УТВЕРЖДЕНО
Решением Совета Директоров
НАО «Южно-Казахстанский
государственный педагогический
университет»
(Протокол №21 от 22.08.2022)

ПОЛОЖЕНИЕ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НЕКОММЕРЧЕСКОГО АКЦИОНЕРНОГО ОБЩЕСТВА «ЮЖНО-КАЗАХСТАНСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТА»

Шымкент, 2022г.

Содержание

1 Общие положения

1.1 Настоящее Положение по информационной безопасности (далее – Положение ИБ) некоммерческого акционерного общества «Южно-Казахстанский государственный педагогический университет» (далее – Общество) 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 настоящем Положении ИБ.

1.2 Под обеспечением ИБ понимается сохранение конфиденциальности, целостности и доступности информации в Обществе. 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.

1.3 Положение ИБ Общества является методологической базой для:

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

1.4 Требования и условия настоящего Положения применяются в отношении всех информационных систем Общества и обязательно к исполнению всеми работниками Общества.

1.5 Действие настоящего Положения распространяется на структурные подразделения Общества, 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 Общества.

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

2 Термины их определения, сокращения и нормативные ссылки

2.1 В настоящем Положении применены следующие термины, их определения и сокращения:

Аутентификация – подтверждение подлинности субъекта или объекта

доступа путем определения соответствия предъявленных реквизитов доступа, реализованными в системе,

база данных (БД) – совокупность данных, организованных согласно концептуальной структуре, описывающей характеристики этих данных, а также взаимосвязи между их объектами,

градация информационной системы по уровням информационной безопасности – разделение информационной системы на классы по уровню предъявляемых к ним требований по обеспечению информационной безопасности;

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

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

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;

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

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

Локально-вычислительная сеть (ЛВС) – сеть, объединяющая абонентов, расположенных в пределах небольшой территории;

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

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;

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

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

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

Центр информационных технологий и телекоммуникации (ЦИТиТ) – оказывает техническое сопровождение и обслуживание каналов связи, функционирование компьютерного оборудования и базового ПО;

Серверное помещение - помещение, предназначенное для размещения серверного, активного и пассивного сетевого оборудования (телекоммуникационного) и оборудования структурированных кабельных систем;

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

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

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

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

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;

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

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

- Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832. «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности»
- СНиП РК 2.02-05-2009 «Пожарная безопасность зданий и сооружений»;
- СН РК 3.02-17-2011 «Структурированные кабельные сети. Нормы проектирования»;
- СТ РК 34.005-2002 «Информационная технология. Основные термины и определения»;
- СТ РК 34.006-2002 «Информационная технология. Базы данных. Основные термины и определения»;
- СТ РК 34.007-2002 «Информационная технология. Телекоммуникационные сети. Основные термины и определения»;

- СТ РК ИСО/МЭК 17799-2006 «Информационная технология. Методы обеспечения защиты. Свод правил по управлению защиты информации»;
- СТ РК ИСО/МЭК 27002-2009 «Информационные технологии. Средства обеспечения. Свод правил по управлению защитой информацию».
- СТ РК ИСО/МЭК 27002-2015 «Средства обеспечения. Свод правил по управлению защитой

3 Основные цели

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

3.2 Основные цели Положения ИБ:

- доступность обрабатываемой информации;
- устойчивое функционирование ИКИ Общества;
- обеспечение конфиденциальности информации, хранящейся, обрабатываемой СВТ и передаваемой по каналам связи;
- целостность и аутентичность информации, хранящейся и обрабатываемой в ИС Общества и передаваемой по каналам связи.

3.3 Для достижения целей поставлены следующие задачи:

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

4 Организация обеспечения ИБ

4.1.3а непосредственную организацию (построение) и обеспечение эффективного функционирования системы защиты информации отвечают:

- ЦИТиТ - структурное подразделение реализующее функционирование ИКИ, СВТ, ИС, ИБ.

- ЦИТиТ по согласованию с курирующим проректором членом Правления Общества определяет основные направления развития мер, направленных на защиту информации от НСД.

5 Категории пользователей ИС

5.1 К категориям пользователей ИС относятся:

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

6Объекты ИБ

6.1 Основными объектами защиты ИБ Общества являются:

- 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;
- 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;
- 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.

6.2 Объекты информационной инфраструктуры включают:

- технологическое оборудование (СВТ, сетевое и кабельное оборудование);

- ИР, содержащие сведения ограниченного доступа;
- программные средства (операционную систему (далее - ОС), СУБД, другое общесистемное и ППО);
- автоматизированные системы связи и передачи данных (средства телекоммуникации);
- каналы связи, по которым передается информация (в том числе ограниченного распространения);
- служебные помещения, в которых циркулирует информация ограниченного распространения;
- технические средства и системы, не обрабатывающие информацию, размещенные в помещениях, где обрабатывается (циркулирует) служебная информация.

6.3 Все средства ИБ до их применения в ИКИ Общества должны быть согласованы с ответственным лицом ЦИТиТ за ИБ и одобрены со стороны курирующего проректора члена Правления Общества. Аппаратные средства и ПО до их применения следует проверять на совместимость с другими компонентами системы.

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

7 Меры по реализации Положения ИБ

7.2 Внутренние пользователи, работающие в ИКИ Общества, обязаны строго соблюдать установленные требования Положения ИБ Общества.

7.3 Функциональные обязанности работников, специалистов по ИБ определяются внутренними регламентирующими документами Общества, должностными инструкциями работников 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».

7.4 Инструкция по обеспечению сохранности информации в НАО «Южно-Казахстанский государственный педагогический университет», составляющей служебную, коммерческую и иную охраняемую законом тайну».

7.5 Ответственное лицо за ИБ организует, выполняет, 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»

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

- оказывает консультации внутренних пользователей Общества с основами ИБ при оказании соответствующих услуг;
- обеспечивает надежность функционирования системы защиты;
- участвует в подготовке технических спецификаций, конструировании и в процессе приобретения программно-аппаратных комплексов;
- осуществляет практическое внедрение аппаратных и программных средств обеспечения ИБ в рамках Общества;
- участвует в формировании требований к ИБ в процессе создания, развития и применения

об ИС;

- участие в проектировании системы защиты, ее испытаниях и приемке в эксплуатацию;
- распределяет между авторизованными внутренними пользователями необходимых реквизитов защиты;
- наблюдает за функционированием системы защиты и ее элементов;
- консультирует внутренних пользователей ИС требованиям безопасной обработки информации;
- контролирует соблюдение внутренними пользователями ИС установленных правил обращения с защищаемой информацией в процессе ее автоматизированной обработки;
- принимает необходимые меры при выявлении попыток НСД к информации и при нарушениях правил функционирования системы защиты;
- участвует в проведении внутреннего аудита и мониторинга информационной безопасности;
- вносит на рассмотрение предложения по использованию криптографических средств защиты информации;
- обеспечивает разграничение прав доступа к информационным системам Общества.

7.7 Ответственное лицо за ИБ и работники ЦИТиТ, должны периодически направляться на обучение по повышению квалификации в области ИБ.

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

8Организационно-правовой статус ответственного лица за ИБ и СА

8.1 Ответственное лицо за ИБ имеет необходимые права:

- мониторинга и контроля информационной инфраструктуры Общества;
- доступа во все помещения Общества, где установлена ИС, СВТ и ЛВС Общества;

- прекращать автоматизированную обработку информации при наличии непосредственной угрозы для защищаемой информации.

8.2 СА по согласованию с ответственным лицом за ИБ имеют право:

- доступа во все помещения Общества, где установлена ИС, СВТ и ЛВС Общества;

- прекращать автоматизированную обработку информации при наличии непосредственной угрозы для защищаемой информации.

9 Общие требования конфиденциальности

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

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

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

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

9.5 При работе ИС Общества 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 Обществ, 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.

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

10.Требования по аутентификации пользователей в системе

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

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

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

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

10.5 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:

- заглавных букв: A, B, C;
- маленьких букв: a, Ь, c;
- цифр: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9;
- символов: '~!@#$%Л&*()_ + -= {}|[]\:

11 Требования конфиденциальности при передаче информации но линиям связи

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

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

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

11.4 Запрещается использовать общедоступные почтовые сервисы Интернета и Интернет- системы мгновенного общения работникам, работающим с конфиденциальной информацией.

12Требования по организации защиты общедоступных ресурсов

12.3 Общедоступные ресурсы (почтовые сервера, web-сервера, web-порталы и другие ресурсы) должны быть размещены в отдельном сегменте (сегментах) ЛВС Общества. Подключение указанных ресурсов к Интернет осуществляется через Единый шлюз доступа в сеть Интернет (Ғ.ТТ1ДИ). При этом должны применяться межсетевые экраны и системы обнаружения и предотвращения вторжений (IDP, IPS, Anti-DDoS).

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

12.5 Интернет-ресурс подключается к сети Интернет через Ғ.ТІТДИ.

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

- санкционирование операций размещения, изменения и удаления информационного контента;
- регистрацию авторства при размещении, изменении и удалении информационного контента;
- проверку загружаемого контента на наличие вредоносного кода;
- контроль целостности размещенного информационного контента;
- контроль аномальной активности пользователей и программных роботов.

С целью контроля обеспечения конфиденциальности должны обеспечиваться следующие мероприятия:

- ежегодная сверка списка официально зарегистрированных пользователей и пользователей, работающих в ИС.
- ежегодный аудит ИБ на соблюдение требований настоящего Положения ИБ.
- постоянный мониторинг инструментальными, программными средствами ИБ ИКИ Общества.

13Общие требования целостности

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

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

14Требования безопасности ИС при разработке, усовершенствовании и обслуживании

14.3 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 Общества.

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

14.5 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.

14.6 Запуск программного средства в эксплуатационную среду должен

осуществляться только при наличии протокола тестирования с положительным заключением.

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

15Требования к компонентам обеспечения ИБ сети передачи данных

15.1 Для обеспечения безопасного функционирования ИС Общества 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.

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

15.3 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.

16Требования к управлению инцидентами безопасности

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

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

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

17Требования к защите информации от несанкционированного доступа

17.1 Защита от НСД должна обеспечивать:

- возможность идентификации на цифровых сертификатах инфраструктуры открытых ключей;
- авторизацию пользователей для доступа к информационно-вычислительным ресурсам системы, требующим наличия соответствующих разрешений;
- персональное определение прав на ввод, корректировку, просмотр данных;

- персональное определение прав на доступ к системным ресурсам;
- аудит событий по идентификации пользователей;
- реализацию в ИС функций распределения пользователей по группам и присвоения им соответствующих прав доступа для предотвращения несанкционированного удаления, копирования, модификации информации;
- защищенные каналы связи на физическом уровне;
- протоколирование работы пользователей с критическими функциями и приложениями ИС.

17.2 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.

18. Требования к применению электронной почты и Интернета

18.1 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:

-уязвимость электронных сообщений по отношению к несанкционированному перехвату и модификации;

-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;

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

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

-последствия для системы безопасности от раскрытия содержания каталогов;

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

18.2 Подключение к сети Интернет должно осуществляться исключительно через Единый шлюз доступа к сети Интернет, не имеющей сопряжения с информационно-коммуникационной и локальной сетью Общества.

19 Требования к резервному копированию и восстановлению

19.1 Резервному копированию подлежит вся информация, обрабатываемая в ИКИ Общества.

19.2 Требования к резервному копированию описаны в Регламенте

резервного копирования и восстановления информации к Положению ИБ.

19.3 Резервное копирование ППО и системного ПО должно производиться ответственными лицами в соответствии с графиком резервного копирования. Все ППО и системное ПО Общества должны реализовываться после объемного и успешного тестирования в отдельной инструментальной среде на предмет применимости, безопасности, воздействия на другие системы и удобство пользования.

19.4 При каждом изменении версии ППО (исправления ошибок, добавление функциональности) старая версия ППО должна храниться в течение 3 месяцев.

20 Требования к антивирусной безопасности

20.1 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.

21 Общие требования доступности

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

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

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

22 Требования к отказоустойчивости

22.1 Аппаратно-программное обеспечение должно обеспечивать выполнение задач ИС Общества со временем однократного простоя не более 10 часов и суммарным временем простоя не более 48 часов в год.

22.2 В случае возникновения внештатной ситуации, произошедшей с производственным сервером ИС, восстановление ППО, системного ПО и ОС должно быть произведено в течение 9 часов.

22.3 Восстановление работоспособности и обеспечение непрерывной работы ИС Общества 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.

22.4 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.

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

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

23Требование к анализу и оценке рисков

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

23.2 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 Общества с целью принятия дальнейших организационно распорядительных мер.

23.3 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».

23.4 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 Общества.

24 Контроль эффективности принимаемых мер защиты

24.1 Для поддержания требуемого уровня ИБ в Обществе 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 Общества.

24.2 Основными механизмами контроля эффективности принимаемых мер защиты являются мониторинг и аудит ИБ Общества.

24.3 Аудит ИБ Общества осуществляется согласно Правилам проведения аудита информационных систем.

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

24.5 Контроль требований настоящего Положения ИБ на соответствие

требованиям ИБ осуществляется работниками по ИБ.

25 Пересмотр Положения ИБ

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

25.2 Пересмотр Положения ИБ производится в целях:

- усовершенствования целей и мер контроля ИБ;
- усовершенствования подхода к управлению ИБ и бизнес-процессами Общества;
- улучшения распределения ресурсов и обязанностей.

25.3 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 Общества.

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

25.5 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.

25.6 Руководством Общества 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 Общества.

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

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

25.9 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».

26 Ответственность

26.1 Ответственное лицо за ИБ совместно с курирующим проректором-членом Правления Общества обеспечивает:

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

26.2 Курирующий проректор-член Правления Общества по представлению ответственного лица за ИБ должен:

- утверждать разрабатываемые, пересматриваемые правовые документы по ИБ Общества;
- вести контроль за эффективностью реализации Положения ИБ;
- утверждать распределение специфических ролей и обязанностей по ИБ;
- инициировать планы и программы по осведомлённости об ИБ;

26.3 Руководители структурных подразделений Общества несут ответственность за выполнение требований Положения, а также за ознакомление с настоящим Положением

26.4 ИБ своих подчиненных, в том числе вновь принятых работников.

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

26.6 Нарушение требований Положения ИБ квалифицируется как дисциплинарный проступок, заключающийся в неисполнении или ненадлежащем исполнении трудовых обязанностей. Работник, допустивший нарушение требований Положения ИБ, привлекается к дисциплинарной ответственности в соответствии с Трудовым кодексом Республики Казахстан и требованием пунктов 8.2.3 и 13.2.3 Государственного стандарта СТ РК ИСО/МЭК 27002-2009 «Информационные технологии. Средства обеспечения. Свод правил по управлению защитой информацию».