SATBAYEV UNIVERSITY	**НЕКОММЕРЧЕСКОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО «КАЗАХСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ имени К.И. САТПАЕВА»**	
Документ СМК 3 уровня	Редакция №4 от «13» октября 2025 г.	Пол. 029-04-03.5.01 – 2025

ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ И ЗАЩИТЫ ДАННЫХ

Пол. 029-04-03.5.01 – 2025

Алматы 2025

ПРЕДИСЛОВИЕ

1 РАЗРАБОТАНО

Директор Института Цифровых Технологий и Профессионального Развития _____ Симонов А.Г.

«____» _____ 2025 г.

2 СОГЛАСОВАНО

Член Правления - Проректор по Академическим вопросам _____ Р.Ускенбаева
«____» _____ 2025 г.

И.о начальника управления юридического обеспечения и государственных закупок _____ Т.Абукенов
«___» _____ 2025 г.

Начальник отдела оценки и качества _____ А.Сауранбаева
«____» _____ 2025 г.

Начальник отдела документационного обеспечения и развития государственного языка _____ Ж. Оракбаева
«____» _____ 2025 г.

3 УТВЕРЖДЕНО решением Правления от « » _____2025г. № ____

4 ВВЕДЕНО взамен редакции № 3 от 1.09.2023

СОДЕРЖАНИЕ

1 Общие положения

Настоящая Политика информационной безопасности НАО "Казахский национальный исследовательский технический университет имени К.И. Сатпаева" (далее - Политика) разработана в соответствии с действующим законодательством Республики Казахстан, нормативными актами и другими внутренними положениями НАО "КазНИТУ имени К.И. Сатпаева" (далее - Университет).

В настоящей Политике применяется следующее определение конфиденциальной информации: «конфиденциальная информация» означает любую и всю информацию о персональных данных пользователей, данных в базах данных программных продуктов, а также любую информацию относительно деятельности Университета и её клиентов (клиентская база), знания, ноу-хау, коммерческая информация, ценообразование, которая каким-либо образом стала известна сотруднику в результате производственной деятельности.

Настоящая политика информационной безопасности Университета предусматривает принятие необходимых мер в целях защиты информационных активов как материальных ценностей Университета от случайного или преднамеренного изменения, раскрытия или уничтожения, а также в целях соблюдения конфиденциальности, целостности и доступности информации, обеспечения процессов информационного взаимодействия с заказчиками и партнерами.

Ответственность за соблюдение информационной безопасности несет каждый сотрудник Университета. Сотрудник должен иметь своевременное и полное обеспечение информацией, необходимой ему для выполнения своих служебных обязанностей.

В целях настоящей Политики используются следующие термины и определения:

- Информационная безопасность — состояние защищенности информации, при котором обеспечены ее конфиденциальность, целостность и доступность.
- Конфиденциальность — свойство информации, заключающееся в ограничении доступа к ней определенных лиц.
- Целостность — свойство информации, заключающееся в ее достоверности и неизменности в процессе ее обработки.
- Доступность — свойство информации, заключающееся в возможности ее использования по назначению в требуемое время и в требуемом месте.
- Угроза информационной безопасности — совокупность условий и факторов, создающих потенциальную или реальную опасность нарушения информационной безопасности.
- Уязвимость информационной безопасности — недостаток или отсутствие необходимого уровня защищенности, который может быть использован для нарушения информационной безопасности.

- Риск информационной безопасности — сочетание вероятности реализации угрозы информационной безопасности и величины возможного ущерба.
- Процессы управления рисками — это набор последовательных действий, направленных на идентификацию, оценку и снижение рисков информационной безопасности.
- Обновления — это изменения, внесенные в программное обеспечение или оборудование для исправления ошибок, устранения уязвимостей или добавления новых функций.
- Конфиденциальная информация – это сведения, не подлежащие свободному распространению, доступ к которым предоставляется только определённым категориям пользователей на основании их должностных обязанностей.
- Принцип «необходимость знать» – это организационный принцип разграничения прав доступа к информационным ресурсам, согласно которому каждый пользователь Университета получает доступ только к тем сведениям и системам, которые необходимы ему исключительно для выполнения должностных обязанностей. Предоставление избыточных прав доступа, выходящих за рамки служебной необходимости, не допускается.
- Персональные данные - любая информация, относящаяся к определенному или определяемому на ее основании субъекту персональных данных, зафиксированная на электронном, бумажном или ином материальном носителе.
- Инструкции и регламенты, журналы - документы, устанавливающие правила и процедуры для организации в целом или для отдельных ее подразделений. Они описывают организационные и технические аспекты информационной безопасности, включая роли и обязанности сотрудников, процессы обработки информации, реагирование на инциденты и т.д.

В настоящей Политике под термином «сотрудник» понимаются все сотрудники Университета, в том числе, работающих в Университете по договорам гражданско-правового характера. Применение настоящей политики должно быть обусловлено в таком договоре.

Информационная безопасность является одним из важнейших аспектов деятельности Университета. Организация стремится обеспечить конфиденциальность, целостность и доступность информации, а также защиту от несанкционированного доступа, использования, раскрытия, изменения, уничтожения или потери данных.

Настоящая Политика должна быть доведена до сведения каждого сотрудника Университета в день заключения трудового договора.

2 Цель Политики

Целями настоящей Политики являются:

- сохранение конфиденциальной информации Университета;
- обеспечивает обучение и осведомленность сотрудников об информационной безопасности.
- Проводит регулярные проверки и аудиты системы информационной безопасности.
- Сохранение конфиденциальности информационных ресурсов Университета;
- сохранение конфиденциальности информации, переданной в любой форме в процессе взаимодействия с заказчиками и партнерами Университета;
- обеспечение доступа к информационным ресурсам Университета для поддержки бизнес деятельности;
- повышение осведомленности пользователей в области рисков, связанных с информационными ресурсами Университета;
- определение степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности в Университете.
- обеспечение информационной безопасности систем и защиты данных в соответствии с международными стандартами ISO/IEC 27001, ISO/IEC 27002

Руководители подразделений Университета должны обеспечить регулярный контроль за соблюдением положений настоящей Политики. Кроме того, должна быть организована периодическая проверка соблюдения информационной безопасности с последующим представлением отчета по результатам указанной проверки руководству Университета.

3 Область применения настоящей Политики

Требования настоящей Политики распространяются на всю информацию, информационные системы и ресурсы обработки информации, находящиеся в распоряжении Университета.

Соблюдение положений настоящей Политики является обязательным для всех работников Университета, включая штатных, временных и привлекаемых на договорной основе специалистов, независимо от занимаемой должности и характера выполняемых функций.

В договорах с третьими лицами, которым предоставляется доступ к информации или информационным ресурсам Университета, должна быть обязательно зафиксирована обязанность по соблюдению требований настоящей Политики, а также иных локальных нормативных актов в области информационной безопасности. Кроме того, с такими лицами подлежит обязательному заключению соглашение о неразглашении конфиденциальной информации (NDA).

Университету принадлежат на праве собственности, включая право интеллектуальной собственности, следующие объекты:

- все программные продукты, аналитические материалы, дизайнерские решения, схемы и иные результаты интеллектуальной деятельности, созданные работниками Университета в рамках исполнения ими трудовых (служебных) обязанностей;
- вся деловая информация, в том числе конфиденциальная, формируемая или используемая в ходе осуществления деятельности Университета;
- лицензионное программное обеспечение, вычислительные ресурсы и иные материальные и нематериальные активы, приобретённые (полученные) и введённые в эксплуатацию в целях реализации уставных задач Университета в соответствии с законодательством Республики Казахстан.

Указанное право собственности также распространяется на:

- голосовую и факсимильную связь, осуществляемую с использованием оборудования Университета;
- содержимое корпоративных почтовых ящиков;
- бумажные и электронные документы, созданные, полученные или обрабатываемые структурными подразделениями и сотрудниками Университета в процессе выполнения ими служебных обязанностей.

4 Требования и рекомендации

4.1 Общие требования к обеспечению доступа к информации

Запрещается предоставление доступа третьим лицам к конфиденциальной информации Университета за исключением случаев взаимодействия Университета с дистрибьюторами и партнерами, определённых соответствующими юридическими документами (дистрибьюторским договором или иным партнерским соглашением, Договор о неразглашении), включающими в себя обязательные условия защиты данных и ответственность за распространение конфиденциальной информации.

4.2 Контроль доступа к информационным системам

Все работы в пределах офисов Университета выполняются в соответствии с должностными обязанностями сотрудников только на компьютерах и иных технических средствах, официально разрешённых к использованию в Университете.

Внос в здания и помещения Университета личных портативных компьютеров, мобильных устройств и внешних носителей информации (диски, флэш-карты и т.п.), а также их вынос за пределы Университета

допускается только по письменному согласованию с непосредственным руководителем и с разрешения ответственного подразделения по информационной безопасности.

Руководители структурных подразделений обязаны периодически пересматривать и актуализировать права доступа своих сотрудников и иных пользователей к информационным ресурсам в соответствии с принципом «необходимость знать». Доступ сотрудников, уволенных или переведённых на иные должности, должен быть незамедлительно аннулирован.

Для обеспечения санкционированного доступа к информационным системам Университета каждый пользователь обязан использовать уникальные именные учётные данные (имя пользователя и пароль). Использование общих (групповых) учётных записей запрещается.

Пароли пользователей должны отвечать требованиям сложности (не менее 8 символов, использование букв верхнего и нижнего регистра, цифр и специальных символов), храниться в тайне и подлежать регулярной смене не реже одного раза в 90 дней. Передача паролей третьим лицам строго запрещается.

При работе за компьютером сотрудники обязаны обеспечивать защиту рабочего места: активировать блокировку экрана либо выходить из системы при каждом покидании рабочего места, даже на непродолжительное время.

Дистанционный доступ к информационным системам Университета допускается только с использованием защищённых каналов связи (VPN, шифрование) и, при необходимости, двухфакторной аутентификации.

Нарушение требований настоящего раздела рассматривается как нарушение политики информационной безопасности и влечёт дисциплинарную ответственность в соответствии с законодательством Республики Казахстан и локальными актами Университета.

4.3 Учётные записи и их безопасность

Пользователи должны руководствоваться рекомендациями по защите своего пароля на этапе его выбора и последующего использования. Категорически запрещается сообщать и передавать свой пароль другим лицам или предоставлять свою учетную запись другим, в том числе членам своей семьи и близким, если работа выполняется дома.

Сотрудники должны создавать для учётных записей сложные пароли, отвечающие рекомендуемым требованиям к сложности паролей – выбирать достаточную длину, разный тип символов, не использовать простые последовательности символов и простые слова, не использовать свои имена, фамилии, номера телефонов.

Сотрудники не должны использовать для рабочих учётных записей пароли, которые они используют для любых других учётных записей, личных или учётных записей других организаций.

Сотрудники должны регулярно выполнять смену паролей.

Для повышения безопасности, Университет может применять методики мониторинга срока действия паролей и установки сроков их действия, для обеспечения исполнения регулярности смены паролей Пользователями.

Университет предоставляет учётные записи сотрудникам и студентам. Университет оставляет за собой право блокировать учётные записи на основании юридических соглашений (договоров) о взаимоотношениях с лицами. Кроме того, Университет может использовать автоматизированные системы поведенческого анализа для блокировки учётных записей. В случае блокировки, при проведении проверки событий, ставших причиной блокировки, сотрудники Университета могут запросить у владельцев учётных записей пояснительные документы.

4.4 Доступ третьих лиц к системам Университета

Под «третьими лицами» понимаются лица, не являющиеся сотрудниками и студентами Университета, включая подрядчиков, временных работников, партнёров, аудиторов, представителей государственных органов и иных организаций.

Доступ третьих лиц к информационным системам и ресурсам Университета допускается только при наличии производственной необходимости, на основании письменного согласования с руководством Университета и при условии строгого соблюдения утверждённых регламентов и процедур.

Предоставляемый доступ должен быть ограничен по объёму и сроку действия, в соответствии с принципом «необходимость знать», и предоставляться исключительно для выполнения конкретных задач.

Все факты предоставления доступа третьим лицам подлежат обязательной регистрации в журнале учёта или информационной системе контроля доступа с указанием основания, ответственного лица и срока действия прав доступа.

Третьи лица обязаны соблюдать требования политики информационной безопасности Университета, а также, при необходимости, подписывать соглашение о конфиденциальности (NDA).

Доступ третьих лиц к информационным системам Университета осуществляется под контролем ответственного сотрудника Университета.

По завершении работ, окончании срока действия договора или отпадении необходимости предоставленный доступ должен быть немедленно аннулирован.

Нарушение данных требований рассматривается как инцидент информационной безопасности и влечёт меры ответственности в соответствии с действующим законодательством и внутренними актами Университета.

4.5 Удаленный доступ

Сотрудники получают право удаленного доступа к информационным ресурсам Университета с учетом их должностных обязанностей. Для предоставления доступа необходимо обосновать потребность и направить запрос на предоставление доступа.

Сотрудникам, которым требуется удаленный доступ к рабочим компьютерам Университета, может быть предоставлена такая возможность для выполнения служебных задач и использования сетевых ресурсов в соответствии с их правами доступа в корпоративной информационной системе.

Сотрудникам, работающим за пределами Университета с использованием компьютера, не принадлежащего Университета, запрещено копирование данных на компьютер, с которого осуществляется удаленный доступ.

Сотрудники и третьи лица, имеющие право удаленного доступа к информационным ресурсам Университета, должны соблюдать требование, исключающее одновременное подключение их компьютера к сети Университета и к каким-либо другим сетям, не принадлежащим Университету.

Все компьютеры, подключаемые посредством удаленного доступа к информационной сети Университета с внешних сетей, должны иметь программное обеспечение антивирусной защиты, имеющее последние обновления.

Для доступа к сетям и ресурсам Университета могут применяться технические средства ограничения доступа для компьютеров, не соответствующих требованиям по наличию обновлений Операционных систем или Программного обеспечения, версий вирусных записей Антивирусного Программного обеспечения или отсутствии защиты.

Запрещается самостоятельная установка, запуск и использование сотрудниками любых программных средств для организации удалённого доступа (например, TeamViewer, AnyDesk и подобные). Программные решения для удалённого подключения допускается использовать только во внутренней сети Университета и исключительно сотрудниками, отвечающими за информационные системы и техническую поддержку. При необходимости получения удалённой помощи сотрудники должны использовать средства демонстрации экрана или контролируемого удалённого подключения, предоставляемые корпоративными коммуникационными инструментами, разрешёнными к использованию в Университете.

4.6 Доступ к сети Интернет

Доступ к сети Интернет обеспечивается только в производственных целях и не может использоваться для незаконной деятельности.

Сотрудникам Университета разрешается использовать сеть Интернет только в служебных целях.

Запрещается посещение любого сайта в сети Интернет, который считается оскорбительным для общественного мнения или содержит информацию сексуального характера, пропаганду расовой ненависти, комментарии по поводу различия/превосходства полов, дискредитирующие заявления или иные материалы с оскорбительными высказываниями по поводу чьего-либо возраста, сексуальной ориентации, религиозных или политических убеждений, национального происхождения или недееспособности. Запрещается доступ к ресурсам экстремистского и террористического характера, порнографического характера, а так же с содержимым, запрещенным Законодательством РК.

Запрещается использование облачных ресурсов для хранения служебной и корпоративной информации с применением личных учётных записей, или учётных записей других организаций. Хранение и отправка/синхронизация данной информации разрешены только в облачных сервисах, являющихся корпоративными и разрешенными для использования в рабочих целях, только с применением корпоративных аккаунтов, предоставленных Университетом. Университет может осуществлять блокирование облачных сервисов, не входящих в перечень корпоративных, с целью предотвращения несанкционированного распространения или утечки служебной информации.

Сотрудникам, имеющим личные учетные записи, предоставленные публичными провайдерами, не разрешается пользоваться ими на оборудовании, принадлежащем Университету.

Перед открытием или передачей другим сотрудникам файлов, полученных из сети Интернет, сотрудник обязан предварительно проверить такие файлы с использованием антивирусного программного обеспечения.

Ответственность за несанкционированное использование сети Интернет, в том числе за доступ к запрещённым ресурсам, ложится на пользователя, за которым закреплена соответствующая учётная запись или рабочее устройство.

Университет имеет право контролировать содержание всего потока информации, проходящей через канал связи к сети Интернет в обоих направлениях. Также применять ограничения в доступе к различным ресурсам, определенным приложениям и протоколам как в ручном режиме, так и с применением автоматических алгоритмов оборудования и/или программного обеспечения и комплексов по обеспечению сетевой и информационной безопасности, на основании регламентирующих или законодательных актов, или на основе принятия решений целесообразности утилизации инфраструктуры и безопасности.

Защита оборудования

Сотрудники должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранится информация Университета.

Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производят только системные администраторы и специалисты службы технической поддержки.

4.7Аппаратное обеспечение

Все компьютерное оборудование (серверы, стационарные и портативные компьютеры), оборудование для хранения данных (карты памяти, портативные жесткие диски, компакт-диски), периферийное оборудование (например, мониторы, принтеры и сканеры), аксессуары (манипуляторы, устройства ввода, дисководы для компакт-дисков), коммуникационное оборудование (например, сетевые адаптеры и концентраторы), для целей настоящей Политики вместе именуются «компьютерное оборудование». Компьютерное оборудование, предоставленное Компанией, является ее собственностью и предназначено для использования исключительно в производственных целях.

Портативные компьютеры, содержащие конфиденциальную информацию или коммерческую тайну Университета, в период их неиспользования должны храниться в запираемом помещении, шкафу или ящике, либо быть защищены другим средством, обеспечивающим равнозначную физическую защиту.

Каждый сотрудник, получивший в пользование портативный компьютер, обязан принять надлежащие меры по обеспечению его сохранности, как в офисе, так и по месту проживания. В ситуациях, когда возрастает степень риска кражи портативных компьютеров, например, в гостиницах, аэропортах, в офисах деловых партнеров и т.д., пользователи обязаны ни при каких обстоятельств не оставлять их без присмотра.

Все компьютеры должны защищаться паролем при загрузке системы, активации по горячей клавиши и после выхода из режима «Экранной заставки». Данные не должны быть скомпрометированы в случае халатности или небрежности, приведшей к потере оборудования. Перед утилизацией все компоненты оборудования, в состав которых входят носители данных (включая жесткие диски), необходимо проверять, чтобы убедиться в отсутствии на них конфиденциальных данных и лицензионных продуктов. Должна выполняться процедура форматирования носителей информации, исключающая возможность восстановления данных.

Перед записью информации на носитель для последующей передачи заказчикам или партнёрам необходимо убедиться, что данный носитель не содержит иных данных. Следует учитывать, что простое форматирование не обеспечивает гарантированного удаления ранее записанной информации; при

необходимости должны применяться средства безопасного удаления данных или использоваться новые (чистые) носители.

Для обеспечения корректного и бесперебойного функционирования финансовых и учетных информационных систем, в частности системы 1С, должен использоваться отдельный выделенный сервер. Доступ к серверу предоставляется исключительно уполномоченным сотрудникам на основании утверждённого перечня.

Смартфоны не относятся к числу устройств, имеющих надежные механизмы защиты данных. В подобном устройстве не рекомендуется хранить конфиденциальную информацию.

4.8 Примеры мер по обеспечению информационной безопасности

Организация может принять следующие меры для обеспечения информационной безопасности своих систем и данных:

- Технические меры — такие, как использование средств защиты от несанкционированного доступа, шифрование данных и резервное копирование.
- Организационные меры — такие, как обучение сотрудников информационной безопасности, создание политики информационной безопасности и проведение регулярных проверок системы информационной безопасности.
- Административные меры — такие, как управление доступом к системе и данным, а также контроль за использованием информационных систем.

4.9 Обзор угроз и уязвимостей

Информационная система может подвергаться различным угрозам и уязвимостям. К наиболее распространенным угрозам относятся:

- Несанкционированный доступ — получение доступа к информации или системе лицами, не имеющими на это права
- Использование — несанкционированное использование информации или системы
- Раскрытие — несанкционированное распространение информации или системы
- Изменение — несанкционированное изменение информации или системы
- Уничтожение — несанкционированное уничтожение информации или системы

К наиболее распространенным уязвимостям относятся:

- Ошибки в программном обеспечении — ошибки в программном обеспечении могут быть использованы злоумышленниками для получения доступа к системе или информации.

- Небезопасные конфигурации — небезопасные конфигурации системы могут сделать ее уязвимой для атак.

- Недостатки в инфраструктуре — недостатки в инфраструктуре системы, такие как слабые пароли или отсутствие резервного копирования, могут сделать ее уязвимой для атак.

4.10 Обновления

Обновления программного обеспечения и оборудования являются важным фактором обеспечения информационной безопасности. Обновления могут содержать исправления ошибок, которые могут быть использованы злоумышленниками для получения доступа к системе или информации. Обновления также могут содержать новые функции, которые могут повысить безопасность системы.

Типы обновлений:

- Исправления ошибок — это обновления, которые устраняют ошибки в программном обеспечении или оборудовании.

- Устранение уязвимостей — это обновления, которые устраняют уязвимости в программном обеспечении или оборудовании.

- Добавление новых функций — это обновления, которые добавляют новые функции в программное обеспечение или оборудование.

Важность обновлений:

- Обновления могут повысить безопасность системы, исправляя ошибки и устраняя уязвимости.

- Обновления могут добавить новые функции, которые могут повысить безопасность системы.

- Не установка обновлений может сделать систему уязвимой для атак злоумышленников.

- Рекомендации по управлению обновлениями:

- Организация должна иметь политику управления обновлениями, которая определяет порядок и сроки установки обновлений.

- Организация должна обеспечить, чтобы сотрудники знали о важности установки обновлений.

Примеры обновлений:

- Обновления программного обеспечения — это исправления ошибок, обновления безопасности и новые функции для программного обеспечения, такого как операционные системы, приложения и веб-браузер.

- Обновления оборудования — это исправления ошибок и обновления безопасности для оборудования, такого как сетевое оборудование, серверы и рабочие станции.

4.11 Программное обеспечение

Все программное обеспечение, установленное на компьютерном оборудовании Университета, является его собственностью (либо используется на основании приобретённых им лицензий) и может применяться исключительно для выполнения производственных задач.

Сотрудникам запрещается устанавливать на предоставленном в пользование компьютерном оборудовании нестандартное, нелицензионное программное обеспечение или программное обеспечение, не имеющее отношения к их производственной деятельности. Если в ходе выполнения технического обслуживания будет обнаружено не разрешенное к установке программное обеспечение, оно будет удалено, а сообщение о нарушении будет направлено непосредственному руководителю сотрудника.

На всех компьютерах должны быть установлены программы, необходимые для обеспечения защиты информации: антивирусное программ ное обеспечение, персональный межсетевой экран.

Сотрудники Университета не должны:

- блокировать антивирусное программное обеспечение;
- устанавливать другое антивирусное программное обеспечение;
- изменять настройки и конфигурацию антивирусного программного обеспечения.

На корпоративные системы применяются ограничительные меры по возможности установки программного обеспечения. Для установки необходимого программного обеспечения на корпоративные устройства, Сотрудники должны обратиться в Отдел технической поддержки на установку необходимого Программного обеспечения. Необходимость установка должна быть обоснована, должна быть обеспечена лицензиями, либо Программное обеспечение должно быть свободного для использования, иметь бесплатную лицензию.

4.12 Рекомендуемые правила пользования электронной почтой

Содержание электронных сообщений должно строго соответствовать корпоративным стандартам в области деловой этики.

Использование электронной почты в личных целях допускается в случаях, когда получение/отправка сообщения не мешает работе других пользователей и не препятствует бизнес деятельности.

Конфиденциальная информация Университета, ни при каких обстоятельствах, не подлежит пересылке третьим лицам по электронной почте.

Сотрудникам Университета запрещается использовать публичные, личные почтовые ящики электронной почты или почтовые ящики других

организаций для осуществления какого-либо из видов корпоративной деятельности. Университет может применять ограничения в доступе к публичным почтовым сервисам.

Использование сотрудниками Университета публичных почтовых ящиков электронной почты осуществляется только при согласовании с руководством Университета.

Сотрудники Университета для обмена документами с бизнес-партнерами должны использовать только свой официальный адрес электронной почты.

Сообщения, пересылаемые по электронной почте, представляют собой постоянно используемый инструмент для электронных коммуникаций, имеющих тот же статус, что и письма, и факсимильные сообщения. Электронные сообщения подлежат такому же утверждению и хранению, что и прочие средства письменных коммуникаций.

В целях предотвращения ошибок при отправке сообщений пользователи перед отправкой должны внимательно проверить правильность написания имен и адресов получателей. В случае получения сообщения лицом, вниманию которого это сообщение не предназначается, такое сообщение необходимо переправить непосредственному получателю. Если полученная таким образом информация является конфиденциальной, об этом следует незамедлительно проинформировать непосредственного руководителя.

Отправитель электронного сообщения, документа или лицо, которое его переадресовывает, должен указать свое имя и фамилию, служебный адрес и тему сообщения.

Ниже перечислены недопустимые действия и случаи использования электронной почты:

- рассылка сообщений личного характера, использующих значительные ресурсы электронной почты;
- групповая рассылка всем пользователям Университета сообщений/писем;
- рассылка рекламных материалов, не связанных с деятельностью Университета;
- подписка на рассылку, участие в дискуссиях и подобные услуги, использующие значительные ресурсы электронной почты в личных целях;
- поиск и чтение сообщений, направленных другим лицам (независимо от способа их хранения);
- пересылка любых материалов, как сообщений, так и приложений, содержание которых является противозаконным, оскорбительным, либо иным недопустимым, что может повлечь уголовное преступление или административный проступок либо приводит к возникновению гражданско-правовой ответственности, беспорядков или противоречит корпоративным стандартам в области этики.

Ко всем исходящим сообщениям, направляемым внешним пользователям, пользователь может добавлять уведомление о конфиденциальности.

Пересылка значительных объемов данных в одном сообщении может отрицательно повлиять на уровень доступности почтового ящика сотрудника. Объем вложений одного письма не должен превышать 36 Мбайт.

4.13 Корпоративные коммуникации

Для служебных коммуникаций сотрудники должны использовать исключительно утвержденные корпоративные мессенджеры, только с применением корпоративных учётных записей — как на рабочих компьютерах, так и, при необходимости, на личных мобильных устройствах, используемых в рабочих целях. Личные устройства, применяемые для корпоративной связи, должны быть защищены от несанкционированного доступа — с помощью пароля, PIN-кода, биометрической аутентификации или иных надежных методов. Университет может применять для аккаунтов корпоративных систем политик, требующих на программном уровне от пользователей исполнения обязательств применения повышенных мер защиты персональных устройств (защита доступа), при использовании на них корпоративных аккаунтов.

Запрещается использовать личные аккаунты в сторонних мессенджерах и социальных платформах (таких, как Telegram, WhatsApp, VK, Yandex Messenger, Viber и другие) для передачи любой информации, касающейся корпоративных дел.

С целью предотвращения утечки служебной, конфиденциальной или персональной информации, запрещается пересылка таких данных (включая документы, сканы, фотографии) через неавторизованные каналы связи, по причине неконтролируемой или ошибочной пересылки документов контрагентами внешним или ошибочным адресатам.

Категорически запрещается пересылать фотографии, сканированные версии внутренних документов, содержащих печати и живые подписи, не предназначенные для распространения, с применением не корпоративных мессенджеров, систем и не корпоративных учётных записей.

4.14 Сообщение об инцидентах информационной безопасности, реагирование и отчетность

Все пользователи должны быть осведомлены непосредственным руководителем о своей обязанности сообщать об известных или подозреваемых ими нарушениях информационной безопасности, а также должны быть проинформированы о том, что ни при каких обстоятельствах они не должны пытаться использовать ставшие им известными слабые стороны системы безопасности.

В случае кражи компьютера следует незамедлительно сообщить об инциденте непосредственному руководителю.

Если имеется подозрение или выявлено наличие вирусов или иных разрушительных компьютерных кодов, то сразу после их обнаружения сотрудник обязан:

- проинформировать специалистов службы поддержки;
- не пользоваться и не выключать зараженный компьютер;
- не подсоединять этот компьютер к компьютерной сети Университета до тех пор, пока на нем не будет произведено удаление обнаруженного вируса и полное антивирусное сканирование специалистами службы поддержки.

4.15 Помещения с техническими средствами информационной безопасности

Конфиденциальные заседания, совещания и иные мероприятия, связанные с обсуждением информации ограниченного доступа, должны проводиться исключительно в помещениях, оборудованных техническими средствами информационной безопасности, обеспечивающими защиту от несанкционированного съёма и утечки информации.

Перечень помещений, оснащённых техническими средствами информационной безопасности, утверждается Руководством Университета. Ответственность за поддержание данных помещений в надлежащем состоянии возлагается на назначенных должностных лиц.

Доступ в такие помещения предоставляется только уполномоченным лицам, включённым в список участников заседания. Присутствие посторонних лиц не допускается.

Использование личных технических средств (мобильные телефоны, ноутбуки, диктофоны, планшеты и иные электронные устройства) в помещениях с техническими средствами информационной безопасности строго запрещается, за исключением случаев, специально оговорённых в регламенте заседания и разрешённых руководителем Университета.

Аудио- или видеозапись, а также фотографирование в ходе конфиденциальных заседаний допускается только сотрудником Университета, назначенным ответственным за подготовку и проведение заседания, и исключительно при наличии письменного разрешения руководителя группы, организующей встречу.

Все материалы, полученные в результате проведения аудио- или видеозаписи (протоколы, электронные носители, файлы), подлежат хранению в установленном порядке в защищённых хранилищах и не могут копироваться, передаваться или уничтожаться без официального разрешения руководства Университета.

Нарушение настоящих требований рассматривается как инцидент информационной безопасности и влечёт дисциплинарную ответственность в

соответствии с законодательством Республики Казахстан и внутренними нормативными актами Университета.

Конфиденциальные встречи (заседания) должны проходить только в защищенных техническими средствами информационной безопасности помещениях.

Перечень помещений с техническими средствами информационной безопасности утверждается Руководством Университета.

Аудио/видео запись, фотографирование во время конфиденциальных заседаний может вести только сотрудник Университета, который отвечает за подготовку заседания, после получения письменного разрешения руководителя группы организации встречи.

4.16 Управление сетью

Сотрудникам Университета запрещается:

- нарушать информационную безопасность и работу сети Университета; сканировать порты или систему безопасности;
- контролировать работу сети с перехватом данных;
- получать доступ к компьютеру, сети или учетной записи в обход системы идентификации пользователя или безопасности;
- использовать любые программы, скрипты, команды или передавать сообщения с целью вмешаться в работу или отключить пользователя оконечного устройства;
- передавать информацию о сотрудниках или списки сотрудников Университета посторонним лицам;
- создавать, обновлять или распространять компьютерные вирусы и прочие разрушительное программное обеспечение.

4.17 Защита и сохранность данных

Ответственность за сохранность данных на стационарных и портативных персональных компьютерах лежит на пользователях.

Необходимо регулярно делать резервные копии всех основных служебных данных и программного обеспечения. Настоятельно рекомендуется сохранять всю служебную информацию в папках рабочей станции, настроенных на синхронизацию с облачным хранилищем корпоративной учётной записи для обеспечения наличия резервной копии и версионности документов. При отсутствии синхронизации возможно сохранение данных через веб-интерфейс облачного хранилища корпоративной учётной записи.

Сотрудники имеют право создавать, модифицировать и удалять файлы и директории в совместно используемых сетевых ресурсах только на тех участках, которые выделены лично для них, для их рабочих групп или к которым они имеют санкционированный доступ.

4.18 Конфиденциальность информации

Конфиденциальность информации означает, что информация доступна только тем лицам, которым она предназначена. Конфиденциальность является одним из основных аспектов информационной безопасности. К такой информации относиться:

- Персональные данные сотрудников, студентов, абитуриентов (ФИО, адреса, телефоны, оценки, медицинские сведения, стипендии и др.).
- Финансово-экономическая информация (бюджет университета, договоры, закупки, бухгалтерская отчётность).
- Научные и исследовательские материалы (результаты исследований, незарегистрированные патенты, проектные работы).
- Внутренняя документация (служебные переписки, приказы, внутренние отчёты, протоколы заседаний).
- Техническая информация (схемы сетевой инфраструктуры, пароли, настройки серверов, доступ к информационным системам).

Таблица 1. Уровни доступа к информации

Уровень доступа	Кто имеет право доступа	Примеры информации
Общедоступная (Public)	Все пользователи без ограничений (студенты, сотрудники, посетители, общественность)	Новости на сайте университета, общие правила приёма, рекламные материалы, расписание открытых мероприятий
Внутренняя (Internal)	Все сотрудники и студенты университета (по учетной записи)	Методические материалы, учебные планы, внутренние приказы, служебные объявления, рабочие графики
Конфиденциальная (Confidential)	Сотрудники, в чьи должностные обязанности входит работа с данной информацией; доступ предоставляется по принципу «необходимость знать»	Персональные данные студентов и сотрудников, экзаменационные результаты, кадровые документы, бухгалтерская отчетность, внутренние отчёты
Ограниченного доступа / строго конфиденциальная (Restricted / Secret)	Ограниченный круг лиц по письменному разрешению руководства университета и при наличии специальных прав доступа	Данные о финансировании, результаты закрытых научных исследований, IT-настройки серверов, административные пароли, протоколы заседаний руководства

Для обеспечения конфиденциальности информации организация может принять следующие меры:

- Использовать средства шифрования для защиты информации от несанкционированного доступа. Шифрование данных позволяет сделать информацию недоступной для злоумышленников, даже если они получат к ней доступ нарушать информационную безопасность и работу сети Университета; сканировать порты или систему безопасности.
- Ограничить доступ к информации только уполномоченным лицам. Организация должна иметь политику управления доступом к информации, которая определяет, кто имеет право доступа к какой информации.
- Правильно уничтожать информацию, которая больше не нужна. Информация, которая больше не нужна, должна быть уничтожена таким образом, чтобы ее нельзя было восстановить.

Примеры мер по обеспечению конфиденциальности информации:

- Использование средств шифрования для защиты данных, передаваемых по сети.
- Использование средств шифрования для защиты данных, хранящихся на носителях информации.
- Использование политик доступа к информации для ограничения доступа к информации только уполномоченным лицам.
- Использование средств удаленного доступа к информации для обеспечения доступа к информации только с авторизованных устройств.
- Регулярное удаление устаревшей или ненужной информации.

4.19 Процессы управления рисками

Основными процессами управления рисками являются:

- Идентификация — выявление потенциальных рисков информационной безопасности
- Оценка — определение вероятности и последствий реализации рисков
- Управление — принятие мер по снижению рисков.
- Мониторинг — отслеживание эффективности мер по снижению рисков.
- Планирование — определение целей и задач управления рисками, а также разработка плана действий.

4.21 Планирование

На этапе планирования организация определяет цели и задачи управления рисками, а также разрабатывает план действий.

Основные задачи планирования включают:

- Определение состава и ответственности участников процесса управления рисками.
- Разработка методологии управления рисками.

- Определение целей и задач управления рисками.
- Определение источников информации для оценки рисков.

5 Идентификация

На этапе идентификации организация выявляет потенциальные риски информационной безопасности.

Основные методы идентификации рисков включают:

- Анализ инцидентов информационной безопасности.
- Анализ нормативно-правовых требований.
- Анализ деятельности организации.
- Анализ угроз и уязвимостей разделение целей и задач управления рисками.

Оценка:

На этапе оценки организация определяет вероятность и последствия реализации рисков.

Основные методы оценки рисков включают:

- Количественная оценка рисков.
- Качественная оценка рисков.

Управление:

На этапе управления организация принимает меры по снижению рисков.

Основные методы управления рисками включают:

- Устранение рисков.
- Снижение вероятности реализации рисков.
- Снижение последствий реализации рисков.

Мониторинг:

На этапе мониторинга организация отслеживает эффективность мер по снижению рисков.

Основные методы мониторинга включают:

- Анализ отчетов о реализации мер по снижению рисков.
- Регулярное проведение оценки рисков.
- Анализ инцидентов информационной безопасности

6 Целостность информации

Целостность информации означает, что информация не была изменена без разрешения. Целостность является одним из основных аспектов информационной безопасности.

Для обеспечения целостности информации организация может принять следующие меры:

- Использовать средства контроля целостности для обнаружения изменений в информации. Средства контроля целостности позволяют определить, была ли информация изменена без разрешения.

- Регулярно резервировать данные для восстановления в случае их изменения или уничтожения. Резервное копирование позволяет восстановить информацию в случае ее изменения или уничтожения.

Примеры мер по обеспечению целостности информации:

- Использование средств контроля целостности для файлов и баз данных.
- Регулярное резервное копирование данных.
- Использование средств шифрования для защиты данных от несанкционированного изменения
- Использование политик доступа к информации для ограничения доступа к данным только уполномоченным лицам

Рекомендации по обеспечению целостности информации:

- Оценка рисков целостности. Организация должна оценить риски нарушения целостности информации и разработать меры по снижению этих рисков.
- Обучение сотрудников. Сотрудники организации должны быть осведомлены о важности целостности информации и о методах ее защиты.

Примеры инцидентов, связанных с целостностью информации:

- Несанкционированное изменение информации.
- Уничтожение или повреждение информации

Влияние инцидентов, связанных с целостностью информации:

- Финансовые убытки
- Потеря репутации
- Нарушение законодательства

Сравнение конфиденциальности и целостности:

Конфиденциальность и целостность являются двумя основными аспектами информационной безопасности. Конфиденциальность означает, что информация доступна только тем лицам, которым она предназначена. Целостность означает, что информация не была изменена без разрешения.

7 Доступность информации

Доступность информации означает, что информация доступна для использования по назначению в требуемое время и в требуемом месте. Доступность является одним из основных аспектов информационной безопасности.

Для обеспечения доступности информации организация может принять следующие меры:

- Использовать средства резервирования для обеспечения доступа к информации в случае сбоя системы. Резервное копирование позволяет восстановить информацию в случае ее потери или повреждения

- Развертывать системы в нескольких географических центрах для обеспечения непрерывности работы. Развертывание систем в нескольких центрах позволяет обеспечить доступ к информации даже в случае сбоя в одном из центров.
- Использовать средства мониторинга и оповещения для своевременного выявления и устранения сбоев. Мониторинг и оповещения позволяют своевременно выявить сбои и принять меры по их устранению.

Примеры мер по обеспечению доступности информации:

- Использование средств резервирования для файлов и баз данных.
- Развертывание систем в нескольких дата-центрах.
- Использование средств мониторинга и оповещения для систем и сетей.
- Использование отказоустойчивых компонентов для систем и сетей.

Рекомендации по обеспечению доступности информации:

- Оценка рисков доступности. Организация должна оценить риски нарушения доступности информации и разработать меры по снижению этих рисков.
- Обучение сотрудников. Сотрудники организации должны быть осведомлены о важности доступности информации и о методах ее обеспечения.
- Регулярный мониторинг и аудит. Организация должна регулярно контролировать эффективность мер по обеспечению доступности информации.

Примеры инцидентов, связанных с доступностью информации:

- Сбой системы или сети.
- Уничтожение или повреждение систем, или сетей.
- Кибератака.

Влияние инцидентов, связанных с доступностью информации:

- Финансовые убытки.
- Потеря репутации.
- Нарушение законодательства.

Лист регистрации изменений к _____

обозначение документа

Порядковый номер изменения	Раздел, пункт документа	Вид изменения (заменить, аннулировать, добавить)	Номер и дата извещения	Изменение внесено	
				Дата	Фамилия и инициалы, подпись, должность