НАО «ЗАПАДНО-КАЗАХСТАНСКИЙ УНИВЕРСИТЕТ ИМЕНИ М.УТЕМИСОВА»

«Утверждаю»
Председатель Правления - Ректор
ЗКУ имени М.Утемисова
_____ Сергалиев Н.Х.
«_25_» _01_____2023 г.

ПОЛИТИКА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НАО «ЗАПАДНО-КАЗАХСТАНСКИЙ УНИВЕРСИТЕТ ИМЕНИ М.УТЕМИСОВА»

Уральск, 2023 год

СОДЕРЖАНИЕ

Термины и определения

В настоящей Политике используются следующие термины:

Аутентификация - проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.

База данных – совокупность данных организованных согласно концептуальной структуре, описывающий характеристику этих данных, а также взаимосвязи между их объектами;

Безопасность информации - защищенность информации от ее нежелательного разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности, а также незаконного ее тиражирования.

Доступность - возможность для авторизованного пользователя информационной системы за приемлемое время получить информационную услугу, предусмотренную функциональностью.

Идентификация - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационная безопасность – комплекс административно-правовых, организационно-распорядительных и технических мер, направленные на обеспечение конфиденциальности, целостности и санкционированной доступности информации в процессе ее сбора, обработки, передачи и хранения.

Информационная система (далее – **ИС**) – система обработки информации совместно с соответствующей организацией, ресурсами такими как человеческие, технические и финансовые ресурс, предоставляющая и распределяющая информацию;

Информационная система (ИС) обработки информации - организационно-техническая структура, представляющая собой совокупность следующих взаимосвязанных компонентов:

- технических средств обработки и передачи данных;
- методов и алгоритмов обработки в виде соответствующего программного обеспечения; - баз данных на различных носителях;
- персонала и пользователей, объединенных по организационно структурному, тематическому, технологическому или другим признакам для выполнения автоматизированной обработки данных.

Конфиденциальность - защита от несанкционированного ознакомления.

Несанкционированное действие - действие субъекта в нарушение установленных в системе правил обработки информации.

Пользователь - субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации.

Риски информационной безопасности – реально или потенциально возможные действия по реализации опасных воздействующих факторов с целью преднамеренного или случайного нарушения режима функционирования объекта.

Сеть (локальная сеть, ЛВС, LAN) - группа точек, узлов или других устройств, соединенных коммуникационным набором оборудования, обеспечивающее соединение станций и передачу между ними информации.

Угроза - реально или потенциально возможные действия по реализации опасных воздействующих факторов с целью преднамеренного или случайного нарушения режима функционирования объекта.

Уязвимость - любая характеристика автоматизированной системы, использование которой может привести к реализации угроз.

Целостность информации – свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому ее состоянию).

Шифрование – преобразование данных в нечитабельную форму, используя ключи шифрования-расшифровки.

IT-инфраструктура – инфраструктура, состоящая из интегрированного комплекса серверного оборудования, сетевого оборудования, информационных систем, программ, сетевых и системных служб.

Нормативные ссылки

1. Настоящий документ разработан в соответствии со следующими нормативно-правовыми актами и документами:

1) Закон Республики Казахстан от 24 ноября 2015 года «Об информатизации»;

2) Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности»;

3) СТ РК 34.005-2002 «Информационная технология. Основные термины и определения»;

4) СТ РК 34.006-2002 «Информационная технология. Базы данных. Основные термины и определения»;

5) СТ РК 34.007-2002 «Информационная технология. Телекоммуникационные сети. Основные термины и определения»;

6) СТ РК ИСО/МЭК 17799-2006 «Информационная технология. Методы обеспечения защиты».

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Политика информационной безопасности некоммерческого акционерного общества «Западно – Казахстанский университет имени М.Утемисова» (далее - Политика) предназначена для определения целей и требований обеспечения информационной безопасности некоммерческого акционерного общества «Западно – Казахстанский университет имени М.Утемисова» (далее - Университет).

1.2 Политика по информационной безопасности учитывает современное состояние и ближайшие перспективы развития корпоративной сети передачи данных (далее - КСПД) Университета, цели, задачи и правовые основы эксплуатации, режимы функционирования, а также анализ угроз безопасности для ее ресурсов.

1.3 Требования Положения распространяются на структурные подразделения Университета, в которых осуществляется автоматизированная обработка информации, в том числе информации с ограниченным распространением (служебная информация) или персональных данных, а также осуществляющих сопровождение, обслуживание и обеспечение функционирования Университета. Политика распространяется также на другие организации и учреждения, осуществляющих взаимодействие с университетом в качестве поставщиков и потребителей (пользователей) информации и услуг.

1.4 Ответственным структурным подразделением за непосредственную организацию (построение) и обеспечение эффективного функционирования системы защиты информации является ЦИТ.

1.5 ЦИТ проводят необходимые технические и организационные мероприятия для обеспечения информационной безопасности.

1.6 Руководитель ЦИТ осуществляет организацию квалифицированной разработки (совершенствования) системы защиты информации и организационного (административного) обеспечения ее функционирования в Университете.

1.7 За соблюдение информационной безопасности в Университете несут ответственность все работники университета.

2 ОСНОВНАЯ ЧАСТЬ

2.1 Цели и задачи

2.1.1 Основной целью, на достижение которой направлены все пункты Политики, является надежное обеспечение информационной безопасности и как следствие недопущение нанесения материального, физического, морального или иного ущерба Университету в результате информационной деятельности.

2.1.2 Указанная цель достигается посредством обеспечения и постоянного поддержания следующего состояния корпоративной сети передачи данных:

- доступность обрабатываемой информации для зарегистрированных пользователей;
- устойчивое функционирование КСПД Университета;
- обеспечения конфиденциальности информации, хранимой, обрабатываемой средствами вычислительной техники (далее - СВТ) и передаваемой по каналам связи;
- целостность и аутентичность информации, хранимой и обрабатываемой информационной системой (далее - ИС) Университета и передаваемой по каналам связи.

2.1.3 Для достижения поставленной цели необходимо решить следующие задачи:

- защита от вмешательства посторонних лиц в процесс функционирования информационных ресурсов Университета;
- разграничение доступа зарегистрированных пользователей к информации, аппаратными, программными и криптографическими средствами защиты, используемыми в ИС;
- контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения;
- защита информации от несанкционированной модификации, искажения;
- контроль целостности используемых программных средств, а также защиту системы от внедрения вредоносного программного обеспечения;
- защиту служебной тайны и персональных данных от утечки, несанкционированного разглашения или искажения при ее обработке, хранении и передаче по каналам связи;
- обеспечение авторизации и аутентификации пользователей, участвующих в информационном обмене;
- своевременное выявление угроз информационной безопасности, причин и условий, способствующих нанесению ущерба;
- создание механизма оперативного реагирования на угрозы информационной безопасности и негативные тенденции;
- создание условий и инструкций для минимизации и локализации нанесенного ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения информационной безопасности.

- создание и обеспечения бесперебойной работы электронного документооборота.

2.2 Пользователи информационных систем

2.2.1 К пользователям информационных систем относятся:

- сотрудники, осуществляющие свою деятельность в Университете и обладающие основными правами и обязанностями в соответствии с законодательством Республики Казахстан;
- вспомогательный персонал, обслуживающий и технический персонал, *в том числе:*
- администраторы корпоративной сети передачи данных, ответственные за сопровождение телекоммуникационного оборудования;
- системные администраторы, ответственные за сопровождение общего и прикладного программного обеспечения;
- разработчики прикладного программного обеспечения;
- инженеры-техники, инженеры-электронщики, технические специалисты;
- потребители услуг – лица и/или сторонние организации, использующие информационные ресурсы Университета.
- студенты и магистранты.

2.3 Модели потенциальных нарушителей

2.3.1 В качестве потенциального нарушителя информационной безопасности рассматривается лицо или группа лиц, состоящих или не состоящих в сговоре, которые в результате умышленных или неумышленных действий могут реализовать разнообразные угрозы информационной безопасности, направленные на информационные ресурсы и нанести моральный и/или материальный ущерб интересам Университета.

2.3.2 Потенциальных нарушителей можно разделить на внутренних и внешних. Внутренними нарушителями могут быть практически все сотрудники Университета и вспомогательный персонал. Их можно разделить на следующие группы в зависимости от уровня доступа к информационным ресурсам корпоративной сети:

- лица, имеющие доступ к информации, составляющую служебную тайну и задействованные в технологии обработки, передачи и хранения информации;
- лица, не имеющие доступ к информации, составляющую служебную тайну, но задействованные в технологии обработки, передачи и хранения информации;
- обслуживающий персонал.

2.3.3 Чтобы построить реальную модель потенциального нарушителя необходимо принять во внимание виды выявленных нарушений, устремлений различных лиц и организаций, а также имеющиеся в Университете интересы других юридических лиц.

2.3.4 В Университете возможны следующие виды нарушений:

- несанкционированное использование программ, могущих негативно повлиять на работоспособность КСПД Университета, снизить ее производительность, а также мешающих корректной работе КСПД (сканеры сети, интенсивный широковещательный трафик и т.п.);

- использование прав локальных администраторов на рабочих станциях пользователей, что дает возможность установки обычному пользователю неограниченного количества программ.

- нарушения сотрудниками вследствие незнания требований информационной безопасности и нормативных правовых актов Университета.

2.3.5 Потенциальные внешние нарушители:

- бывшие сотрудники и вспомогательный персонал;

- представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности (энерго-, водо-, теплоснабжения и т.п.);

- посетители (приглашенные представители организаций, граждане);

- представители фирм, поставляющих технику, программное обеспечение, услуги и т.п.

2.4 Назначение, нормативная и правовая база Политики

2.4.1 Настоящее Политика детализирует требования по решению вопроса обеспечения информационной безопасности в единой информационной телекоммуникационной среде, объединяющей ИС Университета.

2.4.2 Политика информационной безопасности Университета является методологической базой:

- выработки и совершенствования комплекса согласованных нормативных, правовых, технологических и организационных мер, направленных на защиту информации;

- обеспечения информационной безопасности;

- координации деятельности территориальных и структурных подразделений при проведении работ по соблюдению требований обеспечения информационной безопасности.

2.4.3 Научно-методической основой Политика является системный подход, предполагающий проведение исследований, разработку системы защиты информации в процессе ее обработки в информационных системах с учетом всех факторов, оказывающих на нее влияние и комплексного применения различных мер и средств защиты.

2.4.4 Основные требования Политика базируются на качественном осмыслении вопросов информационной безопасности, не концентрируя внимание на экономическом (количественном) анализе рисков и обосновании необходимых затрат на защиту информации.

2.5 Средства и меры защиты информации

2.5.1 Объекты Информационные безопасности

2.5.1.1 Основными объектами защиты ИБ университета являются:

- информационные ресурсы с ограниченным доступом, составляющие тайну, чувствительные по отношению к несанкционированным воздействиям и нарушению их безопасности, в том числе открытая (общедоступная) информация, независимо от формы и вида представления;

- процессы и человеческие ресурсы обработки информации в ИС — информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, персонал разработчиков, внутренние пользователи системы и ее обслуживающий персонал;

- информационная инфраструктура, включающая системы обработки и анализа информации, передачи и отображения, в том числе каналы информационного обмена, объекты и помещения, в которых размещены ИР и компоненты ИС.

2.5.1.2 Объекты информационной инфраструктуры включают:

- Технологическое оборудование (сетевое и кабельное оборудование);

- Информационные ресурсы, содержащие сведения ограниченного доступа;

- программные средства (операционную систему (далее - ОС), СУБД, другое общесистемное и ППО,

- автоматизированные системы связи и передачи данных (средства телекоммуникации);

- каналы связи, по которым передается информация (в том числе ограниченного распространения);

- служебные помещения, в которых циркулирует информация ограниченного распространения;

- технические средства и системы, не обрабатывающие информацию, размещенные в помещениях, где обрабатывается (циркулирует) служебная информация.

2.5.2 Средства и меры защиты от утечки информации по каналам связи

2.5.2.1 Ответственное лицо за ИБ организует, выполняет, контролирует и координирует вопросы и работы, связанные с защитой информации в соответствии с требованиями.

2.5.2.2 Защита информации от утечки по каналам их передачи из/в Университете достигается, путем применения комплексных программных, технических средств защиты и организационных мер.

2.5.2.3 Для выявления утечки информации необходим систематический контроль возможности образования каналов утечки и оценки их опасности в пределах контролируемой зоны.

2.5.2.4 В соответствии с используемыми каналами передачи электронной информации в Университете предусматриваются необходимые технические средства защиты (межсетевой экран и т.п.). Организуется система регистрации, передачи, приема и хранения носителей информации, предусматриваются надлежащие способы их уничтожения, с целью исключения возможности восстановления записанных на них сведений. Технические каналы передачи информации оснащаются соответствующими

средствами защиты. Создается надежная система охраны зданий и сооружений, организуется пропускной режим в помещения Университета (турникет) для предотвращения доступа посторонних лиц.

2.5.3 Меры по защите средств вычислительной техники

2.5.3.1 В случае обнаружения фактов НСД к информационным ресурсам и системам Университета или выявления потенциальной угрозы информационной безопасности сотрудники ЦИТ немедленно информирует руководителя.

2.5.4 Защита от аппаратных спецвложений, нелегального внедрения и использования неучтенных программ

2.5.4.1 Для предотвращения аппаратных спецвложений используются меры физической защиты, устанавливаются средства видеонаблюдения и контроля доступа в серверное помещение Университета.

2.5.5 Защита от несанкционированного копирования данных пользователем

2.5.5.1 Служебная и иная защищаемая информация, обрабатываемая и хранящаяся в информационных системах Университета подлежит копированию и передаче третьему лицу только с разрешения Председателя Правления - ректора по согласованию с руководителем ЦИТ.

2.5.5.2 Защита информации от утечки по каналам их передачи из/в Университете достигается, путем применения комплексных программных, технических средств защиты и организационных мер.

2.5.5.3 Для выявления утечки информации необходим систематический контроль возможности образования каналов утечки и оценки их опасности в пределах контролируемой зоны. Закрытие и локализация каналов утечки обеспечивается организационно-техническими мерами.

2.5.5.4 В соответствии с используемыми каналами передачи электронной информации в Университете предусматриваются необходимые технические средства защиты (межсетевой экран и т.п.). Организуется система регистрации, передачи, приема и хранения носителей информации, предусматриваются надлежащие способы их уничтожения, с целью исключения возможности восстановления записанных на них сведений. Технические каналы передачи информации оснащаются соответствующими средствами защиты. Создается надежная система охраны зданий и сооружений, организуется пропускной режим в помещения Университета (турникет) для предотвращения доступа посторонних лиц.

2.5.3 Меры по защите средств вычислительной техники

2.5.3.1 Защита СВТ от несанкционированного доступа в Университете строится по нескольким направлениям. Создаются автоматизированные средства регистрации пользователей, система блокирования учетных записей и оповещения сотрудников об угрозе или проникновении в СВТ.

2.5.3.2 Определяются организационные меры по предотвращению несанкционированного доступа (далее НСД), в том числе в случае утраты/компрометации паролей и выхода из строя СВТ.

2.5.4 Защита от аппаратных спецвложений, нелегального внедрения и использования неучтенных программ

2.5.4.1 Для предотвращения аппаратных спецвложений используются меры физической защиты, устанавливаются средства видеонаблюдения и контроля доступа в серверное помещение Университета.

2.5.5 Защита от действий вредоносных программ, вирусов

2.5.7.1 В целях защиты от действий вредоносных программ и вирусов в Университете используются «иммуностойкие» программные средства, защищенные от возможности несанкционированной модификации, специальные программы-анализаторы, осуществляющие постоянный контроль за возникновением отклонений в деятельности прикладных программных продуктов, периодическую проверку наличия возможных следов вирусной активности, а также входной контроль новых программ перед их использованием.

2.5.5.2 Организационные меры изложены в правилах по антивирусной защите компьютеров и серверов.

2.5.6 Требования по организации защиты общедоступных ресурсов

2.5.6.1 Общедоступные ресурсы (почтовые сервера, web-сервера, web-порталы и другие ресурсы) должны быть размещены в отдельном сегменте ЛВС университета. Подключение указанных ресурсов к Интернет осуществляется через Единый шлюз доступа в сеть Интернет (ЕШДИ). При этом должны применяться межсетевые экраны и системы обнаружения и предотвращения вторжений (IDP, IPS, Anti-DDoS).

2.5.6.2 Интернет-ресурс подключается к сети Интернет через ЕШДИ.

2.5.6.3 Для подключения устройств к сети Университета необходимо установить сертификат безопасности с сайта https://sts.kz/ .

2.5.6.4 Для обеспечения ИБ Интернет-ресурсов необходимо применять систему управления содержимым, выполняющую:

- Санкционирование операций размещения, изменения и удаления информационного контента;
- регистрацию авторства при размещении, изменении и удалении информационного контента;
- проверку загружаемого контента на наличие вредоносного кода;
- контроль целостности размещенного информационного контента;
- контроль аномальной активности пользователей и программных роботов.

2.5.6.5 С целью контроля обеспечения конфиденциальности должны обеспечиваться следующие мероприятия:

- постоянный мониторинг инструментальными, программными средствами ИБ Информационно-коммуникационной инфраструктуры университета.

2.5.7 Требования безопасности ИС при разработке, усовершенствовании и обслуживании

2.5.7.1 Разработка программных средств или изменение исходного кода в рамках сопровождения программных средств должно осуществляться в разработочной среде.

2.5.7.2 Измененное программное средство должно пройти тестирование на предмет соответствия установленным требованиям ИБ и совместимости с другими программными средствами. Тестирование проводится разработчиками совместно с ответственным лицом за ИБ, результаты тестирования должны быть отражены в протоколе тестирования.

2.5.7.3 Запуск программного средства в эксплуатационную среду должен осуществляться только при наличии протокола тестирования с положительным заключением.

2.5.7.4 Требования безопасности должны учитывать ценность информационных активов, потенциальный ущерб бизнес-процессу.

2.5.8 Требования к применению электронной почты и Интернета

2.5.8.1 Для уменьшения риска, которому подвергаются производственные процессы и система безопасности, связанного с использованием электронной почты, следует применять (по необходимости) соответствующие средства контроля, которые должны учитывать:

- уязвимость электронных сообщений по отношению к несанкционированному перехвату и модификации;
- уязвимость данных, пересылаемых по электронной почте, по отношению к ошибкам, например, неправильная переадресация или направление сообщений не по назначению, а также надежность и доступность сервиса в целом;
- правовые соображения, такие как необходимость проверки источника сообщений и др.;
- последствия для системы безопасности от раскрытия содержания каталогов;
- необходимость принятия защитных мер для контроля удаленного доступа пользователей к электронной почте.

2.5.8.2 Подключение к сети Интернет должно осуществляться исключительно через Единый шлюз доступа к сети Интернет, не имеющей сопряжения с информационно-коммуникационной и локальной сетью университета.

2.5.9 Защита от ввода ошибочных данных

2.5.9.1 Данные, вводимые в приложениях проверяются программными и техническими средствами, чтобы гарантировать их правильность и соответствующее использование. Ввод информации осуществляется уполномоченным на это персоналом.

2.5.10 Меры по защите системы архивирования

2.5.10.1 Определяется порядок резервного копирования, хранения и восстановления программных продуктов и информационных систем. Хранилище резервных копий размещается в помещении специально оборудованным согласно Плану по обеспечению непрерывной деятельности информационных систем. Обеспечивается санкционированный доступ к

хранилищу резервных копий для своевременного восстановления информации и информационных систем в случае сбоя, аварии и иных нештатных ситуациях.

2.5.10.2 Разрабатывается План по обеспечению непрерывной деятельности информационных систем, в котором также определяются меры по защите архивов на случай возникновения аварий, стихийных бедствий и других нештатных ситуаций, согласно правилам по резервному копированию информации.

2.6 Требования к управлению инцидентами безопасности

2.6.1 О случаях нарушения ИБ следует сообщать незамедлительно ответственному лицу за ИБ.

2.6.2 Должны быть установлены зоны ответственности и процедуры, чтобы гарантировать быструю, результативную и упорядоченную реакцию на инциденты в системе защиты информации.

2.6.3 Должны быть приняты механизмы для ведения мониторинга инцидентов в системе защиты информации и постоянно их контролировать.

2.7 Требования к отказоустойчивости

2.7.1 Аппаратно-программное обеспечение должно обеспечивать выполнение задач ИС университета со временем однократного простоя не более 10 часов и суммарным временем простоя не более 48 часов в год.

2.7.2 В случае возникновения внештатной ситуации, произошедшей с производственным сервером ИС, восстановление ППО, системного ПО и ОС должно быть произведено в течение 9 часов.

2.7.3 Восстановление работоспособности и обеспечение непрерывной работы ИС университета производится согласно, параграфа 8 Постановления Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно коммуникационных технологий и обеспечения информационной безопасности.

2.7.4 Система хранения данных должна предусматривать автоматический периодический контроль целостности дисков, анализ плохих секторов, проверку состояния резервных батарей, без вмешательства администратора и без влияния на работу пользователей.

2.7.5 Система хранения данных должна обеспечивать возможность «горячей» замены дисков.

2.7.6 Бесперебойное электропитание обеспечивается источником бесперебойного питания (ИБП) необходимой мощности, который должен гарантировать, как минимум, корректное завершение работы приложений и ОС при отключении внешнего электропитания.

3. ТРЕБОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Настоящее Политика определяет требования в следующих областях обеспечения информационной безопасности:

3.1 Обучение и информированность персонала.

3.2 Парольная Политика.

3.3 Политика резервного копирования.

3.4 Антивирусная Политика.

3.5 Политика управления инцидентами по ИБ.

3.6 Политика использования не корпоративных почтовых адресов для обмена служебными сообщениями по электронной почте.

3.7 Политика по физической безопасности в Университете

3.8 Политика использования и управления внешними съемными носителями информации (все виды носителей) и регламент эксплуатации данных носителей.

3.9 Правила доступа к сети Интернет.

3.10 Политика удаленного доступа.

3.11 Политика межсетевого экранирования.

3.1 Обучение и информированность персонала

Для обеспечения должного уровня ИБ, работники структурных подразделений Университета должны быть хорошо информированы в данных вопросах и при необходимости дополнительно обучены. Для этого в Университете должна быть организована эффективная система обучения и контроля знаний работников в области ИБ, включающая:

- обучение вопросам обеспечения ИБ в Университете при найме на работу;
- ознакомление с действующими нормативными документами по вопросам ИБ;
- при необходимости периодический контроль знаний по вопросам ИБ, в части касающейся выполняемых работниками Университета функций по защите информационных активов;
- при необходимости повышение квалификации лиц, выполняющих функции специалистов ИБ, сетевых администраторов, системных администраторов, путем обучения их на специализированных курсах по вопросам ИБ;
- организацию доступа работников Университета к нормативным документам по вопросам ИБ для самостоятельного изучения.

3.2 Парольная Политика

Основным инструментом защиты информационных систем Университета и информации хранящейся в них (далее - ИС), является персонализированная учетная запись, состоящая из идентификатора и пароля. Пароль должен выбираться пользователем ИС самостоятельно. Пароли должны соответствовать следующим требованиям:

- минимальная длина пароля пользователя должна быть не менее 7 символов;

- при смене пароля пользователь не должен повторно использовать предыдущие три пароля;

- минимальная длина пароля службы администрирования и системных учетных записей (root, administrator и т.п.) должна быть не менее 12 символов, история паролей при смене не менее 20 паролей;

- пароли должны быть сложными, состоять из комбинации цифр, букв в верхнем и нижнем регистре;

- пароли не должны включать в себя легко вычисляемые сочетания символов (имена, фамилии, номера телефонов, словарные слова и т.п.) и какие-либо сокращения;

- имена учетных записей запрещено использовать в качестве паролей. Пользователь должен обеспечить конфиденциальность личного пароля. Передача пароля другим коллегам, работникам Службы ИТ, Руководству или другим третьим лицам строго запрещена. При работе с паролями должны выполняться следующие требования:

- после первого входа в ИС, пользователю должна быть предоставлена возможность смены пароля;

- пользователь должен сменить временный пароль после первого входа в ИС;

- пароли стандартных «по умолчанию» учетных записей ИС должны быть изменены;

- при вводе пароль не должен отображаться на экране в открытом виде;

- пользователь должен блокировать сеанс работы, если оставляет свое рабочее место на длительное время;

- сеансы работы, оставленные пользователем без присмотра, должны автоматически блокироваться по истечению 15 минут;

- записи о паролях в ИС должны храниться в зашифрованном виде и быть доступны только их владельцу;

- пользователям запрещено записывать, хранить свои пароли на бумажном носителе;

- выдача пользователям временного пароля или активация заблокированной учетной записи (включая учетные записи пользователей временно не имеющих доступа к ИС) выполнятся только по заявке Руководителем структурного подразделения, в котором работает пользователь.

В следующих случаях требуется немедленная смена пароля, независимо от предписанных выше интервалов смены:

- имеется подозрение, что учетная запись была скомпрометирована;

- пароль был сообщен кому-либо непреднамеренно;

- пароль был использован другим лицом при аварийных ситуациях.

3.3 Политика резервного копирования

В целях защиты информации от преднамеренного или непреднамеренного ее уничтожения и фальсификации должно быть обеспечено обязательное резервирование всей информации, являющейся важной. При взаимодействии и по согласованию с владельцами информации должны быть выполнены следующие работы:

- классификация информации, подлежащей резервному копированию и/или архивированию;
- расчет объема информации, подлежащей резервному копированию и/или архивированию;
- определение методов резервного копирования;
- определение ответственных лиц за хранение и резервирование информации;
- определение и согласование сроков хранения резервных и/или архивных копий, схемы ротации носителей и их количество;
- определение требований к восстановлению и тестированию резервных копий ИС.

3.4 Антивирусная Политика

Для защиты ИС и своевременного блокирования вредоносных программ (далее - Вирусов), в Университете должна применяться Система Антивирусной Защиты.

Система Антивирусной Защиты должна отвечать следующим требованиям:

- мониторинг возможных каналов проникновения Вирусов на всех средствах обработки информации, должен производиться в режиме реального времени;
- не реже одного раза в неделю должна производиться полная проверка средств обработки информации на предмет наличия Вирусов;
- пользователи средств обработки информации не должны иметь возможность отключения или изменения настроек антивирусного приложения;
- пользователи должны иметь возможность инициировать частичную или полную проверку средства обработки информации на предмет наличия Вирусов;
- обновление баз Вирусных сигнатур должно производиться регулярно, но не реже одного раза в сутки;
- обновление клиентских баз Вирусных сигнатур и приложения должно производиться незамедлительно после получения данных обновлений.

3.5 Политика управления инцидентами по ИБ

Для инцидентов в области ИБ должны выполнятся следующие мероприятия:

- немедленное реагирование на инцидент (защита системы);

- предоставление информации об инциденте руководителю структурного подразделения;

- анализ инцидента;

- восстановление работоспособности ИС, возобновление учебного процесса и бизнес процессов Университета;

- расследование причин инцидента, установление виновных;

- выработка корректирующих шагов (при необходимости) направленных на улучшение системы обеспечения ИБ;

3.6 Политика использования не корпоративных почтовых адресов для обмена служебными сообщениями по электронной почте

Работники не должны использовать внешнюю электронную почту как официальное средство связи. В тех случаях, когда нарушение настоящего положения повлекли за собой утечку конфиденциальной информации, несанкционированное копирование, модификацию, блокирование или уничтожение информации, а также в случаях создания ситуаций, которые потенциально могли бы привести к таким последствиям, необходимо выполнить мероприятия по управлению инцидентами в области ИБ, согласно политике.

3.7 Политика по физической безопасности в Университете

Все объекты критичные с точки зрения информационной безопасности (все сервера баз данных, телефонная станция, маршрутизатор, файервол) должны находиться в отдельном помещении, доступ в которое разрешен только работникам, имеющими соответствующее разрешение от Руководителя ЦИТ. Доступ в помещение посторонним лицам запрещен. Технический персонал, осуществляющий уборку помещения, ремонт оборудования, обслуживание кондиционера и т.п. может находится в помещении только в присутствии работников, имеющих право находится в помещении для выполнения своих должностных обязанностей.

3.8 Политика использования и управления внешними съемными носителями информации (все виды носителей) и регламент эксплуатации данных носителей

Внешние носители информации (USB флэш накопители, внешние жесткие диски, коммуникаторы, портативные компьютеры и т.д.) могут быть использованы с учетом следующих исключений:

- рекомендуется хранить информацию на зашифрованном внешнем съемном носителе;

- хранение служебной информации на личных внешних съемных носителях запрещено;

- запрещено передавать внешние съемные носители информации третьим лицам;

- запрещено оставлять внешние съемные носители информации без присмотра.

3.9 Правила доступа к сети Интернет

Доступ к развлекательным, вредоносным сайтам, а также к социальным сетям может быть заблокирован по инициативе руководства университета. При работе в корпоративной сети Университета и сети Интернет работникам запрещается:

- рассылать информацию коммерческого характера (SPAM);
- скачивать и устанавливать на компьютер программное обеспечение не входящее в список разрешенного к использованию;
- посещать интернет-ресурсы, не имеющие непосредственного отношения к работе и выполнению служебных обязанностей;
- осуществлять подписку на рассылку информации непроизводственного характера;
- сообщать адрес электронной почты в непроизводственных целях;
- использовать Интернет для получения материальной выгоды или непроизводственных целей, в том числе осуществляя торговлю через Интернет.

3.10 Политика удаленного доступа

Удаленный доступ к ИС через сеть Интернет или каналы связи, не находящиеся под контролем университета, должен быть защищен посредством использования технологии VPN. Используемые в университете средства реализации технологии VPN должны обеспечивать выполнение следующих требований:

- наличие уникального идентификатора у каждого пользователя;
- шифрование среды передачи данных;
- при необходимости проверка соответствия конфигурации пользовательских устройств, требованиям корпоративных политик;
- использование защищенных протоколов передачи данных.

3.11 Политика межсетевого экранирования

В Университете должны быть реализованы межсетевые экраны, которые классифицируются по следующим признакам:

- по исполнению (аппаратно-программный и программный);
- по используемой технологии (контроль состояния протокола, на основе модулей посредников (proxy)). Конфигурация межсетевого экрана должна быть полностью формализована. Межсетевые экраны должны управлять всем входящим и исходящим трафиком.

4. ПЕРЕСМОТР, ВНЕСЕНИЕ ИЗМЕНЕНИЙ, ХРАНЕНИЕ И РАССЫЛКА.

4.1 Пересмотр Политики ИБ

4.1.1 Развитие, пересмотр и оценку Политика ИБ осуществляет Руководитель ЦИТ на основе ежегодного анализа и оценки рисков ИБ.

4.1.2 Пересмотр Политики ИБ производится в целях:

- усовершенствования целей и мер контроля ИБ;
- усовершенствования подхода к управлению ИБ и бизнес-процессами университета;
- улучшения распределения ресурсов и/или обязанностей.

4.1.3 Политика ИБ должно пересматриваться в соответствии с изменениями, влияющими на основу первоначальной оценки риска, путем выявления существенных инцидентов нарушения ИБ, появления новых уязвимостей или изменения организационной/технологической инфраструктуры, изменении основных характеристик бизнес-процессов университета.

4.1.4 В случае появления существенных изменений в технологиях, обеспечивающих ИБ, в целях обеспечения конфиденциальности, целостности, доступности информации, а также адекватности и эффективности применяемых мер ИБ.

4.1.5 В случае возникновения дополнительных замечаний и предложений со стороны внутренних и внешних пользователей к изменениям норм Политика ИБ данные предложения анализируются Руководитель ЦИТ и при необходимости вносятся для утверждения.

4.1.6 Руководством университета может инициироваться независимый пересмотр Политика ИБ. Такой пересмотр проводится лицом, не имеющим прямого отношения к пересматриваемой области безопасности, например, функция внутреннего аудита осуществляется независимым менеджером или организацией третьей стороны, специализирующейся на таких пересмотрах.

4.1.7 Политика ИБ должно быть пересмотрено после проведения анализа и оценки рисков ИБ для университета, по итогам которых, с учетом исправления выявленных недостатков необходима ее актуализация.

4.1.8 Пересмотр Политика ИБ должен осуществляться в соответствии с руководством по реализации Государственного стандарта Республики Казахстан.

РАЗРАБОТАНО:

Руководитель центра
информационных технологий  Кушеккалиев А.Н.

СОГЛАСОВАНО:

Директор департамента
по стратегическому
развитию и инновациям  Имашев Э.Ж.

Член Правления-Проректор
по академическим вопросам  Кайсагалиева Г. С.