НАО «Атырауский университет имени Х.Досмухамедова»

УТВЕРЖДАЮ
Председатель правления-Ректор
НАО «Атырауский университет
имени Х.Досмухамедова»
_____ С.Н.Идрисов
«22» 09 2025 г.

ПОЛИТИКА

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ НАО «АТЫРАУСКИЙ УНИВЕРСИТЕТ ИМЕНИ Х.ДОСМУХАМЕДОВА»

№ 246

Атырау 2025 год

	Должность	Ф.И.О.	Подпись	Дата
Разработал	Руководитель отдела технического, IT обслуживания и обеспечения информационной безопасности	А.И.Абилов		
Согласовано	Проректор по академическим вопросам	А.Е.Чукуров		
	Вице проректор (цифровой офицер)	Ж.У.Сулейменова		
	Руководитель офис мониторинга качества	Ж.Т.Кайшыгулова		
	Юрист	К.С.Куанов		19.09.2025

Содержание

1 Общие положения и область применения

1.1 Настоящая Политика информационной безопасности НАО «Атырауский университет имени Х.Досмухамедова» (далее - Политика) определяет цели, задачи, руководящие принципы и практические приемы в области обеспечения информационной безопасности НАО «Атырауский университет имени Х.Досмухамедова» (далее –Университет).

1.2 Под информационной безопасностью в настоящей Политике понимается состояние защищенности электронных информационных ресурсов, информационных систем и баз данных Университета от внешних и внутренних угроз, которые могут привести к материальному ущербу, нанести ущерб репутации или повлечь нанесение иного ущерба Университету, сотрудникам и обучающимся.

1.3 Политика входит в состав нормативно-справочной документации Университета, является обязательным для исполнения всеми сотрудниками Университета, а также доводиться до сведения иных третьих лиц, имеющих доступ к информационным системам и документам Университета.

1.4 НАО «Атырауский университет имени Х.Досмухамедова» принимает правовые, организационные и технические меры, необходимые для обеспечения исполнения законодательства о персональных данных, либо обеспечивает их принятие.

2 Обозначения

В настоящем Политики применяются следующие термины и определения:

- Мониторинг безопасности - постоянное наблюдение за объектом информатизации с целью выявления и идентификации событий информационной безопасности;
- Аутентификация – способ проверки подлинности пользователя при помощи комбинации различных параметров, в том числе генерации и ввода паролей или аутентификационных признаков (цифровых сертификатов, токенов, смарт-карт, генераторов одноразовых паролей и средств биометрической идентификации);
- Кибератака - это преднамеренное злонамеренное действие или комплекс действий, нацеленных на компьютерные системы, сети или устройства с целью получить несанкционированный доступ, украсть, повредить или уничтожить данные, нарушить работу систем, а также причинить финансовый, репутационный или иной ущер;
- Фаерволы (или брандмауэры, межсетевые экраны)- это системы защиты, которые выступают в роли "цифровой стены", контролируя и фильтруя сетевой трафик (данные), чтобы блокировать нежелательные или вредоносные сетевые подключения и защищать компьютерные сети и устройства от киберугроз;
- DDoS-атака (распределённая атака типа «отказ в обслуживании») — это кибератака, в которой множество устройств, часто объединённых в сеть (ботнет), одновременно отправляют огромный объём запросов на целевой сервер, сервис или сеть. Цель такой атаки — перегрузить ресурсы системы, чтобы сделать её недоступной для обычных пользователей и вызвать «отказ в обслуживании»;
- Вирус – это вид вредоносного программного обеспечения, который способен самостоятельно размножаться и распространяться на другие компьютеры, а также нарушать работу компьютера, повреждать данные и красть личную информацию пользователя;
- Вредоносное программное обеспечение (или malware) — это любое программное обеспечение, намеренно созданное для нанесения вреда

компьютерной системе, кражи личных данных, нарушения работы устройств или получения несанкционированного доступа к ним. К вредоносному ПО относятся вирусы, черви, трояны, шпионские программы (шпионы), программы-вымогатели (ransomware) и другие типы киберугроз

3 Сокращения

ИБ – Информационная безопасность
ПО – программное обеспечение
ИС – информационная система
СУИБ – система управления информационной безопасностью
РСП – Руководитель структурного подразделения
ОМК – Офис мониторинга качества

4 Нормативные ссылки

Политика разработана и устанавливает процедуры в соответствии с требованиями и рекомендациями следующих документов:

4.1 Закон Республики Казахстан от 24 ноября 2015 года № 418-V «Об информатизации»;

4.2 Закон Республики Казахстан от 16 ноября 2015 года № 401-V «О доступе к информации»;

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

4.4 СТ РК ISO/IEC 27001-2023 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования»;

4.5 СТ РК ISO/IEC 27005-2022 «Информационные технологии. Методы обеспечения безопасности. Менеджмент риска информационной безопасности»

4.6 Устав НАО «Атырауский университет им. Х.Досмухамедова», утвержденный приказом Председателя Комитета государственного имущества и приватизации Министерства финансов Республики Казахстан от 05 июня 2020 года № 350;

5 Задачи и фукнции ИБ

5.1 Настоящая Политика разработана с целью реализации комплекса организационных и технических мероприятий, направленных на защиту электронных информационных ресурсов, информационных систем, баз данных Университета от неавторизованного доступа, использования, раскрытия, искажения, изменения или уничтожения.

5.2 Задачи ИБ в университете включают в себя широкий спектр мероприятий и действий, направленных на обеспечение защиты информации и сетевой инфраструктуры:

- Защита конфиденциальности данных: Защита электронных информационных ресурсов, ИС, баз данных Университета, личных данных сотрудников, обучающихся, финансовой информации, исследований и других конфиденциальных данных от противоправных действий злоумышленников, потенциальных угроз, от несанкционированного доступа, утечек или кражи. Сохранение конфиденциальности информации, переданной в любой форме в процессе взаимодействия с заказчиками и партнерами Университета;
- Обеспечение целостности данных: Обеспечение целостности, недопущение несанкционированных изменений или повреждений электронных информационных ресурсов, ИС и баз данных Университета;

- Обеспечение доступности данных: Обеспечение доступа к ИС Университета для авторизованных пользователей в необходимом объеме для поддержания непрерывности учебных и административных процессов университета;
- Управление доступом: Разграничение доступа сотрудников к аппаратным, программным, информационным системам и информационным ресурсам Университета в зависимости от ролей и полномочий пользователей;
- Улучшение системы резервного копирования и восстановления данных: Обновление системы резервного копирования и восстановления данных для обеспечения надежной защиты и быстрого восстановления критически важных информационных ресурсов и баз данных;
- Защита от вредоносных программ и угроз: Предотвращение и минимизация последствий кибератак, таких как DDoS-атаки, вирусы, вредоносное ПО и другие угрозы ИБ. Развитие инфраструктуры СУИБ, включая установку и настройку современных средств защиты (файерволы, системы обнаружения вторжений, антивирусные решения, СКУД и т.д.);
- Обновление аппаратных средств: Замена устаревшего оборудования (серверов сетевых устройств, хранилищ данных) на более современные модели с улучшенными характеристиками безопасности;
- Улучшение программного обеспечения: Обновление операционных систем, баз данных, антивирусных программ и другого программного обеспечения до актуальных версий с последними обновлениями безопасности;
- Улучшение системы управления событиями: Развитие процессов и системы управления событиями (SIEM), которая позволяет собирать, анализировать и реагировать на события безопасности в реальном времени;
- Соответствие законодательству и регулированиям: Выполнение требований законодательства и нормативно-правовых актов Республики Казахстан в области информационной безопасности, разработка и совершенствование нормативно-правовой базы по информационной безопасности и защите персональных данных. Обеспечению;
- Обучение и осведомленность: Повышение уровня осведомленности среди сотрудников университета о методах защиты информации и правилах безопасного поведения в сети. Проведение обучающих сертификационных курсов для ИТ-специалистов и администраторов по информационной безопасности;
- Реагирование на инциденты: Разработка и реализация инструкций по реагированию на инциденты информационной безопасности. Минимизация потерь и восстановление программных и технических средств, а также информации, вследствие кризисных (нештатных) ситуаций. Расследование причин возникновения таких ситуаций и принятие мер по их предотвращению в будущем;
- Управление рисками: Оценка и управление рисками, связанными с информационной безопасностью, с учетом изменяющейся угрозной среды. Минимизация уровня рисков и снижение потенциального ущерба от аварий, непреднамеренных ошибочных действий сотрудников Университета, технических сбоев;
- Мониторинг безопасности: Мониторинг событий безопасности для раннего обнаружения потенциальных инцидентов и атак. Оценка текущего состояния технических средств и инфраструктуры, используемых для

обеспечения информационной безопасности. Выявление устаревших или недостаточных компонентов.

6 Принципы ИБ

6.1 Принципы информационной безопасности Университета представляют собой основные руководящие принципы и подходы, которые должны соблюдаться для обеспечения защиты информации от различных угроз:

6.2 Целостность: Этот принцип заключается в обеспечении точности, целостности и полноты информации. Информация должна быть защищена от несанкционированных изменений или модификаций, которые могут повлиять на её правильность или достоверность.

6.3 Конфиденциальность: Принцип конфиденциальности требует, чтобы доступ к конфиденциальной информации был предоставлен только авторизованным пользователям, которым это необходимо для выполнения их рабочих обязанностей или задач. Защита от несанкционированного доступа к информации играет ключевую роль в обеспечении конфиденциальности.

6.4 Доступность: Принцип доступности гарантирует, что информация и связанные с ней системы должны быть доступны для авторизованных пользователей в нужное время и место.

6.5 Аутентификация: Принцип аутентификации предполагает проверку подлинности пользователей, устройств или систем, которые пытаются получить доступ к информации или ресурсам. Это включает использование паролей, электронно-цифровой подписи и других методов для идентификации пользователей.

6.6 Авторизация: Принцип авторизации определяет права и привилегии доступа авторизованных пользователей к определенным ресурсам и данным.

6.7 Невозможность отказа в обслуживании: Принцип невозможности отказа в обслуживании гарантирует, что отправитель или получатель не может отрицать факт отправки или получения сообщения или данных. Это обеспечивается через использование аутентификации.

6.8 Разделение обязанностей: Принцип разделения обязанностей направлен на предотвращение возможности злоупотребления системными привилегиями за счет разделения ключевых функций между различными сотрудниками или группами.

6.9 Отделение данных: Принцип отделения данных обеспечивает разделение чувствительных данных от менее чувствительных или публичных данных, что помогает минимизировать риски утечек информации.

6.10 Персональная ответственность: в соответствии с этим принципом распределение прав и обязанностей сотрудников должно быть построено таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

6.11 Законность: Соблюдение требований законодательства Республики Казахстан в области информационной безопасности.

7 Практические приемы ИБ

7.1 Практические приемы информационной безопасности играют важную роль в защите информации, баз данных и информационных систем от различных угроз. Основные практические приемы, используемые в Университете:

- Обучение и осведомленность пользователей: Обучение пользователей основам безопасного поведения в интернете, фишинговым атакам, защите паролей и т.д.

- Управление доступом: Определение прав доступа, назначение ролей для авторизованных пользователей к электронным информационным ресурсам и ИС Университета;
- Обновление программного обеспечения: Регулярное обновление операционных систем, прикладного программного обеспечения и антивирусных программ до последних версий. Установка патчей безопасности для закрытия известных уязвимостей;
- Шифрование данных: Использование шифрования данных при их хранении и передаче через сеть. Реализация шифрования дисков и файлов для защиты конфиденциальных данных;
- Резервное копирование данных: Регулярное создание резервных копий данных и их хранение в защищенных местах;
- Мониторинг и регистрация событий: Использование системы мониторинга безопасности для обнаружения аномалий и потенциальных инцидентов безопасности. Анализ и регистрация событий для оперативного реагирования на угрозы;
- Физическая безопасность: Обеспечение физической безопасности серверных помещений. Использование систем контроля доступа и видеонаблюдения в Университете;
- Защита от вредоносного ПО и кибератак: Установка антивирусных программ и файерволов на всех компьютерах и серверах;
- Мониторинг безопасности: организационные и технические мероприятия, направленные на проведение мониторинга безопасного использования элетронных информационных ресурсов, информационных систем и баз данных Университета;
- Соблюдение нормативных требований: Выполнение всех требований по защите данных, установленных законодательством РК и внутренними документами Университета.

8 Права и ответственность

8.1 Все сотрудники обязаны использовать информационные ресурсы Университета квалифицированно, эффективно и придерживаясь правил этики;

8.2 Руководство университета обеспечивает необходимыми ресурсами для реализации политики информационной безопасности, включая финансирование обучения, внедрения необходимых технологий и средств защиты для ИБ;

8.3 Руководители структурных подразделений, несут персональную ответственность за ознакомление работников с политикой ИБ, обязаны незамедлительно сообщать ответственному за ИБ сотруднику Университета о всех инцидентах, подозрительных ситуациях связанных с нарушениями требований информационной безопасности;

8.4 Внедрение и поддержание политики безопасности является совместным усилием всех участников Университета, начиная от руководства и заканчивая пользователями информационных систем. Это помогает минимизировать риски утечек данных, нарушений безопасности и обеспечивает защиту ценной информации университета;

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

9 Заключительные положения

9.1 Настоящее Политика вступает в силу с момента его утверждения Председателем правления- ректором Университета.

9.2 Политика и изменения в него утверждаются приказом Председателя правления-ректора НАО «Атырауский университет имени Х.Досмухамедова»

9.3 Копию утвержденной Политики руководитель доводит до сведения работников подразделения под роспись в Листе ознакомления.

При приеме на работу в Университет или переводе на другую должность руководитель и работники должны быть ознакомлены с данной Политикой.

10 Порядок внесения изменений

10.1 В Политике могут вноситься изменения без предварительного уведомления субъектов персональных данных и прочих лиц. Актуальная редакция Политики размещается на корпоративном сайте (портале) НАО «Атырауский университет им. Х.Досмухамедова» по адресу: https://atyrau.edu.kz

10.2 Пересмотр Политики осуществляется по мере необходимости. За внесение изменении и дополнении в подлинник и учётные рабочие экземпляры несёт ответственность РСП.

10.3 Внесение изменении и дополнении в Политику осуществляет разработчик путем разработки нового документа и его согласования и утверждения в установленном порядке по разрешению проректора по академическим вопросам и оформляется документально за его подписью.

10.4 После утверждения Политики экземпляр-оригинал разработчик передает в ОМК для регистрации и хранения. За передачу в ОМК и доработку устаревших, утративших силу Политики несет ответственность РСП.

10.5 Утверждение нового варианта Политики является основанием для изъятия утративших силу вышеуказанных документов.

10.6 Замену утративших силу документов в ОМК осуществляет руководитель подразделения - разработчик Политики.

10.7 Основанием для внесения изменении и дополнении в Политику может являться:

- вновь введённые изменения и дополнения в нормативно-правовые акты, имеющие силу закона;
- приказы Председателя правления- ректора;
- перераспределение обязанностей между структурными подразделениями;
- реорганизация структурных подразделений;
- при изменении названия организации или структурного подразделения.

ЛИСТ ОЗНАКОМЛЕНИЯ

№ п/п	Ф.И.О. работника	Должность	Дата ознакомления	Подпись работника

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ

№ п/п	№ раздела, подраздела, пункта, подпункта документа СМК	Дата введения изменения	Основание (№, дата приказа)	Дата введения изменения	Подпись лица, внёсшего изменение