Политика
информационной безопасности НАО «Карагандинский технический университет имени Абылкаса Сагинова»

Обозначения и сокращения

ЭЦП – электронно-цифровая подпись
АРМ – автоматизированное рабочее место
ИС – информационная система
ИБ – информационная безопасность
ОСБ – отдел собственной безопасности
ДОТ– департамент обеспечения трансформации
МЭ – межсетевой экран
НСД – несанкционированный доступ
ОС – операционная система
ПДн – персональные данные
ПО – программное обеспечение
СЗИ – средства защиты информации
СКЗИ – средства криптографической защиты информации
Суперпользователь – администратор ИС, имеющий право на выполнение всех без исключения операций

Введение

Политика информационной безопасности Университета (далее – Политика) разработана в соответствии с требованиями действующего законодательства и нормативных актов Республики Казахстан. При разработке данного документа использовались:

от 24 ноября 2015 года № 418-V	Закон Республики Казахстан «Об информатизации»
от 5 июля 2004 года № 567-II (с изменениями и дополнениями по состоянию на 10.01.2022 г.)	Закон Республики Казахстан «О связи»
от 16 ноября 2015 года № 401-V (с изменениями и дополнениями по состоянию на 02.03.2022 г.)	Закон Республики Казахстан «О доступе к информации»
от 20 декабря 2016 года № 832	Единые требования в области информационно коммуникационных технологий и обеспечения информационной безопасности, утвержденные постановлением Правительства Республики Казахстан
	Международные стандарты в области информационной безопасности ISO/IEC 27001 Information technology – Code of practice for information security management, ISO/IEC 27002 Information technology - Security techniques - Code of practice for information security management

Предметом настоящего документа является:
-порядок доступа к информационным системам;
-сетевая безопасность;
-локальная безопасность;
-физическая безопасность (доступ в помещения);
-обеспечение защиты персональных данных;
-дублирование, резервирование и хранение информации;
-ответственность за соблюдение положений Политики ИБ

Общие положения

1. Цели и задачи

Концептуальная схема информационной безопасности Университета направлена на защиту его информационных активов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации и обеспечение нормального функционирования технологических процессов.

Направление информационной безопасности создано в отделе собственной безопасности со следующими задачами и функциями:

– разработка и совершенствование нормативно-правовой базы обеспечения информационной безопасности;

– выявление, оценка и прогнозирование угроз информационной безопасности;

– организация технической защиты информации, участие в проектировании систем защиты;

– проведение периодического контроля состояния ИБ, учет и анализ результатов с выработкой решений по устранению уязвимостей и нарушений;

– контроль за использованием закрытых каналов связи и ключей с цифровыми подписями;

– организация плановых проверок режима защиты, и разработка соответствующей документации, анализ результатов, расследование нарушений;

– разработка и осуществление мероприятий по защите персональных данных;

– организация взаимодействия со всеми структурами, участвующими в их обработке, выполнение требований законодательства к информационным системам персональных данных, контроль действий операторов, отвечающих за их обработку.

2. Организационно-правовой статус сотрудников информационной безопасности:

- сотрудники имеют право беспрепятственного доступа во все помещения, где установлены технические средства с Информационными системами, право требовать от руководства подразделений и администраторов ИС прекращения автоматизированной обработки информации, персональных данных, при наличии непосредственной угрозы защищаемой информации;

- имеют право получать от пользователей и администраторов необходимую информацию по вопросам применения информационных технологий, в части касающейся вопросов информационной безопасности;

- главный специалист по ИБ имеет право проводить аудит действующих и вновь внедряемых ИС, ПО, на предмет реализации требований защиты и обработки информации, соответствию требований законодательства, запрещать их эксплуатацию,

если не отвечают требованиям или продолжение эксплуатации может привести к серьезным последствиям в случае реализации значимых угроз безопасности;

-сотрудники имеют право контролировать исполнение утвержденных нормативных и организационно-распорядительных документов, касающихся вопросов информационной безопасности.

Область действия

Требования настоящей Политики распространяются на всех сотрудников Университета (штатных, временных, работающих по контракту и т.п.).

Положения настоящей Политики применимы для использования во внутренних нормативных и методических документах, а также в договорах с контрагентами.

Порядок доступа пользователей к информационным системам, в которых обрабатывается информация конфиденциального характера

Управление доступом к информационным системам реализовано с помощью штатных средств (операционных систем MS Windows Server, Linux и используемых ими СУБД) в целях идентификации и проверки подлинности субъектов доступа при входе в ИС, а также для их регистрации входа (выхода) в систему (из системы).

Все действий пользователей ИС регистрируются в журналах событий системного и прикладного ПО. Данные электронные журналы доступны для чтения, анализа и резервного копирования только администратору соответствующего ПО, который несет персональную ответственность за полноту и точность отражения в журнале имевших место событий. Он же, по запросу, выборочно передает данные из журналов сотруднику ИБ ДОТ.

При необходимости сотруднику ИБ ДОТ предоставляется административный доступ к серверам и базам данных по служебной записке на имя директора ДОТ.

Запрещается доступ суперпользователей к серверам и базам данных под единой или предопределенной учетной записью.

Повышение привилегий администратором для ранее существовавших учетных записей или создание новых административных групп согласовывается с сотрудником ИБ ДОТ.

Любой доступ к базам данных ИС без фиксации в соответствующих журналах или лог-файлах запрещен.

В случае увольнения сотрудника, имеющего права суперпользователя, пароли доступа к серверам и базам данных меняются в тот же день.

Процедура внесения изменений в информационные системы разработчиками для обеспечения политики информационной безопасности университета:

Анализ требований безопасности:

1.1. Провести тщательный анализ требований безопасности, предъявляемых к информационным системам университета.

1.2. Определить критические области и потенциальные уязвимости, которые требуют немедленного внимания.

Планирование изменений:

2.1. На основе результатов анализа безопасности разработать подробный план внесения изменений.

2.2. Определить приоритеты и последовательность внедрения мер безопасности.

Разработка и тестирование:

3.1. Начать разработку необходимых изменений в информационных системах согласно утвержденному плану.

3.2. После завершения разработки провести всестороннее тестирование, чтобы гарантировать эффективность изменений и отсутствие ошибок.

Внедрение изменений:

4.1. После успешного тестирования развернуть изменения в производственной среде с соблюдением всех процедур развертывания.

4.2. Обеспечить создание резервных копий данных перед внесением изменений, чтобы предотвратить потерю информации.

Мониторинг и обслуживание:

5.1. После внедрения изменений обеспечить стабильную и безопасную работу информационных систем.

5.2. Реализовать механизмы мониторинга безопасности для оперативного обнаружения и предотвращения возможных угроз.

Оценка и доработка:

6.1. Периодически оценивать эффективность внесенных изменений и анализировать возможные слабые места.

6.2. Производить необходимые корректировки и улучшения в соответствии с изменяющимися требованиями безопасности.

Эта процедура предназначена для обеспечения безопасности информационных систем университета и улучшения защиты данных от потенциальных угроз. Все внесенные изменения должны строго соответствовать политике информационной безопасности университета и быть регулярно оцениваемыми и обновляемыми с учетом развивающихся технологий и угроз безопасности.

Сетевая безопасность

2.1 Доступ из Интернет в сеть университета:

−доступ во внутреннюю сеть осуществляется только через настроенный межсетевой экран;

−доступ из вне периметра сети разрешен только по распоряжению директора ДОТ с согласованием у ответственного сотрудника ДОТ, по определенному порту и на определенное время;

−не допускается удаленный доступ в локальную сеть с использованием не персонифицированных, групповых и анонимных учетных записей;

−не допускается использование программ удаленного администрирования типа TeamViewer. Как исключение, по согласованию с сотрудником ИБ ДОТ возможно подключение для удаленной настройки ПО на ограниченное время. Настройка и конфигурация средств обнаружения вторжений, межсетевых экранов должны обеспечивать оперативное обнаружение несанкционированного доступа к ресурсам сети для принятия мер блокирования проникновения нейтрализации последствий.

При администрировании удаленного доступа к ресурсам корпоративной сети Университета предъявляются следующие требования:

−удаленный доступ пользователей к ресурсам и сервисам компьютерной сети университета обеспечивается на основе зарегистрированных персональных учетных записей, с использованием технологии VPN, других протоколов шифрования;

−доступ предоставляется сроком на 3 месяца, при необходимости продлевается с разрешения директора ДОТ;

−делается соответствующая запись в Журнале учета предоставления удаленного доступа;

−список сотрудников, которым предоставлен удаленный доступ поддерживается в актуальном состоянии и передается в ДОТ по запросу.

В целях обеспечения безопасности и нормального функционирования компьютерных сетей запрещается:

−самовольно подключать компьютерное оборудование (беспроводные точки доступа, маршрутизаторы, компьютеры и др.) к сети университета и присваивать ему сетевое имя и адрес без согласования с ДОТ;

−перемещать компьютеры между сетевыми розетками и другими коммуникационными устройствами без согласования с ДОТ;

−использовать информационные ресурсы университета для сетевых игр, распространения коммерческой рекламы; организации СПАМа.

−сканировать узлы сети неуполномоченными на то сотрудниками.

2.2. Средства защиты, маршрутизаторы и межсетевые экраны:

В Университете используется система межсетевого экранирования, которая реализует функции фиксации во внутренних журналах информации о проходящем IP-трафике, фильтрацию пакетов служебных протоколов, блокирования доступа не идентифицированного объекта.

Для анализа защищенности ИС сотрудниками ИБ ДОТ применяются специализированные программно-аппаратные средства – сканеры безопасности. Проводится выявление и анализ уязвимостей и несоответствия в настройках ОС, ПО, СУБД, сетевого оборудования. Выявленные уязвимости протоколируются и передаются в ДОТ для устранения в установленные сроки. Запрещается использовать ПО снятое с поддержки, имеющее уязвимости, с просроченными сертификатами.

Подсистема обнаружения вторжений, обеспечивает выявление сетевых атак на элементы ИС подключенные к сетям общего пользования и (или) международного обмена.

Функционал подсистемы реализуется программными и программно-аппаратными средствами, на межсетевых экранах. Администратор сети ведет протоколирование и регулярный мониторинг доступа, контролирует содержание трафика с использованием специализированного ПО, проводит анализ лог-файлов.

На межсетевом экране заводится лог-файл, куда записываются все обращения к ресурсам (попытки создания соединений). Доступ к лог-файлам имеют администратор сети и сотрудник ДОТ.

Анализ лог-файлов проводится с применением соответствующего ПО (анализатор логов) сотрудником ДОТ

Сотрудник ИБ ДОТ должен иметь независимый доступ к элементам системы защиты для контроля настроек конфигураций, просмотра системных журналов.

Доступ из одного сегмента сети в другой ограничивается и разделяется маршрутизаторами. Настройкой маршрутизаторов занимается отдел сетевого и системного администрирования.

Приобретение и установка средств и систем защиты ИС осуществляются по согласованию с сотрудником ИБ ДОТ.

Локальная безопасность

3.1 Антивирусная защита

Антивирусная защита предназначена для обеспечения антивирусной защиты серверов и АРМ пользователей Университета.

На каждом работающем компьютере, или сервере при вводе в эксплуатацию или после переустановки ОС сотрудниками ДОТ в обязательном порядке устанавливается и активируется антивирусная программа. Установка средств антивирусного контроля (в

том числе настройка параметров средств антивирусного контроля) на АРМ, серверах, осуществляется специалистами структурных подразделений и ДОТ в соответствии с руководствами по применению конкретных антивирусных средств.

Отключение или не обновление антивирусных средств не допускается. Установка и обновление антивирусных средств в организации контролируется централизованно ответственным сотрудником ДОТ.

Система обнаружения атак, встроенная в антивирусную программу, сохраняет информацию об атаках и подозрительной активности в лог-файлы, которые анализирует ответственный сотрудник ДОТ и высылает генерируемые системой отчеты о сетевых атаках и вирусной активности сотруднику ИБ ДОТ.

В случае массированной вирусной атаки сотрудники ДОТ определяют масштаб заражения, принимают меры к локализации, блокированию распространения, совместно с сотрудником ИБ ДОТ определяют источник заражения, характер действия и распространения вируса, нейтрализуют последствия атаки. При необходимости ставятся патчи и необходимые обновления ПО, закрывающие уязвимости, используемые вирусами.

3.2 Защита электронного документооборота.

Передача информации конфиденциального характера за периметр сети осуществляется только по защищенным каналам. Защищенные каналы строятся с использованием криптозащиты, на базе решений VipNet, VPN или других.

Криптографическая защита предназначена для исключения НСД к защищаемой информации в системе электронного документооборота Directum, при ее передаче по каналам связи сетей общего пользования и (или) международного обмена.

3.3 Разграничение прав доступа к информационным системам и системам хранения данных, защита от НСД

Для доступа к информационным системам университета сотрудник должен ввести логин и пароль.

При предоставлении доступа к ОС, приложениям ИС, реализуется принцип минимума привилегий доступа.

В целях защиты информации организационно и технически разделяются подразделения Университета, имеющие доступ и работающие с различной информацией (в разрезе ее конфиденциальности и смысловой направленности). Данная задача решается с использованием возможностей конкретных ИС, где в целях обеспечения защиты данных доступ и права пользователей ограничивается набором прав и ролей. В случае обработки информации конфиденциального характера права назначаются администратором ИС по ролевой матрице доступа, в соответствии с функциональными обязанностями, определяемыми должностью и по служебной записке руководителя подразделения, согласованной с сотрудником ДОТ.

Администратором ИС проводится анализ журналов доступа к ресурсам ИС, фиксируются попытки НСД, о которых докладывается ответственному сотруднику ИБ ДОТ.

Не допускается использование учетных записей уволенных сотрудников.

3.4 Использование электронной почты, сети Интернет

Не допускается распространять материалы, использование и распространение которых ограничено действующим законодательством РК.

Пересылка информации конфиденциального характера осуществляется только с использованием корпоративной почты.

Электронная почта на рабочем месте сотрудника используется только для служебной, и иной, предусмотренной должностными обязанностями переписки.

Логин и пароль к корпоративной электронной почте для сотрудников выдает ответственный сотрудник ДОТ по служебной записке на имя директора ДОТ, для студентов – по студенческому билету.

Запрещается открывать письма с подозрительными вложениями, с незнакомого адреса и.т.п., о получении подобных писем сообщается сотруднику ИБ ДОТ.

Запрещается публиковать информацию конфиденциального характера в социальных сетях, пересылать через системы мгновенного обмена сообщениями.

Запрещается использование облачных сервисов на рабочих местах сотрудников, обрабатывающих информацию конфиденциального характера.

Доступ через беспроводную сеть разрешается только к общедоступным ресурсам сети. Беспроводные точки устанавливают и администрируют сотрудники ДОТ.

Самостоятельно скачивать и устанавливать программное обеспечение разрешается только уполномоченным на то сотрудникам ДОТ.

Запрещается несогласованная с ДОТ установка роутеров WiFi.

Парольная политика

Длина пароля должна быть не менее 8 символов.

Пароль должен содержать как минимум одну цифру.

Пароль должен содержать как минимум одну букву в верхнем регистре.

Пароль должен содержать как минимум один специальный символ (например, !, @, #, $, %).

Запрещено использование очень простых и распространенных паролей (например, "password", "123456" и т.п.).

Пароли должны быть уникальными для каждого аккаунта, не используйте один и тот же пароль на разных сервисах или системах.

Регулярно обновляйте пароли.

Не позволяйте передавать пароли другим лицам или хранить их в незащищенной форме.

В случае подозрений на компрометацию пароля, немедленно измените его.

Пароль не должен содержать персональную информацию (имя, дата рождения и т.п.).

Физическая безопасность

Все объекты критичные с точки зрения информационной безопасности (сервера баз данных, маршрутизаторы) находятся в контролируемых зонах.

В контролируемых зонах университета ведется видеонаблюдение. На территории университета действует пропускной режим.

Обработка персональных данных

Все сотрудники Университета, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные внутренними нормативными документами правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности обработки ПДн.

Компетентность пользователей в области обеспечения ИБ достигается обучением правилам безопасной (с точки зрения ИБ) работы, осведомленности об источниках потенциальных угроз и периодическими проверками их знаний и навыков. Занятия с пользователями проводятся сотрудником ИБ ДОТ на регулярной основе не реже двух раз в год.

При допуске сотрудника к выполнению обязанностей связанных с обработкой персональных данных непосредственный начальник подразделения, в которое он поступает, организует ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, подает служебную записку директору ДОТ о предоставлении доступа к ИСПДн с указанием предполагаемой роли сотрудника.

Далее сотрудник проходит инструктаж у администратора безопасности ИСПДн, и расписывается об ознакомлении с Положением о защите персональных данных и Порядком обеспечения конфиденциальности при обработке персональных данных, получает у администратора ИСПДн логин и пароль к учетной записи с правами, согласно ролевой матрицы доступа.

Порядок работы с запросами на предоставление сведений по персональным данным определяется утвержденными локальными нормативными документами.

Сотрудники Университета должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица.

Сотрудникам, обрабатывающим ПДн, запрещается устанавливать любое программное обеспечение, подключать личные мобильные устройства и отчуждаемые незарегистрированные в ОСБ носители информации, а так же записывать на них защищаемую информацию, за исключением случаев, предусмотренных функциональными обязанностями.

Сотрудникам запрещается разглашать содержание защищаемой информации, которая стала им известна при работе с информационными системами Университета, третьим лицам, согласно Положения о защите персональных данных.

Дублирование, резервное копирование и хранение информации

Для обеспечения физической целостности данных, во избежание умышленного или неумышленного уничтожения или искажения защищаемой информации и конфигураций информационных систем организуется резервное копирование баз данных, конфигураций, файлов настроек, конфигурационных файлов.

Для обеспечения гарантированного восстановления особо важной информации, которая может быть утеряна вследствие аппаратных сбоев, воздействия вирусов-шифровальщиков производится ежедневное резервное копирование содержимого дисков. Данный процесс запускается автоматически с использованием инкрементального резервного копирования.

Ответственными за организацию резервного копирования, хранения копий и восстановления информации являются администраторы ИС, ответственные сотрудники ДОТ.

Еженедельно архивная копия базы данных ИСПДн дублируется сотрудником ИБ ДОТ с использованием соответствующего оборудования и программного обеспечения.

Ответственность за соблюдение положений Политики ИБ

Общее руководство обеспечением информационной безопасности осуществляет директор ДОТ.

Ответственным за поддержание положений настоящей Политики в актуальном состоянии, создание, внедрение и внесение изменений в процессы информационной безопасности является директор ДОТ.

Степень ответственности за нарушение требований локальных нормативных актов в области ИБ определяется в каждом конкретном случае

Руководители структурных подразделений, несут персональную ответственность за обеспечение ИБ в возглавляемых ими подразделениях, обязаны незамедлительно сообщать в ДОТ о всех инцидентах, связанных с нарушениями требований информационной безопасности.

Порядок пересмотра Политики ИБ

Пересмотр Политики информационной безопасности производится не реже одного раза в три года и имеет целью приведение в соответствие определенных Политикой защитных мер реальным условиям и текущим требованиям к защите информации.

Внеплановое внесение изменений в настоящую Политику может производиться по результатам анализа инцидентов ИБ, актуальности, достаточности и эффективности используемых мер обеспечения ИБ, результатам проведения внутренних аудитов ИБ и других контрольных мероприятий