НАО «Костанайский

региональный университет

им. Ахмет Байтұрсынұлы»

BU

BAITURSYNULY

UNIVERSITY

Утверждаю

Председатель Правления -

Ректор

_____ С.Куанышбаев

_____ 2024 г.

ПОЛИТИКА

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ НАО «КОСТАНАЙСКИЙ РЕГИОНАЛЬНЫЙ УНИВЕРСИТЕТ ИМЕНИ АХМЕТ БАЙТҰРСЫНҰЛЫ»

П 054-2024

Костанай

Предисловие

1 РАЗРАБОТАНО отделом разработки и сопровождения программного обеспечения

2 ВНЕСЕНО отделом разработки и сопровождения программного обеспечения

3 УТВЕРЖДЕНО И ВВЕДЕНО В ДЕЙСТВИЕ: решением Правления общества, протокол от 17.07.2024 года № 08

4 РАЗРАБОТЧИК:
В. Гриднева – начальник отдела разработки и сопровождения программного обеспечения;

5 ЭКСПЕРТЫ:
А.Шмит – начальник отдела технического обеспечения

6 ПЕРИОДИЧНОСТЬ ПРОВЕРКИ 3 года

7 ВВЕДЕНО впервые

Содержание

Глава 1. Общие положения и область применения

1. Настоящая Политика информационной безопасности НАО «Костанайский региональный университет имени Ахмет Байтұрсынұлы» (далее - Политика) определяет цели, задачи, руководящие принципы и практические приемы в области обеспечения информационной безопасности НАО «Костанайский региональный университет имени Ахмет Байтұрсынұлы» (далее –Университет).

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.

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.

Глава 2. Нормативные ссылки

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

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

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

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

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

6) Устав НАО «Костанайский региональный Университет имени А.Байтурсынова», утвержденный приказом Председателя Комитета государственного имущества и приватизации Министерства финансов Республики Казахстан от 05 июня 2020 года № 350;

7) СО 081-2022 Стандарт организации. Делопроизводство;

8) ДП 082-2022 Документированная процедура. Управление документацией.

Глава 3. Обозначения и сокращения

5. В настоящем Положении применяются следующие термины и определения:
1) ИБ – Информационная безопасность
2) ПО – программное обеспечение
3) ИС – информационная система
4) СУИБ – система управления информационной безопасностью

Глава 4. Основные цели и задачи ИБ

6. 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.

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

1) 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

2) Обеспечение целостности данных: Обеспечение целостности, недопущение несанкционированных изменений или повреждений электронных информационных ресурсов, ИС и баз данных Университета

3) Обеспечение доступности данных: Обеспечение доступа к ИС Университета для авторизованных пользователей в необходимом объеме для поддержания непрерывности учебных и административных процессов университета.

4) Управление доступом: Разграничение доступа сотрудников к аппаратным, программным, информационным системам и информационным ресурсам Университета в зависимости от ролей и полномочий пользователей.

5) 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.

6) 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.).

7) Обновление аппаратных средств: Замена устаревшего оборудования (серверов, сетевых устройств, хранилищ данных) на более современные модели с улучшенными характеристиками безопасности.

8) Улучшение программного обеспечения: Обновление операционных систем, баз данных, антивирусных программ и другого программного обеспечения до актуальных версий с последними обновлениями безопасности.

9) Улучшение системы управления событиями: Развитие процессов и системы управления событиями (SIEM), которая позволяет собирать, анализировать и реагировать на события безопасности в реальном времени.

10) Соответствие законодательству и регулированиям: Выполнение требований законодательства и нормативно-правовых актов Республики Казахстан в области информационной безопасности, разработка и совершенствование нормативно-правовой базы по обеспечению информационной безопасности и защите персональных данных.

11) 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.

12) 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.

13) 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.

14) 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.

Глава 5. Принципы ИБ

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

1) 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.

2) 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.

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

4) 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.

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

6) 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.

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

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

9) 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.

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

Глава 6. Практические приемы ИБ

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

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

2) Управление доступом: Определение прав доступа, назначение ролей для авторизованных пользователей к электронным информационным ресурсам и ИС Университета.

3) Обновление программного обеспечения: Регулярное обновление операционных систем, прикладного программного обеспечения и антивирусных программ до последних версий. Установка патчей безопасности для закрытия известных уязвимостей.

4) Шифрование данных: Использование шифрования данных при их хранении и передаче через сеть. Реализация шифрования дисков и файлов для защиты конфиденциальных данных.

5) Резервное копирование данных: Регулярное создание резервных копий данных и их хранение в защищенных местах.

6) Мониторинг и регистрация событий: Использование системы мониторинга безопасности для обнаружения аномалий и потенциальных инцидентов безопасности. Анализ и регистрация событий для оперативного реагирования на угрозы.

7) Физическая безопасность: Обеспечение физической безопасности серверных помещений. Использование систем контроля доступа и видеонаблюдения в Университете.

8) Защита от вредоносного ПО и кибератак: Установка антивирусных программ и файерволов на всех компьютерах и серверах.

9) Мониторинг безопасности: организационные и технические мероприятия, направленные на проведение мониторинга безопасного использования элетронных информационных ресурсов, информационных систем и баз данных Университета;

10) Соблюдение нормативных требований: Выполнение всех требований по защите данных, установленных законодательством РК и внутренними документами Университета.

Глава 7. Ответственность

10. Все сотрудники обязаны использовать информационные ресурсы Университета квалифицированно, эффективно и придерживаясь правил этики.

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

12. 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.

13. 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.

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

Глава 8. Порядок внесения изменений

15. Внесение изменений в настоящее Политику осуществляется по инициативе начальника отдела разработки и сопровождения программного обеспечения, начальника отдела технического обеспечения, начальника отдела управления персоналом, проректором по исследованиям, инновациям и цифровизации в соответствии с ДП 082-2022 Документированная процедура. Управление документацией.

Глава 9. Согласование, хранение и рассылка

16. Согласование, хранение и рассылка положения производятся в соответствии ДП 082-2022 Документированная процедура. Управление документацией.

17. Настоящая Политика согласовывается с проректором по исследованиям, инновациям и цифровизации, начальником отдела правового обеспечения и государственных закупок, начальником отдела управления персоналом и начальником отдела документационного обеспечения.

18. Подлинник настоящего Политики вместе с «Листом согласования» передается на хранение в ОДО по акту приема-передачи.

19. Рабочий экземпляр настоящей Политики размещается на сайте Университета с доступом из внутренней корпоративной сети.