SATBAYEV UNIVERSITY	НЕКОММЕРЧЕСКОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО «КАЗАХСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ имени К.И. САТПАЕВА»	
Документ СМК 3 уровня	Редакция №3 от «1» 09 2023 г.	Пол. 029-03-03.5.01 – 2023

ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ И ЗАЩИТЫ ДАННЫХ

Пол. 029-03-03.5.01 -2023

Алматы 2023

ПРЕДИСЛОВИЕ

1 РАЗРАБОТАНО

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

«_25_» _08_____ 2023 г.

2 СОГЛАСОВАНО

Член Правления - Проректор по академическим вопросам _____ Жаутиков Б.А.

«_31_» _08_____ 2023 г.

Начальник отдела оценки и качества _____ Сауранбаева А.

«_29_» _08_____ 2023 г.

И.о Начальника Управления отдела юридического обеспечения и государственных закупок _____ Зиманов Е.

«_28_» _08_____ 2023 г.

3 УТВЕРЖДЕНО решением Правления от «_01_» _____09_____2023г. № _13_

4 ВВЕДЕНО взамен редакции № 2 от 26.09.2022г

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

В настоящей Политике под термином «сотрудник» понимаются все сотрудники Университета, в том числе, работающих в Университета 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 Университета.

– 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 и ресурсы обработки информации Университета. Соблюдение настоящей Политики обязательно для всех сотрудников (как постоянных, так и временных). В договорах с третьими лицами, получающими доступ к информации Университета, должна быть оговорена обязанность третьего лица по соблюдению требований настоящей Политики. При взаимодействии с третьими лицами обязательно подписание соглашения о неразглашении информации.

Университета принадлежит на праве собственности (в том числе на праве интеллектуальной собственности): все разработанные нанятыми сотрудниками Университета программные продукты, аналитические данные, дизайн, схемы, а также вся деловая информация, лицензионное программное обеспечение и вычислительные ресурсы, приобретенные (полученные) и введенные в эксплуатацию в целях осуществления ею деятельности в соответствии с действующим законодательством. Указанное право собственности распространяется на голосовую и факсимильную связь, осуществляемую с использованием оборудования Университета, содержание ящиков электронной почты, бумажные и электронные документы всех функциональных подразделений и сотрудников Университета.

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 официальными должностными обязанностями только на компьютерах, разрешенных к использованию в Университета.

Внос в здания и помещения Университета личных портативных компьютеров и внешних носителей информации (диски, дискеты, флэш-карты и т.п.), а также вынос их за пределы Университета производится только при согласовании с непосредственным руководителем.

Руководители подразделений должны периодически пересматривать права доступа своих сотрудников и других пользователей к соответствующим информационным ресурсам.

В целях обеспечения санкционированного доступа к информационному ресурсу, любой вход в систему должен осуществляться с использованием уникального именного имени пользователя и пароля.

В процессе своей работы сотрудники обязаны устанавливать парольную защиту каждый раз, когда покидают свое рабочее место.

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 учётный 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.

4.4 Доступ третьих лиц к системам Университета

Доступ третьих лиц к информационным системам Университета должен быть обусловлен производственной необходимостью. В связи с этим, доступ к информационным ресурсам Университета должен быть согласован с руководством 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 для работы необходим доступ к рабочим компьютерам Университета, может быть предоставлен удаленный доступ к данным рабочим местам, с которых они могут выполнять работы и иметь доступ к сетевым ресурсам Университета в соответствии с правами 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 установка, запуск и использование программ для организации удаленного доступа. Программные решения для удаленного подключения сотрудников Информационных систем и технической поддержки могут использовать только во внутренней сети Университета. Для возможности удаленной помощи Сотрудники могут использовать возможности контролируемого удаленного подключения или демонстрации экрана, предоставляемые корпоративными коммуникаторами, разрешенными 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 также 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

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

Сотрудники Университета перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов.

Университет имеет право контролировать содержание всего потока информации, проходящей через канал связи к сети Интернет в обоих направлениях. А также применять ограничения в доступе к ресурсам как в ручном режиме, так и с применением автоматических алгоритмов оборудования и/или программного обеспечения и комплексов по обеспечению сетевой и информационной безопасности.

4.7 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.

4.8 Аппаратное 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, факс-модемы, 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.

Пользователи портативных компьютеров, содержащих информацию, определенную как конфиденциальную, и составляющую коммерческую тайну Университета, обязаны обеспечить их хранение в физически защищенных помещениях, запираемых ящиках рабочего стола, шкафах, или обеспечить их защиту с помощью аналогичного по степени эффективности защитного устройства, в случаях, когда данный компьютер не используется.

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.

При записи какой-либо информации на носитель для передачи его заказчикам или партнерам по бизнесу, необходимо убедиться в том, что носитель чист, то есть не содержит никаких иных данных. Простое переформатирование носителя не дает гарантии полного удаления записанной на нем информации.

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

4.9 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.

4.10 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.

4.11 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

– Неустановка 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-браузеры

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

4.12 Программное обеспечение

Все программное обеспечение, установленное на предоставленном Компанией компьютерном оборудовании, является собственностью Университета и должно использоваться исключительно в производственных целях.

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 программное 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.

4.13 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, непристойным, злонамеренным, оскорбительным, угрожающим, клеветническим, злобным или способствует поведению, которое может рассматриваться как 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 25 Мбайт.

4.14 Корпоративные коммуникации

Для оперативных коммуникаций сотрудников необходимо использовать корпоративные мессенджеры как на рабочих компьютерах, так и на личных мобильных устройствах. При этом, мобильные устройства должны быть защищены от доступа к содержимому посторонними лицами. Методы защиты доступа должны обеспечивать защиту устройства паролем, пин-кодом, с применением биометрии пользователя или иными методами

защиты. Запрещается использование коммуникаторов и мессенджеров с личными аккаунтами по любым корпоративным вопросам.

В целях исключения утечки информации по причине случайной отправки документов внешним или ошибочным адресатам, категорически запрещается пересылка внутренних документов, их сканированных вариантов или фотографий, содержащих печати и росписи.

4.15 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.

4.16 Помещения с техническими средствами информационной безопасности

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.

4.17 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.

4.18 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.

4.19 Конфиденциальность информации

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

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 доступрушать 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.

4.20 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.

5 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.

6 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 ределение целей и задач управления рисками

6.1 Оценка

На этапе оценки организация определяет вероятность и последствия реализации рисков.

Основные методы оценки рисков включают:

– Количественная оценка рисков.
– Качественная оценка рисков.

6.2 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

6.3 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.

7 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.

8 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