



НАО «Атырауский университет имени Х.Досмухамедова»

УТВЕРЖДАЮ

Председатель правления-Ректор
НАО «Атырауский университет
имени Х.Досмухамедова»

С.И.Идрисов

«23» 02 2026 г.



ПОЛОЖЕНИЕ

**ОБ ОТДЕЛЕ ТЕХНИЧЕСКОГО, ИТ ОБСЛУЖИВАНИЯ И ОБЕСПЕЧЕНИЯ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
НАО «АТЫРАУСКИЙ УНИВЕРСИТЕТ ИМЕНИ
Х.ДОСМУХАМЕДОВА»**

№ 119

Атырау 2026 год

	Должность	Ф.И.О.	Подпись	Дата
Разработал	Руководитель отдела технического, ИТ обслуживания и обеспечения информационной безопасности	А.И.Абилов		
Согласовано	Проректор по академическим вопросам	А.Е. Чукуров		
	Вице проректор (цифровой офицер)	Ж.У. Сулейменова		
	Руководитель офиса мониторинга качества	Ж.Т. Кайшыгулова		
	Юрист	К.С. Куанов		23.02.2026

 ATYRAU UNIVERSITY	НАО «Атырауский университет имени Халела Досмухамедова»	Издание: первое
	ОБ ОТДЕЛЕ ТЕХНИЧЕСКОГО, ИТ ОБСЛУЖИВАНИЯ И ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НАО «АТЫРАУСКИЙ УНИВЕРСИТЕТ ИМЕНИ Х.ДОСМУХАМЕДОВА»	Стр. 3 из 13

Содержание

1	Общие положения и область применения	4
2	Структура Отдела	4
3	Нормативные ссылки	5
4	Сокращения	6
5	Основные цели и задачи Отдела	6
6	Функции деятельности отдела	8
7	Принципы деятельности отдела	8
8	Практические приёмы работы Отдела	9
9	Ответственность	10
10	Порядок внесения изменений	10
11	Лист ознакомления	12
12	Лист регистрации изменений и дополнений	13

 ATYRAU UNIVERSITY	НАО «Атырауский университет имени Халела Досмухамедова»	Издание: первое
	ОБ ОТДЕЛЕ ТЕХНИЧЕСКОГО, ИТ ОБСЛУЖИВАНИЯ И ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НАО «АТЫРАУСКИЙ УНИВЕРСИТЕТ ИМЕНИ Х.ДОСМУХАМЕДОВА»	Стр. 4 из 13

1 Общие положения и область применения

- 1.1 Настоящее Положение определяет правовой статус, цели, задачи, функции, права и ответственность отдела технического, ИТ обслуживания и обеспечения информационной безопасности (далее — Отдел) НАО «Атырауский университет имени Халела Досмухамедова» (далее — Университет).
- 1.2 Отдел является структурным подразделением Университета и создаётся, реорганизуется и ликвидируется приказом Председателя Правления – Ректора Университета.
- 1.3 В своей деятельности Отдел руководствуется:
- Уставом Университета;
 - внутренними нормативными документами Университета;
 - настоящим Положением.
- 1.4 Отдел подчиняется непосредственно Проректору по академическим вопросам/ Вице проректору (цифровой офицер) (в соответствии с организационной структурой).
- 1.5 Структура и штатная численность Отдела утверждаются в установленном порядке. Положение входит в состав нормативно-справочной документации Университета, является обязательным для исполнения всеми сотрудниками Университета, а также доводится до сведения иных третьих лиц, имеющих доступ к информационным системам и документам Университета. Актуальная редакция Положения размещается на корпоративном сайте (портале) НАО «Атырауский университет имени Х.Досмухамедова» по адресу: <https://atyrau.edu.kz>
- 1.6 Положение и изменения в него утверждаются приказом Председателя Правления – Ректора НАО «Атырауский университет имени Х.Досмухамедова».

2 Структура Отдела

- 2.1 Структура Отдела формируется с учётом задач цифрового обеспечения деятельности Университета и утверждается приказом Председателя Правления – Ректора НАО «Атырауский университет имени Халела Досмухамедова».
- 2.1.1 В состав Отдела входят следующие структурные единицы:
- Сектор системного администрирования;
 - Сектор технической поддержки;
 - Сектор информационной безопасности.
- 2.1.2 Руководство Отделом осуществляет руководитель Отдела.
- 2.1.3 Ответственные лица секторов распределяются руководителем Отдела.
- 2.2 Сектор системного администрирования**
- 2.2.1 Сектор системного администрирования осуществляет:
- администрирование серверной инфраструктуры и систем хранения данных;
 - сопровождение корпоративных информационных систем и образовательных платформ;
 - администрирование локальной вычислительной сети и сетевого оборудования;
 - управление доменной инфраструктурой и учетными записями пользователей;
 - организацию резервного копирования и восстановления данных;
 - обеспечение функционирования корпоративной электронной почты и облачных сервисов.

 ATYRAU UNIVERSITY	НАО «Атырауский университет имени Халела Досмухамедова»	Издание: первое
	ОБ ОТДЕЛЕ ТЕХНИЧЕСКОГО, ИТ ОБСЛУЖИВАНИЯ И ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НАО «АТЫРАУСКИЙ УНИВЕРСИТЕТ ИМЕНИ Х.ДОСМУХАМЕДОВА»	Стр. 5 из 13

2.2.2 Сектор несёт ответственность за бесперебойную работу серверной и сетевой инфраструктуры Университета.

2.3 Сектор технической поддержки

2.3.1 Сектор технической поддержки осуществляет:

- приём и обработку заявок пользователей;
- установку, настройку и обслуживание компьютерной и периферийной техники;
- техническое сопровождение учебных аудиторий, лабораторий и административных подразделений;
- консультирование работников и обучающихся по вопросам эксплуатации ИТ-оборудования и программного обеспечения;
- участие в инвентаризации оборудования.

2.3.2 Сектор обеспечивает своевременное реагирование на инциденты и минимизацию простоев оборудования.

2.4 Сектор информационной безопасности

2.4.1 Сектор информационной безопасности осуществляет:

- реализацию организационных и технических мер по защите информации;
- контроль соблюдения требований законодательства Республики Казахстан в сфере защиты персональных данных;
- мониторинг инцидентов информационной безопасности;
- администрирование средств антивирусной защиты и систем разграничения доступа;
- проведение инструктажей и консультаций по вопросам информационной безопасности;
- участие в разработке внутренних нормативных документов по защите информации.

2.4.2 Сектор организует мероприятия по предотвращению утечки, несанкционированного доступа и утраты информации.

2.5 Взаимодействие секторов

2.5.1 Секторы осуществляют деятельность во взаимосвязи и координации между собой.

2.5.2 Распределение конкретных обязанностей между работниками секторов определяется руководителем Отдела.

3 Нормативные ссылки

3.1 Положение разработано и устанавливает процедуры в соответствии с требованиями и рекомендациями следующих документов:

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

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

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

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

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

 ATYRAU UNIVERSITY	НАО «Атырауский университет имени Халела Досмухамедова»	Издание: первое
	ОБ ОТДЕЛЕ ТЕХНИЧЕСКОГО, IT ОБСЛУЖИВАНИЯ И ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НАО «АТЫРАУСКИЙ УНИВЕРСИТЕТ ИМЕНИ Х.ДОСМУХАМЕДОВА»	Стр. 6 из 13

- 3.7 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;
- 3.8 Закон Республики Казахстан «Об образовании»;
- 3.9 Закон Республики Казахстан «О персональных данных и их защите»;
- 3.10 Иными нормативными правовыми актами Республики Казахстан;

4 Сокращения

- 4.1 В настоящем Положении применяются следующие термины и определения:
 ИБ – Информационная безопасность
 ПО – программное обеспечение
 ИС – информационная система
 СУИБ – система управления информационной безопасностью
 РСП – Руководитель структурного подразделения
 ОМК – Офис мониторинга качества

5 Основные цели и задачи Отдела

- 5.1 Обеспечение устойчивого, безопасного и бесперебойного функционирования информационно-коммуникационной инфраструктуры Университета, развитие цифровой образовательной среды и поддержка процессов цифровой трансформации.
- 5.2 Обеспечение бесперебойной работы серверного оборудования, сетевой инфраструктуры и пользовательских рабочих мест.
- 5.3 Администрирование корпоративных информационных систем, образовательных платформ и официального веб-ресурса Университета.
- 5.4 Обеспечение защиты персональных данных обучающихся и работников.
- 5.5 Организация резервного копирования и восстановления данных.
- 5.6 Техническая поддержка работников и обучающихся.
- 5.7 Участие в цифровой трансформации образовательного и управленческого процессов.
- 5.8 Настоящее Положение 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.
- 5.9 Задачи ИБ в университете включают в себя широкий спектр мероприятий и действий, направленных на обеспечение защиты информации и сетевой инфраструктуры:
- 5.10 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.

 ATYRAU UNIVERSITY	НАО «Атырауский университет имени Халелы Досмухамедова»	Издание: первое
	ОБ ОТДЕЛЕ ТЕХНИЧЕСКОГО, ИТ ОБСЛУЖИВАНИЯ И ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НАО «АТЫРАУСКИЙ УНИВЕРСИТЕТ ИМЕНИ Х.ДОСМУХАМЕДОВА»	Стр. 7 из 13

- 5.11 Обеспечение целостности данных: Обеспечение целостности, недопущение несанкционированных изменений или повреждений электронных информационных ресурсов, ИС и баз данных Университета.
- 5.12 Обеспечение доступности данных: Обеспечение доступа к ИС Университета для авторизованных пользователей в необходимом объеме для поддержания непрерывности учебных и административных процессов университета.
- 5.13 Управление доступом: Разграничение доступа сотрудников к аппаратным, программным, информационным системам и информационным ресурсам Университета в зависимости от ролей и полномочий пользователей.
- 5.14 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.
- 5.15 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 и т.д.).
- 5.16 Обновление аппаратных средств: Замена устаревшего оборудования (серверов, сетевых устройств, хранилищ данных) на более современные модели с улучшенными характеристиками безопасности.
- 5.17 Улучшение программного обеспечения: Обновление операционных систем, баз данных, антивирусных программ и другого программного обеспечения до актуальных версий с последними обновлениями безопасности.
- 5.18 Улучшение системы управления событиями: Развитие процессов и системы управления событиями (SIEM), которая позволяет собирать, анализировать и реагировать на события безопасности в реальном времени.
- 5.19 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.
- 5.20 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.
- 5.21 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.
- 5.22 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.
- 5.23 Мониторинг безопасности: Мониторинг событий безопасности для раннего обнаружения потенциальных инцидентов и атак. Оценка текущего состояния технических средств и инфраструктуры, используемых для обеспечения

 ATYRAU UNIVERSITY	НАО «Атырауский университет имени Халела Досмухамедова»	Издание: первое
	ОБ ОТДЕЛЕ ТЕХНИЧЕСКОГО, ИТ ОБСЛУЖИВАНИЯ И ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НАО «АТЫРАУСКИЙ УНИВЕРСИТЕТ ИМЕНИ Х.ДОСМУХАМЕДОВА»	Стр. 8 из 13

информационной безопасности. Выявление устаревших или недостаточных компонентов.

6 Функции деятельности отдела

6.1 Техническое обслуживание:

- установка, настройка и сопровождение компьютерной и периферийной техники;
- обслуживание серверного оборудования и систем хранения данных;
- модернизация технической инфраструктуры.

6.2 Администрирование информационных систем:

- сопровождение автоматизированных систем управления учебным процессом;
- управление учетными записями пользователей;
- администрирование корпоративной электронной почты;
- обеспечение функционирования локальной вычислительной сети и доступа к сети Интернет.

6.3 Информационная безопасность:

- реализация организационных и технических мер защиты информации;
- контроль доступа к информационным ресурсам;
- обеспечение антивирусной защиты;
- мониторинг инцидентов информационной безопасности.

6.4 Учёт и отчётность:

- ведение реестра ИТ-оборудования;
- участие в инвентаризации;
- подготовка аналитических и технических отчетов.

7 Принципы деятельности отдела

Деятельность Отдела осуществляется на основе следующих принципов:

- 7.1 **Законность.** Строгое соблюдение законодательства Республики Казахстан, внутренних нормативных документов Университета и требований в области образования, информатизации и защиты персональных данных.
- 7.2 **Непрерывность функционирования.** Обеспечение круглосуточной готовности информационно-коммуникационной инфраструктуры и минимизация простоев информационных систем.
- 7.3 **Информационная безопасность.** Приоритет защиты информации, предотвращение несанкционированного доступа, утечки, искажения или утраты данных.
- 7.4 **Конфиденциальность.** Обеспечение сохранности персональных данных обучающихся и работников, а также служебной информации.
- 7.5 **Системность и комплексность.** Реализация комплексного подхода к развитию и сопровождению ИТ-инфраструктуры с учетом стратегических целей Университета.
- 7.6 **Оперативность.** Своевременное реагирование на обращения пользователей и инциденты, принятие мер по быстрому восстановлению работоспособности систем.
- 7.7 **Профессионализм и компетентность.** Осуществление деятельности квалифицированными специалистами с постоянным повышением уровня профессиональной подготовки.

 ATYRAU UNIVERSITY	НАО «Атырауский университет имени Халела Досмухамедова»	Издание: первое
	ОБ ОТДЕЛЕ ТЕХНИЧЕСКОГО, ИТ ОБСЛУЖИВАНИЯ И ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НАО «АТЫРАУСКИЙ УНИВЕРСИТЕТ ИМЕНИ Х.ДОСМУХАМЕДОВА»	Стр. 9 из 13

- 7.8 Прозрачность и подотчетность.** Ведение установленной отчетности, документирование процессов и обеспечение контроля за результатами деятельности Отдела.
- 7.9 Развитие и инновационность.** Внедрение современных цифровых технологий и участие в реализации программ цифровой трансформации Университета.
- 8 Практические приёмы работы Отдела**
- 8.1 Планирование и организация работы**
- Составление ежемесячных и квартальных планов технического сопровождения и обновления ИТ-инфраструктуры.
 - Распределение задач между секторами: системного администрирования, технической поддержки и информационной безопасности.
 - Ведение календаря профилактических работ и плановых обновлений программного обеспечения.
- 8.2 Обработка заявок пользователей**
- Приём и регистрация всех обращений через единый портал или электронную почту службы поддержки.
 - Категоризация инцидентов по уровню срочности и влияния на учебный процесс.
 - Назначение ответственных сотрудников и контроль сроков выполнения.
- 8.3 Техническое обслуживание**
- Периодическая проверка и профилактическое обслуживание серверов, рабочих станций и сетевого оборудования.
 - Регулярное обновление операционных систем и программного обеспечения с учетом рекомендаций производителей.
 - Проверка и замена изношенных комплектующих и расходных материалов.
- 8.4 Администрирование информационных систем**
- Настройка и поддержка учетных записей пользователей, прав доступа и групповых политик.
 - Мониторинг работы серверов и сетевых сервисов.
 - Проведение резервного копирования и проверка восстановления данных.
- 8.5 Обеспечение информационной безопасности**
- Регулярное сканирование сети на наличие угроз и уязвимостей.
 - Контроль антивирусной защиты, фаерволов и систем фильтрации.
 - Проведение инструктажей для сотрудников и студентов по безопасному использованию информационных ресурсов.
- 8.6 Методическая и консультационная поддержка**
- Консультирование преподавателей и сотрудников по использованию цифровых образовательных ресурсов и офисных приложений.
 - Проведение семинаров и тренингов по новым ИТ-системам и цифровым инструментам.
 - Составление руководств и памяток для пользователей.
- 8.7 Контроль и отчетность**
- Ведение журналов регистрации работ, инцидентов и выполненных заявок.
 - Составление ежемесячных и квартальных отчетов о состоянии ИТ-инфраструктуры и выполненных работах.
 - Анализ проблемных зон и подготовка предложений по оптимизации работы Отдела.

 ATYRAU UNIVERSITY	НАО «Атырауский университет имени Халела Досмухамедова»	Издание: первое
	ОБ ОТДЕЛЕ ТЕХНИЧЕСКОГО, IT ОБСЛУЖИВАНИЯ И ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НАО «АТЫРАУСКИЙ УНИВЕРСИТЕТ ИМЕНИ Х.ДОСМУХАМЕДОВА»	Стр. 10 из 13

9 Ответственность

- 9.1 Отдел и его сотрудники несут ответственность в соответствии с законодательством Республики Казахстан за:
- 9.1.1 Нарушение требований по защите персональных данных;
 - 9.1.2 Утрату, искажение либо разглашение информации;
 - 9.1.3 Ненадлежащее исполнение должностных обязанностей.
 - 9.1.4 Все сотрудники обязаны использовать информационные ресурсы Университета квалифицированно, эффективно и придерживаясь правил этики.
 - 9.1.5 Руководство университета обеспечивает необходимыми ресурсами для реализации политики информационной безопасности, включая финансирование обучения, внедрения необходимых технологий и средств защиты для ИБ.
 - 9.1.6 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.
 - 9.1.7 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.
 - 9.1.8 Степень ответственности за нарушение требований локальных нормативных актов в области ИБ определяется в каждом конкретном случае.
 - 9.1.9 Копию утвержденного Положения руководитель доводит до сведения сотрудников подразделения под роспись в Листе ознакомления.

10 Порядок внесения изменений

- 10.1 Настоящее Положение вступает в силу со дня утверждения приказом Председателя Правления – Ректора Университета.
- 10.2 Изменения и дополнения в настоящее Положение вносятся приказом Председателя Правления – Ректора Университета.
- 10.3 Пересмотр Положение осуществляется по мере необходимости. За внесение изменения и дополнения в подлинник и учётные рабочие экземпляры несёт ответственность РСП.
- 10.4 Внесение изменения и дополнения в Положение 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.
- 10.5 После утверждения Положение экземпляр-оригинал разработчик передает в ОМК для регистрации и хранения. За передачу в ОМК и доработку устаревших, утративших силу Положение несет ответственность РСП.
- 10.6 Утверждение нового варианта Положение является основанием для изъятия утративших силу вышеуказанных документов.
- 10.7 Замену утративших силу документов в ОМК осуществляет руководитель подразделения - разработчик Положение.
- 10.8 Основанием для внесения изменения и дополнения в Положение может являться:

 ATYRAU UNIVERSITY	НАО «Атырауский университет имени Халела Досмухамедова»	Издание: первое
	ОБ ОТДЕЛЕ ТЕХНИЧЕСКОГО, IT ОБСЛУЖИВАНИЯ И ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НАО «АТЫРАУСКИЙ УНИВЕРСИТЕТ ИМЕНИ Х.ДОСМУХАМЕДОВА»	Стр. 11 из 13

- 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.

