МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РЕСПУБЛИКИ КАЗАХСТАН

ТОО «Иностранное учебное заведение «UNIVERSITY OF INNOVATION AND TECHNOLOGY»

«Утверждено»
Провост «University of Innovation and Technology»
Нуланов Ш.Н.
«4» апреля 2026 г.
На основании решения УС

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ТОО «Иностранное учебное заведение «University of Innovation and Technology»

Алматы, 2026

1. Общие положения

1.1. Обеспечение информационной безопасности ИТ-инфраструктуры университета от случайных или направленных атак, а также образовательных материалов и иной информации ограниченного доступа в условиях широкой доступности Интернета является одной из важных задач современного университета. В современных условиях информационные ресурсы являются стратегическим активом. Нарушение их конфиденциальности, целостности и доступности может привести к репутационным, финансовым и правовым рискам

1.2. Настоящая Политика информационной безопасности (далее - Политика) определяет основы обеспечения информационной безопасности, цели, задачи, принципы и меры по защите информации и информационных систем ТОО «Иностранное учебное заведение «University of Innovation and Technology» (далее - Университет).

1.3. Политика разработана в соответствии с законодательством Республики Казахстан Законом Республики Казахстан «Об информатизации» № 418-V от 24 ноября 2015 года, иными законодательными актами в сфере информационной безопасности, международными стандартами в области информационной безопасности (в т.ч. ISO/IEC 27001) и внутренними требованиями Университета.

1.4. Политика обязательна для исполнения всеми сотрудниками, обучающимися, партнёрами, имеющими доступ к информационным ресурсам организации.

2. Термины и определения

• информатизация - организационный, социально-экономический и научно-технический процесс, направленный на автоматизацию деятельности субъектов информатизации;

• объекты информатизации - электронные информационные ресурсы, программное обеспечение, интернет-ресурс и информационно - коммуникационная инфраструктура;

• информационная безопасность в сфере информатизации (далее - информационная безопасность) - состояние защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз;

• информационная система - организационно-упорядоченная совокупность информационно-коммуникационных технологий, обслуживающего персонала и технической документации, реализующих определенные технологические действия посредством информационного взаимодействия и предназначенных для решения конкретных функциональных задач;

• информационно-коммуникационная инфраструктура - совокупность объектов информационно-коммуникационной инфраструктуры, предназначенных для обеспечения функционирования технологической среды

в целях формирования электронных информационных ресурсов и предоставления доступа к ним;

• аудит информационной системы - независимое обследование информационной системы в целях повышения эффективности ее использования;

• объекты информационно-коммуникационной инфраструктуры - информационные системы, технологические платформы, аппаратно - программные комплексы, серверные помещения, центры обработки данных, сети телекоммуникаций, а также системы обеспечения информационной безопасности и бесперебойного функционирования технических средств;

• информационно-коммуникационные технологии - совокупность методов работы с электронными информационными ресурсами и методов информационного взаимодействия, осуществляемых с применением аппаратно-программного комплекса и сети телекоммуникаций;

• угроза информационной безопасности - совокупность условий и факторов, создающих предпосылки к возникновению инцидента информационной безопасности;

• мониторинг событий информационной безопасности - постоянное наблюдение за объектом информатизации с целью выявления и идентификации событий информационной безопасности;

• событие информационной безопасности - состояние объектов информатизации, свидетельствующее о возможном нарушении существующей политики безопасности либо о прежде неизвестной ситуации, которая может иметь отношение к безопасности объектов информатизации;

• инцидент информационной безопасности - отдельно или серийно возникающие сбои в работе информационно-коммуникационной инфраструктуры или отдельных ее объектов, создающие угрозу их надлежащему функционированию и (или) условия для незаконного получения, копирования, распространения, модификации, уничтожения или блокирования электронных информационных ресурсов;

• средство защиты информации - программное обеспечение, технические и иные средства, предназначенные и используемые для обеспечения защиты информации;

• многофакторная 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.

3. Цели и задачи

Целью Политики является создание и поддержание системы защиты информации, гарантирующей ее безопасное использование.

Задачи:

- обеспечение конфиденциальности, целостности, непрерывности и доступности информации;

- предотвращение несанкционированного доступа, модификации или уничтожения данных;

- обеспечение устойчивости бизнес-процессов и образовательной деятельности;

- формирование культуры безопасного обращения с информацией;

- выявление и минимизация рисков;

- защита персональных данных, коммерческой и служебной информации.

4. Область применения

4.1. Действие Политики распространяется на:

- информационные системы, базы данных, локальные и облачные сервисы;

- компьютерное и сетевое оборудование;

- мобильные устройства и съемные носители;

- печатные и электронные документы;

- персональные данные сотрудников, обучающихся и партнеров.

5. Основные принципы информационной безопасности

• Законность - соблюдение законодательства РК в области защиты информации и персональных данных;

• Системность - охват всех процессов и подразделений;

• Непрерывность - постоянное совершенствование мер информационной безопасности;

• Целостность - защита данных от искажений, потерь и несанкционированных изменений;

• Доступность - своевременный доступ к информации для выполнения служебных обязанностей;

• Конфиденциальность - доступ к информации предоставляется только уполномоченным лицам либо предоставление прав только по необходимости;

• Ответственность - закрепление обязанностей и полномочий.

6. Объекты защиты

• Информационные системы и базы данных Университета;

•Персональные данные сотрудников, ППС и обучающихся Университета;

• Документы на бумажных и электронных носителях Университета;

• Технические средства и сети связи Университета;

• Репутация и имидж Университета.

7. Угрозы и риски

• Утечка и несанкционированное использование данных;

• Кибератаки (вирусы, фишинг, взлом)

• Технические сбои, отказ оборудования;

• Ошибки и халатность сотрудников;
• Внешние воздействия (пожары, стихийные бедствия).

8. Ответственность и роли

8.1. Ректор Университета утверждает Политику и обеспечивает ее реализацию.

8.2. Руководством Университета вводится система классификации данных (открытая, служебная, конфиденциальная).

8.3. Приказом ректора Университета назначается ответственное лицо - сотрудник Офиса технического обеспечения.

8.4. Офис технического обеспечения внедряет технические меры защиты, разрабатывает процедуру защиты информации, регламент доступа к информации, проводит регулярный мониторинг событий безопасности и регистрируют инциденты, осуществляют внутренние проверки и тестируют уязвимости, предоставляет отчетность руководству Университета по результатам аудита.

8.5. Руководители структурных подразделений контролируют соблюдение Политики на местах.

8.6. Сотрудники и обучающиеся обязаны соблюдать правила и немедленно сообщать о возможных инцидентах.

9. Меры защиты информации

Офис технического обеспечения принимает следующие меры защиты информации:

• использование паролей и многофакторной аутентификации;
• антивирусная защита, межсетевые экраны и системы обнаружения вторжений;
• шифрование каналов передачи данных и носителей;
• регулярное резервное копирование и тестирование восстановления;
• ограничение доступа на основе ролевой модели;
• обучение сотрудников правилам информационной безопасности.

10. Заключительные положения

10.1. Актуализация Политики информационной безопасности осуществляется руководством Университета и вступает в силу с момента утверждения ректором Университета.

10.2. Настоящая Политика действует до замены новым, но не более 3 лет. При необходимости в Политику информационной безопасности могут быть внесены изменения и дополнения с заменой на новое в случаях ребрендинга и реорганизации Университета.

10.3. Оригинал Политики хранится в Службе контроля качества, копия - в Офисе технического обеспечения.