УТВЕРЖДЕНО
Решением Совета директоров
НАО «Актюбинский региональный
университет им. К. Жубанова»
(Протокол №5 от «14» июня 2021 г.)

ПОЛОЖЕНИЕ
ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
НАО «АКТЮБИНСКИЙ РЕГИОНАЛЬНЫЙ УНИВЕРСИТЕТ ИМ. К. ЖУБАНОВА»

Актобе, 2021

ДАННОЕ ПОЛОЖЕНИЕ РАЗРАБОТАНО

Директором Центра стратегического планирования _____ Балгинова К.М.

Директором Департамента информационных технологий _____ Кочетков О.Г.

1. Термины их определения, сокращения и нормативные ссылки

В настоящем Положении по информационной безопасности (далее – Положение ИБ) применены следующие термины, их определения и сокращения:

1.1. **Аутентификация** подтверждение подлинности субъекта или объекта доступа путем определения соответствия предъявленных реквизитов доступа, реализованными в системе;

1.2. **База данных (БД)** – совокупность данных, организованных согласно концептуальной структуре, описывающей характеристики этих данных, а также взаимосвязи между их объектами;

1.3. **Градация информационной системы по уровням информационной безопасности** – разделение информационной системы на классы по уровню предъявляемых к ним требований по обеспечению информационной безопасности;

1.4. **Информационные ресурсы (ИР)** – это совокупность данных: текст; графика; аудио; видео и др. хранящаяся в информационных системах.

1.5. **Информационная система (ИС)** – система, предназначенная для хранения, обработки, поиска, распространения, передачи и предоставления информации с применением аппаратно-программного комплекса;

1.6. **Информационная безопасность (ИБ)** все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, не отказоустойчивости, подотчетности, аутентичности и достоверности информации или средства ее обработки;

1.7. **Электронные информационные ресурсы (ЭИР)** – электронные систематизированные массивы информации (информационные БД), содержащиеся в ИС, объединенные соответствующим программным обеспечением и представляющие интерес для пользователей информации;

1.8. **Информационно-коммуникационная инфраструктура (ИКИ)** – совокупность средств вычислительной техники, телекоммуникационного оборудования, каналов передачи данных и ИС, средств коммутации и управления информационными потоками;

1.9. **Локально-вычислительная сеть (ЛВС)** — сеть, объединяющая абонентов, расположенных в пределах небольшой территории;

1.10. **Несанкционированный доступ к информации (НСД)** – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами;

1.11. **Нормативные правовые акты (НПА)** – письменный официальный документ установленной формы, принятый должностным(и) лиц(ом/ами), устанавливающий правовые нормы, изменяющий, прекращающий или приостанавливающий их действие, а также документ в электронно-цифровой форме, идентичный письменному официальному документу и удостоверенный посредством электронной цифровой подписи;

1.12. **Пользователь ИС** – субъект, обращающийся к ИС за получением необходимых ему электронных ИР и пользующийся ими;

1.13. **Программное обеспечение (ПО)** – совокупность компьютерных программ системы обработки информации и программных документов, необходимых для эксплуатации этих программ;

1.14. **Прикладное ПО (ППО)** – ПО (или программа), которое предназначено для решения прикладной задачи;

1.15. **НАО «Актюбинский региональный университет имени К.Жубанова»** (далее – университет);

1.16. **Департамент информационных технологий ДИТ)** – оказывает техническое сопровождение и обслуживание каналов связи, функционирование компьютерного оборудования и базового ПО;

1.17. **Серверное помещение** – помещение, предназначенное для размещения серверного, активного и пассивного сетевого оборудования (телекоммуникационного) и оборудования структурированных кабельных систем;

1.18. **Система управления базами данных (СУБД)** – совокупность программных и языковых средств, обеспечивающих управление БД;

1.19. **Системное ПО** – совокупность компьютерных программ для обеспечения работы вычислительного оборудования;

1.20. **Системный администратор (СА)** – лицо, ответственное за правильное функционирование сервера и настройки ПО на сервере;

1.21. **Инженер-программист** – специалист, занимающийся программированием, то есть созданием компьютерных программ;

1.22. **Служба технической поддержки** – сервисная структура, разрешающая проблемы пользователей с компьютерами (как аппаратным, так и программным обеспечением) и оргтехникой;

1.23. **Специализированное ПО** – компьютерные программы, применяемые для решения вспомогательных и сервисных задач;

1.24. **Средства вычислительной техники (СВТ)** – совокупность программных и технических элементов систем обработки информации, в том числе ввода или вывода, способных функционировать самостоятельно или в составе других систем;

1.25. **Сеть интернет** – система сетей, обеспечивающая доступ к международным ресурсам;

1.26. Основными НПА, государственными и международными стандартами, используемыми при разработке настоящего Положения ИБ, являются:

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

2) СНиП РК 202-05-2009 «Пожарная безопасность зданий и сооружений»;

3) СН РК 3.02-17-2011 «Структурированные кабельные сети. Нормы проектирования»;

4) СТ РК 34.005-2002 «Информационная технология. Основные термины и определения»;

5) СТ РК 34.006-2002 «Информационная технология. Базы данных. Основные термины и определения»;

6) СТ РК 34.007-2002 «Информационная технология. Телекоммуникационные сети. Основные термины и определения»;

7) СТ РК ИСО/МЭК 17799-2006 «Информационная технология. Методы обеспечения защиты. Свод правил по управлению защиты информации»;

8) СТ РК ИСО/МЭК 27002-2015 «Средства обеспечения. Свод правил по управлению защитой информации».

2. Основные цели

2.1. Настоящее Положение по информационной безопасности (ИБ) разработано с учетом текущего состояния и ближайших перспектив развития информационно-коммуникационной инфраструктуры (далее – ИКИ) университета. В положении описаны цели, задачи и правовые основы эксплуатации, режимы функционирования, а также анализ угроз безопасности.

2.2. Основные цели Положения ИБ:

1) доступность обрабатываемой информации;
2) устойчивое функционирование ИКИ университета;
3) обеспечение конфиденциальности информации, хранящейся обрабатываемой СВТ и передаваемой по каналам связи;
4) целостность и аутентичность информации, хранящейся и обрабатываемой в ИС университета и передаваемой по каналам связи;

2.3. Для достижения целей поставлены следующие задачи:

1) формирование и проведение единой политики в области обеспечения ИБ в университете;
2) обеспечение бесперебойной работы университета и сведение к минимуму экономического ущерба от реализации угроз ИБ, посредством их предупреждения, предотвращения;
3) определение процедур, направленных на выявление, отражение и ликвидацию последствий реализации различных угроз безопасности информации;
4) определение требований к содержанию процедур по управлению информатизацией в рамках университета с учетом необходимости решения задач обеспечения ИБ;
5) координация деятельности университета при проведении работ в ИКИ с соблюдением требований стандартов обеспечения ИБ;
6) повышение уровня защищенности ИКИ университета;
7) на основе Положения ИБ строится управление ИБ.

3. Область действия

3.1. Действие настоящего Положения ИБ распространяется на структурные подразделения университета, в которых осуществляется обработка информации, в том числе автоматизированная, содержащая административные данные, информацию с ограниченным распространением (служебная информация), или персональные данные, а также на организации, осуществляющие разработку, сопровождение, обслуживание функционирования ИС университета.

3.2. Область действия ИБ других ИС определяется их владельцами. В случае если данные ИС состоят в ИКИ университета, условия ИБ оговариваются в рамках договоров ИБ или совместных правилах взаимодействия между владельцем ИС и университетом.

4. Положение ИБ

4.1. Настоящее Положение ИБ разработано, основываясь на принципах и в соответствии с требованиями и рекомендациями законодательства Республики Казахстан в области ИБ, в том числе основываясь на документах, перечисленных в пункте 1.24 раздела 1 настоящего Положения ИБ.

4.2. Под обеспечением ИБ понимается сохранение конфиденциальности, целостности и доступности информации. Конфиденциальность информации обеспечивается путем предоставления доступа к информации только авторизованным лицам, целостность – путем внесения в данные исключительно авторизованных изменений, доступность – путем предоставления доступа к данным авторизованным лицам для выполнения их служебных обязанностей.

4.3. Положение ИБ университета является методологической базой для:

1) выработки и совершенствования комплекса согласованных нормативных, правовых, технологических и организационных мер, направленных на защиту информации;
2) обеспечения ИБ;
3) координации деятельности структурных подразделений университета при проведении работ по соблюдению требований обеспечения ИБ.

4.4. Требования и условия настоящего Положения ИБ применяются в отношении всех ИС университета.

5. Организация обеспечения ИБ

5.1. За непосредственную организацию (построение) и обеспечение эффективного функционирования системы защиты информации отвечают:

1) ДИТ – структурное подразделение реализующее функционирование ИКИ, СВТ, ИС, ИБ.
2) ДИТ по согласованию с курирующим проректором членом Правления университета определяет основные направления развития мер, направленных на защиту информации от НСД.

6. Категории пользователей ИС

6.1. К категориям пользователей ИС относятся:

1) внутренние пользователи – сотрудники университета, имеющие авторизованный доступ к ИР, осуществляющие свою деятельность и обладающие основными правами и обязанностями в соответствии с законодательством Республики Казахстан;
2) внешние пользователи – потребители услуг университета, в том числе лица, использующие ИР университета;
3) вспомогательные персонал – обслуживающий, технический персонал и владельцы других ИС, осуществляющих взаимодействие в университете, в том числе:
   - администраторы ЛВС, ответственные за сопровождение телекоммуникационного оборудования;
   - СА;
   - разработчики ППО;
   - инженеры-системотехники, технические специалисты (системно-техническое обслуживание) и др.

7. Объекты ИБ

7.1. Основными объектами защиты ИБ университета являются:

1) ИР с ограниченным доступом, составляющие тайну, чувствительные по отношению к несанкционированным воздействиям и нарушению их безопасности,

в том числе открытая (общедоступная) информация, независимо от формы и вида представления;

2) процессы и человеческие ресурсы обработки информации в ИС – информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, персонал разработчиков, внутренние пользователи системы и ее обслуживающий персонал;
3) информационная инфраструктура, включающая системы обработки и анализа информации, передачи и отображения, в том числе каналы информационного обмена, объекты и помещения, в которых размещены ИР и компоненты ИС.

7.2. Объекты информационной инфраструктуры включают:

1) технологическое оборудование (СВТ, сетевое и кабельное оборудование);
2) ИР, содержащие сведения ограниченного доступа;
3) программные средства (операционную систему (далее – ОС), СУБД, другое общесистемное и ППО);
4) автоматизированные системы связи и передачи данных (средства телекоммуникации);
5) каналы связи, по которым передается информация (в том числе ограниченного распространения);
6) служебные помещения, в которых циркулирует информация ограниченного распространения; секретная комната с отдельным каналом интернет (прокторинг)
7) технические средства и системы, не обрабатывающие информацию, размещенные в помещениях, где обрабатывается (циркулирует) служебная информация.

8. Категории ИР, подлежащих защите

8.1. В подсистемах ИС университета циркулирует информация, содержащая сведения ограниченного распространения (персональные данные, служебная, финансовая информация) и открытые сведения.

9. Меры по реализации Положения ИБ

9.1. Внутренние пользователи, работающие в ИКИ университета, обязаны строго соблюдать установленные требования Положения ИБ университета.

9.2. Функциональные обязанности сотрудников, специалистов по ИБ определяются внутренними регламентирующими документами университета, должностными инструкциями сотрудников и документируются в соответствии с Положением ИБ и требованиями пункта 8.1.1 Государственного стандарта Республики Казахстан СТ РК ИСО/МЭК 27002-2015 «Средства обеспечения. Свод правил по управлению защитой информации».

9.3. Инструкция по обеспечению сохранности информации о НАО «Актюбинский региональный университет им. К. Жубанова», составляющей служебную, коммерческую и иную охраняемую законом тайну.

9.4. Ответственное лицо за ИБ организует, контролирует и координирует вопросы и работы, связанные с защитой информации в соответствии с требованиями пунктов 6.1.2-6.1.7 Государственного стандарта Республики Казахстан СТ РК ИСО/МЭК 27002-2009 «Средства обеспечения. Свод правил по управлению защитой информации».

9.5. Ответственное лицо за ИБ в рамках обеспечения ИБ проводит следующие виды работ:

1) участвует в подготовке технических спецификаций, конструировании и в процессе приобретения программно-аппаратных комплексов;
2) осуществляет практическое внедрение аппаратных и программных средств обеспечения ИБ в рамках университета;
3) участвует в формировании требований к ИБ в процессе создания, развития и применения ИС;
4) участие в проектировании системы защиты, ее испытаниях и приемке в эксплуатацию;
5) распределяет между авторизованными внутренними пользователями необходимых реквизитов защиты;
6) наблюдает за функционированием системы защиты и ее элементов;
7) уведомляет внутренних пользователей ИС требованиям безопасной обработки информации;
8) контролирует соблюдение внутренними пользователями ИС установленных правил обращения с защищаемой информацией в процессе ее автоматизированной обработки;
9) принимает необходимые меры при выявлении попыток НСД к информации и при нарушениях правил функционирования системы защиты;
10) участвует в проведении внутреннего аудита и мониторинга информационной безопасности;
11) вносит на рассмотрение предложения по использованию криптографических средств защиты информации;
12) обеспечивает разграничение прав доступа к информационным системам университета.

9.6. Ответственное лицо за ИБ и сотрудники ДИТ, должны периодически направляться на обучение по повышению квалификации в области ИБ.

9.7. Внутренние и внешние пользователи, работающие в ИКИ университета, по мере необходимости (либо при наличии уровня доступа к оборудованию, содержащему или обрабатывающему конфиденциальную информацию) проходят обучение.

10. Организационно-правовой статус ответственного лица за ИБ и СА

10.1. Ответственное лицо за ИБ имеет необходимые права:
1) мониторинга и контроля информационной инфраструктуры университета;
2) доступа во все помещения университета, где установлена ИС, СВТ и ЛВС университета;
3) прекращать автоматизированную обработку информации при наличии непосредственной угрозы для защищаемой информации.

10.2. СА по согласованию с ответственным лицом за ИБ имеют право:
1) доступа во все помещения университета, где установлено ИС, СВТ и ЛВС университета;
2) прекращать автоматизированную обработку информации при наличии непосредственной угрозы для защищаемой информации.

11. Общие требования конфиденциальности

11.1. Главными требованиями конфиденциальности являются предотвращение утечки (разглашения) какой-либо конфиденциальной информации и обеспечение предоставления информации только авторизованным лицам.

11.2. Подключения внутренних пользователей к ИС университета должны фиксироваться в полном и тщательном виде с сохранением данной информации (логирование) на срок не менее 1 года.

11.3. Служебная и иная защищаемая информация, обрабатываемая и хранящаяся в ИС университета, подлежит копированию и передаче третьему лицу только с официального разрешения курирующего проректора-члена Правления.

11.4. При работе с ИС университета должна исключаться возможность наблюдения за отображаемой информацией на экране монитора внутреннего пользователя посторонними лицами.

11.5. При работе ИС университета должны использоваться специальные лицензионные программные или аппаратные средства, обеспечивающие защиту от вредоносных программ, вирусов и сетевых атак. Для защиты от нелегального внедрения и использования неучтенных программ в университет, кроме мероприятий, включающих физическую защиту, должен проводиться мониторинг системных журналов, на рабочие станции внутренних пользователей должен устанавливаться базовый комплекс ПО. В базовый комплекс ПО включается лицензионное ПО, необходимое для обеспечения работоспособности СВТ.

11.6. Соблюдение требований конфиденциальности внутренними пользователями и вспомогательным персоналом при работе с ИС университета должно обеспечиваться соглашением о конфиденциальности.

12. Требования по аутентификации пользователей в системе

12.1. Все внутренние пользователи, работающие в ИС университета, должны проходить безопасную аутентификацию исключающую возможность утечки и перехвата авторизованных данных.

12.2. Для аутентификации внутренних пользователей в ИС создаются уникальные идентификационные учетные записи (логин, пароль).

12.3. Ответственность за сохранность и неразглашение сведений об учетной записи возлагается на внутренних пользователей ИС.

12.4. Учетные записи внутренних пользователей должны создаваться и удаляться только при наличии соответствующих документов или записей.

12.5. Требования к организации парольной защиты действиям внутренних пользователей и обслуживающего персонала ИС при работе с паролями, личный пароль должен быть не менее 8 символов и не включать слова из общего словаря, при этом включать минимум три следующих набора символов:

а) заглавных букв: A, B, C;
б) маленьких букв: a, Ь, c;
в) цифр: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9;

13. Требования конфиденциальности при передаче информации по линиям связи

13.1. Передача информации университета должна осуществляться по собственным либо арендуемым волоконно-оптическим каналам, на больших расстояниях.

13.2. Серверное, телекоммуникационное оборудование и структурированная кабельная система должны иметь документальное подтверждение соответствия требованиям в области технического регулирования и иметь сертификат соответствия требованиям ИБ.

13.3. Запрещается использовать почтовые адреса электронной почты университета при регистрации на сайтах и при участии в форумах или интернет-конференциях (за исключением случаев, когда это относится к мероприятиям, связанным с профессиональной деятельностью сотрудника).

13.4. Запрещается использовать общедоступные почтовые сервисы Интернета и Интернетсистемы мгновенного общения сотрудникам, работающим с конфиденциальной информацией.

14. Требования по организации защиты общедоступных ресурсов

14.1. Официальный интернет-ресурс размещается на единой платформе Интернет-ресурсов и регистрируется в доменной зоне edu.kz (zhubanov.edu.kz).

14.2. Для обеспечения ИБ Интернет-ресурсов необходимо применять систему управления содержимым (контентом), выполняющую:

1) санкционирование операций размещения, изменения и удаления информационного контента;

2) регистрацию авторства при размещении, изменении и удалении информационного контента;

3) проверку загружаемого контента на наличие вредоносного кода;

4) контроль целостности размещенного информационного контента;

5) контроль аномальной активности пользователей и программных роботов.

С целью контроля обеспечения конфиденциальности должны обеспечиваться следующие мероприятия:

1) ежегодная сверка списка официально зарегистрированных пользователей и пользователей, работающих в ИС.

2) ежегодный аудит ИБ на соблюдение требований настоящего Положения ИБ.

3) постоянный мониторинг инструментальными, программными средствами ИБ ИКИ университета.

15. Общие требования целостности

15.1. Главным требованием целостности является обеспечение изменения информации только авторизованными лицами.

15.2. Для обеспечения целостности и безопасности ИС университета перед установкой нового/разработанного ПО, а также обновления имеющегося ПО должны быть внедрены процедуры тщательного тестирования и проверки соответствия требованиям ИБ.

16. Требования безопасности ИС при разработке, усовершенствовании и обслуживании

16.1. Требования к элементам обеспечения ИБ до разработки ИС необходимо идентифицировать и согласовать с ответственным лицом за ИБ и внести на утверждение курирующему проректору члену Правления университета.

16.2. Разработка программных средств или изменение исходного кода в рамках сопровождения программных средств должно осуществляться в разработочной среде.

16.3. Измененное программное средство должно пройти тестирование на предмет соответствия установленным требованиям ИБ и совместимости с другими программными средствами. Тестирование проводится разработчиками совместно с ответственным лицом за ИБ, результаты тестирования должны быть отражены в протоколе тестирования.

16.4. Запуск программного средства в эксплуатационную среду должен осуществляться только при наличии протокола тестирования с положительным заключением.

16.5. Требования безопасности должны учитывать ценность информационных активов, потенциальный ущерб бизнес-процессу.

17. Требования к компонентам обеспечения ИБ сети передачи данных

17.1. Для обеспечения безопасного функционирования ИС университета необходимо использовать технические решения, обеспечивающие разделение и изоляцию информационных потоков различных подразделений, межсетевые экраны для контроля и ограничения доступа в системы обнаружения и предотвращения вторжений.

17.2. Защита коммуникаций от незаконного подключения кроме средств санкционированного электронного и физического доступа, осуществляется программными, техническими средствами и организационными мерами. Проведение необходимых мероприятий для своевременного выявления, предупреждения и пресечения неправомерных действий лиц по получению доступа к коммуникациям.

17.3. Для выявления утечки информации необходим систематический контроль возможности образования каналов утечки и оценки их опасности в пределах контролируемой зоны. Закрытие и локализация каналов утечки обеспечивается организационно-техническими мерами, а также сертифицированными DLP технологиями при их наличии.

18. Требования к управлению инцидентами безопасности

18.1. О случаях нарушения ИБ следует сообщать незамедлительно ответственному лицу за ИБ.

18.2. Должны быть установлены зоны ответственности и процедуры, чтобы гарантировать быструю, результативную и упорядоченную реакцию на инциденты в системе защиты информации.

18.3. Должны быть приняты механизмы для ведения мониторинга инцидентов в системе защиты информации и постоянно их контролировать.

19. Требования к защите информации от несанкционированного доступа

19.1. Защита от НСД должна обеспечивать:

1) возможность идентификации на цифровых сертификатах инфраструктуры открытых ключей;
2) авторизацию пользователей для доступа к информационно-вычислительным ресурсам системы, требующим наличия соответствующих разрешений;
3) персональное определение прав на ввод, корректировку, просмотр данных;
4) персональное определение прав на доступ к системным ресурсам;
5) аудит событий по идентификации пользователей;
6) реализацию в ИС функций распределения пользователей по группам и присвоения им соответствующих прав доступа для предотвращения несанкционированного удаления, копирования, модификации информации;
7) защищенные каналы связи на физическом уровне;

8) протоколирование работы пользователей с критическими функциями и приложениями ИС.

19.2. Физический доступ к основным носителям информации (накопителей, дисков, серверному оборудованию и т.д.) ограничивается в соответствии с Правилами организации физической защиты средств обработки и безопасной среды функционирования информационных ресурсов.

20. Требования к применению электронной почты и Интернета

20.1. Для уменьшения риска, которому подвергаются производственные процессы и система безопасности, связанного с использованием электронной почты, следует применять (по необходимости) соответствующие средства контроля, которые должны учитывать:

1) уязвимость электронных сообщений по отношению к несанкционированному перехвату и модификации;

2) уязвимость данных, пересылаемых по электронной почте, по отношению к ошибкам, например, неправильная переадресация или направление сообщений не по назначению, а также надежность и доступность сервиса в целом;

3) влияние изменения характеристик коммуникационной среды на производственные процессы, например, влияние повышенной скорости передачи данных или изменения системы адресации между организациями и отдельными лицами;

4) правовые соображения, такие как необходимость проверки источника сообщений и др.;

5) последствия для системы безопасности от раскрытия содержания каталогов;

6) необходимость принятия защитных мер для контроля удаленного доступа пользователей к электронной почте.

21. Требования к антивирусной безопасности

21.1. Антивирусные программные средства обнаружения вирусов следует применять для проверки серверов, рабочих станций ИС и переносных носителей информации на наличие вирусов. Антивирусные программные средства должны регулярно обновляться и использоваться в соответствии с Правилами организации антивирусного контроля.

22. Общие требования доступности

22.1. Главным требованием доступности является обеспечение своевременного и правомерного доступа пользователей к информации.

22.2. В случае возникновения аварий, стихийных бедствий и иных внештатных ситуаций должны быть предусмотрены соответствующие меры защиты, непрерывной работы и восстановления.

22.3. Информация об авариях, стихийных бедствиях и иных внештатных ситуациях должны фиксироваться в полном и тщательном виде на срок не менее 1 года.

23. Требования к отказоустойчивости

23.1. Аппаратно-программное обеспечение должно обеспечивать выполнение задач ИС университета со временем однократного простоя не более 24 часов и суммарным временем простоя не более 120 часов в год.

23.2. В случае возникновения внештатной ситуации, произошедшей с производственным сервером ИС, восстановление ППО, системного ПО и ОС должно быть произведено в течение 24 часов.

23.3. Восстановление работоспособности и обеспечение непрерывной работы ИС университета производится согласно, Параграфа 8 Постановления Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности.

23.4. Система хранения данных должна предусматривать автоматический периодический контроль целостности дисков, анализ плохих секторов, проверку состояния резервных батарей, без вмешательства администратора и без влияния на работу пользователей.

23.5. Система хранения данных должна обеспечивать возможность «горячей» замены дисков.

23.6. Бесперебойное электропитание обеспечивается источником бесперебойного питания (ИБП) необходимой мощности, который должен гарантировать, как минимум, корректное завершение работы приложений и ОС при отключении внешнего электропитания.

24. Требование к анализу и оценке рисков

24.1. Положение ИБ первоначально должно основываться на данных, полученных в результате анализа и оценки рисков ИБ.

24.2. С целью совершенствования Положения ИБ должен проводиться ежегодный анализ и оценка рисков ИБ. Данный анализ основывается на данных ежегодного аудита ИБ и вносится курирующему члену Правления университета с целью принятия дальнейших организационно-распорядительных мер.

24.3. Анализ и оценка рисков должны проводиться в соответствии с руководством по реализации Государственного стандарта Республики Казахстан СТ РК ИСО/МЭК 17799-2006 «Информационная технология. Методы обеспечения защиты. Свод правил по управлению защиты информации».

24.4. На основе результатов анализа затрат и выгод рисков, ответственное лицо за ИБ определяет наиболее экономически эффективные меры для снижения риска. Выбранные меры должны объединить технические, эксплуатационные и управленческие меры для обеспечения надлежащей безопасности для ИКИ университета.

25. Контроль эффективности принимаемых мер защиты

25.1. Для поддержания требуемого уровня ИБ в университете ответственное лицо за ИБ осуществляет постоянный контроль эффективности принимаемых мер защиты. Основным критерием при этом является то, что риски защищаемых ресурсов находятся в диапазонах, приемлемых для университета.

25.2. Основными механизмами контроля эффективности принимаемых мер защиты являются мониторинг и аудит ИБ университета.

25.3. Аудит ИБ университета осуществляется согласно Правилам проведения аудита информационных систем.

25.4. Результаты аудита могут служить основанием для пересмотра некоторых пунктов Положения ИБ и внесения в него необходимых корректировок.

25.5. Контроль требований настоящего Положения ИБ на соответствие требованиям ИБ осуществляется сотрудниками по ИБ.

26. Пересмотр Положения ИБ

26.1. Развитие, пересмотр и оценку Положения ИБ осуществляет ответственное лицо за ИБ на основе ежегодного анализа и оценки рисков ИБ,

26.2. Пересмотр Положения ИБ производится в целях:

1) усовершенствования целей и мер контроля ИБ;
2) усовершенствования подхода к управлению ИБ и бизнес-процессами университета;
3) улучшения распределения ресурсов и/или обязанностей.

26.3. Положение ИБ должно пересматриваться в соответствии с изменениями, влияющими на основу первоначальной оценки риска, путем выявления существенных инцидентов нарушения ИБ, появления новых уязвимостей или изменения организационной/технологической инфраструктуры, изменении основных характеристик бизнес-процессов университета.

26.4. В случае появления существенных изменений в технологиях, обеспечивающих ИБ, в целях обеспечения конфиденциальности, целостности, доступности информации, а также адекватности и эффективности применяемых мер ИБ.

26.5. В случае возникновения дополнительных замечаний и предложений со стороны внутренних и внешних пользователей к изменениям норм Положения ИБ данные предложения анализируются ответственным лицом за ИБ и при необходимости вносятся для утверждения.

26.6. Руководством университета может инициироваться независимый пересмотр Положения ИБ. Такой пересмотр проводится лицом, не имеющим прямого отношения к пересматриваемой области безопасности, например, функция внутреннего аудита осуществляется независимым менеджером или организацией третьей стороны, специализирующейся на таких пересмотрах. Результаты независимого пересмотра документируются в виде отчета и доводятся до сведения председателя Правления университета.

26.7. Положение ИБ должно быть пересмотрено после проведения анализа и оценки рисков ИБ для университета, по итогам которых, с учетом исправления выявленных недостатков необходима ее актуализация.

26.8. при утверждении новой редакции Положения ИБ номер редакции указывается на титульном листе под наименованием документа, к примеру: Ред. 1

26.9. Пересмотр Положения ИБ должен осуществляться в соответствии с руководством по реализации Государственного стандарта Республики Казахстан СТ РК ИСО/МЭК 17799-2006 «Информационная технология. Методы обеспечения защиты. Свод правил по управлению защиты информации».

27. Ответственность

27.1. Ответственное лицо за ИБ совместно с курирующим проректором-членом Правления университета обеспечивает:

1) определение целей ИБ в соответствии с организационными требованиями и интеграцией в бизнес-процессы университета;
2) контроль выполнения всех пунктов настоящего Положения ИБ;
3) четкое управление и зримую поддержку инициатив в области поддержки ИБ университета;
4) предоставление ресурсов для обеспечения ИБ;
5) контроль издания и доведения до сведения утвержденных документов до пользователей ИКИ университета.

27.2. Курирующий проректор-член Правления университета по представлению ответственного лица за ИБ должен:

1) утверждать разрабатываемые, пересматриваемые правовые документы по ИБ университета;
2) вести контроль за эффективностью реализации Положения ИБ;
3) утверждать распределение специфических ролей и обязанностей по ИБ;
4) инициировать планы и программы по осведомлённости об ИБ;

27.3. Руководители структурных подразделений университета несут ответственность за выполнение требований Положения, а также за ознакомление с настоящим Положением ИБ своих подчиненных, в том числе вновь принятых сотрудников.

27.4. При нарушении требований Положения ИБ, повлекших за собой моральный и материальный ущерб для университета, причастные сотрудники привлекаются к ответственности в соответствии с законодательством Республики Казахстан.

27.5. Нарушение требований Положения ИБ квалифицируется как дисциплинарный проступок, заключающийся в неисполнении или ненадлежащем исполнении трудовых обязанностей. Сотрудник, допустивший нарушение требований Положения ИБ, привлекается к дисциплинарной ответственности в соответствии с Трудовым кодексом Республики Казахстан.

СОГЛАСОВАНО:

Проректор по стратегическому развитию и цифровизации _____ Бекбауова А.У.

Юрист _____ Алиманова Л.Б.