Приложение (-ия) к приказу ректора от 20.11.2025 №1866/П

УТВЕРЖДЕНО

Подлинник электронного документа, подписанного ЭП, хранится в системе электронного документооборота АлтГУ

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Сертификат: 009D6B8A7CE4B0ED25CD20F5D4D1BFD775
Владелец: Жданова Евгения Анатольевна

Дата подписания: 20.11.2025 19:01:11 UTC+7
Действителен: с 09.06.2025 по 02.09.2026

Приложение 1

Положение по организации антивирусной защиты в Алтайском государственном университете

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с Федеральными законами №149-ФЗ «Об информации, информационных технологиях и о защите информации», №152-ФЗ «О персональных данных», №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», постановлением Правительства РФ №1119, требованиями ФСТЭК России, а также внутренними нормативными актами Алтайского государственного университета, включая Политику информационной безопасности.

1.2. Положение устанавливает требования к организации антивирусной защиты информационной инфраструктуры АлтГУ (Оператора), включая информационные системы персональных данных (далее – ИСПДн), корпоративные сервисы, локальные вычислительные сети и автоматизированные рабочие места. Определяет ответственность должностных лиц, работников, участвующих в эксплуатации, администрировании и сопровождении ИС, за выполнение мероприятий по защите информации от вредоносного программного обеспечения (далее – ПО).

1.3. Цель антивирусной защиты – обеспечение устойчивого функционирования ИТ-инфраструктуры Оператора, предотвращение потери, искажения, блокирования, несанкционированного доступа или распространения информации вследствие воздействия вредоносного ПО.

1.4. Основные задачи антивирусной защиты:

– предотвращение проникновения и распространения вредоносного ПО;

– своевременное выявление и нейтрализация заражённых объектов;

– проведение профилактических мероприятий с применением средств диагностики, мониторинга и анализа событий безопасности;

– обеспечение контроля состояния защищённости информационных ресурсов на всех этапах эксплуатации.

1.5. Защите подлежат все компоненты инфраструктуры, включая серверы, автоматизированные рабочие места (АРМ) пользователей и администраторов.

1.6. Основные источники проникновения вредоносных программ:

– съемные носители (USB, внешние диски и др.);

– корпоративная и локальная сеть, электронная почта, интернет;

– программы и файлы из недоверенных источников.

2. Организация мероприятий по антивирусной защите

2.1. Вся деятельность по антивирусной защите проводится под контролем Управления информатизации АлтГУ. Организация, координация и контроль мероприятий по антивирусной защите осуществляются ответственным за организацию антивирусной защиты, назначаемым приказом ректора.

2.2. Все АРМ, серверы и устройства подключаются к корпоративной сети только при наличии сертифицированных ФСТЭК средств антивирусной защиты, поддерживающих централизованное управление и автоматическое обновление сигнатур.

2.3. Обновление антивирусных баз выполняется автоматически, при сбоях — вручную ответственным лицом с проверкой целостности обновлений.

2.4. Мероприятия по антивирусной защите включают:

– регулярное обновление ПО;

– контроль целостности;

– ограничение использования внешних носителей;

– анализ событий безопасности;

– автоматическое и ручное сканирование;

– изоляцию или удаление заражённых файлов;

– расследование инцидентов, документирование результатов.

2.5. Все действия субъектов ИТ-инфраструктуры касаемые средств антивирусной защиты, фиксируются средствами мониторинга и отчетности.

2.6. Управление информатизации проводит ежеквартальный внутренний аудит соблюдения данных требований, результаты документируются и направляются начальнику управления информатизации.

3. Профилактические мероприятия по антивирусной защите

3.1. Регулярное проведение профилактических мероприятий по антивирусной защите является обязательной мерой, направленной на предотвращение появления и распространения вредоносных программ в информационной инфраструктуре Оператора.

3.2. Профилактические мероприятия обязательны и включают

К основным профилактическим мероприятиям относятся:

– еженедельная быстрая автоматическая антивирусная проверка всех активных рабочих станций и серверов;

– еженедельная выборочная проверка элементов инфраструктуры антивирусными средствами, включая системы хранения данных и общие сетевые ресурсы, независимо от наличия признаков заражения;

– постоянное отслеживание информации о новых вредоносных программах, способах их распространения и актуальных уязвимостях через официальные источники (вендоры средств защиты, CERT, ГосСОПКА и т. д.);

– информирование работников Оператора о новых типах вредоносного ПО, методах социальной инженерии и рекомендациях по безопасной работе в сети;

– ограничение физического и логического доступа к элементам информационной инфраструктуры третьих лиц, не уполномоченных на выполнение работ;

– обучение, инструктаж пользователей и администраторов по работе с ИС и реагированию на инциденты.

3.2. При обнаружении заражения вредоносным программным обеспечением на

автоматизированном рабочем месте (АРМ) или сервере, подключённом к локальной вычислительной сети, обязательной внеплановой проверке подлежат все АРМ, серверы и иные устройства, входящие в тот же сетевой сегмент, а также системы, использующие общие ресурсы данных и программное обеспечение.

Результаты внеплановой проверки документируются в установленном порядке и направляются начальнику отдела защиты информации.

4. Действия при выявлении признаков вредоносного программного обеспечения

4.1. При возникновении подозрения на наличие вредоносного программного обеспечения (ошибки в работе приложений, появление посторонних графических или звуковых эффектов, искажения данных, исчезновение файлов, частые сообщения о системных сбоях, существенное замедление работы и т. п.) работник обязан немедленно прекратить работу с подозрительным устройством.

При наличии соответствующих прав он должен самостоятельно выполнить внеочередную антивирусную проверку средствами защиты, установленных на рабочем месте, либо обратиться к администратору средств антивирусной защиты.

4.2. При подозрении на наличие вредоносного ПО на серверах, файловых серверах или интернет-шлюзах ответственный организует внеочередную проверку указанных систем с привлечением специалистов отдела телекоммуникаций.

4.3. В случае подтверждения факта заражения вредоносным программным обеспечением ответственный за организацию антивирусной защиты проводит анализ ситуации, определяет источник заражения, масштаб распространения и возможные последствия инцидента. По результатам анализа принимается решение о способе нейтрализации угрозы - лечении заражённых объектов, их изоляции либо удалении. При необходимости оформляется отчёт об инциденте информационной безопасности.

5. Применение средств антивирусной защиты

5.1. Обнаруженные вредоносные программы подлежат лечению или удалению средствами антивирусной защиты в автоматическом режиме. Если автоматическое устранение невозможно, обработка выполняется вручную ответственным администратором Управления информатизации.

5.2. В случае повреждения или уничтожения вредоносным ПО файлов баз данных, системных компонентов или пользовательских данных, ответственный за обеспечение информационной безопасности организует восстановление информации с использованием последней актуальной резервной копии.

5.3. После удаления вредоносного ПО и восстановления данных проводится повторная антивирусная проверка системы с использованием актуальных антивирусных баз. Перед повторной проверкой заражённое устройство должно быть перезагружено.

5.4. Обязательному антивирусному контролю подлежит любая информация, получаемая или передаваемая по телекоммуникационным каналам (включая электронную почту, сетевые ресурсы и облачные сервисы), а также данные, размещённые на съёмных носителях информации.

5.5. Все файлы, подлежащие архивному хранению, должны проходить антивирусный контроль до помещения в архив. Электронные архивы подлежат периодической проверке не реже одного раза в квартал - в автоматическом или ручном режиме.

5.6. Любое устанавливаемое или обновляемое программное обеспечение должно быть предварительно проверено на отсутствие вредоносных компонентов средствами антивирусной защиты. Установка неподтверждённого программного обеспечения без проверки запрещена.

5.7. В организации должно применяться централизованное управление всеми инструментами антивирусной защиты.

6. Ответственность

6.1. Ответственный за антивирусную защиту обеспечивает соблюдение требований настоящего регламента, организует контроль исполнения и принимает меры при выявлении нарушений.

6.2. Работники университета несут ответственность за нарушение требований настоящего регламента в соответствии с законодательством Российской Федерации, локальными нормативными актами университета и условиями трудовых договоров.

7. Заключительные положения

7.1. Положение, а также изменения в него утверждаются приказом ректора.

7.2. Контроль выполнения настоящего положения осуществляется управлением информатизации АлтГУ.

7.3. Настоящее положение подлежит пересмотру при изменении инфраструктуры или нормативных актов.

Приложение 2

Регламент организации доступа в сеть Интернет в подразделениях, обрабатывающих персональные данные и (или) иную конфиденциальную информацию в Алтайском государственном университете

1. Общие положения

1.1. Настоящий Регламент устанавливает порядок организации и контроля доступа к сети Интернет в структурных подразделениях ФГБОУ ВО «Алтайский государственный университет» (далее – Университет), осуществляющих обработку персональных данных и иной конфиденциальной информации.

1.2. Цель Регламента – минимизация рисков утечки информации, заражения вредоносным программным обеспечением и несанкционированного доступа к информационным ресурсам Университета при использовании сети Интернет.

1.3. Действие Регламента распространяется на все структурные подразделения Университета, где осуществляется обработка персональных данных и (или) иной конфиденциальной информации, а также на работников и обучающихся, использующих автоматизированные рабочие места (АРМ) в таких подразделениях.

1.4. При разработке Регламента учтены требования:

– Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных».

– Постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

– Приказ ФСТЭК России от 11 февраля 2013 года № 17 «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 февраля 2013 года № 21 «Об утверждении Требований по обеспечению безопасности информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

– Приказ ФСТЭК России от 9 февраля 2021 года № 117 «Об утверждении Требований к созданию систем защиты информации в государственных информационных системах». Локальных нормативных актов Университета в области информационной безопасности.

1.5. Основные определения:

Персональные данные – любая информация, относящаяся к определённому или определяемому на основании такой информации физическому лицу.

Конфиденциальная информация – это документированная или иным образом зафиксированная информация, представляющая собой сведения о лицах, предметах, фактах, событиях, процессах, имеющая действительную или потенциальную коммерческую ценность и доступ к которой ограничен согласно законодательству РФ и внутренним нормативным актам университета.

«Белые списки» интернет-ресурсов – это перечень сайтов и онлайн-ресурсов, доступ к которым разрешён для пользователей сети организации.

Информационная безопасность – состояние защищённости информационных ресурсов от угроз, обеспечивающее целостность, конфиденциальность и доступность информации.

Пользователь – сотрудник или студент, имеющий право на доступ к ресурсам сети Интернет университета.

Администратор сети – уполномоченное лицо, ответственное за организацию, настройку и контроль доступа к корпоративной сети.

2. Организация доступа

2.1. Доступ в сеть Интернет подразделений, обрабатывающих персональные данные и (или) иную конфиденциальную информацию, предоставляется исключительно по «белым» спискам разрешённых интернет-ресурсов.

2.2. Запрещается использование сети Интернета для доступа к ресурсам, не связанным с рабочими задачами, которые могут угрожать конфиденциальности и безопасности персональных данных.

2.3. Перечень подразделений, для которых применяется данный порядок, утверждается ректором Университета по представлению проректора по цифровому развитию и/или начальника управления информатизации.

2.4. Доступ к сети Интернет осуществляется с использованием программно-аппаратных средств, таких как UserGate, прокси-сервер или иные средства, которые позволяют обеспечивать использование «белого списка», а также обеспечивать регистрацию обращений и фильтрацию трафика в соответствии с установленными списками

2.5. Ответственность за техническую реализацию мер фильтрации несет управление информатизации Университета.

2.6. В случае выявления инцидентов, угрожающих безопасности персональных данных, доступ пользователя ограничивается или временно блокируется до устранения угрозы.

3. Порядок формирования и изменения «белого списка»

3.1. Первичное формирование «белого списка» интернет-ресурсов осуществляется управлением информатизации на основании служебной необходимости и требований информационной безопасности.

3.2. Добавление нового ресурса или исключение ранее внесённого ресурса из «белого списка» производится на основании служебной записки руководителя структурного подразделения на имя проректора по цифровому развитию, либо посредством направления заявки через специализированную форму на портале поддержки пользователей.

3.3. Управление информатизации выполняет обязательный анализ каждого запрашиваемого ресурса, включающий:

– проверку на наличие вредоносной активности, признаков участия в ботнет-сетях, фишинговых схемах или распространении вредоносного программного обеспечения;

– оценку соответствия ресурса служебным задачам подразделения;

– проверку соблюдения принципа минимально необходимого доступа.

3.4. По итогам анализа принимается решение о включении интернет-ресурса в «белый список» либо об отказе с указанием причин. Срок рассмотрения обращения не должен превышать одного рабочего дня.

3.5. Обновлённая версия «белого списка» утверждается проректором по цифровому развитию и вводится в действие управлением информатизации.

3.6. Ведение актуальной версии «белого списка», обеспечение его доступности для ответственных лиц и контроль за корректностью применения осуществляется управлением информатизации.

4. Обязанности и ответственность

4.1. Управление информатизации обеспечивает ведение журналов обращений к Интернет-ресурсам, их хранение не менее 1 месяца и проводит анализ на предмет нарушений.

4.2. Отдел защиты информации проводит периодическую проверку корректности применения «белых списков» и выявления несанкционированных обращений.

4.3. Сетевые администраторы обязаны обеспечивать конфиденциальность учетных данных, вести учет и журналирование доступа и своевременно реагировать на инциденты.

4.4. Руководители подразделений обязаны информировать управление информатизации о выявленных нарушениях порядка доступа.

4.5. Работники Университета, нарушающие настоящий Регламент, несут дисциплинарную ответственность в соответствии с трудовым законодательством и локальными нормативными актами Университета.

5. Заключительные положения

5.1. Регламент утверждается приказом ректора.

5.2. Контроль выполнения настоящего регламента осуществляется управлением информатизации АлтГУ совместно с уполномоченными лицами по защите персональных данных.

5.3. Изменения и дополнения в регламент вносятся на основании изменений в законодательстве и решений руководства университета.

5.4. Ознакомление с регламентом обязательно для всех сотрудников, имеющих доступ к сети Интернет в подразделениях, работающих с персональными данными и (или) иной конфиденциальной информацией.

Приложение 3

Регламент по организации доступа внешних пользователей к сети Интернет через корпоративную сеть Алтайского государственного университета

1. Общие положения

1.1. Настоящий Регламент определяет порядок предоставления временного доступа для внешних пользователей (участников мероприятий, слушателей программ дополнительного профессионального образования, командированных лиц, приглашённых специалистов и иных пользователей, не состоящих в трудовых отношениях с ФГБОУ ВО «Алтайский государственный университет» (далее – Университет)) к сети передачи данных АлтГУ с выходом в сеть Интернет.

1.2. Цель Регламента – обеспечение безопасного, контролируемого и документально подтверждённого доступа внешних пользователей к сети Интернет с соблюдением требований законодательства Российской Федерации в области информационной безопасности и защиты персональных данных.

1.3. Ответственным за организацию и техническое сопровождение доступа внешних пользователей является управление информатизации АлтГУ.

1.4. Настоящей Регламент разработан в соответствии Федеральным законом № 152-ФЗ «О персональных данных», Федеральным законом № 187-ФЗ «О безопасности критической информационной инфраструктуры», Приказом ФСТЭК России № 117 от 11.04.2025 «Об утверждении требований о защите информации», Постановлением Правительства РФ № 758 от 31.07.2014 об организации публичного Wi-Fi с идентификацией пользователей и иными локальными нормативными актами АлтГУ и внутренними политиками безопасности.

1.5. Основные определения:

Внешние пользователи – лица, не состоящие в трудовых отношениях с университетом, включающие участников мероприятий, слушателей программ дополнительного профессионального образования, командированных лиц, приглашённых специалистов, представителей организаций с которыми работает университет и других лиц, которым временно предоставляется доступ к сети передачи данных университета.

Внутренние пользователи – сотрудники и штатные работники Алтайского государственного университета, а также обучающиеся по основным образовательным программам (студенты и обучающиеся), для которых организован постоянный доступ к корпоративной сети в рамках исполнения служебных обязанностей либо в целях обеспечения учебного процесса.

Гостевой Wi-Fi – это отдельная беспроводная сеть, созданная для временного доступа внешних пользователей к сети Интернет через корпоративную инфраструктуру. Гостевой Wi-Fi изолирован от основного корпоративного сегмента, обеспечивая безопасность информационных ресурсов организации и контролируемый доступ посторонних лиц.

2. Организация доступа

2.1. Для обеспечения доступа внешних пользователей по беспроводной сети, создается отдельная выделенная сеть (VLAN), изолированная от основной корпоративной инфраструктуры АлтГУ.

2.2. Авторизация внешних пользователей в сети осуществляется одним из двух способов:

– путем создания временной учетной записи;

– по номеру мобильного телефона с использованием информационной системы поддержки Гостевого WiFi.

2.3. При доступе в сеть Интернет ведется автоматический учет регистрационных данных пользователей, их действий и регистрация событий безопасности в журналах безопасности. Логи авторизации и сетевой активности подлежат хранению не менее трёх лет в соответствии с требованиями законодательства Российской Федерации.

2.4. Внешним пользователям предоставляется доступ исключительно к сети Интернет про протоколы http и https. Вся передача данных осуществляется с фильтрацией и ограничением трафика в соответствии с нормативными актами РФ, включая блокировку ресурсов, запрещённых к распространению на территории Российской Федерации.

2.5. Порядок предоставления доступа при проведении мероприятий (например, во время конференций, олимпиад, форумов и т.п.).

2.5.1. В случае проведения мероприятий, рассчитанных на неограниченный круг лиц, может быть организован доступ к Гостевой сети WiFi с аутентификацией по номерам телефонам.

2.5.2. Для организации временного доступа внешних пользователей руководитель структурного подразделения (или иной сотрудник АлтГУ ответственный за проведение или организацию мероприятия) подаёт служебную записку на имя проректора по цифровому развитию не менее чем за три рабочих дня до проведения мероприятия.

2.5.3. В служебной записке указываются:

– наименование подразделения и ответственное лицо;

– цель проведения мероприятия;

– место проведения (аудитория, корпус);

–сроки проведения (с указанием времени начала и завершения);

– примерное количество пользователей, которым требуется доступ.

2.5.4. После согласования служебной записки отдел телекоммуникаций управления информатизации организует настройку доступа и соответствующего оборудования для организации работы Гостевого Wi-Fi.

2.6. Порядок предоставления доступа слушателям ДПО, обучающимся по дополнительным программам, а также иным лицам (командированным пользователям, экспертам, и другим физическим лицам, длительное время находящимся на территории АлтГУ).

2.6.1. В случае персонализированного доступа физическому лицу к корпоративной сети университета создается уникальная учетная запись временного срока действия.

2.6.2. Предоставление доступа осуществляется на основании служебной записки руководителя структурного подразделения – инициатора мероприятия или начальника управления ДПО, направляемой на имя проректора по цифровой трансформации.

2.6.3. В служебной записке указываются:

– фамилии, имена и отчества пользователей;

– наименование организации (при наличии);

– цель предоставления доступа (дистанционные занятия, участие в конференции, выполнение экспертных функций и др.);

– срок действия учётных записей (дата начала и окончания).

2.6.4. В отдельных случаях может быть запрошено управление информатизации может запросить письменное согласие на обработку персональных данных с внешним пользователем.

2.6.5. После проверки правомерности доступа, инициатор запроса на создание учетной записи может получить мотивированный отказ в доступе со стороны начальника Управления информатизации.

2.6.6. Доступ предоставляется только к образовательным и информационным ресурсам, необходимым для выполнения заявленных целей, а также к сети Интернет с обязательной фильтрацией трафика в соответствии с действующим законодательством.

2.6.7. По окончании заявленного периода учётные записи внешних пользователей автоматически блокируются и хранятся не менее трех лет.

2.6.8. Ответственность за достоверность представленных сведений и соблюдение сроков доступа несёт руководитель подразделения, направивший служебную записку.

2.7. Предоставление доступа при проведении тестирований на временных автоматизированных рабочих мест.

2.7.1. В случае необходимости организации рабочих мест (АРМ) для прохождения тестирования подаётся служебная записка на имя проректора по цифровому развитию.

2.7.2. В служебной записке дополнительно указываются:

– фамилии, имена и отчества пользователей;

– цель предоставления доступа (например, дистанционные занятия, выполнение тестовых заданий, доступ к образовательным ресурсам и др.);

– количество требуемых АРМ (ноутбуков);

– время и продолжительность проведения тестирования;

– место проведения и ответственный представитель подразделения.

2.7.3. После согласования управление информатизации обеспечивает подключение оборудования к выделенной VLAN, настройку авторизации и контроль доступа пользователей на период тестирования.

5. Требования к безопасности

5.1. Все пользователи обязаны соблюдать правила безопасности при использовании сети Интернет, воздерживаться от действий, способных нанести ущерб любым информационным ресурсам, и не передавать конфиденциальную информацию через незащищённые каналы связи.

5.2. Внешний пользователь самостоятельно обеспечивает актуальную антивирусную защиту и иные меры безопасности на личных устройствах (мобильных телефонах, планшетах, ноутбуках), подключаемых к гостевой сети.

5.3. Все факты подключения пользователей к гостевой беспроводной сети подлежат обязательной регистрации в электронных журналах. Журналы подключений хранятся в течение 3 лет в соответствии с настоящим Регламентом и требованиями законодательства.

5.4. Для предотвращения несанкционированного доступа в гостевой сети применяются комплексные технические меры защиты, включая обязательную аутентификацию пользователей, изоляцию гостевого сегмента, фильтрацию трафика.

5.5. Доступ к ресурсам, содержащим запрещённую, вредоносную и др. информацию, блокируется в соответствии с законодательством Российской Федерации и локальными актами Университета.

5.6. При выявлении нарушений требований безопасности, попыток обхода технических ограничений, распространения вредоносного ПО или иных противоправных действий, учётная запись внешнего пользователя может быть заблокирована без возможности дальнейшего использования гостевой сети.

6. Права и обязанности пользователей

6.1. Пользователи обязаны соблюдать регламенты доступа в Интернет, а также действующее законодательство в сфере информационной безопасности.

6.2. Пользователи обязаны использовать доступ только для заявленных целей.

6.3. Пользователям запрещается передавать свои учётные данные, коды авторизации или иные идентификаторы третьим лицам, а также допускать использование доступа иными лицами под своей учетной записью.

6.4. Пользователи должны информировать о подозрительных инцидентах или нарушениях управление информатизации.

7. Контроль и ответственность

7.1. Контроль за соблюдением настоящего Регламента возлагается на управление информатизации АлтГУ.

7.2. Нарушители несут ответственность в соответствии с законодательством РФ и локальными актами университета.

8. Заключительные положения

8.1. Регламент, а также изменения в него утверждаются приказом ректора.

8.2. Пересмотр и актуализация положения производится не реже одного раза в год.

8.3. Контроль выполнения настоящего регламента осуществляется управлением информатизации АлтГУ.

Приложение 4

Регламент фильтрации и обработки электронной почты в корпоративной почтовой системе

1. Общие положения

1.1. Настоящий регламент устанавливает требования и порядок фильтрации, обработки и передачи сообщений в корпоративной почтовой системе университета с целью обеспечения безопасности информационных ресурсов, персональных данных и иной конфиденциальной информации от несанкционированного доступа, утечки и вредоносных воздействий в корпоративной почтовой системе ФГБОУ ВО «Алтайский государственный университет» (далее – Университет).

1.2. Регламент обязателен для всех подразделений и сотрудников, использующих корпоративную электронную почту АлтГУ.

1.3. Настоящей Регламент разработан в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказами ФСТЭК России, локальными документами АлтГУ: политикой информационной безопасности, положение о корпоративной электронной почте, другими нормативными и методическими актами в области защиты информации и электронного взаимодействия.

1.4. Основные определения

Корпоративная электронная почта – это комплекс программных и технических средств, предоставляющий пользователям сервис электронной почты в домене университета (например, @asu.ru, @mail.asu.ru и т.д.), предназначенный для служебной переписки, обмена служебной и конфиденциальной информацией внутри университета, а также для официальных коммуникаций с внешними контрагентами.

Личная электронная почта – электронный почтовый ящик, созданный и используемый работником университета или студентом на сторонних почтовых сервисах (например, Gmail, Mail.ru, Yandex и др.), предназначенный для личного общения и не предназначенный для служебных целей и передачи служебной или конфиденциальной информации университета.

2. Порядок использования корпоративной электронной почты

2.1. Корпоративная почтовая система предназначена для служебной переписки работников и подразделений Университета. Использование личных почтовых сервисов (Gmail, Mail.ru, Yandex и др.) для служебных целей, а также для передачи конфиденциальной или официальной информации Университета запрещено.

2.2. Доступ к корпоративной электронной почте предоставляется всем работникам Университета после оформления трудовых отношений. Учетная запись является персональной; передача пароля третьим лицам не допускается.

2.3. Создание корпоративного почтового ящика для структурного подразделения осуществляется на основании служебной записки, направляемой на имя проректора по цифровому развитию, в установленном порядке.

2.4. Корпоративная электронная почта используется для регистрации на внешних информационных системах и сервисах, применяемых в служебной деятельности. Использование личных электронных почтовых ящиков для этих целей не допускается.

3. Фильтрация и обработка электронной почты

3.1. Входящие и исходящие сообщения фильтруются централизованно через корпоративный почтовый шлюз с антивирусной проверкой, спам-фильтрацией, DMARC/SPF/DKIM-валидацией отправителя и блокировкой подозрительных вложений.

3.2. Технологии Zero Trust: каждый элемент электронной переписки-письмо, вложение, ссылка – должен рассматриваться как потенциально подозрительный до подтверждения его легитимности.

3.3. Администрирование почтовой системы осуществляет управление информатизации, за соблюдение требований по информационной безопасности и обработке ПДн отвечает отдел защиты информации, за соблюдение правил работы с ПДн и конфиденциальной информации каждый работник в пределах своей ответственности.

4. Защита информации при передаче электронной почты

4.1. Передача сообщений, содержащих персональные данные или иную конфиденциальную информацию, допускается только с использованием средств криптографической защиты информации (СКЗИ), сертифицированных в установленном порядке, либо в виде зашифрованных архивов, защищённых стойким алгоритмом шифрования.

4.2. При передаче вложений, содержащих персональные данные, служебную или внутреннюю документацию Университета, необходимо:

– использовать шифрование вложений с применением сертифицированных СКЗИ (например, «КриптоПро CSP», «ViPNet», «Signal-COM» и др.);

– в случае отсутствия технической возможности использования СКЗИ – упаковывать вложения в архив с шифрованием имён файлов и паролем (7-Zip, WinRAR или аналогичные средства, поддерживающие алгоритмы AES-256 или ГОСТ);

– пароль от архива передавать по иному каналу связи, отличному от канала отправки письма (по телефону, в мессенджере с сквозным шифрованием, либо при личной передаче);

– любые вложения с ПДн или служебной документацией должны шифроваться и сопровождаться маркером «Содержит ПДн» или «Конфиденциально».

4.3. Пересылка писем с персональными данными на внешние адреса без шифрования запрещается. Исключения допускаются только в случаях, прямо установленных внутренними нормативными актами Университета и на основании поручения руководителя.

4.4. При необходимости передачи конфиденциальной информации за пределы корпоративного домена (asu.ru) допускается использование только утверждённых защищённых каналов связи, включая:

– корпоративные VPN-соединения (VipNet, Континент);

– защищённые системы электронного документооборота;

– шифрованные контейнеры (например, VeraCrypt, 7zip) при передаче крупных объёмов данных (допускается также использовать корпоративное облачное хранилище cloud.asu.ru).

4.5. Пользователи корпоративной почты обязаны:

– использовать корпоративную почту исключительно для выполнения служебных обязанностей и деловой переписки, связанной с деятельностью университета;

– соблюдать требования настоящего Регламента, а также «Положения о корпоративной электронной почте Алтайского государственного университета»;

– не использовать корпоративную почту для регистрации на сторонних интернет-ресурсах, не связанных с деятельностью университета;

– не передавать свои учетные данные (логин и пароль) третьим лицам.

4.6. При работе с входящей и исходящей корреспонденцией пользователи обязаны:

– проверять полученные вложения с помощью установленного антивирусного программного обеспечения перед их открытием или сохранением;

– не переходить по гиперссылкам, содержащимся в письмах от неизвестных отправителей либо в письмах, вызывающих подозрение (в том числе при наличии ошибок в тексте, несоответствии домена отправителя, неожиданного содержания);

– незамедлительно уведомлять управление информатизации или отдел защиты информации о получении подозрительных сообщений, особенно содержащих вложения, ссылки или запросы на предоставление персональных данных, учетных данных или иной конфиденциальной информации;

– в случае выявления признаков заражения компьютера или блокировки доступа к почтовому ящику прекратить работу с почтой и сообщить специалистам технической поддержки управления информатизации.

4.7. Фишинг и социальная инженерия.

Под фишингом понимаются рассылки и сообщения, направленные на получение информации (персональных данных, реквизитов банковских карт, логинов и паролей и пр.) путем введения пользователя в заблуждение.

При работе с почтой запрещается:

– переходить по ссылкам из писем, предлагающих обновить пароль, подтвердить учетную запись, оплатить услуги или получить «премию»;

– открывать вложения с расширениями .exe, .bat, .cmd, .scr, .js, а также архивы (zip, rar, 7z), полученные от неизвестных источников;

– отвечать на подобные письма, пересылать их другим пользователям или выполнять содержащиеся в них инструкции.

4.8. Все письма, имеющие подозрения на спам, автоматически помечаются программными средствами фильтрации. Подозрительные письма имеют пометку [SPAM] [MASSMAIL]. Пользователь обязан проверять её содержимое с особой осторожностью.

5. Контроль и аудит

5.1. Управление информатизации осуществляет ведение журналов событий корпоративной почтовой системы, включая сведения об отправке, приёме и попытках доставки сообщений с недоверенных адресов. Журналы хранятся не менее трёх лет.

5.2. Отдел защиты информации регулярно анализирует журналы событий, выявляет инциденты информационной безопасности и оценивает потенциальные угрозы.

6. Ответственность пользователей

6.1. Пользователи корпоративной почтовой системы обязаны:

– использовать корпоративную электронную почту исключительно для служебных целей;

– соблюдать требования настоящего регламента и локальных нормативных актов Университета в области информационной безопасности;

– обеспечивать сохранность своих учётных данных и не допускать их передачи третьим лицам;

– незамедлительно информировать отдел защиты информации о подозрительных письмах, попытках фишинга, появлении вредоносных вложений и иных аномалиях в работе почты;

– проверять вложения антивирусным программным обеспечением, воздерживаться от открытия подозрительных ссылок и своевременно уведомлять о любых признаках возможного заражения.

6.2. Пользователям запрещается:

– использовать личные почтовые сервисы (gmail.com, mail.ru, yandex.ru и др.) для служебной переписки и передачи рабочих документов;

– направлять служебную информацию на внешние адреса без производственной необходимости и без согласования с руководителем;

– хранить служебную переписку на личных устройствах, сторонних облачных сервисах или иных неконтролируемых ресурсах;

– использовать корпоративный почтовый ящик для регистрации на сторонних интернет-ресурсах, не связанных с выполнением трудовых обязанностей;

– передавать письма, содержащие персональные данные или иную конфиденциальную информацию, без соблюдения установленных требований по их защите и без проверки корректности адресатов;

– открывать вложения, запускать исполняемые файлы или переходить по ссылкам из писем, полученных с неизвестных либо сомнительных источников;

– отключать или обходить средства защиты, встроенные в корпоративную почтовую систему, а также предпринимать попытки обхода механизмов фильтрации;

– использовать корпоративную электронную почту для личных конфликтов, распространения непроверенной информации, споров, политических высказываний или иной деятельности, способной нанести ущерб деловой репутации Университета.

6.3. Работники, нарушившие порядок фильтрации и обработки почтовых сообщений, несут дисциплинарную ответственность в соответствии с трудовым законодательством и локальными нормативными актами Университета.

6.4. Системные администраторы несут ответственность за корректность настройки фильтрации, защиты и обработки почтового трафика в пределах своих должностных обязанностей.

7. Заключительные положения

7.1. Регламент утверждается приказом ректора.

7.2. Регламент подлежит пересмотру не реже одного раза в три года либо при изменении нормативных требований.

7.3. Контроль за исполнением Регламента возлагается на проректора по цифровому развитию и начальника управления информатизации.

1. Список информационных ресурсов

	Назначение	DNS внешний
1	АИС Система заявок на мероприятия	ais-events.asu.ru
2	Большой Алтай - III международный алтаистический форум 2023	altai2023.asu.ru
3	V Международный образовательный форум «Алтай - Азия 2022»	altaiasia2022.asu.ru
4	VI Международный образовательный форум «Алтай - Азия 2024»	altaiasia2024.asu.ru
5	Абитуриент АГУ	abiturient.asu.ru
6	Флора Алтая	altaiflora.asu.ru
7	Архивные фонды Первой всеобщей переписи населения Российской империи 1897 года	arch1897.histcensus.asu.ru
8	Алтайская школа политических исследований	ashpi.asu.ru
9	Археологический портал	archaeology.asu.ru
10	Ассоциация азиатских университетов	aauniv.org
11	БиоАзияАлтай2021	bioasia.asu.ru
12	БИО-360: социально-ориентированная цифровая платформа с роликами формата 360 градусов.	bio360.asu.ru
13	Биоразнообразие алтае-саянского экорегиона	bioaltai-sayan.ru
14	Информационная система Кейс	case.asu.ru
15	Ботанический журнал Turczaninowia	turczaninowia.asu.ru
16	Веб-конструктор мероприятий с осуществлением поддержки мероприятий в Телеграм	meetup.asu.ru
17	Веб-приложение для управления контентом дополненной реальности	ar-cms.asu.ru
18	Вестник психологии и педагогики Алтайского государственного университета	bppasu.ru
19	Единое окно образовательных ресурсов	edu.asu.ru
20	Школа кибербезопасности	cbs.asu.ru
21	База данных размеров геномов хозяйственно-ценных, редких и эндемичных растений	genome.asu.ru
22	Международная научно-практическая конференция «Высокопроизводительные вычислительные системы и технологии в научных исследованиях, автоматизации управления и производства (ВВСТ)»	conf-hpcst.asu.ru
23	Журнал "Юрислингвистика"	legallinguistics.ru
24	Журнал «Известия Алтайского государственного университета»	izvestiya.asu.ru
25	Здоровье человека, теория и методика физической культуры и спорта	hpcas.ru
26	Изучаем русский язык - узнаём Россию	rusolymp.asu.ru
27	Институт истории и международных отношений	hist.asu.ru
28	ИС "Социально-демографические процессы на Алтае в материалах церковного учета XVIII - начала XX вв"	histdem.asu.ru
29	Кафедра археологии, этнографии и музеологии	kaei.asu.ru
30	Цифровая кафедра	digitalup.asu.ru
31	Кафедра отечественной истории	koi.hist.asu.ru
32	Кафедра всеобщей истории	kvimo.hist.asu.ru

33	Кафедра иностранных языков ИИМО	lingva.asu.ru
34	Литература Алтая	lit-alt.asu.ru
35	Карта корпусов АГУ	map.asu.ru
36	Институт математики и информационных технологий	math.asu.ru
37	40 лет Математическому факультету	math40.asu.ru
38	Энциклопедия противодействия киберпреступности	epk.asu.ru
39	Медиа.Hub	mediahub.asu.ru
40	Колледж АлтГУ	college.asu.ru
41	Лаборатория фундаментальной и прикладной зоологии	appzoo.asu.ru
42	Портал по сравнительной морфологии спор папоротников	mgplants.asu.ru
43	Личный кабинет АГУ	lk.asu.ru
44	Международный институт экономики, менеджмента и информационных систем	miemis.asu.ru
45	Календарь научно-технических мероприятий	events.asu.ru
46	IV Международный форум по интеграционным процессам в этнокультурной сфере	forum-integration.asu.ru
47	Жизнь и борьба: основные страницы биографии и боевого пути М.В. Фрунзе	frunze.hist.asu.ru
48	Научные журналы АлтГУ	journal.asu.ru
49	Основной сайт Колледж АГУ	new.college.asu.ru
50	Генеалогическое древо	gen-tree.asu.ru
51	ИС Историческое профессиоведение	occupations.asu.ru
52	Кафедра востоковедения	orient.asu.ru
53	ПрофПоддержка: платформа поддержки научной деятельности ППС	helper.asu.ru
54	Проекты по Первой всеобщей переписи населения Российской империи 1897 года	histcensus.asu.ru
55	Тестирование по информатике	it-math.asu.ru
56	Историческая информатика	kleio.asu.ru
57	Российско-азиатский юридический журнал	ralj.ru
58	Чек-лист и определитель лишайников	lichens.asu.ru
59	Русский язык как иностранный	rki.asu.ru
60	АГУ, главная страница	asu.ru
61	Дополнительное профессиональное образование	dpo.asu.ru
62	Институт биологии и биотехнологии	bio.asu.ru
63	Институт гуманитарных наук	ign.asu.ru
64	Сайт Издательство АГУ	publish.asu.ru
65	База данных "Фитолитные спектры фитоценозов юга Западной Сибири"	phytolith.asu.ru
66	Институт географии	geo.asu.ru
67	Институт химии и химико-фармацевтических технологий	chem.asu.ru
68	Практикуемся в языках	lingvo.asu.ru
69	Региональный центр переподготовки и повышения квалификации преподавателей	cppkp.asu.ru
70	Школьник АГУ	school.asu.ru
71	Научные журналы АГУ	new.journal.asu.ru
72	Историческая статистика Алтая	statalt.hist.asu.ru
73	Чуйский тракт - туристский меридиан Сибири	turtrakt.asu.ru

74	Удостоверяющий центр Алтайского государственного университета	uc.asu.ru
75	Универсум - Академия креативного образования	universum.asu.ru
76	Население городов Сибири на рубеже XIX-XX вв.	person1897.histcensus.asu.ru
77	Институт цифровых технологий, электроники и физики	phys.asu.ru
78	Газета Алтайского государственного университета «За науку!»	zn.asu.ru
79	Фонд целевого капитала	fund.asu.ru
80	Региональный Антитеррористический Центр на базе юридического института	ranmc.law.asu.ru
81	Центр R&D - Приоритет 2030	rnd.asu.ru
82	Южно-сибирский ботанический сад	ssbg.asu.ru
83	Профессии и занятия населения Российский Империи конца XIX – начала XX века	stat1897.histcensus.asu.ru
84	Рубцовский институт (филиал) АлтГУ	rb.asu.ru
85	АКТРУ	aktru.asu.ru
86	Облачное хранилище Cloud ASU	cloud.asu.ru
87	Приоритет – 2030	dockermf.asu.ru
88	Видео портал	video.asu.ru
89	Научный депозитарий «Virtual Herbarium ALTB	altb.asu.ru
90	GeoMixer	geomixer.asu.ru
91	Система опросов Алтайского государственного университета	survey.asu.ru
92	Юридический институт (тестовый сервер)	test.law.asu.ru
93	Шахты	mmis.asu.ru
94	Научная библиотека АГУ	www.lib.asu.ru
95	Электронная библиотечная система АГУ	elibrary.asu.ru
96	Журнал Известия АГУ	izvestia.asu.ru
97	Битрикс24	corp.asu.ru
98	Личный кабинет абитуриента	lk.abiturient.asu.ru
99	Личный кабинет ДПО	lk.dpo.asu.ru
100	Большой Алтай	bolshoy-altay.asu.ru
101	Служба поддержки пользователей	support.asu.ru
102	Сервер обновлений GNU/Linux в АлтГУ	linuxupdate.asu.ru
103	Учитель будущего	uchitel.asu.ru
104	Хостинг сервер	hosting1.asu.ru
105	Оплата услуг АГУ	pay22.asu.ru
106	Хостинг сервер	hosting2.asu.ru
107	Хостинг сервер	hosting3.asu.ru
108	Юридический институт	new.law.asu.ru
109	Apache Кафедры теорфизики	theory.asu.ru
110	Цифровой университет АлтГУ	portal.edu.asu.ru
111	Платформа ДПО Алтайского государственного университета	dpo.edu.asu.ru
112	Почта АГУ	mail.asu.ru
113	Открытый университет АлтГУ	public.edu.asu.ru

2. Архивные домены с переадресацией.

DNS внешний	Редирект на
arts.asu.ru	сайт ИГН
fmc.asu.ru	сайт ИГН
ipo.asu.ru	сайт ИГН
psy.asu.ru	сайт ИГН
socio.asu.ru	сайт ИГН
econ.asu.ru	сайт МИЭМИС
chemwood.asu.ru	Научные журналы АГУ
bioaltai-sayan.asu.ru	Биоразнообразие алтае-саянского экорегиона
hcod.asu.ru	Профессии и занятия населения Российский Империи конца XIX – начала XX века