителей криминогенной и преступной среды. Все это в совокупности является элементами методики криминологического прогнозирования, которое вплетается в оперативно-розыскные мероприятия при реализации форм ОРД (поиске, профилактике, разработке). Естественно, вопросы моделирования и прогнозирования необходимо решать, используя современные информационные технологии и программные средства.

Резюмируя, стоит отметить, что на наш взгляд реализация предложенных рекомендаций и мер поспособствует развитию информационной безопасности и в должной мере будет осуществлена как общая, так и частная превенция компьютерных преступлений.

Список литературы

1. Поляков, В.В. Обстановка совершения преступлений в сфере компьютерной информации как элемент криминалистической характеристики / В.В. Поляков // Известия Алтайского государственного университета. – 2013. – № 2. – С. 114 - 116.
2. 30 сентября – День Интернета в России [Электронный ресурс] // Официальный сайт Министерства внутренних дел Российской Федерации. – Режим доступа: http://mvd.ru/news/item/146788/. – Загл. с экрана.
3. Мазуров В.А. Преступность в сфере высоких технологий: Понятие, общая характеристика, тенденции // Вестник Томского государственного университета. 2007. № 300-1. С. 153.
4. Поляков, В.В. Анализ высокотехнологичных способов неправомерного удаленного доступа к компьютерной информации / В.В. Поляков, С.М. Слободян // Известия Томского политехнического университета. – 2007. – Т. 310, № 1. – С. 212 – 216.

5. Маркушин А.Г. Оперативно-розыскная деятельность. Москва: Изд-во Юрайт, 2013. С. 13-14.
6. Поляков, В.В. Особенности расследования неправомерного удаленного доступа к компьютерной информации: автореф. дис. … канд. юрид. наук: 12.00.09 / В.В. Поляков. – Омск, 2008. – 28 с.
7. Горянинов К.К., Овчинский В.С., Синилов Г.К. Теория оперативно-розыскной деятельности. Москва: Изд-во ИНФРА-М, 2014. С. 328.
8. Федеральный закон от 12.08.1995 N 144-ФЗ (ред. от 21.12.2013) Об оперативно-розыскной деятельности // Собрание законодательства РФ. 14.08.1995. N 33. ст. 3349.
9. Горянинов К.К., Овчинский В.С., Синилов Г.К. Теория оперативно-розыскной деятельности. Москва: Изд-во ИНФРА-М, 2014. С. 335.

ГЕНЕРАЦИЯ ПАКЕТОВ С ПРОИЗВОЛЬНЫМ СОДЕРЖИМЫМ

К.Ю. Манзюк, АлтГУ, физико-технический факультет, 3 к.
Научный руководитель – ***А.В. Мансуров,*** к.т.н., доцент.

Задача генерации кадров/пакетов сетевого обмена с произвольным содержимым является достаточно актуальной как для вопросов исследования механизмов безопасности сетевого обмена и безопасности сетевых сервисов, так и для практического изучения принципов безопасной работы сетевых сервисов в условиях учебной лаборатории ФТФ. Данное исследование предполагает изучение принципов формирования сетевых кадров/пакетов с произвольной нагрузкой и последующую разработку приложения, специализированного на учебном лабораторном применении при выполнении лабораторных работ в учебной лаборатории безопасности информационных сетей.

Существующие программные средства генерации пакетов с произвольным содержимым являются либо излишне сложными, либо, наоборот, слишком простыми и непригодными для простого решения возникающих задач. Немаловажный аспект — это простой интерфейс, возможность модификации заголовков протоко-

лов начиная с 2го уровня в рамках 7уровневой модели ОСИ, наличие шаблонов для заполнения пакетов под конкретные задачи, бесплатность ПО. Очевидно, что рациональнее подойти к этому вопросу в виде разработки собственного приложения, отвечающего поставленным требованиям.

Структура разработанного в рамках исследования генератора кадров/пакетов с произвольной полезной нагрузкой выглядит следующим образом — интерфейс программы с возможностью модифицировать и управлять параметрами полезной нагрузки на различных уровнях (от 2 до 7), модуль формирования полезной нагрузки в виде стека различных популярных сетевых протоколов + поддержка шаблонов для выполнения действий по быстрому формированию полезной нагрузки, модуль взаимодействия с драйвером сетевого устройства (посредством ядра ОС или специальной библиотеки) для отправки сформированного кадра/пакета.

Графический интерфейс реализован при помощи библиотек Qt. Модуль по формированию полезной нагрузки реализован на языке C. Набор шаблонов динамически расширяется путем добавления новых. В настоящее время реализованы шаблоны для генерации произвольной полезной нагрузки ARP-ответа и DNS-ответа, что является достаточным для осуществления популярных сетевых атак «man in the middle», связанной с преднамеренной модификацией злоумышленником ARP- и DNS-кешей компьютеров, работающих в локальной сети.

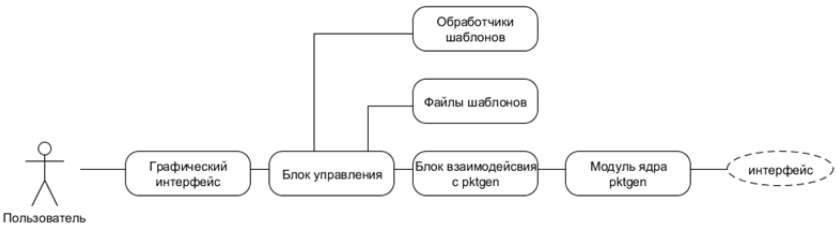


Рис. 1. Структура разработанного программного решения в нотации UML.

Модуль взаимодействия с драйвером сетевого устройства использует специальные RAW-сокеты для отправки сформированного набора данных непосредственно в сетевое устройство для дальнейшей передачи по сети. Также модуль поддерживает работу

со специализированным модулем ядра ОС Линукс — pktgen, который используется для генерации трафика. После запуска модуль pktgen, создает поток ядра и привязывает его к CPU, к потоку привязываются устройства через которые будет проходит сгенерированный, такие как /dev/eth[0], /dev/vlan[]. Соответственно 1 CPU — 1 поток, 2 CPU — 2 потока и так далее. К каждому CPU можно привязать несколько устройств, с разными настройками, что дает необходимую гибкость в управлении генератором.

Разрабатываемый генератор пакетов с шаблоном формирования ARP-ответа является удобным средством для изучения популярной модельной атаки «man in the middle», когда происходит подделка ARP-ответов и внесение искаженной информации в ARP-таблицы устройств, обмен между которыми необходимо перехватить. Каждый компьютер составляет свою ARP-таблицу, которую затем использует для преобразования IP адресов в Ethernet адреса. Для этого посылается широковещательный ARP-запрос в сеть (тут будет кадр презентации с примерным видом запроса). Его можно интерпретировать следующим образом: "Если ваш IP-адрес совпадает с указанным, то сообщите мне ваш Ethernet-адрес". Все сетевые устройства получают этот запрос и, если указанный IP-адрес совпадает со своим, то создается ARP-ответ (кадр с ответом). Суть атаки «man in the middle» заключается в том, что при получении ARP-запроса он А к В дать корректный ARP-ответ, «представившись» В, аналогично проделать при ARP-запросе от В к А. Таким образом все общение между А и В будет осуществляться через «человека по середине».

Генератор нам нужен для того, чтобы сформировать ARP-ответ и отправить его в сеть.

Возможность подключения дополнительных шаблонов позволит выполнять более сложные сетевые атаки, связанные с подменой и отправкой искаженной информации в сетевой обмен атакуемых целей. Кроме этого, данный генератор является потенциально ценным инструментом для исследования эффективности работы средств защиты и безопасности локальных корпоративных сетей, протоколов безопасного обмена между сетевыми службами.

Список литературы

1. Столлингс В. Современные компьютерные сети: пер. с англ. СПб. Питер, 2003. 783 с. (Сер. "Классика computer science").

2. Таненбаум Э. Компьютерные сети: пер. с англ. СПб. Питер, 2003. 992 с. (Сер. "Классика computerscience").
3. Иванов И.П., Бойченко М.К. Мониторинг ресурсов узлов корпоративной сети // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение. 2010. № 2. С. 114‑120.

РАЗРАБОТКА ГЕНЕРАТОРА РЕЧЕПОДОБНОЙ ПОМЕХИ В ПРОГРАММНОЙ СРЕДЕ LABVIEW

Я.И. Грачева, АлтГУ, физико-технический факультет, 5 к.
Научный руководитель – ***А.В. Егоров,*** к.ф.-м.н., доцент.

Человеческий разговор, и в частности переговоры, остается важнейшим каналом информационного взаимодействия. Очень часто развитие и введение в эксплуатацию новых систем связи сосредоточено на совершенствование именно этого метода общения. Одновременно усиливается потребность в обеспечении конфиденциальности речевого обмена и защите информации, имеющей речевую природу [1]. В настоящий момент разработан достаточно широкий арсенал различных средств защиты (формальных и неформальных), которые могут обеспечить требуемый уровень защищенности разного рода информации, в том числе и речевой. Из существующих методов защиты речевого сигнала широкое применение нашли методы активной акустической маскировки. В частности в целях данной маскировки используют такие виды помех как белый шум и «речеподобная» помеха.

В настоящей работе был разработан виртуальный прибор, позволяющий генерировать практически любую помеху в зависимости от выбранных параметров и базы файлов. Существует возможность его применения в учебных целях. Прибор создан в среде графического программирования, которая широко используется в промышленности, образовании и научно-исследовательских лабораториях в качестве стандартного инструмента для сбора данных и управления приборами. LabVIEW - мощная и гибкая программная среда, применяемая для проведения измерений и анализа полученных данных [2].

В системах акустической и виброакустической маскировки, как правило, используются шумовые помехи следующих видов: "белый" шум (с постоянной спектральной плотностью в рече-

вом диапазоне частот); "розовый" шум (с тенденцией спада спектральной плотности 3 дБ на октаву в сторону высоких частот); шум с тенденцией спада спектральной плотности 6 дБ на октаву в сторону высоких частот; шумовая "речеподобная" помеха (с огибающей амплитудного спектра, подобной речевому сигналу) [3].

Для исследования эффективности защиты акустического канала связи использовались помехи: белый шум, «речеподобная» типа речевой хор и комбинированная «речеподобная». Для проведения испытаний: в программе Audacity был сгенерирован белый шум; так же в программе Audacity была сформирована «речеподобная» помеха типа речевой хор, методом наложения нескольких звуковых файлов (музыкальный фрагмент, женская, мужская, смешанная речь); в среде разработки LabVIEW был создан виртуальный прибор, генерирующий комбинированную «речеподобную» помеху (рис.1.).

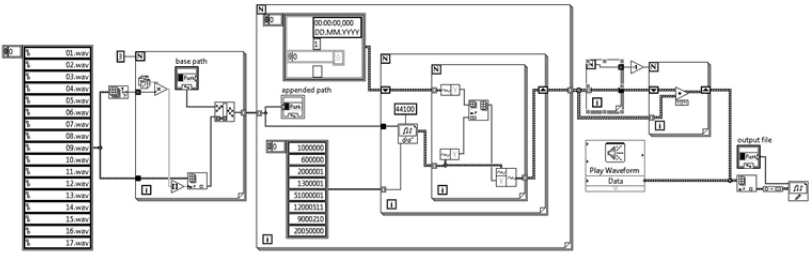


Рис. 1. Блок-схема виртуального прибора генерации речеподобной помехи.

На вход прибора подавалась библиотека из двадцати файлов, состоящая из звуков речи в диапазоне звучания от 90 до 1000 Гц. При смешивании наиболее приемлемым для слуха количеством являются три файла, они выбирались из библиотеки случайным образом, во избежание вырезания одинаковых участков. Далее в каждом файле бралось определенное количество различных его участков по одной секунде. На следующем шаге все файлы накладывались друг на друга. На выходе воспроизводилась и записывалась получившаяся комбинированная «речеподобная» помеха.

Для оценки защищенности канала был использован артикуляционный метод совместно с методом измерения разборчивости по эквиваленту затухания. Артикуляционные испытания эффективно-

сти помехи были реализованы с помощью программы Audacity. Испытания проводила бригада операторов в составе одного диктора, не имеющего явных дефектов речи, и тридцати аудиторов в возрасте от 18 до 51 года, не имеющих дефектов слуха. При подготовке к проведению измерений была осуществлена запись тестового речевого текста (артикуляционных таблиц слов), читаемого диктором. Каждая таблица содержала 10 слов. Диктором было записано 10 таблиц. На них были независимо наложены: сгенерированный в программе Audacity белый шум; сформированная программе Audacity «речеподобная» помеха типа речевой хор; сгенерированная в приборе комбинированная «речеподобная» помеха. Наложение шума происходило в диапазоне [-35; 10] дБ с градацией в 5 дБ.

Проанализировав полученные данные, был получен график зависимости словесной разборчивости от интегрального отношения сигнал/шум (рис. 2.). По оси абсцисс расположен исходный уровень шума в дБ, а по оси ординат словесная разборчивость в процентах.

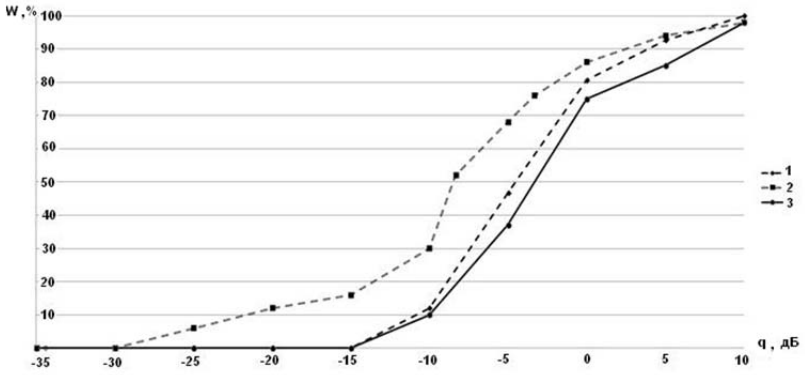


Рис. 2. График зависимости словесной разборчивости W (%) от интегрального отношения сигнал/шум q (дБ) (1 – сигнал + речеподобная помеха типа речевой хор; 2 – сигнал + белый шум; 3 – сигнал + комбинированная речеподобная помеха (прибор)

В результате эксперимента видно, что программная реализация комбинированной «речеподобной» помехи имеет лучшие результаты стойкости зашумления по сравнению с ручным набором помехи в виде «речеподобной» типа речевой хор и белого

шума. Результаты эксперимента согласовываются с литературными данными [4]. Прибор может быть использован для разработки генераторов шума, а так же применяться как встроенный в программно-аппаратный комплекс.

Список литературы

1. А.М. Гришин, Методы защиты речевой информации. // Прикладная Дискретная Математика. – М.:2008. - №2 – С. 67-70.
2. Джеффри Тревис. LabVIEW для всех: Пер. с англ. Клушин Н. А. - М.: ДМК Пресс; ПриборКомплект, 2005. 544 с.
3. Хорев А.А., Макаров Ю.К. К оценке эффективности защиты акустической (речевой) информации // Специальная техника. – М.: 2000. – № 5 – С. 46 - 56.
4. Хорев А.А., Макаров Ю.И. Оценка эффективности систем виброакустической маскировки // Вопросы защиты информации. – М.:2001. - №1 – С. 21 – 28.

ПАССИВНОЕ ПРОСЛУШИВАНИЕ И ПЕРЕХВАТ ПАКЕТОВ В БЕСПРОВОДНОЙ WI-FI-СЕТИ

П.С. Ладыгин, АлтГУ, физико-технический факультет, 3к.
Научный руководитель – ***А.В. Мансуров,*** к.т.н., доцент.

В беспроводной сети, построенной по традиционной технологии Wi-Fi, все беспроводные устройства включены в единую среду доступа, образуя один гигантский «хаб» (концентратор) – и любое беспроводное устройство может «видеть» всех беспроводных соседей в сети. При этом приемник, работающий в пассивном режиме (только прослушивание), вообще невозможно определить. Таким образом становится возможен перехват данных посылаемых клиентом на сервер и соответствующий ответ сервера на запрос. Данную особенность беспроводных сетей может использовать злоумышленник, пользуясь своим Wi-Fi – адаптером, который переключается в режим получения всех пакетов (т.н. promiscous-mode), с последующим разбором и анализом полученной информации. [1,2]

Таким образом, технология перехвата трафика подразумевает прослушивание сети, захват, декодирование, исследование и

интерпретацию данных, передающихся по сети. Целью подобных атак является похищение информации, обычно такой, как идентификационные номера пользователей, данные о функционировании сети, номера кредитных карт, файлов и т.д. Подобная «пассивная» атака, при которой атакующие не могут быть замечены в сети, затрудняет ее определение, делает ее достаточно опасной, но в то же время достаточно интересной для выполнения исследования и разработки законченного программного решения для реализации такой атаки.

Исследование включает в себя разработку программного решения, которое осуществляет перехват информации, передающейся по беспроводной сети, и ее последующую обработку. Перехваченная информация должна пройти дешифрацию (если это необходимо), и дальше подвергнута анализу и обработке для получения осмысленного результата в виде служебных сообщений сети, элементов сетевого обмена, а также законченных логических блоков (файлов), которые могут передаваться по беспроводной сети и содержаться в захваченном сетевом трафике.

Начальным этапом создания программного решения является написание функционала для анализа и обработки данных на уровне стека протоколов. В качестве первого шага реализован процесс анализа стека протоколов со 2 по 7 уровни и обработка наиболее популярного протокола HTTP, что позволяет находить и сохранять в виде отдельных файлов передаваемые по сети документы и объекты (изображения, аудио/видео и пр.)

Для захвата пакетов пользователь выбирает сетевую карту, которая переводится в т.н. promiscous-режим. Следует отметить, что не каждая карта имеет такую функциональную возможность. Далее осуществляется захват пакетов.

Стандартной процедурой начала сетевого обмена между компьютером «жертвы» и сервером по протоколу TCP [3] является передача пустого пакета с флагом SYN=1. Зафиксировав этот флаг, рабочая программа создает поток, в который будет помещаться вся информация, посылаемая на сервер. Далее, сервер отвечает своему клиенту на запрос тоже пустым пакетом с флагом SYN=1, что создает второй поток. Туда будет записываться вся информация, отправляемая сервером клиенту. После этого происходит обмен между компьютером «жертвы» и сервером при по-

мощи протокола более высокого уровня (HTTP), который сохраняется в созданные потоки.

На рис. 1 изображен пример сохраненного html-запроса.

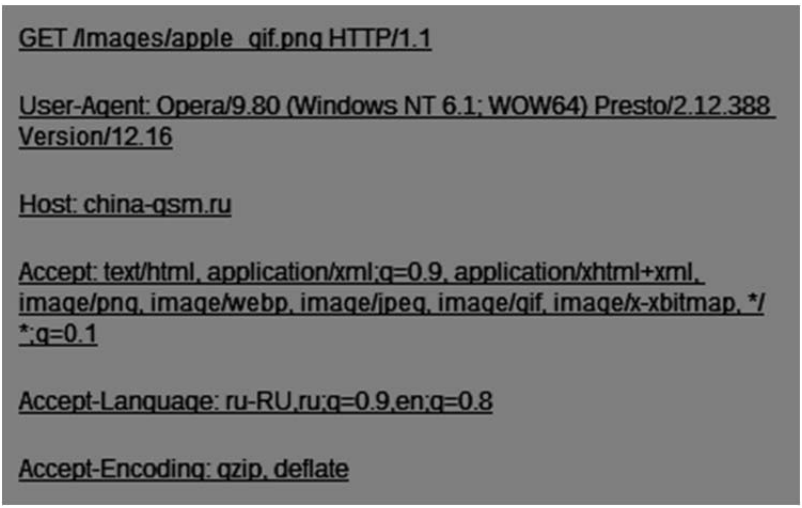


Рис.1. Пример сохраненного html-запроса.

На рис.1 можно увидеть, что компьютер «жертвы» запрашивает изображение с расширением .png, программа фиксирует название этого изображения («apple_gif.png») и запоминает. Помимо этого в запросе может содержаться информация об аутентификации, пароли, сообщения, запрашиваемая информация для поисковых систем и др., которая также сохраняется программой.

Далее, сервер отвечает компьютеру «жертвы» на запрос пакетом, содержащим сообщение с кодом 200 OK [4] (рис.2). Это означает что соответствующий запрос получен. Внутри этого пакета содержится само изображение (на это указывает поле «Content-type»). Рабочая программа фиксирует начало передаваемого изображения и в отдельный поток отправляет код этого изображения. Помимо изображения сервер может отвечать и html-документом, и архивом, и другой информацией, которая также сохраняется программой.

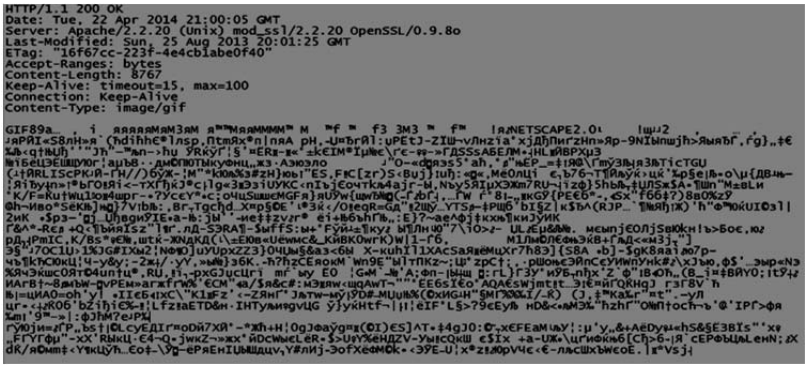


Рис.2. Пример сохраненного html – ответа.

Трудоемким в процессе перехвата пакетов является осуществление дешифрации содержимого кадров сетевого обмена (при использовании алгоритмов шифрования WEP, WPA и др. [5]), а также анализ и работа со стеком используемых в сети протоколов от сетевого до самого высокого прикладного уровня.

Таким образом, рабочая программа представляет с собой приложение, позволяющее осуществлять перехват пакетов, передающихся по беспроводной Wi-Fi — сети. Программа анализирует полученные данные, вплоть до седьмого уровня стека протоколов, сохраняет информацию, передающуюся по протоколу HTTP, в отдельные файлы, согласно её типу. Вся информация, которая передается согласно другим протоколам или зашифрована сохраняется в «сыром» виде, что позволяет производить её анализ отдельно.

Дальнейшая работа планируется над расширением функциональности модуля анализа и обработки стека протоколов, а также поддержку процедур дешифровки захваченного трафика, анализа служебной информации беспроводной сети и сохранение критичного информационного обмена сетевых сервисов, отвечающих за вопросы аутентификации, авторизации и контроля доступа к сетевым ресурсам локальной сети.

Список литературы

1. Олифер В.Г. Компьютерные сети (принципы, технологии, протоколы) 3-е издание / В.Г. Олифер, Н.А. Олифер - СПб.:«Питер», 2006. - 284 с.

2. Безопасность сетей 802.11 — основные угрозы/Хабрахабр. [Электронный ресурс]. // Режим доступа: http://habrahabr.ru/post/151126/. - Загл. с экрана. Дата обращения: 31.04.2014.
3. Танненбаум Э. Компьютерные сети. 4-е изд. / Э. Танненбаум - СПб.: «Питер», 2003. - 572 с.
4. Танненбаум Э. Компьютерные сети. 4-е изд. / Э. Танненбаум - СПб.: «Питер», 2003. - 736 с.
5. Мэрритт М. Безопасность беспроводных сетей / М. Мэрритт, Д. Поллино; Пер. с англ. А.В. Семенова — М.: Компания АйТи; ДМК Пресс, 2004. - 288 с.

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС ОЦЕНКИ ЗАЩИЩЕННОСТИ АКУСТИЧЕСКОГО КАНАЛА СВЯЗИ

А.В. Одинцова, АлтГУ физико-технический факультет, 5 к.
Научный руководитель – ***А.В. Егоров,*** к.ф.-м.н., доцент.

В настоящее время существуют несколько методик оценки разборчивости речи в акустическом канале связи. Применительно к оценке защищенности речевой информации наибольшую популярность получили формантные методы, которые, в сущности, являются различными версиями единого формантного подхода.

Многообразие версий объясняется недостаточной изученностью вопросов формантой разборчивости речи. Для проведения исследований в этой области необходима гибкая система по оценке защищенности акустического канала связи, позволяющая использовать и сравнивать различные методы. Представленные на рынке аппаратно-программные комплексы используют закрытые алгоритмы вычисления разборчивости речи, что является неприемлемым для научных исследований.

В настоящей работе разработана автоматизированная система оценки защищенности акустического канала связи, которая позволяет оценивать уровень разборчивости речи, используя различные методики.

Ключевым понятием в теории разборчивости речи является понятие форманта, которая характеризует области максимальной

концентрации энергии в спектре звука речи. Каждый звук имеет несколько формант и свою индивидуальную спектральную огибающую [1].

Разборчивость речи, в соответствии с международным стандартом ISO/TR 4870, определяется как «степень, с которой речь может быть понята (расшифрована) слушателями». Различают формантную *R*, слоговую *S*, словесную *W* и фразовую *I* разборчивости. Между ними существует однозначная связь (для данного языка), установленная экспериментальным путем на основе так называемых артикуляционных испытаний [2].

В настоящее время существуют следующие отечественные версии формантного подхода оценки разборчивости речи: Н.Б. Покровского, Ю.С. Быкова, М.А. Сапожкова. А также зарубежные: AI (Articulation Index), SII (Speech Intelligibility Index). В каждой из перечисленных версий формантную разборчивость R определяют как среднюю вероятность отсутствия маскировки речи шумом:

$$R = \sum_i^n R_i = \sum_i^n k_i * K_{pi}, \quad (1)$$

где k_i – весовой коэффициент, определяющий вероятность пребывания формант в i–ой полосе частот;

K_{pi} – коэффициент восприятия речи (вероятность отсутствия маскировки речи шумом в i–ой полосе частот).

Основные отличия вариантов формантного метода заключаются в различном толковании и учете влияния частных параметров – формантного спектра речи и коэффициентов восприятия формант [3].

На базе формантного подхода был создан программно-аппаратный комплекс оценки защищенности акустического канала связи, который состоит из: персонального компьютера с установленным пакетом LabVIEW, измерительного микрофона RFT MV201, микрофонного усилителя Robotron 00 011, пистонфона 05 001, акустического излучателя.

На рисунке 1 представлена схема измерений при оценке защищенности акустического канала связи.

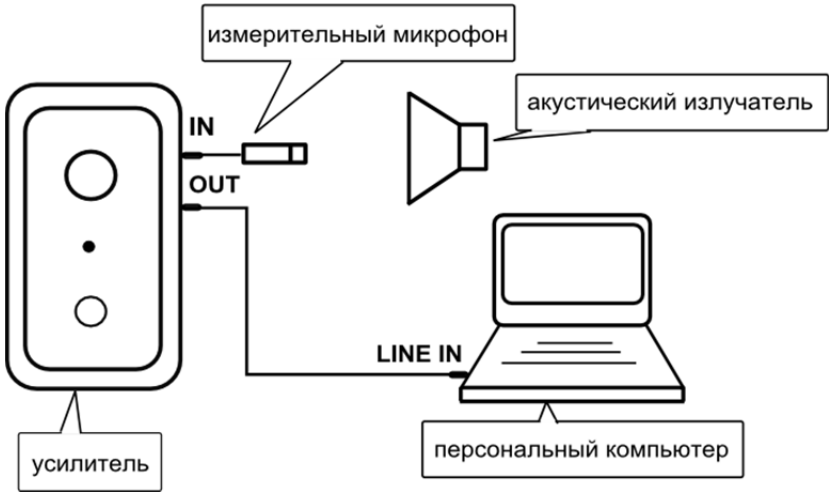


Рис. 1. Схема измерений при оценке защищенности речевой информации.

Работа программы состоит из четырех этапов: калибровка измерительного тракта, измерение уровня шума, измерение уровня сигнала на фоне шума, расчет параметров акустического канала связи. Измерения проводятся в 5-ти октавных полосах.

Калибровка измерительного тракта комплекса проводилась с помощью пистонфона, который представляет собой переносной эталон для измерения звукового давления.

С помощью разработанной установки провели исследования в 5-ти контрольных точках и сравнили результаты измерений с показаниями аппаратно-программного комплекса VNK-012GL.

В таблице 1 представлены результаты измерений уровней шума, сигнала на фоне шума и рассчитанных значений уровня сигнала в контрольной точке №1 без применения активных средств защиты:

Таблица 1

Результаты измерений уровня шума и сигнала в контрольной точке №1

КТ №1	Шум Uш, дБ		Сигнал + шум Uс+ш, дБ		Сигнал Uс, дБ	
F, Гц	ПАК	VNK	ПАК	VNK	ПАК	VNK
250	54	51	57	55	54	53
500	49	48	53	51	51	48
1000	47	45	57	56	57	56
2000	38	41	58	60	58	60
4000	31	34	51	54	51	54

Результаты измерений, полученных с помощью разработанного комплекса и VNK-012GL, расходятся не более чем на 3 дБ. Эти различия обусловлены погрешностью измерений, разными способами калибровки измерительного тракта, а также непостоянным характером шумового фона. Проведенное сравнение разработанного программно-аппаратного комплекса (ПАК) и VNK-012GL позволяет убедиться в корректности работы его измерительной части.

По результатам измерений произведен расчет словесной разборчивости речи (Таблица 2). Для расчета использовался метод Покровского Н.Б., адаптированный в соответствующую методику российскими исследователями Хоревым А.А., Железняком В.К., Макаровым Ю.К [4].

Таблица 2

Результаты измерений уровня словесной разборчивости W

КТ	Интегральный параметр W	
	без защиты	с защитой
КТ №1	0,99	0,66
КТ №2	0,99	0,81
КТ №3	0,99	0,76
КТ №4	0,98	0,62
КТ №5	0,98	0,57

Стоит отметить, что разработчики аппаратно-программного комплекса VNK-012GL используют уникальные коэффициенты восприятия речи, методику построения которых не приводят в описании программного обеспечения. Это не дает нам возможности оценивать корректность результатов расчета разборчивости речи настоящей методикой на основе результатов VNK-012GL.

В ходе проделанной работы были изучены основные версии формантного подхода оценки разборчивости речи, определены их различия и составлены алгоритмы расчета. Автоматизирован процесс измерения и оценки уровня защищенности акустического канала связи. Разработанный виртуальный прибор состоит из отдельных подпрограмм, представляющих собой отдельные модули расчета и измерения. Такая структура программы удобна для исследований, так как позволяет выбирать необходимый метод измерения и, соответственно, расчета разборчивости речи. Разработанный программно-аппаратный комплекс может быть использован в учебных и исследовательских целях в области защиты речевой информации в акустическом канале связи.

Список литературы

1. Физический энциклопедический словарь. – М.: Сов. энциклопедия, 1984. – 944 с.
2. Покровский Н.Б. Расчет и измерение разборчивости речи. – М.: Связьиздат, 1962. С. 142-147.
3. Гавриленко А.В., Дидковский В.С., д-р техн. наук, Продеус А.Н., канд. техн. наук Сопоставление версий формантного метода оценки разборчивости речи // Электроника и связь. Тематический выпуск «Проблемы электроники» . 2008 С. 227 – 231.
4. Железняк В.К., Макаров Ю.К., Хорев А.А. Некоторые методические подходы к оценке эффективности защиты речевой информации // Специальная техника. – № 4. – 2000. – С. 39–45.

ПРИМЕНЕНИЕ МЕТОДОВ МНОГОМЕРНОГО АНАЛИЗА ДАННЫХ В СЕЛЕКТИВНЫХ ПОИСКОВЫХ СИСТЕМАХ

А.А. Пирогов, АлтГУ, физико-технический факультет, 5 к.
Научный руководитель – ***А.В. Егоров,*** к.ф.-м.н., доцент.

Значение информации в жизни любого цивилизованного общества непрерывно возрастает. Развитие новых информационных технологий сопровождается такими негативными явлениями, как промышленный шпионаж, компьютерные преступления и несанкционированный доступ к секретной и конфиденциальной информации. Поэтому защита информации является важнейшей государственной задачей в любой стране [1].

Для выявления технических каналов утечки информации широко применяются металлодетекторы. Металлодетектор должен обеспечивать селективное обнаружение определенных металлических или металлосодержащих объектов поиска на фоне металлических предметов личного пользования, обычно имеющихся у людей [1]. Для проведения точного селективного поиска необходимо производить классификацию проводящих объектов, которая затруднена из-за присутствия мешающих факторов. Для уменьшения влияния посторонних факторов хорошо зарекомендовали себя методы анализа многомерных данных (АМД) [2].

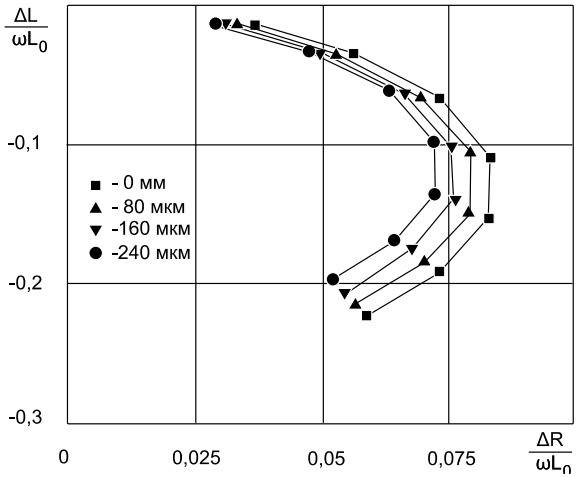


Рис. 1. Годографы для образцов с одинаковой электропроводностью и разным диэлектрическим зазором

Целью данной работы является применение математического аппарата методов анализа многомерных данных для решения задачи классификации в селективных поисковых системах.

Основной составляющей любого металлодетектора является индуктивный датчик. Характеристиками датчика являются индуктивность и внутреннее сопротивление. Когда металлический предмет попадает в переменное магнитное поле, создаваемое датчиком, индуктивность и активное сопротивление датчика изменяется. Зависимость изменения характеристик от параметров объекта и от режима контроля выражается годографами, поскольку электрические сигналы могут быть представлены векторами на комплексной плоскости напряжения [3]. В данной работе при проведении измерений использовался параметрический датчик накладного типа, представляющий собой катушку индуктивности, помещенную в феррит. В качестве образцов выступали металлические предметы, мешающими факторами являлись электропроводность образцов (они изготовлены из различных металлов) и диэлектрическая прокладка, фактически являющаяся изменяемым расстоянием от образца до датчика. Для определения характеристик датчика, регистрации их изменения, построения годографов (рис.1) и накопления данных для анализа был разработан ряд виртуальных приборов в среде LabVIEW.

Любая задача классификации решается на основе анализа значений атрибутов, признаков объекта, в данном случае координаты точек годографов являются вектором признаков металлических образцов. Измерения проводились на 7-ми частотах, таким образом вектор имеет размерность равную 14-ти. Для осуществления АМД и построения моделей классификации было проведено 20 измерений, и 6 измерений было накоплено для тестирования.

АМД – это современный подход к моделированию многомерных (многофакторных) процессов и явлений, основанный на применении проекционных математических методов, позволяющих выделять в больших массивах данных скрытые (латентные) переменные и анализировать связи, существующие в изучаемой системе [4]. Метод главных компонент (МГК) является одним из основных способов уменьшить размерность данных, потеряв наименьшее количество информации [5]. МГК разделяет матрицу данных X на две части: «содержательную» и «шум» [4].

К накопленным многомерным данным был применён МГК с помощью программы Unscrambler, в результате чего на полученном графике (рис.2) была видна чёткая группировка образцов на 4 группы по различной электропроводности металла и на 5 групп в зависимости от толщины диэлектрической прокладки.

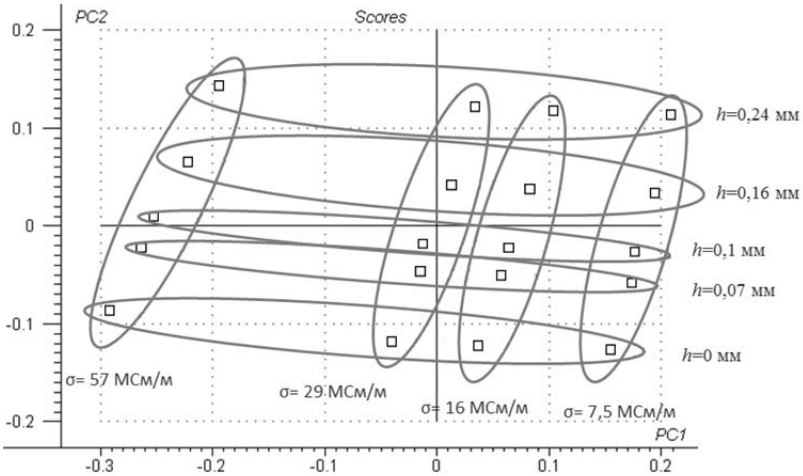


Рис. 2. График счетов для 20 образцов, участвующих в построении модели.

Для построения двух регрессионных моделей (для электропроводности и для толщины диэлектрической прокладки) применялось многомерное моделирование методом Проекций на Латентные Структуры (ПЛС). Данный метод применяется для построения моделей, используемых для предсказания значения определённой переменной на основе значений вектора признаков, полученного при новых измерениях [4].

Таким образом, в результате применения метода ПЛС с помощью программы Unscrambler были получены модели для определения электропроводности и диэлектрического зазора. На графике, изображённом на рисунке 3 видна четкая группировка всех калибровочных отсчётов, отмеченных круглыми маркерами, на 4 непересекающиеся группы, в зависимости от толщины зазора. Треугольными маркерами отмечены тестовые измерения, не

участвующие в построении модели. По оси абсцисс на графике откладывается фактическое значение переменной, относительно которой строится модель, в данном случае толщина зазора, по оси ординат – предсказанное.

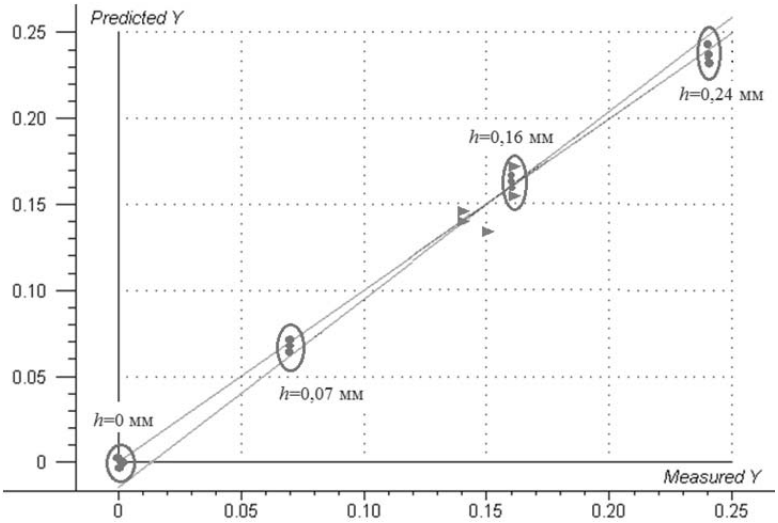


Рис. 3. График предсказанных и измеренных толщин диэлектрических прокладок.

В ходе проделанной работы был разработан виртуальный прибор для определения вектора признаков индуктивного датчика, была накоплена база данных с измерениями векторов признаков металлических образцов, был проведён многомерный анализ полученных данных и конечным результатом проделанной работы стали две построенные модели, позволяющие предсказывать значения электропроводности металлических образцов и расстояние до измерительного датчика. Перспективность применения полученных результатов заключается в возможности программно-аппаратной реализации построенных моделей, которую возможно будет применять в системах селективного обнаружения металлических проводящих объектов.

Список литературы

1. Зайцев, А.П. Технические средства и методы защиты информации: Учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В.

Мещеряков и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: Машиностроение, 2009. – 508 с.
2. Егоров А.В., Парфенова А.В. Применение методов многомерного анализа для интерпретации результатов вихретокового контроля пористых металлических материалов // Известия АлтГУ. – 2011. – №1.
3. Приборы для неразрушающего контроля материалов и изделий. Справ. в 2-х кн. Кн. 2/ под ред. В.В.Клюева. – М.: Машиностроение, 1976. – 326 с.
4. Эсбенсен К. Анализ многомерных данных. Избранные главы / Пер. с англ. С.В. Кучерявского; Под ред. О.Е. Родионовой. – Черноголовка: Изд-во ИПХФ РАН, 2005. – 157 с.
5. Егоров А.В., Кучерявский С.В., Поляков В.В. Применение метода главных компонент для акустико-эмиссионной диагностики алюминиевых сплавов // Известия АлтГУ. – 2007. – №1.

ОТВЕТСТВТЕННОСТЬ ЗА НАРУШЕНИЕ АВТОРСКИХ ПРАВ В ИНФОСФЕРЕ СЕТИ ИНТЕРНЕТ

А.С. Ткачева, АлтГУ, юридический факультет, 4 к.
Научный руководитель – ***В.А. Мазуров,*** к.ю.н, доцент.

Огромное количество нарушений исключительных прав на результаты интеллектуальной деятельности происходит в результате использования сети Интернет. На бескрайних просторах всемирного виртуального пространства в массовом порядке размещаются аудиовизуальные произведения, фотографии, различные рисунки и чертежи, художественные произведения и т.д., как правило, во многих случаях без согласия правообладателей, что приводит к ущемлению их прав, поскольку только они вправе давать согласие на такое размещение. Кроме того, за использование объектов авторского права полагается выплата вознаграждения, которое в случае нарушения прав на результаты интеллектуальной деятельности авторы не получают.

К основным способам незаконного использования объектов авторского права и (или) смежных прав в Интернете относятся:

- рассылка объектов авторского (смежного) права адресатам;
- открытие доступа к объектам авторского (смежного) права неограниченному кругу лиц. [1]

При этом второй способ следует признать наиболее опасным, поскольку он создает условия для массовых нарушений авторских и смежных прав, приводит к неконтролируемому воспроизведению и распространению произведений.

Сущность нарушений авторских и смежных прав в сети та же, что и нарушений за ее пределами: посягательства совершаются как в отношении личных неимущественных прав, так и в отношении прав на использование охраняемых объектов. Однако такие нарушения обладают определенной спецификой, выражающейся, в частности, в сложности контроля над использованием размещенных объектов, в особенностях пресечения совершаемых нарушений. Здесь отсутствуют материальные носители, которые можно было бы признать контрафактными и конфисковать.

Наиболее острым и дискуссионным вопросом при нарушении интеллектуальных прав в Интернете можно назвать определение ответственности лиц, вовлеченных в распространение в сети материалов, содержащих интеллектуальную собственность. В процессе распространения таких материалов посредством использования Интернета можно выделить два вида субъектов.

- лицо, загрузившее интеллектуальную собственность в сеть (провайдер);
- информационный посредник (лицо, осуществляющее технические услуги).

В судебной практике отмечается, что при рассмотрении дел о привлечении владельцев социальных и файлообменных сайтов к ответственности за нарушение исключительных прав следует учитывать степень вовлечения провайдера в процесс передачи, хранения и обработки информации, возможность контролировать и изменять ее содержание. Провайдер не несет ответственности за передаваемую информацию, если он не инициирует ее передачу, не выбирает получателя информации, не влияет на ее целостность, а также принимает превентивные меры по предотвращению использования объектов исключительных прав без согласия правообладателя. [2]

При рассмотрении подобных дел необходимо проверять:

1. получил ли провайдер прибыль от деятельности, связанной с использованием исключительных прав других субъектов,

которую осуществляли лица, пользующиеся услугами этого провайдера;

2. установлены ли ограничения объема размещаемой информации, ее доступности для неопределенного круга пользователей, предусмотрена ли в пользовательском соглашении обязанность пользователя по соблюдению законодательства РФ при размещении контента и безусловное право провайдера удалить незаконно размещенный контент;
3. есть ли технологические условия (программы), способствующие нарушению исключительных прав, и специальные эффективные программы, позволяющие предупредить, отследить или удалить размещенные контрафактные произведения.

Следует также оценивать действия провайдера по удалению, блокированию спорного контента или доступа нарушителя к сайту при получении извещения правообладателя о факте нарушения исключительных прав, а также в случае иной возможности узнать (в том числе из широкого обсуждения в средствах массовой информации) об использовании его интернет-ресурса с нарушением исключительных прав других лиц. При отсутствии со стороны провайдера в течение разумного срока действий по пресечению таких нарушений либо в случае его пассивного поведения, демонстративного и публичного отстранения от содержания контента суд может признать наличие вины провайдера в допущенном правонарушении и привлечь его к ответственности (Постановление Президиума ВАС РФ от 01.11.2011 N 6672/11).

При этом важно иметь в виду, что за нарушение исключительных прав при размещении на интернет-сайте объектов интеллектуальной собственности ответственность должен нести пользователь (владелец) сайта, а не владелец сервера, на дисковом пространстве которого размещен такой сайт (Постановление ФАС ЦО от 20.01.2012 по делу N А09-3432/10). [3]

Для решения проблемы ответственности лиц, вовлеченных в распространение материалов, нарушающих интеллектуальные права в сети Интернет, выдвигаются различные предложения. Е.Э. Чуковская и М.Ю. Прокш указывали, что "контроль за соблюдением авторского и смежных прав в сети Интернет должен основываться на контроле информационных посредников и лиц, незаконно размещающих контент, а не обычных пользователей сети Ин-

тернет. Информационные посредники сети Интернет (операторы связи, владельцы интернет-сайтов и доменных имен и др.) должны нести ответственность за нарушение авторских и смежных прав на общих основаниях при наличии вины, за исключением случаев, когда они не знали и не должны были знать о незаконности контента и не видоизменяли контент или в случае получения письменного заявления правообладателя своевременно приняли необходимые и достаточные меры по устранению последствий нарушения его прав. При этом лица, незаконно размещающие контент в сети Интернет, должны нести ответственность независимо от информационного посредника либо солидарно с ним при наличии вины последнего.

В приведенных вариантах, включающих как одного, так и нескольких субъектов, на которых предлагалось возложить ответственность за нарушение интеллектуальных прав в сети Интернет, можно выделить информационного посредника в качестве ключевого субъекта. Воздействие на него способно наиболее эффективно повлиять на распространение интеллектуальной собственности в Интернете.

Статья 1253.1. ГК РФ введенная Федеральным законом от 02.07.2013 N 187-ФЗ предусматривает особенности ответственности информационного посредника. [4]

Информационный посредник - это лицо, осуществляющее передачу материала в информационно-телекоммуникационной сети, в том числе в сети "Интернет", лицо, предоставляющее возможность размещения материала или информации, необходимой для его получения с использованием информационно-телекоммуникационной сети, лицо, предоставляющее возможность доступа к материалу в этой сети, - информационный посредник - несет ответственность за нарушение интеллектуальных прав в информационно-телекоммуникационной сети на общих основаниях, предусмотренных Кодексом, при наличии вины с учетом особенностей.

Информационный посредник, осуществляющий передачу материала в информационно-телекоммуникационной сети, не несет ответственность за нарушение интеллектуальных прав, произошедшее в результате этой передачи, при одновременном соблюдении следующих условий:

1. он не является инициатором этой передачи и не определяет получателя указанного материала;
2. он не изменяет указанный материал при оказании услуг связи, за исключением изменений, осуществляемых для обеспечения технологического процесса передачи материала;
3. он не знал и не должен был знать о том, что использование соответствующих результатов интеллектуальной деятельности или средства индивидуализации лицом, инициировавшим передачу материала, содержащего соответствующие результат интеллектуальной деятельности или средство индивидуализации, является неправомерным.

Информационный посредник, предоставляющий возможность размещения материала в информационно-телекоммуникационной сети, не несет ответственность за нарушение интеллектуальных прав, произошедшее в результате размещения в информационно-телекоммуникационной сети материала третьим лицом или по его указанию, при одновременном соблюдении информационным посредником следующих условий: [5]

1. он не знал и не должен был знать о том, что использование соответствующих результата интеллектуальной деятельности или средства индивидуализации, содержащихся в таком материале, является неправомерным;
2. он в случае получения в письменной форме заявления правообладателя о нарушении интеллектуальных прав с указанием страницы сайта и (или) сетевого адреса в сети "Интернет", на которых размещен такой материал, своевременно принял необходимые и достаточные меры для прекращения нарушения интеллектуальных прав. Перечень необходимых и достаточных мер и порядок их осуществления могут быть установлены законом.

К информационному посреднику, который не несет ответственность за нарушение интеллектуальных прав, могут быть предъявлены требования о защите интеллектуальных прав, не связанные с применением мер гражданско-правовой ответственности, в том числе об удалении информации, нарушающей исключительные права, или об ограничении доступа к ней.

Стоит помнить, что размеры, порядок привлечения к ответственности пользователя - вопросы, в которых следует быть крайне щепетильным. Безусловно, заслуживает внимания предложение К. Васичкина о введении "в статью 1253.1 ГК РФ подпункта 4 п. 2, требующего, чтобы информационный посредник по запросу суда предоставил всю имеющуюся у него информацию о третьем лице, которому был присвоен указанный в запросе сетевой адрес, и подпункта 3 п. 3, указывающего, что информационный посредник по письменному запросу правообладателя обязан предоставить сетевой адрес лица, разместившего материал, права на который заявит лицо, выступившее в качестве правообладателя и представившее подтверждающие документы, либо по запросу суда". Однако нельзя забывать, что сведений о пользователе может оказаться крайне мало, что может затруднить исполнение судебных актов.

Уголовная ответственность за нарушение авторских и смежных прав предусмотрена Уголовным кодексом, а именно ст. 146 УК РФ: [6]

Существенные проблемы в теории уголовного права и на практике вызывает установление размера нарушения авторских или смежных прав в случае, когда экземпляры произведения размещаются в глобальной сети Интернет, в локальных и иных компьютерных сетях с ограниченным либо неограниченным кругом пользователей, т. е. доводятся до всеобщего сведения таким образом, что любое лицо может получить доступ к произведению из любого места и в любое время по собственному выбору. Такое размещение является одним из способов использования авторских (смежных) прав.

Проблема определения размера нарушения авторских или смежных прав в настоящее время является малоисследованной, что также затрудняет на практике применение соответствующих норм уголовного закона. [7]

Одним из комплексных исследований проблем нарушения авторских и смежных прав в Интернете является работа Л.А. Корневой, которая совершенно справедливо отмечает, что Интернет– высококриминогенная среда распространения «интеллектуального пиратства», характеризующаяся неуклонным ростом количества преступлений в сфере авторских и смежных прав, их латентно-

стью, транснациональностью, высокотехнологичностью и отсутствием адекватного законодательного регулирования как на международном, так и на национальном уровне.

Л.А. Корнева предлагает свой способ определения криминообразующих признаков нарушения авторских и смежных прав применительно к данной среде: «В связи с тем, что произведения, размещенные в Интернете, нельзя назвать экземплярами, а определить стоимость их довольно сложно, особенно если автор таких прав никому не собирается их предоставлять, криминообразующим признаком незаконного использования имущественных авторских и смежных прав по ч. 2 ст. 146 УК РФ должен выступать не размер стоимости таких прав (предмет преступления), а "цель извлечения дохода", где цель – признак субъективной стороны, а доход — предмет преступления. Размер дохода должен рассчитываться исходя из стоимости контрафакта, заявленной правонарушителем. В отношении размещения контрафакта в Интернете крупным должен считаться любой размер дохода, так как, во-первых, установить его просто невозможно, например в случае файлообмена, во-вторых, само «доведение до всеобщего сведения» уже оконченное правонарушение, и свободный доступ к информации в Интернете создает условия для массовых, не ограниченных кругом лиц нарушений прав интеллектуальной собственности». Отметим также, что данный криминообразующий признак (цель извлечения дохода) автор предлагает ввести в диспозицию ч. 2 ст. 146 УК РФ, исключив из нее признаки «в крупном размере» и «с целью сбыта», а под доходом предлагается понимать денежную сумму, которую рассчитывал получить правонарушитель, но в размере не менее пятидесяти тысяч рублей.

В частности, введение в качестве обязательного признака субъективной стороны состава данного преступления цели – о извлечение дохода делает не преступными все случаи незаконного использования объектов авторского права и (или) смежных прав, совершенного в иных целях, что случается далеко не редко. Для правообладателя не имеет значения, какие цели преследовало лицо, незаконно использующее его произведение, будь то корысть или тщеславие, экономия времени и т. д., в связи с чем ставить в зависимость от цели вопросы преступности (общественной опасности) данного деяния было бы неправильным. Также нельзя со-

гласиться с тем, что критерием общественной опасности данного преступления должен выступать предполагаемый доход преступника, рассчитываемый исходя из стоимости контрафактных экземпляров произведений (фонограмм), поскольку она существенно (в разы) ниже стоимости легальных экземпляров, что, в свою очередь, приведет к многократному и неоправданному увеличению «порога преступности деяния» и, соответственно, к ослаблению уголовной политики государства в данной сфере.

Вместе с тем представляется оправданным предложение Л.А. Корневой о том, что при незаконном использовании объектов авторского права и смежных прав в Интернете размер преступного посягательства не должен выступать обязательным признаком состава данного преступления, так как приоритет следует отдавать охране этих прав от незаконного использования неограниченным кругом лиц.

Конечные пользователи в случае незаконного использования объектов авторского права (воспроизведение, распространение и т.д.) при наличии всех необходимых признаков состава преступления, в том числе осведомленности о незаконности своих действий, также могут быть субъектами преступления, предусмотренного ч. 2 ст. 146 УК РФ. [8]

Таким образом, устанавливая осведомленность лица о контрафактности произведений, необходимо учитывать как объективные, так и субъективные критерии. К первым относятся качество контрафактной продукции, наличие предупреждений о незаконности использования, факты привлечения к административной ответственности по ст. 7.12 КоАП РФ и т. д. Ко вторым – наличие у лица познаний, позволяющих отличать контрафактный экземпляр произведения от оригинального, обусловленных опытом работы соответствующим образованием, квалификацией, навыками и т. д.

Процесс распространения информации в Интернете между пользователями и владельцами сайтов невозможен без участия провайдеров, выступающих в качестве посредников.

Таким образом, если с первыми двумя категориями (пользователями и владельцами сайтов) все более или менее ясно, то в отношении уголовной ответственности провайдеров ведутся бурные теоретические дискуссии.

Как указывают в своих работах В.Н. Щепетильников и И.М. Рассолов, технические возможности провайдера воздействовать на информационное содержимое сервера породили институт ответственности провайдера, в рамках которого выделились три основных направления:

- провайдер несет абсолютную ответственность за любые действия пользователей, независимо от осведомленности о фактах нарушения законодательства об интеллектуальной собственности;
- провайдер не несет ответственности за действия пользователей при соблюдении определенных условий взаимодействия с иными субъектами информационного обмена (в первую очередь, с правообладателями);
- провайдер ни при каких условиях не несет ответственности за действия пользователей.

В целом следует согласиться с мнением Л.А. Корневой о том, что провайдер может признаваться исполнителем рассматриваемого преступления, если он непосредственно сам незаконно размещает объекты авторского (смежного) права на своем сервере, предоставляя к ним доступ неограниченному количеству пользователей, т. е. является контент-провайдером. Если провайдер занимается только хостингом, т. е. предоставлением на договорной основе третьим лицам физического дискового пространства на сервере для хранения и обработки информации, а также для обеспечения работы веб-сайтов, то он может быть признан пособником преступления, предусмотренного ч. 2 ст. 146 УК РФ, если он заведомо знал о том, что такие лица занимаются незаконным использованием объектов авторского (смежного) права, и при наличии иных необходимых признаков соучастия (совместность, единый умысел, двухсторонняя виновная связь). При отсутствии же в рассматриваемой ситуации указанных признаков (так называемой субъективной совместности действий), представляется, провайдер не может быть привлечен к уголовной ответственности за незаконное использование объектов авторского права и (или) смежных прав, так как фактически он осуществляет хранение контрафактных экземпляров произведений на сервере без цели сбыта. Поскольку данный вопрос является достаточно сложным, а его решение неоднозначным, то имеется необходимость урегулирования

ситуации на законодательном уровне. В любом случае необходимо принятие нормы, обязывающей провайдеров убирать из сети контрафактные произведения либо запрещать к ним доступ при наличии осведомленности об их размещении на сервере. И наконец, провайдеры доступа, которые выступают лишь связующим звеном между конечными пользователями и ресурсами Интернета, обеспечивая перемещение цифровой информации, не могут выступать в качестве субъекта преступления, предусмотренного ч. 2 ст. 146 УК РФ, так как они физически не могут отследить и проверить содержание перемещаемых данных, при этом вполне допуская, что среди всего объема информации имеются контрафактные объекты. [9]

Таким образом, правоприменителям следует учитывать, что в процесс незаконного оборота контрафактных экземпляров произведений в Интернете вовлечено большое количество лиц и зачастую «пираты» не могут обойтись без участия легальных организаций, предоставляющих доступ в сеть (провайдеров) и обеспечивающих прием, перечисление платежей от пользователей. Юридическая оценка должна быть дана действиям каждого из таких лиц.

Список литературы

1. Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 N 230-ФЗ (ред. от 23.07.2013) (с изм. и доп., вступающими в силу с 01.09.2013)
2. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 05.05.2014) (с изм. и доп., вступ. в силу с 16.05.2014)
3. Васильева Т.В. О соблюдении авторских прав в эпоху развития высоких технологий // Современное право. 2011. N 5. С. 102 - 106.
4. Васичкин К.А. Ответственность за нарушение интеллектуальных прав в сети Интернет // Законодательство и экономика. 2013. N 9.
5. Давыдова П.А. Некоторые проблемы привлечения к ответственности пользователей социальных сетей // URL: http://cgpartner.ru/2012/03/nekotorye-problemy-privlecheniya-k-otvetstvennosti-polzovatelej-socialnyx-setej-2

6. Николаев В. Искоренить контрафакт в Рунете // ЭЖ-Юрист. 2013. N 47.
7. Чуковская Е.Э., Прокш М.Ю. Использование результатов творческой деятельности в Интернете: возможный подход к регулированию // Журнал российского права. 2013. N 2.
8. Чуковская Е.Э., Прокш М.Ю. Использование результатов творческой деятельности в Интернете: возможный подход к регулированию // Журнал российского права. 2013. N 2.
9. Щепетильников В. Н. Уголовно-правовая охрана электронной информации: дис. канд. юрид. наук. Елец, 2006. С. 111—112.

УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ПРАВ И СВОБОД ГРАЖДАН В ИНТЕРНЕТЕ

Н.О. Шуплецова, АлтГУ, юридический факультет, 3 к.
Научный руководитель – ***И.А. Анисимова,*** к.ю.н., доцент.

В России, как и во всем мире, стремительно развиваются Интернет-технологии, совершенствуются формы передачи информации, личных контактов, деловых взаимоотношений. Но права и свободы граждан в Интернете фактически не защищены, и их нарушения становятся все более частым и масштабным явлением.

Одним из примеров таких нарушений является нашумевший случай, произошедший в США. Кристофер Чейни был признан судом Лос-Анджелеса виновным в незаконном прослушивании телефонных разговоров и взломе персональных компьютеров более 50 голливудских знаменитостей, в результате чего в Интернет попали интимные фотографии актрисы Скарлетт Йоханссон, певицы Кристины Агилеры и других. По американским законам Чейни грозило наказание до шестидесяти лет тюремного заключения, но «хакер» согласился сотрудничать со следствием. Приняв во внимание эти обстоятельства, суд ограничился относительно мягким приговором. В итоге Чейни приговорили к 120 месяцам тюремного заключения и выплате компенсаций на сумму 76 тысяч долларов. Правонарушитель признался, что взламывал почтовые аккаунты своих жертв, используя функцию "Забыли пароль" и отвечая на секретные вопросы [1].

Если бы данные преступления были совершены в Российской Федерации, какому наказанию был бы подвергнут виновный? Очевидно, что суд квалифицировал бы деяния по следующим составам: нарушение неприкосновенности частной жизни (ст. 137 УК РФ), нарушение тайны переписки (ст. 138 УК РФ), неправомерный доступ к компьютерной информации (ст. 272 УК РФ). Таким образом, в российском праве существуют основания для привлечения за данное деяние к уголовной ответственности.

Для определения размера наказания за совершенное Кристофером Чейни преступление необходимо квалифицировать действия хакера в соответствии с нормами российского уголовного права.

Итак, Кристофер Чейни:

- незаконно собрал и распространил сведения о частной жизни 50 знаменитостей без их согласия, чем нарушил неприкосновенность их частной жизни и совершил преступление, предусмотренное ч. 1 ст. 137 УК РФ, за что следует наказание от штрафа в размере до двухсот тысяч рублей или в размере заработной платы за период до восемнадцати месяцев до лишения свободы на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет;
- нарушил тайну переписки своих жертв - преступление, предусмотренное ч. 1 ст. 138 УК РФ, за что следует наказание от штрафа в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев до исправительных работ на срок до одного года;
- осуществил неправомерный доступ к компьютерной информации, повлекший ее копирование, - преступление, предусмотренное ч. 1 ст. 272 УК РФ, за что следует наказание от штрафа в размере до двухсот тысяч рублей или в размере заработной платы за период до восемнадцати месяцев до лишения свободы на срок до двух лет.

При определении степени наказания российский суд руководствовался бы положениями ст. 69 УК РФ (назначение наказания по совокупности преступлений). Следуя алгоритму, установ-

ленному ст. 69 УК РФ, максимальное окончательное наказание по совокупности указанных преступлений может быть назначено не более трех лет лишения свободы. Этот срок определен исходя из того, что наиболее строгое наказание предусмотрено ч. 1 ст. 137 УК РФ - в виде двух лет лишения свободы, а окончательное наказание не может превышать более чем наполовину максимальный срок или размер наказания за наиболее тяжкое из совершенных преступлений (2 + (2:2) = 3) [2]. Учитывая обстоятельство, что обвиняемый пошел на сделку со следствием, наказание могло быть смягчено, тем более виновный признался, что совершил данные преступления «из чистого любопытства». И действительно, безработный 35-летний Чейни жил с бабушкой, не был криминальным гением и уж тем более профессиональным хакером [3].

Разница в наказаниях очевидна. Кроме того, возникают сомнения в том, что по данным фактам вообще было бы возбуждено уголовное дело и велось расследование.

На основании мониторинга приговоров по 65 уголовным делам можно сделать следующий вывод: в 74% случаев наказанием, назначаемым за перечисленные преступления, выступает штраф, в 17% случаев – обязательные работы, в 9% - иные виды наказаний. Причем ни в одном приговоре не был назначен штраф в полном объеме.

Практика показывает, что штраф по ч. 1 ст. 137 УК РФ назначается в размере 10-15 тыс. рублей; при совершении нескольких преступлений – может достигать 35 тыс. рублей при возможном максимальном наказании в 200 тыс. рублей. Таким образом, несмотря на достаточно высокую общественную опасность данных преступных деяний, общество не воспринимает их как «преступления», а назначаемые на практике наказания не обеспечивают реализацию целей, предусмотренных ст. 43 УК РФ. Решением данной проблемы может являться установление минимальных (нижних) границ наказания и увеличение максимальных (верхних) границ назначения наказания. Например, от 100 тыс. рублей до 500 тыс. рублей – за преступление, предусмотренное ч. 1 ст. 137 УК РФ; от 50 тыс. рублей до 200 тыс. рублей – за преступление, предусмотренное ч. 1 ст. 138 УК РФ; от 100 тыс. рублей до 500 тыс. рублей - за преступление, предусмотренное ч. 1 ст. 272 УК РФ.

Для сравнения можно привести пример из проанализированной судебной практики, где выявлено наиболее строгое наказание. 26 июля 2011 года Исакогорский районный суд г. Архангельска вынес приговор генеральному директору ООО "Гелиос" Анне Ковалевой. Она признана виновной в совершении преступлений, предусмотренных ч. 1 ст. 272 УК РФ и ч. 1 ст. 138 УК РФ. Установлено, что Ковалева умышленно с целью ознакомления с конфиденциальной информацией, неоднократно (в период апрель-сентябрь 2010 года) осуществляла неправомерный доступ к охраняемой законом компьютерной информации в локальной сети "Интернет". Путем обмана пользователей социальной сети "В контакте" получила доступ к их личным данным, и с целью нарушения тайны переписки, без согласия потерпевшей В., зарегистрировала страницу в социальной сети "В контакте" с указанием персональных данных потерпевшей, в дальнейшем, используя указанную страницу, осуществляла личную переписку от ее имени, и знакомилась с содержанием писем, адресованных потерпевшей. Приговором суда Ковалевой назначено наказание в виде 10 месяцев 5 дней лишения свободы, на основании ст. 73 УК РФ условно с испытательным сроком на 6 месяцев [4]. Хотя в данном случае суд необоснованно не вменил виновной еще и ч. 1 ст. 137 УК РФ.

По степени тяжести эти преступления отнесены основным составом к категории небольшой тяжести. Такое положение вещей подтверждает версию о том, что частная жизнь граждан не является пока для общества и государства приоритетным объектом уголовно-правовой охраны. Хотя порой такие деликты наносят непоправимый вред личности[5].

Список литературы.

1. Денисов, А. Если бы это произошло у нас, какая была бы ответственность? / А. Денисов // Административное право. - 2012. - № 2. – С. 34-39.
2. The Man Who Hacked Hollywood [Электронный ресурс]. URL: http://www.gq.com/news-politics/newsmakers/201205/chris-chaney-hacker-nude-photos-scarlett-johansson?printable=true (дата обращения: 07.04.2014).
3. Комментарий к Уголовному кодексу Российской Федерации (постатейный) / А. В. Бриллиантов, Г. Д. Долженкова, Я. Е.

Иванова и др.; под ред. А. В. Бриллиантова. - М.: Проспект, 2010. - 1392 с.
4. Приговор Кристоферу Чейни вынесен [Электронный ресурс]. URL: http://www.xakep.ru/magazine/xa/169/xa_169.pdf (дата обращения: 07.04.2014).
5. Гендиректор осуждена за переписку "ВКонтакте" [Электронный ресурс]. URL: http://pravo.ru/news/view/47465/ (дата обращения: 03.04.2014).
6. Кадников, Б.Н. Уголовно-правовая охрана неприкосновенности частной жизни / Б.Н. Кадников; под. ред. Н.Г. Кадникова. - М.: Юриспруденция, 2011. - 136 с.

ПРОБЛЕМЫ АУТЕНТИФИКАЦИИ В СТУДЕНЧЕСКОЙ ИНТЕРАКТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ

А.Т. Эдокова, АлтГУ, физико-технический факультет, 1 к.
Научный руководитель – ***В.В. Белозерских,***
старший преподаватель.

Период конца XX – начала XXI века ознаменовался бурным развитием информационных технологий. На сегодняшний день нет ни одной области человеческой деятельности, где они не нашли бы свое применение. Информация сегодня - средство обеспечения успеха в бизнесе и поэтому является объектом основательного контроля. К сожалению, интерес к взлому или несанкционированному использованию информационных систем постоянно растет, и поэтому требуются серьезная многоуровневая защита. Существенно вырастает цена, которую приходится платить правообладателю информации, не предпринимающему должных усилий по защите своих тайн.

Поэтому сегодня, для того чтобы данные не были уничтожены или модифицированы несанкционированным образом нужно решать различные проблемы их защиты. Одним из путей решения этих проблем является использование аутентификации, на рассмотрении которой остановимся подробнее на примере студенческой интерактивной информационной системы.

Немного расскажем о самой системе. С точки зрения пользователя клиентский терминал представляет из себя LCD панель

на которую выводится информация. Панель установлена таким образом, чтобы исключить прямой физический контакт между пользователями и системой. Их взаимодействие осуществляется с помощью жестов, посредством обработки изображений с видеокамеры. Для реализации этих возможностей, в качестве клиентского устройства используется микрокомпьютер RPi. Raspberry Pi это компактный микрокомпьютер размером с банковскую карту. Данный микрокомпьютер имеет 512 Мб ОЗУ и 700 МГц ARM процессор и имеет производительность на уровне Pentium III – 600 МГц. Может работать под многими ОС, включая те, что основаны на ядре Linux.

Что касается реализации всей системы, то она выполнена на 3-х уровневой клиент-серверной архитектуре, с использованием собственной виртуальной сети.

Рис.1. Упрощенная схема информационной системы.

Пересылка данных от сервера клиенту предполагает передачу с использованием протоколов TCP/UDP, но с формированием собственных криптографически защищеных пакетов, с целью ограничения внешнего доступа злоумышленников к системе и нарушения её нормального функционирования.

Основными механизмами защиты информации предлагается аутентификация (установление подлинности) и шифрование.

Аутентификацию можно разделить на два вида: аутентификацию пользователя и аутентификацию источника данных.

В данной работе рассмотрен только механизм аутентификации пользователя.

Подсистема аутентификации пользователей — важнейший компонент системы информационной безопасности, и ее значение трудно переоценить. Подсистема аутентификации подтверждает личность пользователя информационной системы и поэтому должна быть надежной и адекватной, то есть исключать все ошибки в предоставлении доступа. [1] Парольная аутентификация (при попытке входа в сеть пользователь набирает свой пароль) является самой экономичной по стоимости, она проста и привычна. При правильном использовании пароли могут обеспечить приемлемый для многих организаций уровень безопасности. Тем не менее, по совокупности характеристик их следует признать самым слабым средством проверки подлинности. Пароль пользователя можно подсмотреть, перехватить в канале связи, да и просто подобрать. В связи с этим, следует признать, что в нашем случае парольная аутентификация является ненадежной. [2]

Поэтому предлагается реализовать аутентификацию пользователя с помощью метода, предложенного Массачусетским технологическим институтом в середине 80-х годов.

В нашем случае сеть - открытая (незащищенная), в узлах которой сосредоточены субъекты – пользователи, а также клиентские и серверные программные системы. Суть метода в том, что каждый субъект обладает секретным ключом. Субъектами в данной системе будут являться клиент (пользователь) – обозначим его К, и сервер – обозначим его С. Чтобы клиент К мог доказать свою подлинность серверу С, он должен не только назвать себя, но и продемонстрировать знание секретного ключа. К не может просто послать С свой секретный ключ, во-первых, потому, что сеть открыта, а, во-вторых, потому, что С не знает (и не должен знать) секретный ключ К. В связи с этим требуется создать доверенную третью сторону, владеющую секретными ключами обслуживаемых субъектов и помогающую им в попарной проверке подлинности. Обозначим третью сторону как А.

Чтобы с помощью А получить доступ к С, К посылает А запрос, содержащий сведения о нем (клиенте) и о запрашиваемой услуге. В ответ А возвращает так называемый билет, зашифрован-

ный секретным ключом сервера, и копию части информации из билета, зашифрованную секретным ключом клиента.

Клиент должен расшифровать вторую порцию данных и переслать ее вместе с билетом серверу. Сервер, расшифровав билет, может сравнить его содержимое с дополнительной информацией, присланной клиентом.

Совпадение свидетельствует о том, что клиент смог расшифровать предназначенные ему данные, то есть продемонстрировал знание секретного ключа. Значит, клиент – именно тот, за кого себя выдает. [3]

Проиллюстрируем описанную процедуру.

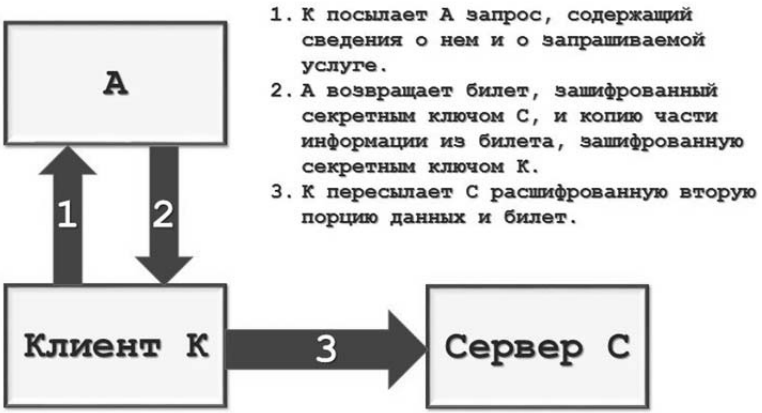


Рис.2. Упрощенная схема предложенного метода аутентификации пользователя.

Так как компонентов сети немного, то создание доверенной стороны А сопряжено с определенными затратами. Для решения этой проблемы нужен дополнительный компонент, например, еще один ПК, который должен работать не прерывно для обеспечения процесса аутентификации. Это и является своеобразной издержкой предложенного механизма аутентификации.

Рис.3. Упрощенная схема информационной системы, которая получится в результате.

Таким образом, можно с большой долей уверенности утверждать, что представленный в работе метод является приемлемым для данной информационной системы, хотя и не лишен определенных издержек.

Список литературы

1. Голов А., Прудников И. Аутентификация пользователей – современные методы // CIO. 2006. №4(93). С. 30-31.
2. Алферов А. П., Зубов А. Ю. Основы криптографии: учебное пособие. Москва: Гелиос АРВ, 2002. - 332 с.
3. Вьюкова Н., Сервер аутентификации Kerberos [Электронный ресурс] – Режим доступа: http://www.osp.ru/os/1996/01/178793/, свободный. – Загл. с экрана

ПРИМЕНЕНИЕ ФУНКЦИЙ УОЛША ДЛЯ ОПРЕДЕЛЕНИЯ ПАРАМЕТРОВ ГАРМОНИЧЕСКИХ СИГНАЛОВ ПРИ НАЛИЧИИ СЛУЧАЙНОЙ ПОМЕХИ В СЕЛЕКТИВНЫХ ПОИСКОВЫХ СИСТЕМАХ

А.В. Герусов, АлтГУ, физико-технический факультет, 5к.
Научный руководитель – ***А.В. Егоров,*** к.ф.-м.н., доцент.

Рост числа объектов информатизации, обрабатывающих и содержащих конфиденциальные данные, ставит жесткие требования к комплексному подходу обеспечения информационной безопасности. Важную роль в решении этой задачи играют различные

технические средства, позволяющие выявлять несанкционированные устройства для съема информации [1]. Эффективность такого обнаружения зависит не только от методов измерений, но и от алгоритмов обработки сигналов, регистрируемых измерительными датчиками. В селективных поисковых системах часто приходится определять параметры гармонических сигналов. Из существующих методов обработки широкое применение нашли цифровые методы [2], использующие аппроксимацию мгновенных значений сигнала исходной модельной функцией. В частности, для синусоидальных сигналов используют гармоническую функцию, где определяемыми параметрами являются амплитуда и начальная фаза. При реализации данного подхода методом наименьших квадратов приходится накапливать сумму произведений мгновенных значений сигнала на значения тригонометрических функций, что предъявляет повышенные требования к производительности микроконтроллеров в портативных поисковых системах. В настоящей работе для определения комплексной амплитуды гармонического сигнала использовали функции Уолша [3], что позволило существенно снизить вычислительную нагрузку на микроконтроллер без ухудшения точности измерений.

В рамках предложенного метода синусоидальный сигнал имеющий амплитуду U_m, начальную фазу φ_0 и постоянное смещение U_0 раскладывается в усеченный ряд Уолша с коэффициентами a_0, a_1 и a_2 равными:

$$a_0 = U_0; \quad a_1 = \frac{2U_m}{\pi}\cos\varphi_0; \quad a_2 = \frac{2U_m}{\pi}\sin\varphi_0 \qquad (1)$$

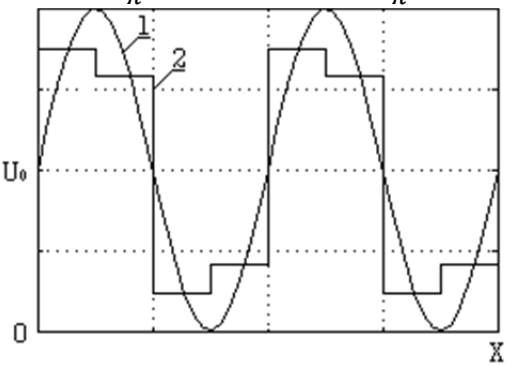


Рис. 1. Исходный сигнал и аппроксимирующий его функциями Уолша.

На рис. 1 в виде кривой 1 показан исходный синусоидальный сигнал, кривой 2 сигнал описывающий усеченный рядом Уолша. Из графика видно, что модельный сигнал очень грубо аппроксимирует синусоиду, но его коэффициенты a_0, a_1 и a_2 содержат всю необходимую информацию об исходном сигнале, то есть постоянное смещение сигнала, средневыпрямленное напряжение гармонического сигнала и его начальную фазу.

Исходя из этого, рассмотрим аппроксимацию дискретных значений сигнала, содержащего N элементов, линейной комбинацией трех первых функций Уолша с весовыми коэффициентами b_0, b_1 и b_2, которые определяются методом наименьших квадратов по массиву дискретных данных $\{(X_i, Y_i)\}$, содержащего N элементов. Значения коэффициентов b_n, при которых сумма квадратов отклонений от экспериментальных точек до аппроксимирующей функции минимальна, определяются из решения следующей системы уравнений:

$$\begin{cases} b_0 = \overline{Y} \\ b_1 = \overline{Y\ \mathrm{wal}(1, X)} \\ b_2 = \overline{Y\ \mathrm{wal}(2, X)} \end{cases}. \qquad (2)$$

Поскольку значения функций Уолша принимают значения либо +1, либо -1, то операция умножения сводится к смене знака соответствующих величин при их суммировании. При этом резко снижаются требования к вычислительной системе.

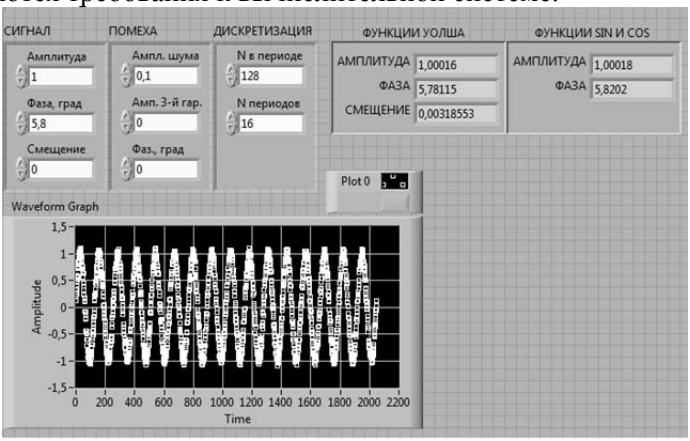


Рис. 2. Лицевая панель виртуального прибора, рассчитывающего амплитуду и начальную фазу гармонического сигнала при наличии случайной помехи.

Для иллюстрации возможности данного метода по определению параметров синусоидальных сигналов при наличии случайной помехи был создан виртуальный прибор в графической среде LabView, рассчитывающий амплитуду и начальную фазу гармонического сигнала при наличии случайной помехи. По заданным с лицевой панели прибора значениям генерируется синусоидальный сигнал и накладывается случайная помеха. При генерации этого сигнала закладывается число точек на 1 период сигнала. Сформированный таким образом массив данных аппроксимируется как функциями Уолша так и тригонометрическими функциями, результаты расчетов исходного сигнала выводятся на лицевую панель прибора.

Был проведен численный эксперимент, в ходе которого обрабатывались массивы данных $\{(X_i, Y_i)\}$, содержащих N=128 отсчетов. Было сгенерировано 10 массивов данных. Для них рассчитывались амплитуда и начальная фаза сигнала. Результаты расчетов приведены в Таблица 1. В ней также представлены средние значения U_m и φ_0 и стандартные отклонения s_U и s_φ для каждого рассмотренного случая. Полученные результаты показывают, что начальные фазы сигнала и его амплитуда, определенные разными методами, с точностью до стандартных отклонений совпадают с истинными значениями.

Таблица 1.

Результаты расчетов амплитуды и начальной фазы гармонического сигнала при наличии случайной помехи.

№ опыта	Параметры сигнала			
	Аппроксимация функциями Уолша		Аппроксимация тригонометрическими функциями	
	U_m , В	φ_0, градус	U_m, В	φ_0, градус
1	1,0008	32,903	0,9935	32,841
2	1,0094	33,242	1,0015	33,364
3	1,0076	33,754	1,0016	33,541
4	1,0114	33,312	1,0046	33,417

5	1,0305	32,794	1,0167	32,925
6	0,9941	33,559	0,9891	33,536
7	1,0160	33,217	1,0032	33,363
8	1,0147	33,077	1,0016	33,281
9	0,9972	33,333	0,9939	33,122
10	1,0113	33,716	1,0025	33,492
среднее арифметическое	1,0093	33,291	1,0008	33,288
стандартное отклонение	0,0105	0,3198	0,0076	0,2482

Апробация предложенного метода обработки свидетельствует о перспективности его применения в системах селективного обнаружения металлических проводящих объектов.

Список литературы

1. Зайцев А.П., Шелупанов А.А, Мещеряков Р.В. и др. Технические средства и методы защиты информации: Учебник для вузов – М.: Машиностроение, 2009. – 508 с.
2. Лайонс Р. Цифровая обработка сигналов. – М.: ООО «Бином-Пресс», 2006. – 656 с.
3. Залманзон Л.А. Преобразование Фурье, Уолша, Хаара и их применение в управлении, связи и других областях М.: Наука, 1989. 496 с.
4. Егоров А.В., Поляков В.В., Иваков С.В. Измерительно-вычислительный комплекс для определения удельной электропроводности и магнитной проницаемости методом вихревых токов // Ползуновский вестник. – 2010. -№2. – С. 129-132.
5. Егоров А.В. Парфенова А.В. применение методов многомерного анализа для интерпретации результатов вихретокового контроля пористых металлических материалов // Известия АлтГУ. – 2011. -№1. – С. 157-159.

ПРОБЛЕМЫ ПРАВОВОЙ ЗАЩИТЫ IT-ТЕХНОЛОГИЙ

МЕТОДЫ ОБРАБОТКИ ФОТОПЛЕТИЗМОГРАММЫ ДЛЯ ВЫЯВЛЕНИЯ СОСТОЯНИЯ СТРЕССА

С.В. Бровко, АлтГУ, физико-технический факультет,3 к.
Научный руководитель – ***Н.Н. Минакова,*** д.ф.-м.н, профессор.

Потребность в том, чтобы выявить лжеца возникла с процессом становления общества. В различное время люди использовали разные методы и способы выявить ложь. Это задача актуально и сейчас. В наше время для этой цели используют полиграф.

Сегодня в обществе уже практически никто не верит в миф о полиграфе, как об устройстве, которое практически со 100% вероятностью может выявить ложь, проходящего на нем тестирование человека. Многие люди знают устройство данного прибора и всеми возможными способами пытаются «обмануть» полиграф. И у многих это выходит.

Одним из важных критериев для верной оценки в полиграфе является «страх», боязнь человека обмануть данное устройство. Во время того как тестируемый отвечает на поставленный вопрос неискренне, он начинает испытывать эмоциональное напряжение от того, что прибор в данный момент выявил его ложь. Тем самым этот миф о полиграфе упрощает детекцию лжи.

Молодежь в большинстве случаев не испытывает страх перед полиграфом, усложняя этим оценку полиграмм так, как физиологические изменения в тот момент, когда тестируемый солгал незначительные, что не позволяет однозначно судить об искренности в момент ответа на поставленный вопрос.

В данной работе рассмотрена фотоплетизмограмма, как один из способов выявления неискренности, через канал сердечной активности. Для более точного выявления состояния стресса тестируемого, были представлены дополнительные способы анализа канала сердечной активности. Построение спектрограммы по Фурье-преобразованию и спектрограмма по Вейвлет-преобразованию. Дополнение способов анализа позволяет более точно сделать выводы о эмоциональном состояние человека в момент опроса.

Полиграф фиксирует физиологическое состояние человека в момент ответа на поставленные вопросы. По реакции его организма производится оценка эмоционального состояния. При стрессе учащается дыхание, сердцебиение и потоотделение на пальцах и ладонях рук. Проблема состоит в том, что многие люди могут контролировать в большей или меньшей степени свое эмоциональное состояние и изменения на каналах полиграфа не значительны, что не позволяет однозначно судить о том, что солгал тестируемый или же сказал правду. Но не все реакции возможно контролировать.

В результате данных эксперимента Раскина можно расположить по значимости данные реакции. Самой значимой будет реакция канала кожного сопротивления так, как физически ее не возможно контролировать. Самой неточным из этих 3-х каналов является канал дыхания. Человеку не нужно тренировать свой организм для того, чтобы дышать равномерно. Средний по значимости будет канал сердечной активности так, как процесс биения сердца практически не возможно контролировать. [1]

Метод регистрации оптической плотности ткани. Регистрируются световые сигналы, как отраженные от биоткани, так и просвечивающие ее. В классическом понимании это метод регистрации изменения объемов отдельных частей тела.

В настоящее время в существующих полиграфах по каналу ФПГ оцениваются только 3 параметра:

1. Число сердечных сокращений в минуту.
2. Объем крови в одном сердечном сокращении.
3. Изменение положения дикротического зубца.

Для измерения канала фотоплетизмограммы был взят полиграф EPOS. Было написано приложение, позволяющее переводить данные с полиграфа EPOS в таблицу CSV, для дальнейшего анализа.

Далее была разработана программа, которая подгружает таблицу CSV. В ней организовано построение графика ФПГ для визуального анализа. Так же для более простого нахождения пульса и анализа сигнала реализован расчет и построение на графике производной графика ФПГ.

Через минимумы не составляет труда рассчитать частоту ударов сердца в минуту, что и является значение пульса. В макси-

мумах же отображается положение дикротического зубца, что не позволит однозначно определить пульс.

Было реализовано построение спектрограммы по преобразованию Фурье (Рис. 1). Построение спектрограммы производится при помощи скрипта написанном на Python2.7.6.1. с использованием подключаемого модуля «matplotlib», в котором реализована функция «specgram». Функцией «specgram» и производится построение спектрограммы по преобразованию Фурье. [2]

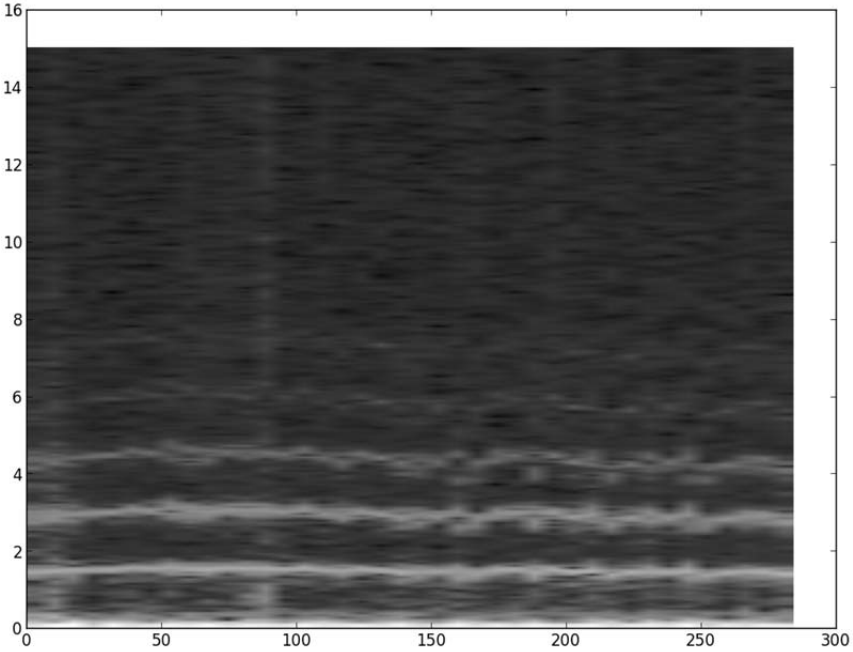


Рис. 1. Построение спектрограммы по преобразованию Фурье.

В свое время выдающимся физиологом XX века П.К. Анохиным был сформулирован принцип оптимального функционирования организма как единого целого. В частности, он считал, что должны быть выполнены определенные частотные соотношения, или частотное согласование, между работой сердца и других органов (печени, легких, почек и др.). Частотное согласование уменьшает ненужные потери энергии. При частотном рассогласовании могут быть нарушены циклы жизнедеятельности некоторых важ-

ных органов, и возникает психоэмоциональное напряжение – стресс. [3]

По частотным рассогласованиям на спектрограмме возможно определить состояние эмоционального напряжения. Они будут проявляться яркими полосами на спектрограмме сигнала.

Построение спектра по Вейвлет-преобразованию было осуществлено с помощью модуля R. W. Fearick (Рис. 2)

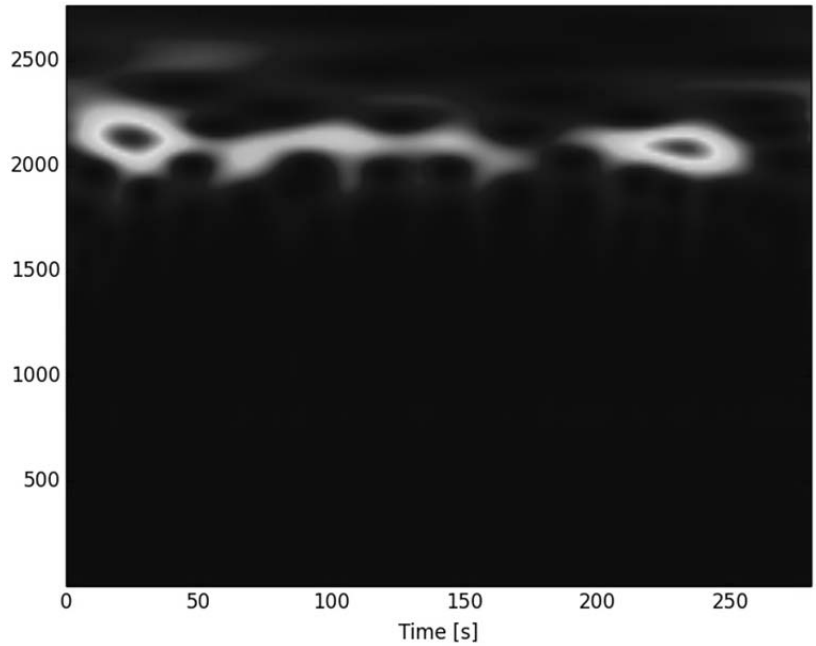


Рис. 2. Построение спектра по Вейвлет-преобразованию.

Спектральные преобразования кардиоинтервалов получили широкое распространение при исследовании вариабельности сердечного ритма (ВСР) при донозологической диагностике функциональных состояний организма. В частности, по мощности спектральных составляющих можно судить о балансе симпатического и парасимпатического отделов вегетативной нервной системы. [4]

По полученным результатам спектрограммы по Вейвлет-преобразованю (Рис. 2) невозможно выявить состояния стресса. Данный модуль не подходит под поставленную задачу. Требуется

написание нового модуля. Для этого нужно подобрать подходящий Вейвлет.

В дальнейшем развитии данной работы планируется выполнить получение более информативной спектрограммы по Вейвлет-преобазованю. Реализовать автоматизацию анализа полученных спектрограмм сигнала для оптимизации и повышения эффективности анализа канала сердечной активности. Планируется рассмотреть другие каналы, используемые в полиграфе с усовершенствованием их анализа по мере необходимости. В перспективе разработать оптимальный метод обсчета полиграмм, с использованием рассмотренных каналов. В результате получить наиболее совершенный полиграф, эффективность которого будет выше существующих.

Список литературы

1. Варламов В.А., Варламов Г.В. Компьютерная детекция лжи – М.: Печатный Дом «Илигар», 2010 – 92с
2. Сайт команды разработчиков «Matplotlib» [Электронный ресурс]: режим доступа - http://matplotlib.org/api/mlab_api.html#matplotlib.mlab.specgram
3. Захаров С.М., Захаров М.С., Знайко Г.Г., Красовский В.Е. Спектральный анализ кардиоинтервалов в донозологической диагностике // Вопросы радиоэлектроники. Сер. ЭВТ. – 2013. – Вып. 3. – с. 6-8
4. Захаров С.М. Вейвлет анализ кардиоинтервалов // Биомедицинская радиоэлектроника – 2012. - №12.

ПРЕДМЕТ ПРЕСТУПЛЕНИЯ, ПРЕДУСМОТРЕННОГО СТ. 138 УК РФ

К.Е. Афанасьева, АлтГУ, юридический факультет, 3 к.
Научный руководитель – ***И.А. Анисимова,*** к.ю.н, доцент.

Право беспрепятственно общаться посредством почты, телеграфа, телефона представляет собой одну из важных гарантий независимости частной жизни человека и гражданина от общества и государства в целом. В ст. 23 Конституции РФ закреплено, что каждый человек имеет право на тайну переписки, телефонных пе-

реговоров, почтовых, телеграфных и иных сообщений. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений влечет ответственность по ст. 138 УК РФ.

Общественная опасность данного преступления определяется тем, что посторонним лицам становится известно содержание писем, переговоров, сообщений без согласия на то лица, которое отправляло или получало такие сообщения, а равно лиц, интересы которых непосредственно затрагивали эти сообщения.

Данные статистики свидетельствуют о том, что нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений как преступление регистрируется не очень часто, но это не снижает его общественной опасности. Так, по этой статье в РФ было осуждено: 1997 г. – всего 7 чел., а в 2009 г. – уже 108 чел. [1]. Как видим, прослеживается тенденция к росту этих преступлений. При этом наиболее сложные и спорные вопросы, возникающие при применении данного состава преступления, связаны с характеристикой его предмета.

Переписка, телефонные переговоры, почтовые, телеграфные и иные сообщения по своей природе представляют собой различные способы обмена информацией, сообщениями между людьми. Переписка может носить личный или деловой характер и осуществляться между физическими лицами, организациями, учреждениями, органами власти. В ст. 23 Конституции РФ речь идет о праве на тайну переписки, которая ведется между физическими лицами, а также между физическими лицами и организациями. Как справедливо отмечает Ф.М. Рудинский, право на тайну переписки обеспечивается именно гражданам, поэтому конституционная норма и, следовательно, ст. 138 УК РФ относится не ко всей переписке (например, служебной, деловой между различными ведомствами), а такой, в которой одним из переписывающихся является гражданин [2].

Итак, предметом рассматриваемого преступления являются сведения, содержащиеся в переписке, телефонных переговорах, почтовых, телеграфных и иных сообщениях физических лиц либо между физическим лицом и организациями, учреждениями, органами власти. Однако в отличие от нарушения неприкосновенности частной жизни при рассматриваемом преступлении не требуется, чтобы сведения составляли личную или семейную тайну.

Важно определить – в каком соотношении в норме, предусмотренной ст. 138 УК РФ, находятся понятия «переписка» и «почтовое телеграфное, телефонное или иное сообщение». Например, в УК Молдовы эти термины используются как синонимы[3]. Российский же законодатель при указании на предмет преступления в ст. 138 УК РФ дословно воспроизводит положение ч. 2 ст. 23 Конституции РФ, из содержания которого усматривается различие в данных терминах. В связи с этим представляется правильной позиция тех специалистов, которые полагают, что ознакомление с содержанием записок в тайниках при конспиративных сообщениях, отлов почтовых голубей в пути следования, перехват писем подследственных, передаваемых из мест предварительного заключения по нелегальным каналам, и тому подобные поступки преступными посягательствами на конституционные права граждан не считаются [4].

Охарактеризуем предмет данного преступления более подробно. В соответствии со ст. 2 ФЗ от 17 июля 1999 г. "О почтовой связи" к почтовым отправлениям относятся письменная корреспонденция, посылки и прямые почтовые контейнеры. Почтовой перепиской следует считать только письменную корреспонденцию. Письменная корреспонденция – это письма, почтовые карточки, секограммы, бандероли и мелкие пакеты. Почтовые отправления в виде посылок, прямых почтовых контейнеров, если они не содержат вложений с письменными сообщениями, предметом рассматриваемого преступления не являются. Посылки и почтовые контейнеры предназначены для пересылки товарно-материальных ценностей. Вскрытие посылок, контейнеров с целью завладения чужим имуществом, которое содержится в них, следует квалифицировать как кражу по ст. 158 УК РФ.

Телефонные переговоры – это обмен речевой информацией между абонентами посредством ее передачи на расстояние с помощью электрических сигналов по проводам или радио (радиотелефонная связь); получила распространение и интернет-телефония (вид электросвязи).

В ряде стран нарушение тайны телефонных переговоров расценивается как одна из разновидностей подслушивания частных разговоров в рамках нормы о посягательствах на неприкосновенность частной жизни (Бельгия, Германия, Голландия) [5].

Телеграфные сообщения осуществляются посредством обмена телеграммами и телексами. Телеграмма – это текстовое сообщение, которое передается средствами телеграфной связи. Услуга "телекс" – это деятельность по установлению временного соединения для приема и передачи текстовых сообщений телеграфной связи между пользовательским оборудованием в сети Телекс.

Под "иными сообщениями" следует понимать пейджинговые и SMS-сообщения, электронную почту, передаваемую в сети Интернет, и др. С развитием современной науки и техники будут появляться новые способы и средства передачи информации на расстояние.

Средства связи вместе со средствами вычислительной техники составляют техническую базу обеспечения процесса сбора, обработки, накопления и распространения информации (ст. 1 ФЗ «О связи»). Из этого следует, что к числу сообщений, нарушение тайны которых подпадает под действие ст. 138 УК РФ, относятся и любые сообщения, передаваемые с помощью самых современных средств передачи информации – локальных и глобальных компьютерных сетей, телефакса и др.

Так, гражданин из чувства ревности к своей бывшей девушке, пытаясь выяснить причину их расставания, обладая достаточными знаниями в области информационных технологий, незаконно зашёл на электронный адрес социальной сети, пользователем которого являлась его бывшая знакомая, где незаконно ознакомился с ее электронной перепиской содержащей сведения личного характера. Он был привлечен к уголовной ответственности по ч. 1 ст. 138 УК РФ [6].

Уголовный Кодекс Украины, называя предмет данного преступления, прямо указывает на корреспонденцию, «передаваемую по компьютеру» (ч. 1 ст. 163) [7]. В Латвии предмет этого преступления именуется «корреспонденцией или информацией, передаваемой по телекоммуникационным сетям» (ч. 1 ст. 144) [8].

В научной литературе высказано мнение о том, что в тайне переписки можно выделить две стороны: тайну содержания и тайну самого факта почтового или телеграфного отправления. Эта точка зрения соответствует действующему законодательству. В ст. 15 ФЗ "О почтовой связи" говорится о том, что информация об ад-

ресных данных пользователей услуг почтовой связи, о фактах почтовых отправлений, телеграфных и иных сообщений, а также сами эти почтовые отправления, телеграфные и иные сообщения являются тайной связи. Следовательно, ответственность по ст. 138 УК должна наступать и в случаях незаконного ознакомления посторонних лиц с информацией о самом факте почтового, телеграфного отправления или телефонного разговора.

Данной позиции придерживается и судебная практика. К примеру, работников телефонной компании, незаконно (без согласия абонента или решения суда) предоставивших информацию о телефонных соединениях абонента третьим лицам, и тем самым нарушившим право на тайну телефонных переговоров, привлекают к ответственности по ст. 138 УК РФ.

К примеру, продавец-консультант одного из магазинов сотовой связи была осуждена по ч. 2 ст. 138 УК РФ. Воспользовавшись своим служебным положением, она без согласия абонента получила через оператора сотовой связи детализацию входящих и исходящих соединений клиента и передала своей знакомой, которой также было предъявлено обвинение в совершении преступления, предусмотренного ч. 1 ст. 138 УК РФ [9].

Кроме того, Конституционный Суд РФ разъяснил, что информацией, составляющей тайну телефонных переговоров, "считаются любые сведения, передаваемые, сохраняемые и устанавливаемые с помощью телефонной аппаратуры, включая данные о входящих и исходящих сигналах соединения телефонных аппаратов конкретных пользователей связи" [10]. Для доступа к этим сведениям, как следовало из разъяснения, необходимо получение судебного разрешения.

Таким образом, предмет рассматриваемого преступления составляют не только сведения, содержащиеся в переписке, телефонных переговорах, почтовых, телеграфных и иных сообщениях, но и общие сведения о совершавшихся физическим лицом телефонных переговорах, сделанных почтовых, телеграфных и иных сообщениях (например, записи учета мобильных звонков).

На основе вышеизложенного отметим следующее. Право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений закреплено в Конституции РФ. Ответственность за нарушение такого права предусмотрена в ст. 138

УК РФ. При применении данного состава преступления необходимо правильно толковать предмет деяния, чтобы выявить – нарушено ли в конкретном случае гарантированное конституционное право человека.

Список литературы

1. Новиков, В.А. Уголовная ответственность за нарушение права на тайну переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений // Законность. 2011. №5, с.1-4. Доступ из справ. – правовой системы «КонсультантПлюс»: постатейные комментарии и книги».
2. Рудинский, Ф.М. Наука прав человека и проблемы конституционного права / Ф.М. Рудинский. Москва: Изд-во ЗАО "ТФ "МИР",2006. 1234 с.
3. Уголовный Кодекс Республики Молдова [Электронный ресурс]. URL: http://base.spinform.ru/show_doc.fwx?rgn=3835 (дата обращения 12.05.2014)
4. Уголовное право. Особенная часть / под ред. В.Н. Петрашева. Москва: Изд-во «ПРИОР», 1999. 608 с.
5. Курс уголовного права. Особенная часть / под ред. Н.Ф. Кузнецовой, И.М.Тяжковой, Г.Н.Борзенкова, В.С. Комиссарова. Москва: «Зерцало», 2002: Т.3. 470 с.
6. Приговор от 28.12.2012 вынесен Дзержинским районным судом г. Новосибирска Новосибирской области [Электронный ресурс]. URL: https://rospravosudie.com/court-dzerzhinskij-rajonnyj-sud-g-novosibirska-novosibirskaya-oblast-s/act-425470944/ (дата обращения 12.05.2014)
7. Уголовный Кодекс Украины [Электронный ресурс]. URL: http://kodeksy.com.ua/ka/ugolovnyj_kodeks_ukraini/statja-163.htm (дата обращения 12.05.2014)
8. Уголовный Закон Латвии [Электронный ресурс]. URL: http://www.pravo.lv/likumi/07_uz.html (дата обращения 12.05.2014)
9. Приговор от 12.09.2013 вынесен Чистопольским городским судом Республики Татарстан [Электронный ресурс]. URL: https://rospravosudie.com/court-chistopolskij-gorodskoj-sud-respublika-tatarstan-s/act-449866919/ (дата обращения 12.05.2014)

10. Об отказе в принятии к рассмотрению запроса Советского районного суда города Липецка о проверке конституционности части четвертой статьи 32 Федерального закона от 16 февраля 1995 года "О связи": Определение Конституционного Суда РФ от 2 октября 2003 г. N 345-О // Вестник Конституционного Суда Российской Федерации. 2004. № 1. С. 50–52.

ДЕЯТЕЛЬНОСТЬ КОЛЛЕКТОРОВ И ЗАЩИТА БАНКОВСКОЙ ТАЙНЫ

Д.А. Голобородько, АлтГУ, юридический факультет, 3 к.
Научный руководитель – ***И.А. Анисимова,*** к.ю.н, доцент.

В современном мире система кредитования получила огромное распространение. К концу 2013 г. долг россиян перед банками составил 10 триллионов рублей, причем необеспеченные кредиты представляют большую часть этой суммы. По оценкам Российской Ассоциации кредитных союзов 10 триллионов рублей задолженности приходится на 55 миллионов россиян. Около 65% этой суммы уходит на дорогие необеспеченные кредиты [1]. Учитывая, что риски при необеспеченном кредитовании выше, да и многие заемщики оказываются недобросовестными, банкам приходится искать различные методы возвращения своих денежных средств.

В последнее время особенное распространение получили организации, которые специализируются на взыскании долгов – коллекторские агенства. Деятельность данных организаций по сути заключается в оказании банкам услуг по возврату просроченной дебиторской задолженности последних, либо вовсе "выкупе" долгов у банков. Часто действия подобных фирм по взысканию задолженности выходят за рамки простых звонков и переходят в угрозы, запугивание клиентов, вымогательство, не говоря уже о физическом воздействии на должников. Данные действия, безусловно, носят противоправный характер и могут быть квалифицированны в определенных случаях по следующим статьям УК РФ: 110, 111, 112, 115, 116, 119, 163 и др. Краеугольным деятельности данных фирм является вопрос о передачи банком им сведений, составляющих банковскую тайну, не подпадает ли такая пе-

редача под действие ст. 183 УК РФ "Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну".

В соответствии со ст. 857 ГК РФ банк гарантирует тайну банковского счета и банковского вклада, операций по счету и сведений о клиенте. Основные юридические гарантии банковской тайны представлены в виде установленной законодательством административной (ст. 13.14 КоАП РФ), гражданско-правовой (ч. 3 ст. 857 ГК РФ) и уголовной (ст. 183 УК РФ) ответственности.

Согласно ч. 2 ст. 183 УК РФ ответственность наступает за незаконные разглашение или использование сведений, составляющих коммерческую, налоговую или банковскую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе. Разглашение – это действие или бездействие, в результате которого информация, составляющая ту или иную тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору [2]. На основе же заключенного договора об оказании услуг коллекторские агентства получают от банков как раз сведения об их должниках, которые, как правило, включают информацию о личности должника, размере долга, номере и дате кредитного договора, сроке просрочки, расчете неустойки и др. [3]. Рынок коллекторских услуг долгое время не работал, так как судебная практика негативно относилась к разного рода уступкам требования. Он начал активно развиваться с 2008 г. в связи с изменением судебной практики в части уступки требований. В информационном письме Президиума ВАС РФ от 30 октября 2007 г. № 120 "Обзор практики применения арбитражными судами положений главы 24 Гражданского кодекса Российской Федерации" в п. 2 выражена позиция, ставшая основой легального развития коллекторского рынка: уступка банком прав кредитора по кредитному договору юридическому лицу, не являющемуся кредитной организацией, не противоречит законодательству [4]. Только в 2012 г. банки продали долгов коллекторам на десятки миллиардов рублей.

Согласно ч. 2 ст. 183 УК РФ однозначно наступает ответственность за разглашение информации составляющей банковскую тайну без согласия ее владельца. Однако спорным является вопрос, когда подобное согласие дано. В ч. 2 ст. 183 УК РФ не конкретизируется, каким образом должно быть дано согласие владельца на передачу его сведений третьим лицам. В связи с этим можно сделать вывод, что для того, чтобы застраховаться от угроз уголовного преследования, банку достаточно зафиксировать любым образом согласие заемщика на распространение сведений, которые подпадают под определение банковской тайны. Например, достаточно вставлять в кредитные договоры (как с организациями, так и с физическими лицами) оговорку о том, что в случае неплатежа банк имеет право в ходе взыскания задолженности передавать сведения о заемщике, указанные в кредитном договоре, третьим лицам [5]. Согласно письму Ассоциации российских банков от 05.10.2010 № А-01/5-747 такой подход и выработан. В кредитный договор включается соответствующее волеизъявление клиента, благодаря чему сведения об операциях по кредитному договору выводятся из-под действия нормы о банковской тайне еще при заключении кредитного договора [6]. Наличие подобной оговорки казалось бы полностью исключает возможность привлечения банка к уголовной ответственности, но ряд правоведов справедливо усматривают противоречия в подобном положении дел [7,8].

В силу п. 2 ст. 857 ГК РФ банк гарантирует тайну банковского счета и банковского вклада, операций по счету и сведений о клиенте. Сведения, составляющие банковскую тайну, могут быть предоставлены только самим клиентам или их представителям, а также представлены в бюро кредитных историй на основаниях и в порядке, которые предусмотрены законом [9]. Государственным органам и их должностным лицам такие сведения могут быть предоставлены исключительно в случаях и порядке, которые предусмотрены законом. Исчерпывающий перечень государственных органов и должностных лиц, имеющих право получать сведения, составляющие банковскую тайну, установлен ст. 26 Федерального закона "О банках и банковской деятельности". Таким образом, сведения, составляющие банковскую тайну, могут быть предоставлены только самим клиентам или их представителям, а

также госорганам и иным лицам в случаях и в порядке, которые предусмотрены законом. Коллекторские агентства ни при каких условиях в данный список не входят.

Проблемы же вызывает оговорка в ч. 2 ст. 183 УК РФ о согласии владельца на передачу информации, составляющей банковскую тайну. Банк не вправе выполнять волю клиента, выраженную в договоре, о предоставлении информации третьим лицам, так как все возможные действия банка императивно предусмотрены законом, и внести изменения в эти нормы не может и клиент, несмотря на то, что информация касается его самого. Информация, подпадающая под правовой режим банковской тайны, не меняет его и в связи с состоявшейся выдачей кредита. Сама банковская операция как таковая не завершена, так как кредитование – это многостадийный и сложный, но единый процесс, который начинается с момента обращения заемщика в банк с заявлением о предоставлении кредита и продолжается до момента полной уплаты всех начисленных по договору сумм. В период исполнения должником обязанности по возврату кредита и уплате процентов могут возникнуть вопросы реструктуризации долга, обеспечения кредита и многие другие, что вполне может быть решено в отношениях с банком, но, скорее всего, невозможно в отношениях с коллекторской организацией [8].

Считаю, что в законодательстве недостаточно внимания уделяется вопросам ответственности за нарушение банковской тайны, что и является одной из причин, по которой ее нарушение часто вообще не рассматривается как проблема. Уголовная ответственность в соответствии с ч. 2 ст. 183 УК РФ действительно, несмотря на указанные выше противоречия, наступает за разглашение банковской тайны лишь при отсутствии согласия владельца информации. Однако в отношении передачи информации, составляющей банковскую тайну, судебная практика противоречива.

Обозначенная проблема требует своего решения, так как часто коллекторская деятельность выходит за рамки закона, да и сама банковская тайна требует более тщательной охраны. Она не может передаваться юридическим лицам, осуществляющим сомнительную с точки зрения закона деятельность. Выходом из данной ситуации может быть либо регулирование деятельности орга-

низаций по сбору долгов путем принятия соответствующего Федерального закона, в котором была бы установлена ответственность коллекторских агентств и их должностных лиц за разглашение сведений, составляющих банковскую тайну. Второй путь состоит во внесении изменений в ч. 2 ст. 183 УК РФ, которыми была бы исключена оговорка о согласии владельца банковской, коммерческой и налоговой тайны на ее разглашение. Считаем второй подход правильным с позиции защиты прав заемщиков, так как, во-первых, органы и должностные лица, которые могут получать сведения составляющие банковскую тайну прямо указаны в законе и расширительного толкования здесь быть не должно. Во-вторых, банки могут получать свои денежные средства, используя государственный механизм защиты. По данным Судебного департамента при Верховном Суде РФ, в 2012 г. в 1,5 раза выросло число исков банков к должникам по кредитам. За 6 месяцев исковые требования банков были удовлетворены в 535 тыс. дел. Общая сумма взысканий по искам о возврате кредитных средств выросла до 148,3 млрд. рублей. При этом в среднем с гражданина взыскивали по 250 тыс. рублей, тогда как в 2011 г. средний долг по искам составлял 306 тыс. рублей. В-третьих, при необходимости и желании клиент сам может передавать сведения любым субъектам, а не поручать это право банкам.

Список литературы

1. Шандрина Т. Долг россиян перед банками в 2013 году составит 10 трлн рублей // Сайт Российской газеты [Электронный ресурс]. URL: http://www.rg.ru/2013/12/16/krediti-site-anons.html
2. Комментарий к Уголовному кодексу Российской Федерации / под ред. А.И. Чучаева. М.: КОНТРАКТ, 2012 // Консультант Плюс: Справочно-правовая система [Электронный ресурс] / ЗАО «Консультант Плюс». – Версия 2014. – Режим доступа: (внутриуниверситетская компьютерная сеть).
3. Конюшко Е.В Гражданско-правовая ответственность за незаконное разглашение банковской тайны как гарантия прав клиента кредитной организации // Право и политика. 2007. № 10 // Консультант Плюс: Справочно-правовая система [Электронный ресурс] / ЗАО «Консультант Плюс». – Версия 2014. – Режим доступа: (внутриуниверситетская компьютерная сеть).

4. Фогельсон Ю.Б. Защита прав потребителей финансовых услуг. М.: Норма, Инфра-М, 2010 // Консультант Плюс: Справочно-правовая система [Электронный ресурс] / ЗАО «Консультант Плюс». – Версия 2014. – Режим доступа: (внутриуниверситетская компьютерная сеть).
5. Иванов Н.С. Защита персональных данных и банковской тайны при взыскании долгов // Юридическая работа в кредитной организации. 2009. № 4. // Консультант Плюс: Справочно-правовая система [Электронный ресурс] / ЗАО «Консультант Плюс». – Версия 2014. – Режим доступа: (внутриуниверситетская компьютерная сеть).
6. Оськина И., Лупу А. Законна ли деятельность коллекторских агентств? // Хозяйство и право. 2011. № 3. // Консультант Плюс: Справочно-правовая система [Электронный ресурс] / ЗАО «Консультант Плюс». – Версия 2014. – Режим доступа: (внутриуниверситетская компьютерная сеть).
7. Воронцова С.В., Золотарева А.Ю. Сохранение банковской тайны и новые электронные технологии // Налоги. 2010. № 22. // Консультант Плюс: Справочно-правовая система [Электронный ресурс] / ЗАО «Консультант Плюс». – Версия 2014. – Режим доступа: (внутриуниверситетская компьютерная сеть).
8. Кукушкин В. Коллекторы в законе // ЭЖ-Юрист. 2012. № 5. // Консультант Плюс: Справочно-правовая система [Электронный ресурс] / ЗАО «Консультант Плюс». – Версия 2014. – Режим доступа: (внутриуниверситетская компьютерная сеть).
9. О кредитных историях: Федеральный закон от 30 декабря 2004 г. № 218-ФЗ // Сайт справочно-правовой системы Консультант Плюс [Электронный ресурс]. URL: http://www.consultant.ru

ПРОБЛЕМЫ ПРИВЛЕЧЕНИЯ К УГОЛОВНОЙОТВЕСТВЕННОСТИ ПО СТ. 274 УК РФ

Р.Г. Диденко, АлтГУ, юридический факультет, 3 к.
Научный руководитель – ***И.А. Анисимова,*** к.ю.н., доцент.

Впервые в УК РФ 1996 г. появилась целая глава (гл. 28), в которой была установлена уголовная ответственность за преступления в сфере компьютерной информации. В эту главу вошли все-

го три статьи – 272, 273, 274. Ст. 274 УК РФ предусматривает ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей. Она имеет целью предупреждение невыполнения пользователями своих профессиональных обязанностей, влияющих на сохранность хранимой и перерабатываемой информации. Федеральным законом № 420-ФЗ от 7 декабря 2011 г. в данные нормы, в том числе и ст. 274 УК РФ были внесены существенные изменения, требующие научного анализа.

Говоря о практике применения ст.ст. 272–274 важно подчеркнуть, что статистка не фиксирует большого количества данных преступлений. Так, доля преступлений в сфере компьютерной информации в общей массе зарегистрированных преступлений составляет порядка 0,3% [1, С. 84]. При этом среди преступлений, предусмотренных гл. 28 УК РФ, рассматриваемое деяние является наименее распространенным. Так, по данным ГИЦ МВД России, каждый год фиксируется единичное количество таких нарушений, например, в 2001 г. – 2 преступления; в 2002 – 88; в 2003 – 1; 2004 – 11, в 2005 г. – 2, в 2006 – 3, в 2007 – 7, в 2008 – 17, в 2009 – 5 [2]. На наш взгляд, приведенные цифры показывают, что правоохранительные органы умеют выявлять и расследовать преступления в сфере компьютерной информации, но они бессильны, когда сама норма сформулирована так, что осудить виновное лицо практически невозможно.

В юридической литературе подчеркивается, что все статьи гл. 28 УК РФ вызывают критику, однако наиболее уязвимой является ст. 274 УК РФ [1, С. 85]. Рассмотрим наиболее проблемные вопросы, возникающие при толковании положений ст. 274 УК РФ.

Для привлечения лица к уголовной ответственности по ч. 1 ст. 274 УК следует установить, какие конкретно правила эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации были нарушены.

Это и есть самая большая сложность в трактовке и применении указанной статьи. Правила могут быть самыми различными: начиная от тех, которые создаются самими разработчиками электронно-вычислительной техники, до правил, которые действуют только на конкретных предприятиях и фирмах, а также правил,

разрабатываемых и утверждаемых соответствующими министерствами и ведомствами, законодательными актами субъектов Федерации. Рассматриваемые правила могут также содержаться в некоторых международных договорах и соглашениях, заключенных Российской Федерацией.

Количество всевозможных правил и инструкций (и их трактовок) неисчерпаемо и устанавливать уголовную ответственность за нарушения их всех вряд ли правомерно. Возникает вопрос: чем же следует руководствоваться, определяя, нарушены ли правила эксплуатации? В специальной литературе рекомендуется руководствоваться государственными стандартами, нормами и правилами (ГОСТ Р МЭК 60950-2002, ГОСТ 26329-84, ГОСТ Р 51318.22-2006) [3, С. 40]. Однако стоит согласиться с мнением Д.А. Зыкова, что в основе данной бланкетной диспозиции должен лежать нормативный правовой акт, принятый соответствующим органом государственной власти. Только тогда применение ст. 274 УК РФ будет законным. [1].

Возможно ли привлечь к уголовной ответственности лицо, которое в результате нарушения эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей повредило не информацию, а работоспособность самой компьютерной техники или ее сети?

Такое последствие не указано ни в одной статье преступлений в сфере компьютерной информации, обязательным условием является вред, причиняемый информации. Значит, если не повреждать и не копировать информацию, можно причинять любой вред компьютерным системам и сетям. Иными словами, формулировка данной статьи не охватывает все возможные общественно опасные последствия данного деяния. Этот недостаток состава преступления, предусмотренного ст. 274 УК РФ должен быть устранен [2].

Существует проблема определения умысла в рассматриваемом составе преступления, осложненном несколькими уровнями общественно опасных последствий.

Полагаем, что субъективная сторона преступления, предусмотренного ст. 274 УК РФ характеризуется виной в форме неосторожности в отношении последствий второго уровня (крупного ущерба). К последствиям первого уровня (копирование, блокиро-

вание, удаление и иные) виновный может относиться как с умыслом, так с неосторожностью. Отношение виновного к тяжким последствиям, закрепленных в ч. 2 ст. 274 УК РФ может быть только неосторожным. При наличии умысла по отношению к общественно опасным последствиям деяние необходимо квалифицировать как самостоятельное преступление в соответствии с причиненным вредом.

Нет единой позиции, охватывается ли «тяжкими последствиями» только имущественный ущерб либо и иные последствия, например, физический вред, тоже входят в объективную сторону преступления.

Исходя из практики применения ст. 274 УК РФ следует констатировать, что, как правило, последствия выражаются только в имущественном ущербе. Однако анализируя конкретный пример, где сотрудник медицинской организации вносит вредоносную программу, что приводит к остановке работы аппарата искусственного дыхания и смерти пациента, мы приходим к выводу, что возможно причинение, в результате совершения данного преступления и физического вреда (тяжкого вреда здоровью, смерти). Однако в этом случае возникает конкуренция норм, предусмотренных ст.ст. 274 и 109 УК РФ. Так же конкуренция возможна и со ст. 143 УК РФ при нарушении требований безопасности работ со средствами обработки информации. Представляется, что ст. 274 УК РФ является специальной по отношению к ст.ст. 109, 143 УК РФ и охватывает последствия, содержащиеся в указанных общих нормах.

Возникает вопрос, будет ли наступать уголовная ответственность за нарушение правил пользования глобальными сетями (интернет).

Ю.И. Ляпунов и В.С. Максимов отмечали применительно к ранее действовавшей редакции ст. 274 УК РФ, что «поскольку речь идет о правилах эксплуатации именно ЭВМ, т.е. аппаратно-технической структуры, то и нарушение их должно затрагивать только техническую сторону несоблюдения требований безопасности компьютерной информации, а не организационную или правовую. К таковым можно отнести: блокировку системы защиты от несанкционированного доступа, нарушение правил электро- и противопожарной безопасности, использование ЭВМ в условиях,

не отвечающих тем, которые установлены документацией по ее применению (по температурному режиму, влажности, величине магнитных полей и т.п.), отключение сигнализации, длительное оставление без присмотра и многие другие» [4, с. 17].

Вместе с тем, по нашему мнению, на данный вопрос можно дать положительный ответ. Сеть «Интернет» представляет собой глобальное объединение компьютерных сетей и информационных ресурсов. Это объединение является децентрализованным, и единого общеобязательного свода правил (законов) пользования сетью «Интернет» не установлено. Существуют, однако, общепринятые нормы работы в сети «Интернет», направленные на то, чтобы деятельность каждого пользователя сети не мешала работе других пользователей. Фундаментальное положение этих норм таково: правила использования любых ресурсов сети «Интернет» (от почтового ящика до канала связи) определяют владельцы этих ресурсов. [3]

Таким образом, нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей могут быть подразделены на физические (неправильное подключение периферийного оборудования, отсутствие устройств бесперебойного питания, нарушение теплового режима в помещении, неправильное подключение компьютера к источникам питания, нерегулярное техническое обслуживание, использование несертифицированных средств защиты и самодельных узлов и приборов и пр.) и интеллектуальные (невыполнение процедуры резервного копирования, несанкционированная замена программного обеспечения, параметров настройки компьютера или компьютерной сети и пр.) [4].

Некоторые авторы, отмечая недостатки положений ст. 274, предлагают исключить данную статью из УК РФ.

Так, Н.А. Лопашенко отмечает, что говоря «о нарушении правил эксплуатации ЭВМ, системы ЭВМ или их сети, необходимость криминализации такого отклоняющегося (безусловно) поведения очевидной не является. Использование законодателем двух уровней последствий в качестве обязательных признаков состава подчеркивает то, что опасность самого деяния не велика» [5].

Однако ст. 274 УК РФ следует не исключать из Уголовного кодекса, а скорректировать формулировку диспозиции данной статьи в целях повышения эффективности рассматриваемой нормы. В порядке обсуждения вопроса мы можем предложить следующую редакцию ст. 274 УК РФ.

Статья 274. Нарушение требований по обеспечению компьютерной безопасности.

1. Нарушение требований использования компьютерной техники или ее сети, если это деяние повлекло по неосторожности крупный ущерб…
2. То же деяние, повлекшее по неосторожности тяжкие последствия.

В ст. 274 УК РФ следует включить Примечание, где конкретизировать, перечень нормативно правовых актов, содержащих требования использования компьютерной техники или ее сети.

Список литературы

1. Зыков Д.А. Проблемы установления уголовной ответственности по статье 274 УК РФ // Вестник Владимирского юридического института. 2011. № 2 (19) С. 84–86. Режим доступа: http://elibrary.ru/download/75303780.pdf
2. Гончарова Д.И. Проблематика уголовной ответственности за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей [Электронный ресурс]. Режим доступа: www.scienceforum.ru/2014/pdf/7415.pdf (дата обращения 01.01.2014).
3. Чекунов И. Г. Киберпреступность: понятие и классификация // Российский следователь. 2012. № 2. С. 37–44.
4. Ляпунов Ю., Максимов В. Ответственность за компьютерные преступления // Законность. 1997. № 1. С. 17.
5. Лопашенко Н.А. Уголовная политика. М., 2009. С. 384–387.

СТ. 137 УК РФ: ПРОБЛЕМЫ КВАЛИФИКАЦИИ

И.Е. Золотарёв, АлтГУ, юридический факультет, 3 к.
Научный руководитель – ***И.А. Анисимова,*** к.ю.н., доцент.

Частная жизнь – это сфера, контролируемая самим человеком и свободная от внешнего воздействия. Государство и законодательство не вправе вторгаться в неё, они лишь ограждают её от постороннего вмешательства [1].

Право на частную жизнь представляет собой достаточно широкое понятие, включающее в себя несколько конкретных правомочий человека. Уголовное право охраняет права и свободы человека от наиболее опасных посягательств. Согласно ч. 1 ст. 137 УК РФ уголовно наказуемыми являются незаконное собирание или распространение сведений о частной жизни лица, которые составляют его личную или семейную тайну.

Для правового регулирования правоотношений, связанных с той или иной тайной, необходимо, чтобы понятие этой тайны и все объективные критерии отнесения сведений к этой тайне были определены в законодательстве – федеральным законом. Только в этом случае будет обеспечено недопущение произвольной трактовки понятия конкретной тайны и как следствие, – не будет неправомерного ограничения прав и свобод человека и гражданина на получение информации.

В действующем российском законодательстве отсутствует нормативное определение личной и семейной тайны. Не закреплены в нем и критерии отнесения той или иной информации к этим видам тайн. Таким образом, использование таких дефиниций как «личная тайна» и «семейная тайна» в правоприменительных решениях, тем более в уголовном обвинении вызывает справедливое сомнение с точки зрения своей конституционности по причине правовой неопределенности этих понятий.

В качестве примера приведём конкретное дело из опубликованной судебной практики:

Лицо обвинялось в том, что он, работая в архиве ИЦ УВД по Архангельской области подготовило базу данных о фактах репрессий в отношении немцев, проживавших в СССР в период Великой Отечественной Войны. Данная база была необходима для создания очередной «Книги памяти репрессированных». Конкрет-

но обвиняемому был поставлен в вину сбор сведений о том, что потерпевшие:

- были вывезены немецкими оккупационными властями в Германию или Польшу, а затем вернулись в СССР по репатриации;
- были призваны и служили в немецкой армии, принимали участие в боевых операциях против Красной Армии;
- были взяты в плен советскими войсками и направлены в лагерь для военнопленных;
- были осуждены советскими судебными органами;
- прибыли из Германии по репатриации и состояли на учете в спецпоселении в Архангельской области.

Тем самым, обвиняемый совершил сбор сведений о частной жизни лиц, составляющих их личную или семейную тайну, нарушив неприкосновенность частной жизни репрессированных спецпоселенцев. Суд первой инстанции признал обвиняемого виновным по ч. 1 ст. 137 УК РФ [2].

При вынесении данного решения суд учитывал положения п. 3 ст. 25 Федерального закона РФ от 22 октября 2004 г. № 125-ФЗ, где закреплено, что ограничение на доступ к архивным документам, содержащим сведения о личной и семейной тайне гражданина, его частной жизни, а также сведения, создающие угрозу для его безопасности, устанавливается на срок 75 лет со дня создания указанных документов. С письменного разрешения гражданина, а после его смерти с письменного разрешения наследников данного гражданина ограничение на доступ к архивным документам, содержащим сведения о личной и семейной тайне гражданина, его частной жизни, а также сведения, создающие угрозу для его безопасности, может быть отменено ранее чем через 75 лет со дня создания указанных документов [3].

Однако при отнесении собранной обвиняемым информации к личной и семейной тайне суд руководствовался исключительно мнением потерпевших – родственников спецпоселенцев, которые считали, что собранные сведения являются их личной или семейной тайной, поскольку они носят некомплиментарный характер и распространение таких сведений может нанести им репутационный ущерб [4].

Данный пример из судебной практики показывает следующее: в практической деятельности, в том числе связанной с доступом к архивным документам, правоприменители, вынося свои решения, не столько ссылаются на закон, сколько мотивируют решения тем, что данные сведения являются личной и семейной тайной для самого потерпевшего. Однако одного лишь желания гражданина скрыть какие-то касающиеся его сведения, пусть даже некомплиментарного характера, не может быть достаточно для их отнесения к какой-либо тайне вообще, и к личной или семейной тайне, в частности. [5]

Нарушение принципа формальной определенности в статье 137 УК РФ заключается в том, что понятия «личная тайна» и «семейная тайна» не имеют четкого, точного, ясного содержания, которое необходимо для привлечения лица к уголовной ответственности за нарушение этих тайн. Неопределенность содержания этих понятий связана с тем, что отсутствует их легальное определение, и, как следствие, правоприменители истолковывают их неоднозначно. В итоге это приводит к нарушению общих принципов права, таких как равенство и справедливость, которым надлежит следовать при введении тех или иных ограничений прав и свобод человека и гражданина. [6]

В приведенном примере судебной практики установление режима личной и семейной тайны для тех или иных сведений о частной жизни поставлено в зависимость в первую очередь от желания (волеизъявления) субъекта (субъектов – если речь идет о семейной тайне), которого (которых) эти сведения касаются, т.е. понятия «личная и семейная тайна» в значительной степени отнесены к субъективным категориям. В правоприменительной практике сложилась ситуация, при которой за собирание и распространение одной и той же информации (например, сведения о социальном происхождении) в одном случае (если лицо решило отнести такую информацию к личной или семейной тайне) субъект может быть привлечен к уголовной ответственности, в другом случае (если лицо не относит такую информацию к личной и семейной тайне) – нет.

Такая ситуация лишает субъекта возможности предвидеть негативные последствия своего поведения, наступающие при использовании информации, касающейся иного лица, поскольку

остается неясным может ли эта информация относиться к личной или семейной тайне.

На основании вышеизложенного мы предлагаем исходить из следующего подхода к пониманию указанных видов тайн.

«Личную и семейную тайны» понимать не как самостоятельные виды тайн, а как собирательные понятия. Такой подход к их пониманию основывается на том, что личная и семейная тайна по сути объединяют в себе уже существующие и закрепленные в отдельных федеральных законах виды тайн, касающиеся разнообразных личных и семейных правоотношений. Например, к личной тайне можно было бы отнести такие виды тайн, как врачебная тайна (установлена ст. 61 Основ законодательства РФ об охране здоровья граждан), тайна завещания (установлена ст. 1123 ГК РФ). Примером же семейной тайны является тайна усыновления (установлена ст. 139 Семейного кодекса РФ). [7]

Кроме того, исправлению создавшейся ситуации может способствовать внесение в ряд нормативных правовых актов (в том числе в архивное законодательство) соответствующих изменений, которые бы восполнили вышеуказанный пробел, а именно законодательно конкретизировали те сведения, которые непосредственно относятся к личной и семейной тайне.

Список литературы

1. Романовский, Г.Б. Право на неприкосновенность частной жизни. М., 2001. С. 58-81.
2. Павлов И.Ю. Конституционно-правовые проблемы толкования ст. 137 УК РФ. Сайт Международной ассоциации содействия правосудию. [Электронный ресурс]. URL: http://www.iuaj.net/node/921 (дата обращения: 07.04.2014).
3. Об архивном деле в Российской Федерации Федеральный закон от 22.10.2004 № 125-ФЗ (ред. от 11.02.2013) // СПС «Консультант Плюс» [Электронный ресурс] – Электр. дан. – Заглавие с экрана. URL: http://www.consultant.ru. (дата обращения 10.05.2014).
4. Российское уголовное право: в 2 т. Т.2. Особенная часть: учебник / Г.Н. Борзенков [и др.]; под ред. Л.В. Иногамовой-Хегай, В.С. Комиссарова, А.И. Рарога. 3-е изд., перераб. и доп. М.: Проспект, 2010. 688 с.

5. Уголовное право России. Общая и особенная часть: учебник / под ред. В.К. Дуюнова. 3-е изд., М.: ПРИОР: ИНФА-М, 2012. 681 с.
6. Замошкин, Ю.А. Частная жизнь, частный интерес, частная собственность // Вопросы философии. 1991. № 1. С. 3-15.
7. Уголовное право. Особенная часть: учебник. 2-е изд. исправ. и доп. / под ред. Л.В. Иногамовой-Хегай, А.И. Рарога, А.И. Чучаева. М.: Юридическая фирма «КОНТРАКТ»: ИНФРА-М, 2008. 560 с.

РАЗРАБОТКА ПРОЕКТА ЭКСПЕРТНОЙ СИСТЕМЫ РЕКОМЕНДАЦИЙ СРЕДСТВ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ОТ УТЕЧКИ ИНФОРМАЦИИ ПО ВИБРОАКУСТИЧЕСКОМУ КАНАЛУ

М.С. Иванов, АлтГУ, физико-технический факультет, 3 к.
Научный руководитель – ***П.В. Малинин,***
преподаватель.

Тенденция развития современных технологий характеризуется постоянным повышением значения и ценности информации. Разнообразные способы и приборы снятия информации по техническим каналам представляют серьезную угрозу компаниям и организациям, заинтересованным в защите конфиденциальных переговоров, а также сохранности конфиденциальной информации. Учитывая особенности расположения большинства офисов коммерческих предприятий и фирм в жилых домах, разъединённых с неизвестными соседями сбоку, сверху и снизу несущими конструкциями с недостаточной защитой от утечки по техническим каналам, задача защиты конфиденциальных переговоров и сохранении конфиденциальной информации становится особо актуальной и достаточно сложной.

Под утечкой информации понимается несанкционированный перенос информации от её источника к злоумышленнику. Физический путь несанкционированного распространения носителя с защищаемой информацией от её источника к злоумышленнику образует канал утечки информации. Технический канал утечки информации представляет совокупность объекта защиты (источ-

ника конфиденциальной информации), физической среды и средства технической разведки (промышленного шпионажа), которыми добываются разведывательные данные [1].

Различают следующие технические каналы утечки информации: видовой (оптический), акустический (виброакустический), радиоэлектронный (электромагнитный и электрический), материально-вещественный.

Обзор средств защиты информации от утечки по виброакустическому каналу.

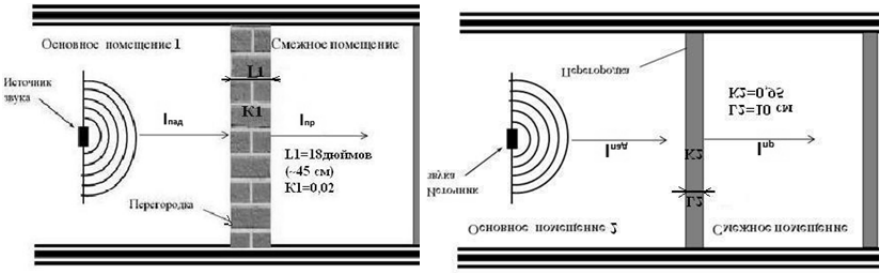
Задачей технических средств защиты информации является либо ликвидация каналов утечки информации, либо снижение качества получаемой злоумышленником информации. Виды средств защиты: пассивные (окна, двери, стены, полы, потолки), активные (шумогенераторы, виброизлучатели).

Пассивное техническое средство защиты – устройство, обеспечивающее скрытие объекта защиты от технических способов разведки путем поглощения, отражения или рассеивания его излучений. Цель пассивного способа – максимально ослабить акустический сигнал от источника звука, например, за счет отделки стен звукопоглощающими материалами. **Активное техническое средство защиты** – устройство, обеспечивающее создание маскирующих активных помех (или имитирующих их) для средств технической разведки или нарушающие нормальное функционирование средств негласного съема информации. Активные способы предупреждения утечки информации можно подразделить на обнаружение и нейтрализацию этих устройств [2].

Меры по определению степени защищенности помещения являются весьма дорогостоящими. Специалисты по защите информации определяют степень защищенности помещения и необходимые защитные меры после проведения соответствующих измерений. Иногда стоимость измерений и защитных мер бывает значительной, что усложняет принятие решения о целесообразности проведения этих мер. Поэтому необходимо предварительно оценивать стоимость средств технической защиты информации. Одним из выходов в данной ситуации является расчет предварительной стоимости средств технической защиты на основе известных характеристик пассивных и активных технических средств защиты и задаваемого уровня защищенности помещения.

В данной работе рассмотрено формирование рекомендаций для абстрактных помещений по обеспечению защиты информации от утечки по виброакустическому каналу.

Пусть помещение 1 (рис. 1 а) изначально не планировалось, как комната переговоров, и перегородка со смежным помещением была выполнена из кирпича. Толщина перегородки L1 = 18 дюймов (~ 45 сантиметров). Воспользовавшись данными [2], которые приведены в таблице, установили, что коэффициент поглощения К1 данной перегородки на частоте 1 КГц при разговоре равен порядка ~0,02. Или, проще говоря, перегородка поглотит 2% издаваемых в помещении звуков. Прослушать данное помещение не составит большого труда.



а) *б)*

Рис. 1. Пример абстрактных помещений. а) – кирпичная перегородка, б) – перегородка из воздухопроницаемого асбестоцемента.

Второе помещение (рис. 1 б) изначально предполагалось для использования в качестве комнаты переговоров. Соответственно, перегородка со смежным помещением была изготовлена из материала с большим коэффициентом поглощения, а именно, из воздухопроницаемого асбестоцемента. Толщина перегородки L2=10 см, коэффициент поглощения К2 данного материала равен 0,95 (поглощает порядка 95% речи). Прослушать данное помещение практически невозможно.

Таблица 1.

Различные материалы и их коэффициенты поглощения.

Поверхности	Частота		
	125 Гц	1 кГц	4 кГц
Кирпичная стена (толщины ~45 см, некрашеная)	0,02	0,04	0,07
Кирпичная стена (толщины ~45 см, крашеная)	0,01	0,02	0,02
Штукатурка для внутренних работ на металлической сетке	0,02	0,06	0,03
Бетон уложенный	0,01	0,02	0,03
Пол из сосновых досок	0,09	0,08	0,10
Акустическая плитка (~1,5 см)	0,50	0,75	0,65
Панели (~2,5 см)	0,35	0,35	0,65
Панели из фанеры (~5 см, воздушная прослойка)	0,30	0,10	0,07
Воздухопроницаемый асбестоцемент (10 см)	0,90	0,95	0,45
Щиты Бекеши(холст, натянутый по вате)	0.80	0.73	0.43

Для того, чтобы достичь большего коэффициента поглощения перегородки №1 и приблизиться к параметрам перегородки №2, тем самым исключить (снизить) утечку информации по виброакустическому каналу можно использовать разные способы:

1. Покрыть кирпичную стену акустической плиткой (5/8 дюйма или ~1,5 см) с коэффициентом поглощения на частоте 1 КГц 0,75 (75% речи). Средняя стоимость такой плитки за 1 кв.м. составляет 3$ или 150 руб.
2. Использовать щиты Бекеши (холст на вате толщиной 40 мм) с коэффициентом поглощения 0,73. Средняя стоимость данного щита составляет ~250руб за 1 кв.м.
3. Установить генератор шума. К примеру, генератор шума Соната РС-1 (базовый набор) стоит 14900 руб.

При выборе ограждающих конструкций выделенных помещений в процессе проектирования необходимо руководствоваться следующими правилами:

- в качестве перекрытий рекомендуется использовать акустически неоднородные конструкции;
- в качестве полов целесообразно использовать конструкции на упругом основании или конструкции, установленные на виброизоляторы;
- потолки целесообразно выполнять подвесными, звукопоглощающими со звукоизолирующим слоем;

- в качестве стен и перегородок предпочтительно использование многослойных акустически неоднородных конструкций с упругими прокладками (резина, пробка, ДВП и т.п.).

Таким образом, достичь требуемого уровня защиты информации от утечки по виброакустическому каналу выделенного помещения можно несколькими путями, которые, в свою очередь, имеют разную стоимость.

С помощью данной экспертной системы рекомендаций средств технической защиты от утечки информации по виброакустическому каналу можно будет получить рекомендации вида: как и какими средствами можно обеспечить защищенность информации от утечки по виброакустическому каналу, также узнать стоимость тех или иных вариантов обеспечения безопасности.

В данной работе была разработана структура системы рекомендаций (рис. 2). Входными являются такие параметры как: коэффициент поглощения К, толщина перегородки L, уровень звукового сигнала I*пр*. Также к таким параметрам относится материал, из которого сделана перегородка. Входные параметры можно увидеть на рис. 1. Используя входные параметры, можно определить, с помощью методики по Н.Б. Покровскому, такую важную характеристику, как разборчивость речи [3,4]. Далее, опираясь и анализируя все имеющиеся параметры и характеристики, экспертная система выдаёт рекомендации мер защиты. На следующем этапе происходит сравнение рекомендаций и происходит выбор оптимальных мер защиты, исходя из преследуемых целей и задач. На выход поступают итоговые рекомендации, полученные в блоке сравнений.

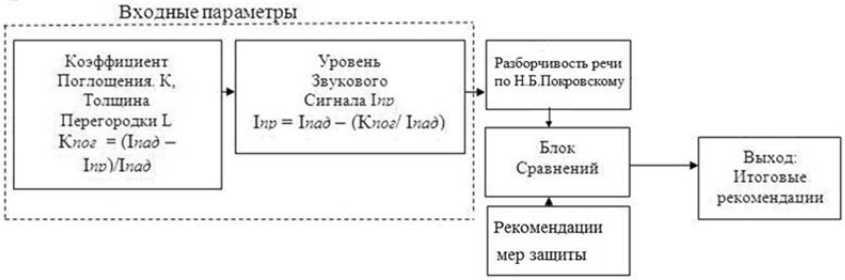


Рис. 2. Структура системы рекомендаций.

Данная работа будет полезна для всех сотрудников, работающих в сфере обеспечения информационной безопасности. Плюс системы рекомендаций – это возможность потенциального заказчика оценить примерную стоимость и возможные конфигурации защиты непосредственно перед работой либо заказом. Данная система рекомендаций будет расширена на другие технические каналы утечки информации.

Список литературы.

1. Торокин А.А. Инженерно-техническая защита информации. – М.: Изд-во Гелиос АРВ, 2005. – 960 с.
2. Халяпин Б.Д. Защита информации. Вас подслушивают? Защищайтесь! – М.: Изд-во Москва «БОЯРД», 2004. – 432 с.
3. Железняк В.К., Макаров Ю.К., Хорев А.А. Некоторые методические подходы к оценке эффективности защиты речевой информации // Специальная техника. – М.: 2000. - №4.
4. Хорев А.А., Макаров Ю.К. К оценке эффективности защиты акустической (речевой) информации // Специальная техника. – М.: 2000. - №5.

СИТУАЦИИ РАССЛЕДОВАНИЯ НЕПРАВОМЕРНОГО ДОСТУПА К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

С.В. Казанцев, АлтГУ, юридический факультет, 5 к.
В.В. Поляков, к.ю.н., доцент.

На первоначальном этапе расследования компьютерных преступлений следователь действует в условиях недостаточной исходной информации по делу. Имеющиеся признаки преступления, как правило, могут быть истолкованы неоднозначно [1]. В таких условиях находит свое применение положение, высказанное В.Е. Корноуховым, согласно которому «для решения той или иной задачи должны разрабатываться и отражаться в методике несколько комплексов следственных действий и оперативно-розыскных мероприятий, которые были бы адаптивны к разным условиям расследования преступлений [2]. В криминалистике эффективно практикуется ситуационный подход в расследовании сложных преступлений [3]. Полагаем, что следственная ситуация - это та

обстановка, которая создается при расследовании преступления и объективно отражает «внутреннее состояние, ход и условия расследования на основе совокупности фактических и иных данных» [4]. Базовым компонентом следственных ситуаций является типичная следственная ситуация, которая требует своих тактико-технических приемов разрешения. Она характеризуется устойчивым комплексом признаков, включающих в себя «общие черты хода и состояния расследования к определенному его моменту» [5], отражающих общие черты криминалистической характеристики данного вида преступлений и наиболее вероятную обстановку их расследования.

На основе совокупности криминалистически значимых данных, характерных для соответствующих ситуаций, можно выдвигать следственные типовые версии [6]:

1. заявление о неправомерном удаленном доступе к компьютерной информации подтверждается, преступление действительно имеет место;
2. заявитель ошибается или заблуждается, неправомерного удаленного доступа к компьютерной информации не произошло;
3. имеет место ложное заявление о неправомерном удаленном доступе к компьютерной информации.
4. Более значимым в практическом плане представляется подразделение следственных ситуаций на следующие группы:
5. конфликтные ситуации, при которых «субъект преступления обладает информацией, но умышленно искажает или скрывает ее» [7];
6. бесконфликтные ситуации, при которых субъект преступления объективно передает следователю искомую информацию, не стремится ее искажать или утаивать;
7. слабоконфликтные ситуации, которые возникают в ситуациях допроса, когда допрашиваемый «обладает искомой информацией, желает ее передать, но в силу субъективных или объективных факторов воспринял, запомнил и, соответственно, передает ее с искажениями» [8].

Особое роль для построения эффективной методики предварительного расследования имеет выделение следственных эта-

пов, объединяющих проверочные и следственные действия в соответствии с имеющей место следственной ситуацией. Можно выделять этап предварительной проверки полученных сведений о преступлении, а также первоначального, неотложного, дальнейшего и заключительного этапов расследования.

С позиций ситуационного подхода первоначальный этап расследования преступлений в сфере компьютерной информации может быть охарактеризован тремя типичными следственными ситуациями, классифицируемыми по субъекту выявления преступления [9].

1. Собственник компьютерной информации обнаружил факт преступления и самостоятельно выявил преступника.
2. Собственник компьютерной информации обнаружил факт преступления, но преступник остается не выявленным.
3. Преступление выявлено правоохранительными органами.

В случае неправомерного удаленного доступа к компьютерной информации эта классификация представляется неполной и должна быть дополнена, по нашему мнению, еще одной типичной следственной ситуацией.

4. Преступление выявлено иным лицом, в качестве которого обычно выступает организация – провайдер, обслуживающая собственника конфиденциальной информации.

Типичная доследственная ситуация на предварительном этапе в случае совершения преступления способом относительно простого удаленного доступа к компьютерной информации характеризуется тем, что потерпевшие (физические или юридические лица) сами обнаруживали преступление.

Изучение приведенных и других ситуаций, возникающих по делам о неправомерном удаленном доступе к компьютерной информации на предварительном следствии является основанием для выбора и использования нужной группы криминалистических рекомендаций [10]. Знание этих рекомендаций способно в значительной степени способствовать эффективному сбору доказательств по преступлениям, связанным с неправомерным доступом к компьютерной информации, совершенным дистанционным образом.

Список литературы

1. Гавло В.К., Поляков В.В. Некоторые особенности расследования преступлений, связанных с неправомерным доступом к компьютерной информации // Известия Алтайского государственного университета. 2006. №2. С. 44-48.
2. Корноухов В.Е. Адаптация типовой методики к условиям расследования конкретного преступления // Уголовно-процессуальные и криминалистические чтения на Алтае: матер. Межрегион. науч.-практ. конф.; под ред. В.К. Гавло. - Барнаул: Изд-во Алт. ун-та, 2003. Вып. 7-8. С. 172-178.
3. Гавло В.К., Поляков В.В. Ситуационный подход в криминалистике по делам о компьютерных преступлениях // Научно-методические и нормативные материалы и документы IV Пленума СибРОУМО по образованию в области информационной безопасности: матер. Пленума и документы конференции: сб. статей: Томск – Барнаул – Белокуриха, 8-13 июня 2010 г. Томск: «В-Спектр», 2010. С. 186 - 187.
4. Гавло В.К. Теоретические проблемы и практика применения методики расследования отдельных видов преступлений. Томск: Изд-во Томского ун-та, 1985. – 333 с.
5. Драпкин Л.Я. Проблемы общей теории раскрытия преступлений и криминалистическая тактика // Криминалистические проблемы следственной тактики: межвуз. сб. науч. трудов. - Свердловск: Изд-во УрГУ, 1981. С. 34.
6. Поляков В.В. Особенности расследования неправомерного удаленного доступа к компьютерной информации: автореф. дис. канд. юрид. наук: 12.00.09. Омск, 2008. 28 с.
7. Баев О.Я. Конфликтные ситуации на предварительном следствии (основы предупреждения и разрешения). - Воронеж: Изд-во ВГУ, 1984. 132 с.
8. Комиссаров В.И., Лакаева О.А. Тактика допроса потерпевших от преступлений, совершаемых организованными группами лиц. – М.: Изд-во «Юрлитинформ», 2004. 160 с.
9. Курс криминалистики: в 3 т. Т. III. Криминалистическая методика: Методика расследования преступлений в сфере экономики, взяточничества и компьютерных преступлений / под ред. О.Н. Коршуновой, А.А. Степанова. – СПб. Изд-во «Юридический центр Пресс», 2004. – 573 с.

10. Поляков В.В. Следственные ситуации по делам о неправомерном удаленном доступе к компьютерной информации // Доклады Томского государственного университета. 2010. N1(21). С. 46 - 50.

КИБЕРТЕРРОРИЗМ: МЕРЫ ПРОТИВОДЕЙСТВИЯ В АСПЕКТЕ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА РОССИИ И СТРАН ЗАРУБЕЖЬЯ

М.Н. Кутявина, Т.И. Рыбина, АлтГУ,
юридический факультет, 4 к.
Научный руководитель – ***В.А. Мазуров,*** к.ю.н., доцент.

Сегодня интернет широко используется не только обычными гражданами, но различными террористическими и экстремистскими организациями и играет большую роль в их деятельности, которая не ограничивается лишь пропагандистской и разъяснительной работой, публикацией материалов определенной направленности и др.

Посредством интернет-ресурсов осуществляется привлечение к подобной деятельности «волонтеров», вербовка новых членов, сбор финансовых средств, планирование и координация совместных действий.

Не вызывает сомнения, что компьютерные преступления во всем мире имеют устойчивую тенденцию к росту, поскольку растет и аудитория пользователей высокими технологиями и Интернет-ресурсами. Ключевым положением борьбы с кибертерроризмом является интеграция правовых систем различных стран (например, сближение уголовного законодательства стран Евросоюза). На первый план, по сравнению с национальным законодательством, выходят инструменты межгосударственного (международного) регулирования, поскольку данная проблема не носит, как правило, каких-либо географических или политических границ.

При этом речь идет не столько о включении международных актов в национальное законодательство путем их ратификации, сколько о добровольном и рациональном учете рекомендаций международных (межправительственных) организаций (ЕС, ООН,

АТР и др.) и опыта развития специального законодательства в других странах.

Для совершенствования российского законодательства это особенно важно, поскольку объективную проблему представляет новизна сферы правового регулирования, отсутствие устоявшейся теоретической основы, что, прежде всего, сказывается на понятийном аппарате по рассматриваемому вопросу.

Между тем, мировым сообществом в данное время наработан определенный положительный опыт борьбы с кибертерроризмом. На международном и межгосударственном уровне принят ряд нормативных правовых актов, регламентирующих данную проблему.

Так, Генеральной Ассамблеей ООН в резолюции 53/70 от 4 декабря 1998 года [1] были затронуты вопросы целесообразности разработки общепринятых международных принципов организации противодействия кибертерроризму, предусматривающих усиление безопасности глобальных информационных и телекоммуникационных систем и борьбу с информационным терроризмом и преступностью.

Значительным шагом в формировании международной правовой базы в данном направлении стало подписание 23 ноября 2001 года представителями стран - членов Совета Европы, США, Канады и Японии Конвенции Совета Европы «О киберпреступности» [2]. Она определяет приблизительный перечень преступлений, совершенных в информационной сфере, против информационных ресурсов или с помощью информационных средств и признает их киберпреступлениями. На сегодняшний день Конвенция подписана 43 членами ЕС и 15 другими странами, включая США. РФ не вошла в число государств, подписавших Конвенцию. В настоящее время это единственный международный акт, содержащий закрепление основ по защите прав человека в киберпространстве. Россия, по всей видимости, пока не готова к полноценному сотрудничеству в данном направлении с зарубежными партнерами. При этом следует отметить, что мировое сообщество также еще находиться в процессе выработки единой политики в указанном вопросе, о чем свидетельствует непрекращающаяся работа представителей различных государств в борьбе с кибертерроризмом.

В последние годы активно прорабатываются вопросы совершенствования нормативной правовой базы стран СНГ в данном направлении. Так, Указ Президента России «О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена» от 12 мая 2004 года N 611 [3] запрещает госорганам пользоваться Интернетом без средств защиты и регламентирует, какие спецслужбы должны за это отвечать. Указ направлен главным образом на обеспечение защиты российского сегмента сети Интернет, в первую очередь - сетевых ресурсов государственных органов, от внешних угроз несанкционированного воздействия. При этом речь идет, в первую очередь, о предотвращении возможных попыток компьютерного «взлома» и получения контроля над сетевыми ресурсами органов власти России с террористическим умыслом.

Россией также была разработана концепция Конвенции об обеспечении международной информационной безопасности 2011 г. Конвенция предполагает полное сохранение государственных суверенитетов и границ национального регулирования в виртуальном пространстве.

В качестве еще одного шага на пути к обеспечению информационной безопасности можно назвать проект «Правил поведения в области обеспечения международной информационной безопасности» [4]. Этот кодекс в сентябре 2011 года Россия, Китай, Узбекистан и Таджикистан предложили распространить в качестве официального документа 66-й сессии Генеральной ассамблеи ООН. Государствам, присоединившимся к правилам, предлагается сотрудничать в борьбе с преступной или террористической деятельностью с использованием информационно-коммуникационных технологий, уважать права и свободы граждан в информационном пространстве, а также способствовать формированию культуры информационной безопасности и защите объектов критической информационной инфраструктуры.

Ряд организационных и практических мер, позволивших создать определенные заделы для создания эффективной системы противодействия кибертерроризму принят и в Республике Казахстан. К примеру, в Уголовный кодекс РК внесены изменения, предусматривающие уголовную ответственность за совершение компьютерных преступлений, в частности, по статье 227 «Непра-

вомерный доступ к компьютерной информации, создание и распространение вредоносных программ для ЭВМ» предусмотрены штраф либо исправительные работы до одного года, либо лишение свободы на срок до пяти лет [5]. В структуре спецслужб образовано специализированное подразделение по борьбе с киберпреступностью. В МВД РК созданы Национальный контактный пункт по борьбе с преступностью в сфере высоких технологий и управление специальной оперативно-аналитической работы и раскрытия преступлений в сфере высоких технологий.

Так же хотелось бы затронуть регулирование исследуемой проблемы в субъектах РФ, в частности в Алтайском крае. Нормативных актов, направленных на регулирование данной проблемы нет, но весьма богата практическая деятельность разных структур: в АК, в различных правоохранительных органонах, существует так называемый отдел «К», отвечающий за компьютерную безопасность. В Алтайском Крае и Республике Алтай существует уникальное коммерческое лицо, единственное на названных территориях, которое оказывает различные услуги по информационной безопасности (выдача лицензий, техническое сопровождение и администрирование сетей передачи данных, защита персональных данных, конфиденциальной информации). Речь идет о Центре информационной безопасности АК. Кроме того показательна тенденция работы органов прокуратуры: активно ведется работа в сфере выявления информационных ресурсов экстремистского и террористического содержания. Всего, в период с 2013 – 14 гг. прокурорами нашего края было подано 20 исковых заявлений об ограничении к разным интернет - ресурсам такого характера. На первый взгляд данная цифра является небольшой, однако, с другой стороны, это немалое количество исков, особенно в виду того, что зачастую правонарушители добровольно удаляют такую информацию или закрывают свой ресурс.

Резюмируя изложенное необходимо подчеркнуть, что кибертерроризм представляет собой глобальную проблему, для решения которой необходима международная координация усилий. Наиболее эффективный способ борьбы с компьютерными преступлениями сегодня - объединение опыта на международном уровне, как правоохранительных органов, так и компаний, специа-

лизирующихся в области информационной безопасности, и их активное тесное сотрудничество.

Предлагаемые нами меры противодействия и предупреждения кибертерроризму:

1. разработка на международном уровне комплексной программы, включающей в себя возможные формы и методы борьбы с кибертеррором (юридические, программные, технологические, организационные, экономические, политические и т.д.);
2. криминализация международного кибертерроризма, законодательное закрепление такого состава преступления как «Международная кибератака»;
3. антитеррористические акции: пропаганда в общественных местах посредством размещения плакатов, баннеров, распространения аудио-, видеоинформации, брошюр и листовок;
4. создание единого списка организаций, деятельность которых признана кибертерроризмом;
5. паспортизация объектов, наиболее подверженных компьютерному террору, разработка паспортов защищенности объектов, информационной (компьютерной) безопасности на основе международного соглашения.

Все эти меры в совокупности между собой и с другими существующими на сегодняшний момент позволят не только снизить уровень ущерба, причиненного киберпреступлениями, но и предупредить кибертеррористов, тем самым даже не допуская осуществления начальных действий кибератак.

Список литературы

1. Генеральная Ассамблея ООН в резолюции 53/70 от 4 декабря 1998 года //Права человека: Сборник международных документов. - М., 1998. – 314 с;
2. Конвенция Совета Европы «О киберпреступности» (Будапешт, 23 ноября 2001 года) // Международное сотрудничество в борьбе с преступностью. Сборник международно-правовых актов.- М., 2000. – 248 с;
3. Указ Президента России «О мерах по обеспечению информационной безопасности Российской Федерации в сфере междуна-

родного информационного обмена» от 12 мая 2004 года N 611// Собрание законодательства РФ, 17.05.2004, № 20, Ст. 1938;
4. Тропинина Т. Л. Киберпреступность и кибертерроризм: поговорим о понятийном аппарате: Сборник научных трудов международной конференции «Информационные технологии и безопасность». Выпуск 3. – К.: Национальная академия наук Украины, 2003. – 178-179 с;
5. Уголовный Кодекс Республики Казахстан от 16.07.1997 № 167-I (в ред. 07.03.2014) // «Ведомости Парламента», 1997 г., № 15, Ст. 211.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПДнВ ВУЗе

К.В. Масалова, АлтГТУ, факультет информационных технологий, 5 к.
Научный руководитель **– *Е.В. Шарлаев,*** к.т.н., доцент.

В силу своей специфики в ВУЗе хранится и обрабатывается огромное количество информации, в том числе персональные данные (ПДн) различных категорий субъектов ПДн. ВУЗы являются операторами ПДн, и соответственно, на них распространяется действие закона о 152-ФЗ «О персональных данных» [1].

Выполнив анализ нормативно-правовой базы, а также практического опыта в области информационной безопасности становится очевидным, что разработать эффективную систему защиты информационных систем можно только в соответствии с требованиями руководящих документов и рекомендаций.

ВУЗы, как правило, обращаются к коммерческим организациям, оказывающим услуги в области защиты информации. Это увеличивает расходы на защиту ПДн, но гарантирует наличие отлаженной системы защиты информации с полным пакетом документации.

Основными проблемами, с которыми сталкиваются при организации защиты ПДн в ВУЗе, являются: территориальная рассредоточенность ресурсов информационных систем, большое количество серверов, к которым привязаны ИСПДн, порой с разными уровнями защищенности, выход многих ИСПДн в глобальные инфо-телекоммуникационные сети и сети общего пользования.

Поэтому самым разумным подходом будет являться рассмотрение каждой ИСПДн отдельно, а уже затем рассматривать их в совокупности.

В соответствии с Постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований», требования по защите персональных данных в ИСПДн зависят от уровня защищенности ИСПДн [2].

Типичная ситуация для ВУЗа – это обработка специальных ПДн субъектов которые могут являться или не являться сотрудниками оператора в количестве до 100 000, актуальные угрозы третьего типа (для АС). Модель угроз строится на основе «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных» разработанной ФСТЭК России в 2008 году. То есть, большая часть ИСПДн будет отнесена к 3 уровню защищенности, однако встречаются ИСПДн с другим уровнем защищенности.

В реальном ВУЗе, который брался за основу разработки, ИСПДн имеют 3 УЗ, соответственно для выполнения большинства требований на АРМ и серверах оказалось достаточно установить антивирусное средство, СЗИ НСД с токеном и персональный межсетевой экран соответствующих классов и сертифицированных ФСБ и ФСТЭК России. При выборе данных средств защиты руководствовались как эффективностью, так и экономической целесообразностью.

На данный момент в учебном заведении уже установлена и настроена данная система защиты персональных данных. Все СЗИ настроены в соответствии с матрицей доступа. ВУЗ, как оператор ПДн, успешно прошел проверку государственных регуляторов на предмет выполнения требований закона №152-ФЗ «О персональных данных».

В силу ряда особенностей операторам ПДн сложно самостоятельно разработать, установить и настроить эффективную, отвечающую всем требованиям законодательства систему защиты, поэтому чаще всего прибегают к услугам коммерческих предприятий, занимающихся информационной безопасностью. Они предлагают ВУЗу индивидуальные проекты, которые согласовываются на всех этапах построения и, при наличии жестких рамок, не позво-

ляющих реализовать ни один из предложенных проектов, ищут альтернативные пути защиты или ухода от защиты.

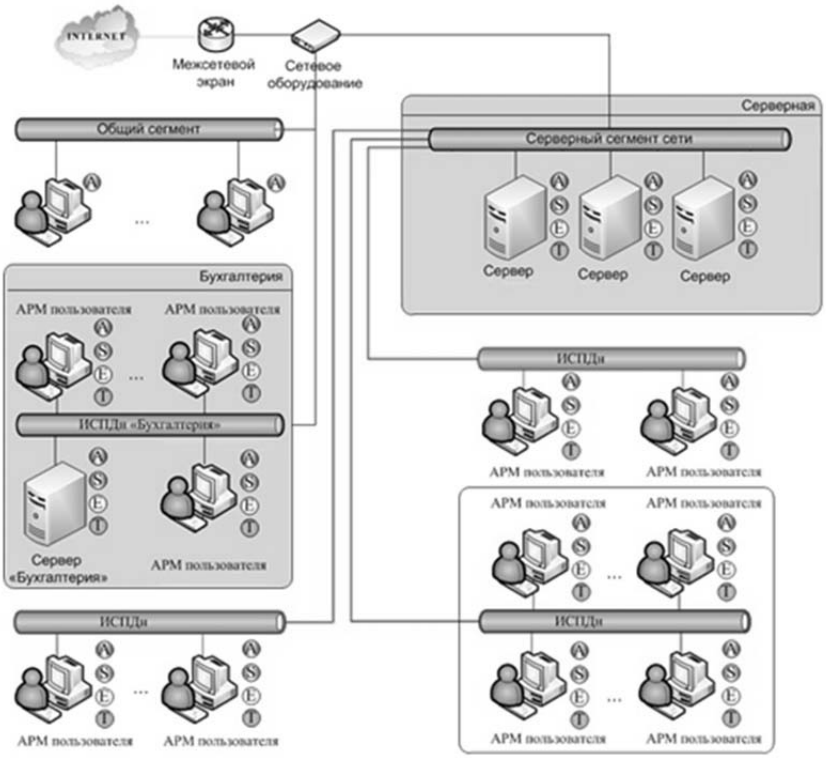


Рис.1 Проект системы защиты персональных данных.

Список литературы

1. О персональных данных: Федеральный закон от 27 июля 2006 № 152-ФЗ (ред. от 23.07.2013 N 205-ФЗ): [Электронный ресурс] – электронные данные. – Программа информационной поддержки российской науки и образования // справочные правовые системы Консультант Плюс: Высшая школа. – 2013. – Режим доступа: http//www.consultant.ru.
2. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: Постановление Правительства РФ от 01.11.2012 № 1119: [Электронный ресурс] – электронные данные. – Програм-

ма информационной поддержки российской науки и образования // справочные правовые системы Консультант Плюс: Высшая школа. – 2013. – Режим доступа: http//www.consultant.ru.
3. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: Приказ ФСТЭК России от 18.02.2013 № 21: [Электронный ресурс] – электронные данные. – Программа информационной поддержки российской науки и образования // справочные правовые системы Консультант Плюс: Высшая школа. – 2013. – Режим доступа: http//www.consultant.ru.

ПРОБЛЕМЫ ОПТИМАЛЬНОСТИ КОНСТРУКЦИИ СТАТЬИ 183 УК РФ

И.С. Паршиков, АлтГУ, юридический факультет, 2 к.
Научный руководитель – ***В.А. Мазуров,*** к.ю.н., доцент.

Актуальность темы выступления заключается в наличии проблем теоретического и практического характера, требующих разрешения.

Так, преступления, предусмотренные статьей 183 УК РФ носят высоко латентный характер, возбуждению уголовных дел во многом оказывает препятствие конструкция указанной статьи.

Ряд ученых правоведов (в частности, Паршин С.М. [1], Мазуров В.А. [2]) полагают, что было бы целесообразным выделить в самостоятельную статью УК РФ ответственность за налоговую тайну, так как по сути это служебная тайна, которая имеет некоторые существенные отличия от коммерческой и банковской тайны.

На основании ФЗ «О коммерческой тайне» [3] под коммерческой тайной понимается режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду; информация, составляющая коммерческую тайну (секрет производства), – сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах ин-

теллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

Служебная тайна. В законодательстве однозначно не определено понятие служебной тайны. Вместе с тем анализ нормативных актов позволяет выявить содержание и основные признаки отнесения информации к служебной тайне.

Служебная тайна – это охраняемые законом конфиденциальные сведения о деятельности государственных органов, доступ к которым ограничен федеральным законом или в силу служебной необходимости, а также ставшие известными в государственных органах и органах местного самоуправления только на законном основании и в силу исполнения их представителями служебных обязанностей, имеющие действительную или потенциальную ценность в силу неизвестности их третьим лицам, к ним нет свободного доступа на законном основании, обладатель сведений принимает меры к их конфиденциальности, незаконное получение или разглашение данных сведений создает угрозу причинения вреда их владельцу, связи с этим ему предоставляется право на защиту в соответствии с законодательством Российской Федерации.

Иными словами, служебная тайна – это информация, доступ к которой ограничен органами государственной власти и федеральными законами. Служебная тайна не подлежит разглашению, кроме случаев, когда те или иные сведения запрашиваются правоохранительными органами (в соответствии с Федеральным законом от 12 августа 1995 г. N 144-ФЗ "Об оперативно-розыскной деятельности" [4]). Согласно Указу Президента РФ от 06.03.97 г. «Об утверждении перечня сведений конфиденциального характера» [5] разница между служебной и коммерческой тайной состоит в том, что коммерческая тайна – это сведения, связанные с коммерческой деятельностью, а служебная тайна – служебные сведения, доступ к которым ограничен органами государственной власти. Для того чтобы разобраться в существе служебной тайны, обратимся к утвержденному Правительством РФ от 03.11.94 (поста-

новление) «Положению о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».

Положение направлено на урегулирование вопросов, связанных с обращением информации в федеральных органах исполнительной власти, а также в подведомственных им предприятиях, в учреждениях и организациях. Определен гриф конфиденциальности информации для служебного пользования. В соответствии с «Положением…» к служебной информации ограниченного распространения относится несекретная информация, касающаяся деятельности организаций, ограничение на распространение которой диктуется служебной необходимостью.

«Положение…» предписывает руководителям федеральных органов исполнительной власти в пределах своей компетенции определять категорию должностных лиц, уполномоченных относить служебную информацию к разряду ограниченного распространения, обеспечивать ее защиту и т. д.

Таким образом, можно утверждать, что потенциальными носителями служебной тайны являются, как минимум, все служащие, которые работают в государственных органах, органах законодательной, исполнительной и судебной власти, а также в подведомственных им предприятиях, учреждениях и организациях.

На основании выше изложенного примером служебной тайны, является **налоговая тайна**. В соответствии с Налоговым кодексом Российской Федерации [6] налоговую тайну составляют любые сведения о налогоплательщике, полученные налоговым органом, органом государственного внебюджетного фонда и таможенным органом. Данные о налогоплательщике, если он является физическим лицом, также одновременно являются его личной тайной – персональными данными.

Поступившая в налоговые органы информация, составляющая налоговую тайну, имеет специальный режим хранения и доступа и соответственно организационно-документационные технологии ее защиты. Доступ к информации, составляющей налоговую тайну, имеют должностные лица по перечням, определяемым Федеральной налоговой службой России, что законодательно закреплено постановлением Правительства Российской Федерации «Об утверждении Положения о Федеральной налоговой службе» [7].

Не однозначно решается вопрос и с банковской тайной. В ст. 857 ГК РФ [8] и Федеральном законе «О банках и банковской деятельности» [9] (ст. 26) речь идет об ответственности за разглашение сведений о счетах, вкладах и операциях по ним, а также о клиентах и корреспондентах.

В приведенных документах просматриваются некоторые элементы содержания и признаки профессиональной тайны. В это содержание входят, прежде всего, сведения, доверенные конкретному лицу или ставшие известными ему в связи с осуществлением своих профессиональных обязанностей. Указанное лицо обязывается сохранять полученные сведения в тайне. В случае их разглашения предусматривается ответственность в соответствии с действующим законодательством.

Таким образом, профессиональная тайна – это охраняемые законом конфиденциальные сведения, доверенные или ставшие известными лицу исключительно в силу исполнения им своих профессиональных обязанностей, не связанных с государственной или муниципальной службой, незаконное получение или распространение которых может повлечь за собой вред правам и законным интересам другого лица, доверившего эти сведения, в связи с этим ему предоставляется право на защиту в соответствии с законодательством Российской Федерации.

Исходя из анализа законодательства и учитывая мнение ученых правоведов, полагаем целесообразным определиться в предмете статьи 183 УК РФ, и уголовно-правовую защиту служебной тайны выделить в отдельную статью УК РФ – «Разглашение служебной тайны». Для этого считаем необходимым принять Федеральный Закон «О служебной тайне», в котором нашли бы законодательное закрепление сведения, относящиеся к служебной тайне. Учитывая то, что на заседании межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности, протоколом от 27 ноября 2001 г. № 4.1 « Основные направления нормативно-правового обеспечения информационной безопасности Российской Федерации» [10] был утвержден перечень первоочередных мер по решению задач нормативно-правового обеспечения государственной политики в области реализации Конституционных прав и свобод человека и гражданина, в котором предусматривалось разработка законопроекта «О слу-

жебной тайне», который на сегодняшний день не принят (проект № 124871-4 внесен депутатам Государственной Думы В.В. Бобыревым, А.Н. Волковым, М.И. Гришанковым, В.В. Дятленко, В.И. Илюхиным, Н.С. Леоновым, В.В. Маргеловым, А.М. Розуваном).

Целью данных преобразований видим упорядочивание системы нормативно-правового регулирования защиты охраняемой законом информации (сведений), для демократизации, законности и исполнимости правового обеспечения информационной безопасности в демократическом государстве.

Список литературы

1. Паршин С.М Теоретико-прикладное исследование: Тайна в уголовном законодательстве. Нижний Новгород, 2006. 207 с.
2. Мазуров В.А., Головин А.В., Поляков В.В. Информационная безопасность: основы правовой и технической защиты информации. Барнаул, 2005. 194 с.
3. Федеральный закон от 29.07.2004 N 98-ФЗ (ред. от 11.07.2011) "О коммерческой тайне".
4. Федеральный закон от 12 августа 1995 г. N 144-ФЗ "Об оперативно-розыскной деятельности".
5. Указ Президента РФ от 6 марта 1997 г. N 188 "Об утверждении перечня сведений конфиденциального характера".
6. "Налоговый кодекс Российской Федерации (часть первая)" от 31.07.1998 N 146-ФЗ.
7. Постановление Правительства РФ от 30.09.2004 N 506 (ред. от 02.11.2013) "Об утверждении Положения о Федеральной налоговой службе".
8. Гражданского кодекса Российской Федерации (ГК РФ) N 51-ФЗ от 30.11.1994 г.
9. Федеральный закон от 02.12.1990 N 395-1 (ред. от 05.05.2014) "О банках и банковской деятельности".
10. Протокол межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности от 27 ноября 2001 г. № 4.1 «Основные направления нормативно-правового обеспечения информационной безопасности Российской Федерации».
11. Уголовный кодекс Российской Федерации (УК РФ) N 63-ФЗ от 13.06.1996 г.

ПРОТИВОДЕЙСТВИЕ РАССЛЕДОВАНИЮ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ НА СТАДИИ ВОЗБУЖДЕНИЯ УГОЛОВНОГО ДЕЛА

Д.А. Першин, АлтГУ, юридический факультет, 5 к.
Научный руководитель – ***В.В. Поляков,*** к.ю.н., доцент.

Преодоление противодействия на стадии возбуждения уголовного дела связано с тем, что преступники стремятся предпринять действия, препятствующие выявлению и расследованию преступления.

Возбуждение уголовного дела предполагает наличие определенной информации, из которой можно сделать вывод о том, что преступление действительно имело место. Данная информация может быть получена уполномоченными на это оперативными сотрудниками, которые передают ее органу следствия. Далее, следователь оценивает эту информацию и принимает решение о возбуждении уголовного дела. В случае, когда поводом или основанием для возбуждения уголовного дела явилось другое обстоятельство, например, заявление потерпевшего, следователь не может занимать пассивную позицию, он должен четко обозначить какую именно информацию ждет от оперативников, проанализировать ее на предмет достоверности, и подумать над тем, какие действия предпринять, чтобы расследование было успешным. Следователь может дать письменное поручение о производстве оперативно-розыскных мероприятий. Как показывает практика расследования уголовных дел по компьютерным преступлениям, такие обращения редко облекаются в письменную форму, а ограничиваются устной просьбой о необходимости получения дополнительной информации. Подобная практика увеличивает оперативность, и способствует соблюдению процессуальных сроков.

Опытные преступники, информированные о протекании расследования, стараются найти в нем уязвимые места для применения мер противодействия [1]. Обычно, с их стороны предпринимаются следующие действия:

1. Дистанционное уничтожение электронных документов или иной информации, хранящейся на компьютере или носителе информации;

2. Создания документов-двойников с целью формирования иллюзии о том, что документ, в котором правоохранительные органы видят информацию о преступлении, на самом деле свидетельствует об обратном;
3. Внесение изменений в учетные и иные данные в программной среде компьютера. Так, например, уничтожается информация, свидетельствующая о неправомерном доступе, или подкидывается информация, которая направляет правоохранительные органы на ложный след, указывающий, что преступление совершено иным лицом;
4. Развертывание в СМИ дискуссии о допустимости действий, схожих с теми, которые составляют конкретное преступление, выявлением или расследованием которого в данный момент занимаются правоохранительные органы. Эти действия рассчитаны на то, чтобы сформировать общественное мнение о несправедливости возможного уголовного преследования, повлиять на взгляды сотрудников правоохранительных органов;
5. Воздействие на конкретных сотрудников правоохранительных органов (нахождение коррупционных и приятельских связей) [2].

С целью преодоления противодействия со стороны преступника и лиц, сочувствующих ему, необходимо соблюдение полной конспирации о планируемых и совершаемых действиях, направленных на сбор информации, которая необходима для решения вопроса о возбуждении уголовного дела. Н.А. Подольный справедливо отмечает, что необходимость конспирации в случае проведения оперативно-розыскных мероприятий с целью выявления компьютерных преступлений является важнейшим условием получения достоверной информации [3]. От потерпевших необходимо потребовать не разглашать сведения, которые могли стать им известны от правоохранительных органов.

Во время принятия решения о возбуждении уголовного дела оперативные сотрудники должны выяснить возможность последующего получения доказательств в результате следственных действий, так как нередки случаи, когда до возбуждения уголовного дела лица дают объяснения, прямо указывающие на виновность

конкретного субъекта, а после возбуждения уголовного дела дают прямо противоположные показания.

Для решения вопросов о преодолении противодействия в стадии возбуждении уголовного дела о преступлениях в сфере компьютерной информации целесообразно привлечение специалистов [4]. С их помощью сформировывается представление не только об общей картине совершенного преступления, но и опасностях, которые могут подстерегать следствие при сборе доказательств [5].

Проблема противодействия расследованию преступлений в сфере компьютерной информации, особенно на стадии возбуждения уголовного дела, является малоизученной и требует дальнейшего исследования.

Список литературы

1. Поляков В.В. Следственные ситуации по делам о неправомерном удаленном доступе к компьютерной информации // Доклады Томского государственного университета. 2010. N1(21). С. 46 - 50.
2. Преодоление противодействия расследованию преступлений в сфере компьютерной информации: монография / под ред. Н.А. Подольного. М.: Юрлитинформ, 2013. – 216 с.
3. Подольный Н.А. Ширманов А.Г. Некоторые особенности выявления, раскрытия и расследования компьютерных преступлений // Российский следователь 2004. №1. С. 11.
4. Поляков В.В. Криминалистическая структура мер предупреждения компьютерных преступлений // Библиотека криминалиста: научный журнал. 2013. №5 (10). С. 287 - 291.
5. Поляков В.В. Особенности подготовки специалистов для расследования преступлений, связанных с неправомерным удаленным доступом к компьютерной информации // Известия Алтайского государственного университета. 2010. N 2/1. С. 96 - 97.

К ВОПРОСУ О ПРЕДМЕТЕ ПРЕСТУПЛЕНИЯ, ПРЕДУСМОТРЕННОГО СТ. 275 УК РФ

А.А. Погосян, АлтГУ, юридический факультет, 3к.
Научный руководитель – ***И.А. Анисимова,*** к.ю.н, доцент.

В теории уголовного права чаще всего под предметом преступления понимаются «материальные предметы внешнего мира, на которые непосредственно воздействует преступник, осуществляя посягательство на соответствующий объект» [1]. Однако такое понимание предмета преступления представляется достаточно упрощенным. Под предметом преступления следует понимать элемент (часть) объекта преступления, воздействуя на который преступник нарушает или пытается нарушить общественное отношение. Именно через предмет преступления причиняется вред охраняемому уголовным законом общественному отношению. При таком подходе под предметом преступления следует понимать как материальное, так и нематериальное благо, в отношении которого происходит непосредственное воздействие преступника [2].

В юридической литературе подчеркивается, что «предмет преступления может иметь важное уголовно-правовое значение, в частности для квалификации преступления, в тех случаях, когда он является обязательным признаком соответствующего состава преступления» [3].

Как показывает анализ научной литературы и опубликованной судебно-следственной практики, деятельность, направленная против внешней безопасности Российской Федерации, чаще всего осуществляется путем выдачи (передачи) сведений, составляющих государственную тайну, а равно передачи иных сведений иностранным государствам, международным либо иностранным организациям или их представителям. Таким образом, вред внешней безопасности Российской Федерации, как объекту преступления, причиняется в связи или через непосредственное воздействие на ту или иную информацию. Из этого можно сделать вывод, что в качестве предмета посягательства при совершении государственной измены выступает именно информация, а также ее материальные носители.

Сведения (информацию), составляющие государственную тайну, как предмет и обязательный признак преступления можно

выделить в составе государственной измены в форме выдачи государственной тайны (первая форма государственной измены). Предметом преступления второй формы государственной измены выступают сведения, составляющие государственную тайну, а равно иные сведения, собираемые по заданию «адресатов» для использования их против безопасности Российской Федерации. Однако в третьей форме государственной измены (в составе оказания финансовой, материально-технической, консультационной или иной помощи иностранному государству, международной либо иностранной организации или их представителям в деятельности, направленной против безопасности Российской Федерации (далее – иное оказание помощи)) в качестве обязательного признака преступления предмет в диспозиции ст. 275 УК РФ прямо не указан. Вследствие этого в отношении толкования предмета иного оказания помощи в специальной литературе высказываются прямо противоположные позиции.

Некоторые ученые полагают, что предметом преступления при совершении государственной измены в данной форме, как и при шпионаже, могут выступать иные сведения. Другие авторы обоснованно уточняют, что эти сведения должны собираться не по заданию «адресатов». Третьи – характеризуя состав государственной измены в форме иного оказания помощи вопрос о предмете данного преступления вообще не исследуют. [4].

Получается, что одна из составляющих предмета государственной измены, в частности, совершаемой в форме иного оказания помощи иностранному государству, международной либо иностранной организации или их представителям, является неопределенной. Она не конкретизируется в уголовном законодательстве, актах официального судебного толкования, т.е. правоприменитель и сам субъект не могут достоверно знать какие конкретно деяния можно считать иным оказанием помощи, а что таковым не должно расцениваться. Данное положение не допустимо. Государственная измена точки зрения основ конституционного строя и безопасности государства является наиболее опасным преступлением, за которое предусмотрено лишение свободы до двадцати лет.

В научных работах, специально посвященных исследованию ст. 275 УК РФ, и судебной практике в качестве предмета гос-

ударственной изменены, совершаемой в форме иного оказания помощи, признаются сведения, не составляющие государственную тайну (иные сведения). Однако к числу иных сведений относятся, не любые данные, а только те, которые собираются не по заданию «адресатов» и, которые по своему содержанию могут быть направлены против безопасности Российской Федерации, использованы в ущерб внешней безопасности страны.

Некоторые авторы предлагают конкретизировать такие сведения. В частности, признавать в качестве таковых данные, содержащие следующую информацию:

- признаваемую конфиденциальной;
- которая может быть использована для совершения преступлений или для облегчения их совершения;
- которая, не составляет государственной тайны, но служит для уточнения, проверки, пополнения имеющихся сведений, относящихся к государственной тайне;
- которая не составляет государственной тайны, однако при обобщении, анализе или в совокупности с уже имеющимися данными позволяет получить новые знания, образующие государственную тайну;
- даже не соответствующую действительности, то есть дезинформацию, которая может быть использована в деятельности, направленной против внешней безопасности Российской Федерации.

Думается, что данный подход является предпочтительным, так как наиболее полно раскрывает предмет иного оказания помощи как формы государственной измены.

Важно подчеркнуть, что перечисленные сведения, составляющие предмет иного оказания помощи, необходимо рассматривать в контексте всех признаков состава государственной измены. Состав государственной измены возможен только в том случае, если сведения предназначаются для использования иностранным государством, международной либо иностранной организацией или их представителями во враждебной деятельности, направленной против внешней безопасности Российской Федерации.

Оконченный состав государственной измены в форме иного оказания помощи образует передача указанных сведений иностранному государству, международной либо иностранной орга-

низации или их представителям. Собирание таких сведений, без задания «адресатов», но в целях передачи им собранной информации, будет образовывать приготовление к государственной измене в форме иного оказания помощи.

На основе вышеизложенного отметим следующее. Законодательно не определена одна из составляющих предмета преступления, предусмотренного ст. 275 УК РФ, в частности предмет государственной измены в форме иного оказания помощи иностранному государству, международной либо иностранной организации или их представителям. Предлагаем, что данный предмет образуют иные сведения, не составляющие государственную тайну: которые признаются конфиденциальной информацией; которые могут быть использованы для совершения преступлений или для облегчения их совершения; которые, служат для уточнения, проверки, пополнения имеющихся сведений, относящихся к государственной тайне; которые при обобщении, анализе или в совокупности с уже имеющимися данными, позволяют получить новые знания, образующие государственную тайну; не соответствующие действительности, то есть дезинформация, которые могут быть использованы в ущерб внешней безопасности Российской Федерации.

Список литературы

1. Словарь по уголовному праву. М.: Издательство БЕК, 1997. 686 с.
2. Российское уголовное право. Общая часть / под ред. В.С. Комиссарова. СПб.: Питер, 2005. 560 с.
3. Дьяков С.В. Преступления против основ конституционного строя и безопасности государства: уголовно-правовое и криминологическое исследование. СПб.: Издательство Р.Асланова «Юридический центр Пресс», 2009. 267 с.
4. Рябчук В.Н. Государственная измена и шпионаж: уголовно-правовое и криминологическое исследование. СПб.: Издательство Р. Асланова «Юридический центр Пресс», 2007. 1002 с.

ПРОБЛЕМЫ ОПРЕДЕЛЕНИЯ ПОНЯТИЯ ЧАСТНОЙ ЖИЗНИ

А.С. Покидова, АлтГУ, юридический факультет, 3 к.
Научный руководитель – ***И.А. Анисимова,*** к.ю.н., доцент.

Право на неприкосновенность частной жизни принадлежит каждому человеку от рождения, при этом данное право позволяет сохранять в тайне сведения, касающиеся его личной или семейной жизни. Человек вправе самостоятельно определять, какие сведения о его личной жизни можно предать огласке, а какие из них являются тайной.

Ст. 8 Европейской конвенции о защите прав человека и основных свобод говорит о недопущении вмешательства в личную и семейную жизнь со стороны государственных органов. Всеобщая декларация прав человека в ст. 12 провозглашает: "Никто не может подвергнуться произвольному вмешательству в его личную и семейную жизнь ". Согласно ч. 1 ст. 23 Конституции РФ, каждый гражданин имеет право на неприкосновенность частной жизни, личную и семейную тайну.

В советское время в правовых актах и научной литературе отсутствовало понятие "частная жизнь". Вместо него использовалось понятие "личная жизнь". "Тем не менее, - отмечал О.Е. Кутафин, - многие положения, выработанные в то время наукой, применимы к понятию "частная жизнь"[1].

В научной литературе понятие частная жизнь исследовалось многими авторами.

Так, Г.Б. Романовский, определяет «частную жизнь» как "нематериальное благо, принадлежащее каждому гражданину от рождения, заключающееся в таких сторонах его внутренней жизни и сферах общения, которые сознательно им сохраняются в тайне от иных субъектов и подлежат безусловной защите в демократическом государстве как в случаях, прямо предусмотренных в законе, так и в иных случаях, и в тех пределах, которые вытекают из существа данного блага и степени соотносимости его осуществления с правами и свободами других граждан". [2].

М.В. Баглай указывает на то, что частную жизнь составляют те стороны личной жизни человека, которые он в силу своей свободы не желает делать достоянием других. Это своеобразный

суверенитет личности, означающий неприкосновенность ее «среды обитания». [3].

Другие авторы предпринимают попытки дать более точное определение данной дефениции. Однако это делается путем перечисления различных сторон жизни индивида, не связанных с его публичной деятельностью, работой, службой (семейные и родственные отношения, состояние здоровья, интимная жизнь, дружеские связи и т.п.).

Понятие «частная жизнь» исследуется и зарубежными авторами. Однако в зарубежном праве используются термины "приватность" и "прайвеси". В европейских странах широко употребляются понятия и слова, производные от латинского "privatus", - а оно соответствует русскому "частное".

Некоторые теоретические исследования зарубежных авторов заслуживают внимания. Авторитетный американский исследователь, автор фундаментального труда "Приватность и свобода" Алан Вестин говорит о четырех формах приватности. Первая - это "уединение", состояние, в котором человек избавлен от наблюдения со стороны других. Вторая - "интимность", замкнутое общение, предполагающее добровольное поддержание контакта с узким кругом лиц. Третья - "сдержанность", т.е. наличие психологического барьера между индивидом и окружающими его людьми. Четвертая - "анонимность", состояние, когда человек, находясь в общественном месте, стремится остаться неузнанным.

Есть и судебное толкование исследуемого понятия. Конституционный Суд РФ в ряде определений отметил, что понятием "частная жизнь" охватывается та область жизнедеятельности человека, которая имеет отношение к отдельному лицу, касается только его и не подлежит контролю со стороны общества и государства, если она, в свою очередь, не носит противоправного характера [4].

Европейский суд по правам человека в своих решениях указывает, что понятие личной жизни является достаточно широким и не поддается исчерпывающему определению. Оно охватывает как физическую, так и моральную стороны жизни индивида. Такие элементы, как, например, половая идентификация, пол, сексуальная ориентация и половая жизнь, относятся к личной жизни [5].

Ст. 137 УК охраняет от посягательств не всю частную жизнь человека, а только лишь ту ее сторону, которая составляет личную

или семейную тайну. В русском языке под тайной понимается "нечто скрываемое от других, известное не всем, секрет" [6].

При разрешении вопросов, связанных с привлечением к уголовной ответственности по ст. 137 УК РФ правоприменитель обязан мотивировать, почему он признал сведения относящимися к частной жизни, и составляют ли они личную и семейную тайну. В связи с этим необходимо законодательно закрепить определение понятия частной жизни. Возможно, это сделать в примечании к ст. 137 УК РФ, но более целесообразно это сделать на уровне отдельного Федерального закона.

В настоящее время в Российской Федерации нет нормативного правового акта, который бы давал точное определение частной жизни и регулировал порядок обращения со сведениями, составляющими личную и семейную тайну. Отдельные нормы можно найти в разных законах и подзаконных актах, но этого недостаточно для эффективной защиты неприкосновенности частной жизни. Например, в США действует специальный Федеральный закон о защите частной жизни человека 1974 г. (The Federal Privacy Act). По мнению некоторых авторов, принятие подобного закона в РФ позволило бы эффективнее защищать право каждого человека на неприкосновенность его частной жизни [7].

Отсутствие законодательного закрепления понятия частной жизни, порождает трудности в правоприменительной практики. Зачастую частную жизнь отождествляют со сферой интимной жизни человека. Например, М. умышленно, противоправно скопировала с мобильного телефона Г.А. на свой мобильный телефон фотографические изображения Г.А. в обнаженном виде. Указанные фотографии составляли ее личную тайну, поскольку содержали изображения в обнаженном виде [8]. Или другой пример: Новоторжин С.В незаконно произвел и установил в косметологическом кабинете и холле салона специальные технические средства, предназначенные для негласного получения информации (видеокамеры), скрытые от посетителей и работников салона. Зная, что в косметологическом кабинете салона оказываются косметологические услуги гражданам, в том числе, интимного характера, осуществил сбор сведений о частной жизни работника косметологического салона, и клиентов данного салона, составляющих их личную тайну, без согласия на то последних, путем сохранения изоб-

ражения с видеокамеры на электронный носитель, чем нарушил неприкосновенность их частной жизни [9].

Учитывая вышесказанное, предлагаем следующее определение «частной жизни». Это совокупность тайн человека как физических, так и моральных, и таких сфер его жизни, неприкосновенность и охрана которых гарантирована Конституцией РФ и другими федеральными законами и для ознакомления с которыми требуется согласие их обладателя либо иные законные основания. Для эффективной защиты этого блага, более детальной регламентации необходимо принятие специального Закона.

Список литературы

1. Кутафин О.Е. Неприкосновенность в конституционном праве Российской Федерации/ О.Е. Кутафин; под ред. О.Е. Кутафина - М., Юристь, 2004. С. 142.
2. Романовский Г.Б. Право на неприкосновенность частной жизни / Г.Б.Романвский; под ред. Г.Б, Романовского - М.,Юристь, 2001. С. 80.
3. Баглай, М.В. Конституционное право Российской Федерации /М.В. Баглай; под ред. М.В. Баглай – М, Норма, 2009. Ст.181
4. «Об отказе в принятии к рассмотрению жалобы граждан Захаркина Валерия Ивановича и Захаркиной Ирины Николаевны на нарушение их конституционных прав пунктом «б» части третьей статьи 125 и частью третьей статьи 127 Уголовно-исполнительного кодекса Российской Федерации»: Определение Конституционного Суда РФ от 9 июня 2005 г. N 248-О.// СПС КонсультантПлюс.
5. Микеле де Сальвия. Прецеденты Европейского суда по правам человека. Руководящие принципы судебной практики, относящиеся к Европейской конвенции о защите прав человека и основных свобод. СПб., 2004. С. 537.
6. Ожегов С.И. Словарь русского языка. / С.И. Ожегов; под ред. С.И. Ожегова - М., Азь, 1992. С. 785.
7. Кадников, Б.Н. Уголовно-правовая охрана неприкосновенности частной жизни / Б.Н. Кадников; под. ред. Н.Г. Кадникова. - М.: Юриспруденция, 2011. - 136 с.
8. Приговор Мирового судьи Кутузовского судебного участка г. Сыктывкара Республики Коми Мамонова Н.В., от «04» апреля 2012 года [Электронный ресурс]. URL:

https://rospravosudie.com/court-kutuzovskij-sudebnyj-uchastok-g-syktyvkara-s/act-204954783/ (дата обращение 05.04.2014).
9. Приговор Мирового судьи судебного участка № 79 Дзержинского района города Волгограда Паталашко Н.В., от «14» января 2011 года. [Электронный ресурс]. URL: https://rospravosudie.com/court-sudebnyj-uchastok-79-dzerzhinskogo-rajona-g-volgograda-s/act-202749002/ (дата обращение 05.04.2014).

ЗНАЧЕНИЕ МЕСТА И ОБСТАНОВКИ СОВЕРШЕНИЯ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ В КРИМИНАЛИСТИЧЕСКОЙ ХАРАКТЕРИСТИКЕ

А.И. Сабылина, АлтГУ, юридический факультет, 1 к.
Научный руководитель – ***В.В. Поляков,*** к.ю.н., доцент.

Криминалистическая характеристика преступлений в сфере компьютерной информации требует изучения вопроса об обстановке совершения преступлений. Данный вопрос в литературе разработан недостаточно и нуждается в дальнейшем исследовании. Обобщенные знания обстановки преступления позволяют акцентировать внимание следствия на более эффективный поиск и установление обстоятельств, входящих в предмет доказывания [1].

В преступлениях в сфере компьютерной информации местом их совершения обычно является помещение, в котором расположена компьютерная техника с информацией, в отношении которой происходят неправомерные действия, а также места использования компьютерной техники преступником. Принципиальные особенности имеют преступления, связанные с неправомерным доступом к компьютерной информации, совершенные дистанционным образом. Особенностью их является то, что в результате использования информационных сетей (проводных и беспроводных технологий) в одном преступлении одновременно могут быть задействованы множество компьютеров. Соответственно, находиться эти компьютеры могут в пространственно удаленных друг от друга местах и даже в разных государствах [2]. Кроме того, для неправомерного удаленного доступа к компьютерной информации особенностью является то, что территорией места происшествия может быть значительное пространство, включающее

помимо места совершения преступления также места подготовки к нему и места сокрытия следов. Это накладывает отпечаток на тактические приемы и используемую технику проведения осмотра места происшествия, обыска и других следственных действий и оперативно-розыскных мероприятий. В частности, по привлечению дополнительных сотрудников правоохранительных органов, использованию специальных программно-аппаратных средств фиксации, изъятия и исследования компьютерной информации. С учетом этого правильное определение границ, например, для осмотра места происшествия, способствует более быстрому раскрытию преступления [3]. В целях эффективного расследования место происшествия по данным делам можно рассматривать как комплекс взаимосвязанных мест:

Наиболее криминалистически значимую информацию представляют следы, оставленные преступником в первой точке, то есть в месте нахождения и непосредственно в самой ЭВМ (портативные, домашние, рабочие и иные компьютеры, используемые при подготовке, совершении и сокрытии преступлений), с которой совершалось преступление. Помимо виртуальных здесь могут иметься традиционные следы, например, следы пальцев рук на клавиатуре, микрочастицы тканей и иные следы жизнедеятельности преступника, которые его персонифицируют.

Другая группа мест локализации следов компьютерных преступлений включает, используемые в преступлении серверы провайдеров, VPN- и прокси-серверы (компьютеры - посредники на которых почти всегда остаются следы неправомерного удаленного доступа к компьютерной информации или проявления сетевого вредоносного программного обеспечения), сетевые шлюзы и маршрутизаторы. Для этих мест характерно наличие таких следов, как лог-файлы, которые привязаны к конкретному IP-адресу. Они могут фиксировать сеансы сетевой связи и включают в себя сведения о логине и пароле, дате, времени и продолжительности соединения, сведения об ЭВМ нарушителя (программное обеспечение, его конфигурация, настройки брандмауэра и браузера), IP адрес компьютера, MAC-адрес сетевой карты, выделенный для определенного сеанса связи, информацию об отправленных и полученных во время соединения, пакетах (время отправки, приема, размер, тип, IP адрес получателя или отправителя и иное).

К местам происшествия нужно отнести также места нахождения ЭВМ, используемых для совершения преступления при наличии сетевого соединения с ними со стороны преступников. Это ЭВМ пользователей, не подозревающих о том, что в отношении них совершено компьютерное преступление, а их компьютеры используются для совершения преступлений. К подобному способу сокрытия своей личности прибегают наиболее опытные и высококвалифицированные преступники, чтобы запутать следствие. В данном случае компьютеры-посредники выбираются по принципу не обеспеченности должной защищенности. Следы на «промежуточных» ЭВМ могут быть оставлены в лог-файлах, ведущихся различным программным обеспечением, протоколах соединений (наиболее важными из них будут те, что отражают соединение с компьютером предполагаемого преступника), хранилищах определенных категорий файлов (похищенных с ЭВМ пользователей, списков паролей, баз данных, вредоносного программ и т.д.).

Большую роль играет ЭВМ потерпевшего по количеству и значимости электронно-цифровых следов-последствий преступления. Здесь содержатся следы в виде вредоносного программного обеспечения (программы-шпионы, собирающие информацию об ЭВМ жертвы, программы типа «троянский конь» (их управляемая часть), программы-крипторы и иные), следов его самоликвидации, изменений в системных реестрах и log-файлах, сведений об изменении, модификации, копировании, удалении файлов, появления новых файлов специфического содержания [4].

В отдельную группу нужно выделить банки, банкоматы, магазины, в которых осуществляются покупки или происходит обналичивание денежных средств, добытых преступным путем. Следует отметить, что следы этой группы мест имеют повышенное значение при высокотехнологичных способах совершения преступлений. Ретроспективная методика расследования, берущая свое начало с поиска следов с ЭВМ потерпевшего, может натолкнуться на обрывы звеньев следовой цепи действий преступника, например, применившего сокрытие следов преступления путем использования VPN, Tor, анонимных прокси-серверов. Обычно в такой ситуации следствие встает в тупик, так как нет возможности прояснить картину преступления дальше. Именно здесь играют

свою роль следы действий преступника или членов его группы при обналичивании денежных средств. У следствия появляется возможность выяснить главное – кто совершил преступление по оставленным в банке, банкомате, магазине традиционным следам, позволяющим персонифицировать личность.

Состояние обстановки является другим важным аспектом и достаточно сильно влияет на поведение участников преступлений в сфере компьютерной информации. Судебно-следственная практика показала, что для совершения преступлений в сфере компьютерной информации преступники в большинстве случаев тщательно к ним готовятся [6]. Они наводят справки и изучают режим работы на объекте, содержащем предмет преступного посягательства, собирают данные о находящихся там средствах и технологиях. Наибольший интерес вызывают характеристики имеющихся программно-аппаратных средств, прежде всего – используемых средств технической защиты информации. Подготовка нередко связана с изучением и приспособлением к выявленной обстановке. С этой целью в обстановку могут вноситься изменения, например, путем внедрения в операционную систему компьютера, принадлежащего жертве преступного посягательства, вредоносной программы для снижения защиты компьютера и открытии возможности осуществления неправомерного удаленного доступа к нему по информационной сети. Так, в результате несанкционированной установки специального программного обеспечения в компьютер одной из организаций г. Минусинска преступником была получена возможность неоднократного неправомерного доступа к ее информационным ресурсам [7]. Установка данной программы снизила уровень защищенности компьютера организации, сделав его уязвимым для массового неправомерного доступа. В данном случае, обстановка для совершения преступления была изменена на благоприятную. В противном случае, когда встречаются незапланированные барьеры, например, сбой в работе программного обеспечения, преступник может воздержаться от реализации задуманного или спонтанно изменить план действий. Важность учета благоприятной и неблагоприятной обстановки до совершения преступления настолько велика, что некоторыми авторами выделяется в качестве самостоятельного элемента криминалистической харак-

теристики и называется причинами и условиями, способствующими совершению преступления.

На первоначальную обстановку преступления влияет наличие и состояние средств защиты компьютерной информации. К названным выше факторам необходимо добавить состояние по соблюдению требований информационной безопасности, сложившаяся на объекте межличностная обстановка и т.д. Для обстановки, в которой возможно совершение рассматриваемого преступления, наиболее свойственно следующее: низкий технический уровень защиты компьютерной информации и слабый контроль за ней, атмосфера невнимательности к случаям нарушения требований информационной безопасности и т.п. Нужно отметить, что в провинциальных городах влияние этого фактора более выражено, что необходимо учитывать для повышения эффективности расследования и предупреждения рассматриваемых преступлений [8].

Даже опытные компьютерные преступники не всегда правильно оценивают обстановку совершения преступления. Выполнив масштабные технические и организационные мероприятия по его подготовке, они могут не придать значения неучтенным или новым факторам и обстоятельствам. Так, преодолев основные средства защиты предмета посягательства и получив доступ к искомой компьютерной информации, преступники не обращают внимание на наличие программ, не препятствующих их дальнейшей деятельности, но ведущих подробную фиксацию их действий. Нередко встречается такая ситуация преступления, когда преступники, неожиданного добившись или получив благоприятные условия для совершения преступления, например, в результате удачного стечения обстоятельств, могут изменить способ совершения преступления, слишком упростив или усложнив его. В результате такой «самодеятельности» преступники забывают, не успевают или пренебрегают сокрыть неспрогнозированные ранее следы преступления.

Таким образом, преступник в сфере компьютерной информации оставляет следы в различных местах, как виртуального мира, так и материального. Поэтому при расследовании преступлений в сфере компьютерной информации необходимо изучать систему различного рода взаимодействующих между собой объек-

тов, явлений и процессов, в совокупности составляющих место и обстановку совершения компьютерных преступлений.

Список литературы

1. Поляков В.В. Обстановка совершения преступлений в сфере компьютерной информации как элемент криминалистической характеристики // Известия Алтайского государственного университета. 2013. № 2. С. 114 - 116.
2. Агибалов А.Ю. Виртуальные следы в криминалистике и уголовном процессе: автореф. дис. канд. юрид. наук. - Воронеж, 2010. С. 21.
3. Бахин В.П., В.С. Биленчук, П.Д. Кузьмичев. Криминалистические приемы и средства разрешения следственных ситуаций - Киев: КВШ МВД СССР им. Ф.Э. Дзержинского, 1991. – С. 98.
4. Поляков В.В., Лапин С.А. Программное обеспечение, используемое для совершения компьютерных преступлений // Ломоносовские чтения на Алтае–2013: матер. Междунар. молодежной школы-семинара (Барнаул, 5-8 ноября 2013 г.). – Барнаул: Изд-во Алт. ун-та, 2013. – Ч. 2 . – С. 15-17.
5. Осипенко А.Л. Сетевая компьютерная преступность: теория и практика борьбы: монография. – Омск: Омская академия МВД России, 2009. С. 243-246.
6. Уголовное дело № 13127428 // Архив суда г. Минусинска. 2005 г.
7. Гавло В.К., Поляков В.В. Некоторые особенности расследования преступлений, связанных с неправомерным доступом к компьютерной информации // Известия Алтайского государственного университета. 2006. №2. С. 44-48.

ОБСТОЯТЕЛЬСТВА, ПОДЛЕЖАЩИЕ УСТАНОВЛЕНИЮ И ДОКАЗЫВАНИЮ ПО ДЕЛАМ О КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЯХ

Л.Г. Суханова, АлтГУ, юридический факультет, магистратура, 2 к.
Научный руководитель – ***В.В. Поляков,*** к.ю.н., доцент.

Расследование компьютерных преступлений представляет собой сравнительно новое веяние в уголовном судопроизводстве. Расследование и раскрытие преступлений в сфере компьютерной

информации сопряжены с решением важной и сложной задачи - изъятием компьютерной информации и рассмотрением ее с точки зрения доказательства по уголовному делу.

Применительно к процессу доказывания компьютерную информацию можно определить как фактические данные, которые существуют в электронном виде, сохраняются в форме, доступной восприятию ЭВМ или человека либо передаются по телекоммуникационным каналам и на основе которых в определенном законом порядке устанавливаются обстоятельства, имеющие значение для правильного разрешения дела [6].

Криминалистическая характеристика преступлений в сфере компьютерной информации и обстоятельства подлежащие установлению и доказыванию по названным преступлениям тесно взаимосвязаны и во многом совпадают по своему содержанию.

В криминалистическую характеристику преступлений в сфере компьютерной информации входят следующие основные данные: о способах совершения преступления и механизме противоправного деяния; средствах совершения противоправного деяния; обстановке и месте совершения преступления; следах преступления; предмете преступного посягательства; лицах, совершающих данные преступления [3].

При расследовании компьютерных преступлений правоохранительные органы обязаны установить обстоятельства, которые подлежат установлению и доказыванию. Можно выделить следующие такие обстоятельства:

1. имело ли место преступление (либо это правонарушение иного рода);
2. каков объект преступного посягательства (данное обстоятельство имеет решающее значение для применения следователем той или иной методики расследования конкретного преступления или их совокупности);
3. каков предмет преступного посягательства;
4. каков способ совершения преступления;
5. место, время (период) и обстоятельства совершения преступления;
6. размер и вид ущерба, причиненного пострадавшему;
7. кто совершил преступление;

8. если преступление совершено группой лиц, то каковы состав группы и роль каждого соучастника;
9. какие обстоятельства способствовали совершению преступления [1].

Вышеуказанные обстоятельства являются основными и подлежат установлению и доказыванию по всем категориям компьютерных преступлений. Однако имеется определенная специфика обстоятельств, подлежащих обязательному установлению и доказыванию при расследовании компьютерных преступлений в зависимости от состава преступления, предусмотренного соответствующими статьями УК РФ.

Полагаем, что при расследовании неправомерного доступа к компьютерной информации подлежат установлению следующие обстоятельства:

- факт неправомерного доступа к компьютерной информации;
- место несанкционированного проникновения в компьютерную систему или сеть;
- время несанкционированного доступа;
- надежность средств защиты компьютерной информации;
- способ совершения несанкционированного доступа;
- лица, совершившие неправомерный доступ к компьютерной информации;
- виновность и мотивы лиц, совершивших неправомерный доступ к компьютерной информации;
- вредоносные последствия неправомерного доступа к компьютерным системам или сетям;
- обстоятельства, способствовавшие неправомерному доступу к компьютерной информации.

Факт неправомерного доступа к информации в компьютерной системе или сети обычно первыми обнаруживают потерпевшие. Однако они не всегда своевременно сообщают об этом правоохранительным органам. Особенно это относится к руководителям кредитно-финансовых учреждений, которые не желают вызывать у клиентов сомнения в надежности своей деловой репутации. Они также опасаются, что по этому факту начнется проведение проверок, ревизий и экспертиз, могущих раскрыть их финансовые и иные служебные тайны, вскрыть какие-то нарушения.

Установить факт неправомерного доступа к компьютерной информации можно и в процессе проведения проверочных мероприятий в стадии возбуждения уголовного дела либо в ходе проведения ревизий, судебных экспертиз, иных следственных действий по уголовным делам, находящимся в производстве следователей, а также при проведении оперативно-розыскных мероприятий [2].

Интерес представляет специфика обстоятельств, которые подлежат установлению и доказыванию по делам, связанным с созданием, использованием и распространением вредоносных компьютерных программ. Причем, создание (включая изменение существующей программы) вредоносной программы означает любую деятельность, направленную на написание вредоносной программы. Создание вредоносной программы - не только творческая деятельность ее автора, но и техническая помощь, оказанная ему другими лицами. Созданием вредоносной программы будет и написание вредоносной программы, лишенной свойства новизны. Создание программы является оконченным преступлением с момента получения объективной формы представления. Под использованием вредоносной программы необходимо понимать ее непосредственное использование для несанкционированного уничтожения, блокирования, модификации, копирования информации, нарушения работы ЭВМ, их системы или сети [7]. Распространение вредоносной программы означает как распространение ее с помощью средств связи, так и простую передачу ее другому лицу в любой форме (в том числе и в виде записи на бумаге).

Распространение машинных носителей вредоносной программы означает передачу носителя другому лицу, включая копирование или дозволение копирования программы на носитель другого лица.

Особенностью неправомерного доступа к компьютерной информации, а также создания, использования и распространения вредоносных программ для ЭВМ является то, что место непосредственного совершения противоправного деяния (место, где выполнялись действия объективной стороны состава преступления) и место наступления вредных последствий (место, где наступил результат противоправного деяния) могут не совпадать [4].

Проблемным вопросом является определение места происшествия, поскольку при совершении одного преступления их может быть несколько: рабочее место, место постоянного хранения или резервирования информации, место подготовки преступления и др. [5].

Чаще обнаруживается место непосредственного использования результатов неправомерного доступа к компьютерной информации, особенно связанного с хищением денежных средств. При обнаружении неправомерного доступа к информации в компьютерной системе или сети следует выявить все места, где расположены компьютеры, имеющие телекоммуникационную связь. Следует установить место хранения информации на машинных носителях, добытых в результате неправомерного доступа к компьютерной системе или сети [8]. При расследовании нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети необходимо обращать внимание на факт преступного нарушения таких правил. Следует не забывать, что под правилами эксплуатации компьютерной системы следует понимать как правила, которые могут быть установлены компетентным государственным органом, так и правила технической эксплуатации и правила работы с программами, установленные изготовителями ЭВМ и иного компьютерного оборудования, правила, установленные разработчиками программ, сетевыми администраторами, а также правила, установленные владельцем компьютерной системы или по его полномочию.

Необходимо прежде всего установить факт существования конкретных правил эксплуатации ЭВМ на данном объекте. Они могут касаться порядка создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю компьютерной информации, защите ее на любой стадии информационного процесса [3]. Результаты анализа компьютерной преступности позволяют прогнозировать усложнение борьбы с нею ввиду того, что способы совершения компьютерных преступлений с каждым годом усложняются и приобретают все более изощренный характер. Более того, совершенствуются навыки преступников, применяемая ими техника, системы связи и передачи информации. Это ведет к увеличению количества преступлений. Изучение вопроса о способе совершения преступ-

лений в сфере компьютерной информации, личности преступников, совершающих такие преступления, а также исследование других обстоятельств, подлежащих установлению и доказыванию, является чрезвычайно важным для достижения цели своевременного выявления, раскрытия и предупреждения компьютерных преступлений.

Список литературы

1. Вехов В.Б. Компьютерные преступления. Способы совершения методики расследования. - М., 1996. - 182 с.
2. Гавло В.К., Поляков В.В. Следовая картина и ее значение для расследования преступлений, связанных с неправомерным удаленным доступом к компьютерной информации // Российский юридический журнал. 2007. №5 (57). С. 146-152.
3. Гаврилин Ю.В. Преступления в сфере компьютерной информации: квалификация и доказывание. Учебное пособие. - М.: ЮИ МВД РФ, 2003. - 245 с.
4. Поляков В.В. Анализ высокотехнологичных способов неправомерного удаленного доступа к компьютерной информации // Известия Томского политехнического университета. 2007. Т. 310. № 1. С. 212 – 216.
5. Протасевич А.А., Зверянская Л.П. Криминалистическая характеристика компьютерных преступлений // Российский следователь. 2013. № 11. С.45-47.
6. Сарапулов А.А. Теоретико-прикладные проблемы доказательств о преступлениях в сфере компьютерной информации // Правовые вопросы связи. 2011. № 1. С. 8-10.
7. Уголовное право Российской Федерации. Особенная часть: Учебник под ред. Л.В. Иногамовой-Хегай, – М.: Инфра-М: Контракт, 2005. – 559 с.
8. Шурухнов Н.Г. Расследование неправомерного доступа к компьютерной информации: учеб. пособ. – М: Московский университет МВД России, 2004. – 351с.

ХАРАКТЕРИСТИКА ЛИЧНОСТИ ПРЕСТУПНИКА, СОВЕРШАЮЩЕГО ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Ю.С. Трушева, АлтГУ, юридический факультет, магистрант 1 к.
Научный руководитель – ***В.В. Поляков,*** к.ю.н., доцент.

Личность преступника всегда была одной из центральных проблем всех наук криминального профиля. Успешное предупреждение преступлений невозможно без изучения криминалистически значимых свойств личности преступника [1].

С распространением компьютерных технологий в повседневной жизни произошло увеличение количества преступных посягательств, совершенных с использованием электронно-вычислительной техники [2].

Компьютерное преступление и личность преступника сильно взаимосвязаны [3]. С точки зрения А.Б. Попова, компьютерных преступников можно разделить на три группы.

Первая группа - начинающие преступники. Чаще всего это выпускники (или студенты старших курсов) технических вузов, имеющие постоянный доступ к ЭВМ, вращающийся в сообществах, интересующихся компьютерными технологиями. Средний возраст – 15–20 лет. Пол – в подавляющем большинстве случаев мужской. Образование – среднее, среднее специальное или высшее, в некоторых случаях неоконченное. Происходят из семей среднего достатка. К компьютерной технике «приобщились» в большинстве случаев уже с 8–9 класса средней школы. Имеют дома один или более персональных компьютеров. Знание компьютерных технологий не ограничивается языками программирования низкого и высокого уровней и включает в себя знание аппаратной части выбранной платформы. Редко работают официально. Связь с внешним миром поддерживают в ограниченном объеме. Преимущественно имеют технического образование, гуманитарные знания не высоки (в письменной речи много грамматических ошибок). В разговоре употребляют особый компьютерный жаргон, сленг, смешивают русский и английский языки. Характеризуются несобранностью, небрежностью, практически постоянно читают литературу «по профессии».

Вторая группа – «закрепившиеся» преступники. Возраст 20–25 лет. Пол – в основном, мужской, но наблюдается тенденция к увеличению числа лиц женского пола (на сегодняшний день это около 5%). Образование – среднее, среднее специальное, высшее и незаконченное высшее, в основном – техническое. При совершении преступлений используют набор заранее подготовленных средств совершения преступлений, готовые решения, разработанные представителями первой группы преступников или другими членами своей группы. Часто являются организаторами хакерских атак с исполнителями из первой группы. В большинстве случаев лица, принадлежащие к этой группе, имеют постоянную работу в качестве технических консультантов и системных администраторов в фирмах, консультантов в компьютерных фирмах (что позволяет им в определенных случаях получать доступ к компьютеру жертвы, устанавливать вредоносное программное обеспечение для дальнейшего использования в преступных целях). Основная сфера «деятельности» – сетевой взлом, отдельные действия в операциях по получению защищенной информации**.**

Третья группа - профессионалы. Возраст 25–45 лет. Пол: мужской – 92%, женский – 8%. Социальное происхождение – семьи с достатком выше среднего. Образование – высшее техническое, возможно не одно. Имеются высокие знания в области компьютерных технологий: люди этой группы владеют несколькими языками программирования всех уровней, в совершенстве знают особенности аппаратной части современных компьютерных систем, имеют навыки профессиональной работы с несколькими компьютерными платформами. Психотип уравновешенный, стойкий к внешним воздействиям, с устоявшимися взглядами и системой ценностей. Личности амбициозные. Работают в основном «для прикрытия», например, начальниками отделов информационных технологий в крупных, в том числе иностранных, компаниях и государственных учреждениях. Основная же деятельность происходит в нелегальной и полулегальной сферах [4].

Н.Н. Федотов приводит следующее описание самых типичных образов компьютерных преступников. Стоит отметить, что наименование каждого типа дается автором условно.

Первый тип – «хакеры». Основной мотивацией хакеров являются исследовательский интерес, любопытство, стремление до-

казать свои возможности, честолюбие. Средства защиты компьютерной информации и ее недоступность они воспринимают как вызов своим способностям. Первой чертой личности «хакера» является эскапизм – бегство от действительности, стремление уйти от реальности, от общепринятых норм общественной жизни в мир иллюзий. «Хакер» имеет узкий круг общения и предпочитает всем другим контактам сетевые. Второй чертой данного типа личности является некриминальная направленность мыслей «хакера». Это, как правило, выливается в уделение малого внимания заметанию следов, непринятие мер конспирации. Часто у него даже отсутствует само осознание того факта, что совершается уголовное преступление.

Несколько более распространенным типом компьютерных преступников являются лица, не слишком хорошо владеющий знаниями в области информационных технологий, но зато владеющими доступом в информационную систему в силу служебного положения – так называемые «инсайдеры». Если для «внешнего» хакера обнаружить уязвимость в информационной системе представляет собой отдельную задачу, то для сотрудника организации почти все уязвимости видны с самого начала. Однако руководители и даже сотрудники службы безопасности, которым доверена такая информационная система, обычно излишне доверяют собственным сотрудникам.

Типичный «инсайдер» совершает компьютерное преступление (лично или в форме подстрекательства, совместно с «внешним» соучастником) с использованием сведений, полученных в силу служебного положения. Такими сведениями могут выступать пароли, знания о конфигурации информационной системы, знания о ее уязвимостях, о принятых процедурах. В ряде случаев этими сведениями «инсайдер» владеет «официально», то есть они ему необходимы для выполнения работы. Часто бывает, что реальный доступ сотрудников к конфиденциальной информации значительно шире, чем формальный или чем необходимый.

Следующий тип преступников совершают преступление из предприимчивых мотивов. Этот тип не является квалифицированным ИТ-специалистом и не имеет служебного положения, которым можно злоупотребить. С самого начала планирования преступления осознается его противозаконность. Решение совершить

преступление именно в компьютерной (сетевой) среде принимается не из-за своих особых знаний в этой области, а исключительно на основе рационального анализа, считая, что так будет выгоднее. Указанному типу преступников отвечает большинство кардеров, спамеров и фишеров.

Стоит отметить интернет-мошенников, которые руководствуются не только извлечением прибыли. Их преступный доход часто бывает меньше, чем средняя зарплата специалиста той же квалификации. Таких компьютерных преступников Н.Н. Федотов относит к «антисоциальному» типу. Мотивом для совершения мошенничества является антисоциальная психопатия (социопатия). Обычно такие типы действуют импульсивно и не склонны к планированию, особенно долгосрочному [5].

Таким образом, оценивая вероятного преступника, важнее всего установить его психотип и уровень технических знаний, а также мотив преступления.

Специфика преступлений, совершаемых в сфере компьютерных технологий, накладывает отпечаток на личность преступника, которая приобретает целый ряд особенностей [6]. Детальное изучение личностных характеристик преступников данной сферы может не только помочь выйти на след виновного, но и может способствовать профилактике данного вида преступлений среди так называемых групп риска.

Список литературы

1. Поляков В.В. Криминалистическая структура мер предупреждения компьютерных преступлений // Библиотека криминалиста: научный журнал. 2013. №5 (10). С. 287 - 291.
2. Поляков В.В. Особенности расследования неправомерного удаленного доступа к компьютерной информации: дис. канд. юрид. наук: 12.00.09 / В.В. Поляков. – Омск, 2008. – 247 с.
3. Попов А.Б. Криминологическая характеристика личности преступника, совершающего преступление, предусмотренное ст. 272 УК РФ // Вестник Тамбовского университета. Серия: Гуманитарные науки. 2009. № 8. С. 411–413
4. Ковалев Д.И. Криминологическая характеристика преступника, совершающего преступление в сфере компьютерной информации // Вестник Академии. 2011. №3. С. 90-92

5. Федотов Н.Н. Форензика – компьютерная криминалистика. Москва: изд-во «Юридический Мир», 2007. С. 41-47.
6. Гавло В.К. Криминалистическая характеристика преступлений в сфере компьютерной информации / В.К. Гавло, В.В. Поляков // Право и государство: приоритеты XXI века: матер. Всерос. науч.-практ. конф. / под ред. В.Я. Музюкина, Е.С. Аничкина. – Барнаул: Изд-во Алт. ун-та, 2007. – С. 503 - 5

Научное издание

ПРОБЛЕМЫ ПРАВОВОЙ И ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ – 2014

Материалы междисциплинарной межвузовской конференции студентов, магистрантов и аспирантов

Дизайн Р.М. Сахатов
Составитель Р.М. Сахатов
под редакцией
В.В. Белозерских
В.В. Русанов

Подписано в печать 1.12.2014 г.
Объем 8,9 уч.-изд. л. Формат 60x84/16. Бумага офсетная.
Тираж 60 экз. Заказ № 2151
Отпечатано ИП Колмогоров И.А.,
656049, г. Барнаул, пр-т Социалистический, 85,
т./ф.: (3852) 36-82-51, concept-print.ru