



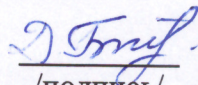
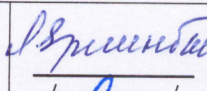
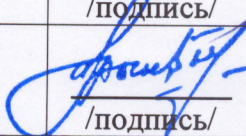
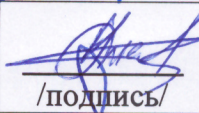
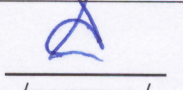
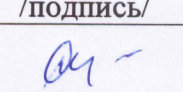
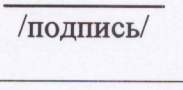
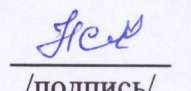
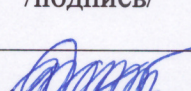
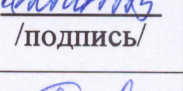
УТВЕРЖДЕНО
Решением Ученого совета
НАО «Таразского университета имени
М.Х.Дулати»
(Протокол № 5 от 25.12.2024 г.)

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НАО «ТАРАЗСКИЙ УНИВЕРСИТЕТ ИМЕНИ М.Х.ДУЛАТИ»

Регистрационный № 16

ТАРАЗ, 2024

ПРЕДИСЛОВИЕ

1. РАЗРАБОТЧИК:	Руководитель Центра проектного управления и цифровизации Толегенова Д.М.	 /подпись/	20.12.24 г.
2. ВВЕДЕНО:	Центр проектного управления и цифровизация		
3. ПЕРИОДИЧНОСТЬ ПРОВЕРКИ	3 года		
4. ВВЕДЕНО ВЗАМЕН	Впервые		
5. РАСПРОСТРАНЕНИЕ:	Факультетам, кафедрами и структурным подразделениям		
6. УТВЕРЖДЕНО И ВВЕДЕНО В ДЕЙСТВИЕ:	Решением Ученого совета НАО «Таразского университета имени М.Х.Дулати» (Протокол № 5 от 25.12.2024 г.)		
7. СОГЛАСОВАНО:	Член правления – проректор по академическим вопросам Еркинбаева Л.К.	 /подпись/	24.12.24 г.
	Член Правления - проректор по науке и цифровизации Орынбаев С.А.	 /подпись/	24.12.24 г.
	Член Правления - проректор по социально – культурному развитию Турлыбек А.Е.	 /подпись/	24.12.24 г.
	И.о. Член Правления - проректор по инфраструктуры Есмаханов Б.М.	 /подпись/	24.12.24 г.
	Член Правления – проректор по стратегическому развитию и интернационализации Есимова Ш.А.	 /подпись/	23.12.24 г.
	Руководитель центра технического сопровождения и IT поддержки Жаукашканов А.К.	 /подпись/	23.12.24 г.
	Руководитель управления стратегического развития Дарибаев Ж.Е.	 /подпись/	23.12.24 г.
	Руководитель отдела аккредитации, рейтинга и обеспечение качества Балкибаева Г.А.	 /подпись/	23.12.24 г.
	Руководитель Юридический службы Самбетов С.Т.	 /подпись/	20.12.24 г.

СОДЕРЖАНИЕ

1. Область применения.....	4
2. Нормативные ссылки.....	5
2.1 Нормативные документы.....	5
3. Основные термины и сокращения.....	6
3.1 Основные термины.....	6
3.2 Сокращения.....	6
4. Ответственность и полномочия.....	7
5. Общеположения.....	7
6. Цель политики.....	8
7. Требования и рекомендации.....	9
8. Планирование.....	11
9. Идентификация	12
10. Целостность информации.....	12
11. Доступность информации.....	14
12. Управление рисками.....	15
Приложение А. Лист ознакомления.....	18
Приложение Б. Лист регистрации изменений.....	19

1. ОБЛАСТЬ ПРИМЕНЕНИЯ

Настоящая «Политика информационной безопасности НАО «Таразский университет имени М.Х.Дулати» - определяет основные принципы, направления и требования по защите информации, является основой для обеспечения режима информационной безопасности и служит руководством при разработке соответствующих положений, правил и инструкций по обеспечению информационной безопасности университета.

Распространяется и обязательна к применению всеми структурными подразделениями и персоналом Университета, в которых осуществляется автоматизированная обработка информации, включая конфиденциальные сведения и/или персональные данные.

Требования также распространяются на другие организации и учреждения, взаимодействующие с Университетом в качестве поставщиков и потребителей информации и услуг на основе соответствующего договора/соглашения (SLA).

Требования распространяются на руководителей и работников всех структурных подразделений Университета и предназначены для обязательного соблюдения.

Политика распространяется на всех сотрудников, студентов, партнеров и третьих лиц, имеющих доступ к информационным системам Университета.

Сотрудники:

- Все постоянные, временные и контрактные сотрудники Университета.
- Те, кто работает на основе гражданско-правовых договоров.
- Лица, работающие по контракту или временно, включая стажеров и практикантов.

Студенты:

- Все зарегистрированные студенты, имеющие доступ к информационным системам Университета.
- Студенты бакалавриата, магистратуры и докторантуры.
- Студенты, участвующие в дистанционном обучении или обменных программах, имеющие удаленный доступ к информационным ресурсам.

Партнеры и третьи лица:

- Внешние организации, консультанты, подрядчики и любые другие лица, взаимодействующие с информационными системами Университета.
- Партнерские образовательные и научно-исследовательские учреждения.
- Внешние поставщики услуг и подрядчики, имеющие доступ к информационным ресурсам Университета по договорным обязательствам.

Политика охватывает все информационные ресурсы Университета, включая, но не ограничиваясь, компьютерные системы, сети, базы данных и документы.

Компьютерные системы:

- Серверы, используемые для хранения и обработки данных.
- Настольные компьютеры и ноутбуки, используемые сотрудниками и студентами.
- Мобильные устройства, такие как планшеты и смартфоны, имеющие доступ к информационным системам Университета.

Сети:

- Локальные сети (LAN), обеспечивающие внутреннее соединение устройств.
- Глобальные сети (WAN), соединяющие различные кампусы и удаленные объекты Университета.
- Беспроводные сети (Wi-Fi), обеспечивающие доступ к интернету и внутренним ресурсам Университета.
- Виртуальные частные сети (VPN), используемые для безопасного удаленного доступа.

Базы данных:

- Все базы данных, содержащие информацию, относящуюся к деятельности Университета.

- Учебные базы данных, содержащие информацию о студентах и образовательных программах.
- Научно-исследовательские базы данных, включающие результаты исследований и публикации.
- Административные базы данных, содержащие информацию о сотрудниках и операциях Университета.

Документы:

- Физические документы, содержащие конфиденциальную информацию, такие как контракты, соглашения и официальные документы.
- Электронные документы, хранящиеся на серверах, рабочих станциях и в облачных хранилищах.
- Документы, создаваемые и обрабатываемые в рамках учебной и научно-исследовательской деятельности, а также административные документы.

2. НОРМАТИВНЫЕ ССЫЛКИ

2.1 Нормативные документы

При разработке настоящей политики информационной безопасности были использованы следующие нормативные документы:

Закон РК	Закон Республики Казахстан «О персональных данных и их защите» – определяет основные требования и правила в области обработки и защиты личных и персональных данных.
Закон РК	Закон Республики Казахстан «Об информатизации» – устанавливает основные правовые нормы, касающиеся использования информационных технологий, обеспечения безопасности информационных систем и развития электронного правительства.
Постановление РК	Постановление Республики Казахстан «Об утверждении требований к обеспечению информационной безопасности» – определяет обязательные требования по организации мер информационной безопасности в государственном и частном секторах.
Постановление РК	Постановление Правительства Республики Казахстан №832 от 20.12.2016 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности» – устанавливает единые требования в области информационной безопасности и информационно-коммуникационных технологий.
Стандарт	Стандарт ISO/IEC 27001 – международный стандарт по созданию и поддержанию системы управления информационной безопасностью
Стандарт	Стандарт ISO/IEC 27002 – руководство по управлению информационной безопасностью, включающее рекомендации по обеспечению информационной безопасности.
Кодекс РК	Уголовный кодекс Республики Казахстан – предусматривает юридическую ответственность за незаконный доступ к информационным системам и несанкционированное использование персональных данных.

3. ОСНОВНЫЕ ТЕРМИНЫ, СОКРАЩЕНИЯ И ОБОЗНАЧЕНИЯ

3.1 Основные термины

В настоящей Политике используются следующие термины и определения:

Информационная безопасность	состояние защищенности информации, при котором обеспечены ее конфиденциальность, целостность и доступность.
Конфиденциальность	свойство информации, заключающееся в ограничении доступа к ней определенных лиц.
Целостность	свойство информации, заключающееся в ее достоверности и неизменности в процессе ее обработки.
Доступность	свойство информации, заключающееся в возможности ее использования по назначению в требуемое время и в требуемом месте.
Угроза информационной безопасности	совокупность условий и факторов, создающих потенциальную или реальную опасность нарушения информационной безопасности.
Уязвимость информационной безопасности	недостаток или отсутствие необходимого уровня защищенности, который может быть использован для нарушения информационной безопасности.
Риск информационной безопасности	сочетание вероятности реализации угрозы информационной безопасности и величины возможного ущерба.
Процессы управления рисками	это набор последовательных действий, направленных на идентификацию, оценку и снижение рисков информационной безопасности.
Обновления	это изменения, внесенные в программное обеспечение или оборудование для исправления ошибок, устранения уязвимостей или добавления новых функций.

3.2 Сокращения

В настоящей Политике используются следующие сокращения:

Университет	НАО «Таразский университет имени М.Х. Дулати»;
ИБ	<i>Информационная безопасность</i> : состояние защищенности информации, при котором обеспечены её конфиденциальность, целостность и доступность.
СМЖ	<i>Система менеджмента качества</i> : система управления, включающая все процессы и процедуры для контроля и улучшения качества образовательных и исследовательских услуг Университета.
СИ	<i>Средства информатизации</i> : устройства и программное обеспечение, используемые для обработки, хранения и передачи информации.
VPN	<i>Виртуальная частная сеть</i> (Virtual Private Network): технология для безопасного удаленного доступа к внутренним сетям Университета.
SLA	<i>Договор об уровне обслуживания</i> (Service Level Agreement): соглашение, устанавливающее уровень качества предоставляемых Университетом услуг и взаимодействий с партнёрами.

ISMS	<i>Система управления информационной безопасностью</i> (Information Security Management System): комплексный подход к управлению и контролю информационной безопасности на уровне организации
------	---

4. ОТВЕТСТВЕННОСТЬ И ПОЛНОМОЧИЯ

4.1 Настоящий документ утверждается решением Ученого совета Таразского университета им. М.Х. Дулати.

4.2 Ответственность за внедрение требований настоящего политики несет Центр проектного управления и цифровизация.

4.3 Ответственность за соответствие настоящего положения требованиям стандарта СТУ 01 «Управление документированной информацией» несет разработчик документа.

4.4 Ответственность за организацию и координацию деятельности по выполнению конкретных этапов процесса, управления документацией и качества конечных результатов несут руководители подразделений, а также должностные лица, являющиеся участниками выполнения конкретного этапа.

4.5 Ответственность за сохранность и несанкционированное копирование настоящего документа, находящегося в подразделении, и утечку служебной информации несут руководители соответствующих подразделений.

4.6 Разработка, оформление, согласование и утверждение настоящего документа, а также внесение в него изменений должно производиться в соответствии с СТУ 01.

4.7 Ответственность за передачу подлинника на хранение в отдел аккредитации, рейтинга и обеспечения качества университета несет разработчик.

4.8 Учетные рабочие экземпляры настоящего положения рассылаются Центром проектного управления и цифровизация по факультетам, кафедрам и структурным подразделениям. Ответственность за тиражирование Политики несет директор издательства Университета.

4.9 Изменения, внесенные в документ СМК, должны быть зарегистрированы в «листе регистрации изменений».

4.10 Ответственность за хранение контрольного экземпляра настоящего Положения университета возлагается на руководителя отдела аккредитации, рейтинга и обеспечения качества.

4.11 В случае нарушения данной политики виновные привлекаются к ответственности по решению специально созданной комиссии.

5. ОБЩИЕ ПОЛОЖЕНИЯ

5.1. Настоящая Политика информационной безопасности НЕКОММЕРЧЕСКОГО АКЦИОНЕРНОГО ОБЩЕСТВА «ТАРАЗСКИЙ УНИВЕРСИТЕТ ИМЕНИ М.Х.ДУЛАТИ» (далее - Политика) разработана в соответствии с действующим законодательством Республики Казахстан, нормативными актами и другими внутренними положениями НЕКОММЕРЧЕСКОГО АКЦИОНЕРНОГО ОБЩЕСТВА «ТАРАЗСКИЙ УНИВЕРСИТЕТ ИМЕНИ М. Х. ДУЛАТИ» (далее - Университет).

5.2. В настоящей Политике применяется следующее определение конфиденциальной информации: «конфиденциальная информация» означает любую и всю информацию о персональных данных пользователей, данных в базах данных программных продуктов, а также любую информацию относительно деятельности Университета и её клиентов (клиентская база), знания, ноу-хау, коммерческая информация, ценообразование, которая каким-либо образом стала известна сотруднику в результате производственной деятельности.

5.3. Настоящая Политика предусматривает принятие необходимых мер в целях защиты информационных активов как материальных ценностей Университета от случайного или преднамеренного изменения, раскрытия или уничтожения, а также в целях соблюдения конфиденциальности, целостности и доступности информации, обеспечения процессов информационного взаимодействия с заказчиками и партнерами.

5.4. Ответственность за соблюдение информационной безопасности несет каждый сотрудник Университета. Сотрудник должен иметь своевременное и полное обеспечение информацией, необходимой ему для выполнения своих служебных обязанностей.

5.5. В настоящей Политике под термином «сотрудник» понимаются все сотрудники Университета, в том числе, работающие в Университете по договорам гражданско-правового характера. Применение настоящей Политики должно быть обусловлено в таком договоре.

5.6. Информационная безопасность является одним из важнейших аспектов деятельности Университета. Организация стремится обеспечить конфиденциальность, целостность и доступность информации, а также защиту от несанкционированного доступа, использования, раскрытия, изменения, уничтожения или потери данных.

5.7. Настоящая Политика должна быть доведена до сведения каждого сотрудника Университета в день заключения трудового договора.

6. ЦЕЛЬ ПОЛИТИКИ

6.1. Целями настоящей Политики являются:

- Сохранение конфиденциальной информации Университета.
- Обеспечение обучения и осведомленности сотрудников об информационной безопасности.
- Проведение регулярных проверок и аудитов системы информационной безопасности.
- Сохранение конфиденциальности информационных ресурсов Университета.
- Сохранение конфиденциальности информации, переданной в любой форме в процессе взаимодействия с заказчиками и партнерами Университета.
- Обеспечение доступа к информационным ресурсам Университета для поддержки бизнес деятельности.
- Повышение осведомленности пользователей в области рисков, связанных с информационными ресурсами Университета.
- Определение степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности в Университете.
- Обеспечение информационной безопасности систем и защиты данных в соответствии с международными стандартами ISO/IEC 27001, ISO/IEC 27002-2023.
- Соблюдение постановления Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности».

6.2. Руководители подразделений Университета должны обеспечить регулярный контроль за соблюдением положений настоящей Политики:

- Назначение ответственных лиц в каждом подразделении для контроля соблюдения политики информационной безопасности.
- Проведение регулярных совещаний и отчетов по вопросам информационной безопасности.
- Организация периодических проверок соблюдения информационной безопасности с последующим представлением отчета по результатам указанной проверки руководству Университета.

- Внедрение системы управления информационной безопасностью (ISMS) для координации и контроля мероприятий по защите информации.

7. ТРЕБОВАНИЯ И РЕКОМЕНДАЦИИ

7.1. Организационные меры

7.1.1. Назначение ответственного за ИБ:

- Назначить руководителя отдела информационной безопасности, ответственного за реализацию и контроль исполнения данной Политики.
- Определить обязанности и полномочия руководителя отдела ИБ, включая разработку и внедрение мер по защите информации.
- Создать комитет по информационной безопасности, включающий представителей различных департаментов, для координации усилий по защите информации.
- Определить регулярные встречи комитета для обсуждения текущих проблем и разработок в области ИБ.

7.1.2. Обучение и повышение осведомленности:

- Проводить регулярные тренинги и обучения для сотрудников и студентов по вопросам ИБ.
- Разработать учебные материалы и курсы по основам ИБ, ориентированные на различные категории пользователей.
- Разработать и распространять материалы по вопросам ИБ (брошюры, плакаты, электронные рассылки).
- Использовать различные каналы коммуникации для обеспечения осведомленности всех заинтересованных сторон.

7.1.3. Управление доступом:

- Обеспечить контроль доступа к информационным системам через использование аутентификации и авторизации.
- Внедрить многофакторную аутентификацию (MFA) для критически важных систем.
- Регулярно пересматривать и обновлять права доступа на основе изменений в должностных обязанностях сотрудников.
- Проводить периодические ревизии учетных записей и прав доступа.

7.2. Технические меры

7.2.1. Защита сети:

- Использовать межсетевые экраны (firewalls) для защиты периметра сети Университета.
- Настроить политики безопасности для фильтрации входящего и исходящего трафика.
- Развернуть системы обнаружения и предотвращения вторжений (IDS/IPS) для мониторинга сетевого трафика и выявления подозрительных действий.
- Регулярно обновлять сигнатуры и правила IDS/IPS для обеспечения их актуальности.
- Устанавливать и регулярно обновлять антивирусное программное обеспечение на всех компьютерах и серверах.
- Обеспечить автоматическое обновление антивирусных баз данных и проведение регулярных сканирований.

7.2.2. Шифрование:

- Применять шифрование для защиты конфиденциальной информации при ее передаче по сети и при хранении на носителях данных.
- Использовать протоколы защищенных соединений (SSL/TLS) для передачи данных.
- Обеспечить использование защищенных каналов связи (например, VPN) для удаленного доступа к информационным ресурсам Университета.
- Настроить VPN с использованием сильных алгоритмов шифрования и аутентификации.

7.2.3. Резервное копирование:

- Разработать и внедрить процедуры регулярного резервного копирования критической информации.
- Определить расписание и частоту выполнения резервных копий.
- Хранить резервные копии в нескольких физических и географически разнесенных местах.
- Обеспечить защищенное хранение резервных копий в удаленных центрах данных. Регулярно тестировать процедуры восстановления данных из резервных копий. Проводить тестовые восстановления данных для проверки работоспособности и актуальности резервных копий.

7.3. Управление инцидентами

7.3.1. Обнаружение инцидентов:

- Разработать процедуры для мониторинга и обнаружения инцидентов ИБ.
- Использовать автоматизированные системы мониторинга и анализа логов для выявления подозрительных действий.
- Использовать системы управления событиями и информацией безопасности (SIEM) для сбора и анализа логов.
- Настроить SIEM для корреляции событий и своевременного обнаружения инцидентов.

7.3.2. Реагирование на инциденты:

- Определить порядок действий в случае инцидента, включая уведомление ответственных лиц, расследование и устранение последствий.
- Разработать план реагирования на инциденты, включающий шаги по уведомлению, расследованию и устранению инцидентов.
- Назначить команду по реагированию на инциденты (CSIRT) и обеспечить ее необходимыми ресурсами и полномочиями.
- Обучить членов CSIRT методам реагирования на различные типы инцидентов и обеспечению взаимодействия с внешними организациями.

7.3.3. Восстановление после инцидентов:

- Обеспечить восстановление систем и данных после инцидентов ИБ для минимизации воздействия на деятельность Университета.
- Разработать процедуры восстановления систем и данных, включающие проверку целостности восстановленных данных.
- Проводить анализ инцидентов для выявления причин и разработки мер по их предотвращению в будущем.
- Проводить послебоевую оценку (post-incident review) для выявления слабых мест и улучшения мер ИБ.

7.4. Соответствие и аудит

7.4.1. Соответствие законодательству:

- Политика ИБ должна соответствовать действующему законодательству Республики Казахстан и международным стандартам.
- Регулярно обновлять Политику в соответствии с изменениями в законодательстве и нормативных актах.
- Обеспечить соблюдение требований нормативных актов и стандартов в области ИБ.
- Проводить обучение и инструктаж сотрудников по вопросам нормативных требований.

7.4.2. Аудит и контроль:

- Проводить регулярные внутренние и внешние аудиты для оценки эффективности мер ИБ и соответствия Политике.
- Назначить ответственных за проведение аудитов и определение частоты их проведения.
- Разрабатывать и внедрять план действий по устранению выявленных недостатков и несоответствий.
- Определить сроки и ответственных за выполнение корректирующих действий.

8. ПЛАНИРОВАНИЕ

8.1. Планирование мероприятий по информационной безопасности должно включать:

8.1.1. Определение ресурсов, необходимых для реализации мер ИБ:

- Оценка текущих и будущих потребностей в области информационной безопасности, включая технические, финансовые и человеческие ресурсы.
- Определение бюджета, необходимого для реализации мероприятий по информационной безопасности.
- Выделение и распределение ресурсов в соответствии с приоритетами и стратегическими целями Университета.

8.1.2. Разработка и утверждение плана мероприятий по улучшению ИБ:

- Разработка детального плана мероприятий, включающего конкретные шаги и действия по улучшению информационной безопасности.
- Включение в план мероприятий по внедрению новых технологий, обновлению программного обеспечения, обучению сотрудников и проведению аудитов.
- Утверждение плана мероприятий руководством Университета для обеспечения его официального статуса и обязательности выполнения.

8.1.3. Установление сроков выполнения мероприятий и ответственных лиц:

- Определение четких сроков для выполнения каждого мероприятия по информационной безопасности.
- Назначение ответственных лиц или групп, которые будут контролировать и выполнять мероприятия.
- Разработка системы отчетности и контроля за выполнением мероприятий, включающей регулярное предоставление отчетов руководству.

8.2. Планы мероприятий должны быть согласованы с руководством Университета и регулярно пересматриваться для учета изменений в законодательстве, технологиях и бизнес-процессах:

- Проведение регулярных встреч с руководством для обсуждения текущего состояния информационной безопасности и прогресса в реализации плана мероприятий.
- Пересмотр планов мероприятий на основе результатов аудитов, изменения законодательных требований, появления новых технологий и изменений в бизнес-процессах.
- Обеспечение гибкости планов мероприятий для адаптации к новым вызовам и изменениям в окружающей среде.

9. ИДЕНТИФИКАЦИЯ

9.1. Идентификация уязвимостей и угроз информационной безопасности должна проводиться на регулярной основе:

- Определение графика регулярных проверок для идентификации уязвимостей и угроз.
- Внедрение процедур для постоянного мониторинга информационных систем и сетей с целью выявления потенциальных уязвимостей и угроз.
- Обеспечение своевременного обновления используемых инструментов и методов для выявления новых уязвимостей и угроз.

9.2. Использовать инструменты и методики для оценки рисков ИБ, такие как анализ уязвимостей, тестирование на проникновение, аудит безопасности:

- Внедрение систем сканирования уязвимостей для регулярного анализа сетевых и программных уязвимостей.
- Проведение регулярного тестирования на проникновение (PenetrationTesting) для оценки защиты от возможных атак и выявления уязвимостей.
- Проведение аудитов безопасности, включающих оценку текущих мер защиты и их соответствия установленным стандартам и лучшим практикам.
- Использование методологий оценки рисков, таких как ISO/IEC 27005, для систематического анализа и управления рисками информационной безопасности.

9.3. Результаты идентификации уязвимостей и угроз должны документироваться и представляться руководству для принятия решений по устранению выявленных проблем:

- Создание подробных отчетов по результатам идентификации уязвимостей и угроз, включающих описание выявленных проблем, их потенциальные последствия и рекомендации по устранению.
- Представление отчетов руководству для принятия решений по реализации корректирующих и профилактических мер.
- Разработка плана действий по устранению выявленных уязвимостей и угроз, включая определение ответственных лиц и установление сроков выполнения.
- Регулярное обновление документации и отчетности в соответствии с новыми выявленными уязвимостями и угрозами, а также принятыми мерами по их устранению.

10. ЦЕЛОСТНОСТЬ ИНФОРМАЦИИ

10.1. Обеспечение целостности информации включает:

10.1.1. Использование методов и средств для защиты данных от несанкционированного изменения:

- Внедрение систем контроля доступа (Access Control) для обеспечения, что только авторизованные пользователи могут изменять данные.
- Использование криптографических методов для проверки целостности данных, таких как цифровые подписи и контрольные суммы (hashing).
- Внедрение систем защиты от несанкционированного изменения данных, включая системы обнаружения изменений (Change Detection Systems).

10.1.2. Внедрение контроля версий для критически важных данных и документов:

- Использование систем управления версиями (Version Control Systems) для отслеживания изменений в документах и данных.
- Обеспечение возможности отката к предыдущим версиям данных и документов в случае выявления несанкционированных или ошибочных изменений.
- Хранение истории изменений и обеспечение их доступности для аудита и анализа.

10.1.3. Регулярное проведение аудитов и проверок целостности данных:

- Планирование и проведение регулярных аудитов информационных систем и данных на предмет целостности.
- Использование автоматизированных инструментов для проверки целостности данных и выявления несоответствий.
- Документирование результатов аудитов и проверок и информирование руководства о выявленных проблемах и принятых мерах по их устранению.

10.2. Все изменения в системах и данных должны быть зафиксированы и задокументированы:

- Внедрение процедур регистрации изменений (Change Management), включающих обязательную фиксацию всех изменений в системах и данных.
- Создание и ведение журналов изменений (Change Logs) с указанием даты, времени, инициатора изменений и описания внесенных изменений.
- Обеспечение доступа к журналам изменений для аудита и анализа.

10.3. Внедрение мер по защите от внутренних и внешних угроз, включая злоумышленные действия и ошибки сотрудников:

- Разработка и внедрение процедур для мониторинга и выявления подозрительной активности внутри организации.
- Внедрение механизмов двухфакторной аутентификации (2FA) для повышения уровня безопасности при доступе к критически важным системам и данным.
- Обучение сотрудников принципам информационной безопасности, включая правила безопасного обращения с данными и реагирования на инциденты.
- Регулярное проведение внутреннего и внешнего тестирования на проникновение (Penetration Testing) для выявления и устранения уязвимостей в информационных системах.

11. ДОСТУПНОСТЬ ИНФОРМАЦИИ

11.1. Обеспечение доступности информации включает:

11.1.1. Разработку и внедрение мер по обеспечению непрерывности бизнес-процессов:

- Определение критически важных бизнес-процессов и разработка планов по обеспечению их непрерывности.
- Внедрение процедур для поддержания работы ключевых систем и сервисов в случае непредвиденных обстоятельств.
- Регулярное тестирование и обновление планов по обеспечению непрерывности бизнес-процессов.

11.1.2. Внедрение систем резервного копирования и восстановления данных:

- Разработка и внедрение политики резервного копирования данных, включая регулярное создание резервных копий.
- Определение критичных данных, подлежащих резервному копированию, и частоты их копирования.
- Хранение резервных копий в защищенных и географически разнесенных местах для предотвращения потери данных в случае катастроф.
- Регулярное тестирование процедур восстановления данных из резервных копий для обеспечения их работоспособности и актуальности.

11.1.3. Обеспечение отказоустойчивости критически важных систем:

- Внедрение мер для обеспечения высокой доступности и отказоустойчивости критических систем, включая использование кластерных технологий и репликации данных.
- Разработка и реализация стратегии обеспечения непрерывной работы серверов, сетевых устройств и других компонентов инфраструктуры.
- Регулярное проведение стресс-тестов для проверки готовности систем к работе в условиях повышенных нагрузок.

11.2. Планирование и проведение регулярных тренировок и тестирований планов восстановления после сбоев и катастроф:

- Разработка сценариев возможных сбоев и катастроф и проведение регулярных тренировок по их отработке.
- Оценка эффективности планов восстановления после каждого тестирования и внесение необходимых корректировок.
- Обучение сотрудников действиям в условиях сбоев и катастроф для обеспечения оперативного и правильного реагирования.

11.3. Обеспечение доступности информации для авторизованных пользователей в требуемое время и в требуемом месте:

- Внедрение систем мониторинга и управления доступом, обеспечивающих своевременный доступ к информации для авторизованных пользователей.
- Разработка процедур для быстрого восстановления доступа к информации в случае возникновения инцидентов.
- Обеспечение круглосуточной поддержки пользователей и оперативного разрешения проблем, связанных с доступом к информации.

Примеры мер по обеспечению доступности информации:

- Использование средств резервирования для файлов и баз данных.
- Развертывание систем в нескольких дата-центрах.
- Использование средств мониторинга и оповещения для систем исетей.

- Использование отказоустойчивых компонентов для систем исетей.
- Рекомендации по обеспечению доступности информации:
- Оценка рисков доступности. Организация должна оценить рискинарушения доступности информации и разработать меры по снижению этихрисков.
- Обучение сотрудников. Сотрудники организации должны бытьосведомлены о важности доступности информации и о методах ееобеспечения
- Регулярный мониторинг и аудит. Организация должна регулярно контролировать эффективность мер по обеспечению доступностиинформации

Примеры инцидентов, связанных с доступностью информации:

- Сбой системы или сети.
- Уничтожение или повреждение систем или сетей.
- Кибератака.
- Влияние инцидентов, связанных с доступностью информации:
- Финансовые убытки.
- Потеря репутации.
- Нарушение законодательства

12. УПРАВЛЕНИЕ РИСКАМИ

Таблица 12.1 – Анализ нежелательного события. Оценка «Вероятность»

Балл	Описание
1	Маловероятно (практически невозможно)
2	Достаточно вероятно
3	Вероятно
4	Очень вероятно

Таблица 12.2 - Анализ нежелательного события. Оценка «Серьезность»

Балл	Описание
1	Очень низкая (последствия нежелательного события незаметны для внешних сторон)
2	Средняя (единичные случаи недовольства потребителей; незначительные затраты на устранение последствий; отсутствие ущерба репутации университета)
3	Высокая (штрафные санкции, значительные затраты для устранения последствий. Недовольство заинтересованных сторон)
4	Катастрофичная (приостановка деятельности, потеря репутации)

Таблица 12.3 - Шкала по приемлемости риска

Серьезность	1	2	3	4
Вероятность				
1	1	2	3	4
2	2	4	6	8
3	3	6	9	12
4	4	8	12	16

Таблица 12.4 - Управление рисками

		Оценка риска	Мероприятия по	Ответственный	Сроки
--	--	--------------	----------------	---------------	-------

№	Риск/нежелательное событие	Описание влияния риска на деятельность/ процесс	Вероятность / частота наступления нежелательного события (В)	Серьезность/потенциальные или реальные последствия нежелательного события (С)	Оценка (В*С)	снижению риска (обработка риска)		исполнения
1	Потеря конфиденциальной информации	Утечка конфиденциальной информации может привести к репутационным потерям и финансовым штрафам	3	4	12	Внедрение строгой системы управления доступом, обучение сотрудников по вопросам ИБ	Руководитель отдела ИБ	До конца квартала
2	Вирусные атаки	Вирусные атаки могут привести к потере данных и снижению производительности системы	4	3	12	Установка антивирусного ПО, регулярное обновление, проверка антивирусных баз	IT-отдел	Ежеквартально
3	Нарушение целостности данных	Ошибки в данных могут привести к искажению информации, что влияет на принятие решений	2	3	6	Регулярное резервное копирование данных и настройка контроля целостности	Ответственный за данные	Ежемесячно
4	Недоступность критически важных систем	Отказ систем может повлиять на процессы учебной и административной деятельности	3	4	12	Разработка планов на случай ЧС, создание резервных копий и настройка резервных серверов	IT-отдел	Полугодие
5	Несанкционированный доступ к информации	Доступ посторонних к учебным данным или персональным данным студентов и сотрудников может привести к утечкам данных	3	4	12	Настройка многофакторной аутентификации, регулярное обновление паролей и контроль учетных записей	Руководитель отдела ИБ	Ежеквартально
6	Кибератаки на учебные порталы	Атаки могут привести к недоступности онлайн-курсов и материалов, прерыванию учебного процесса	3	3	9	Использование межсетевых экранов (firewalls), мониторинг сетевого трафика, внедрение SIEM-систем	IT-отдел	Постоянно
7	Потеря данных при технических сбоях	Сбои оборудования могут привести к утрате критически важных учебных и исследовательских данных	3	4	12	Настройка регулярного резервного копирования и использование систем аварийного восстановления	IT-отдел	Еженедельно
8	Низкая осведомленность сотрудников в области ИБ	Ошибки и неосторожность сотрудников могут привести к случайной утечке или изменению данных	4	2	8	Проведение регулярного обучения по информационной безопасности и тестирования знаний сотрудников	Отдел кадров	Полугодие
9	Отсутствие обновлений программного обеспечения	Использование устаревшего ПО может повысить уязвимость систем к атакам	3	3	9	Регулярное обновление и установка патчей для всех систем и приложений	IT-отдел	Ежемесячно
10	Нарушение работы систем из-за человеческого фактора	Некорректные действия или ошибки сотрудников могут повлиять на функционирование систем	2	3	6	Внедрение процедуры многоэтапной проверки операций, ограничение прав доступа для определенных задач	Руководитель подразделения	Постоянно

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

[illegible]