18/1-93 29.05.2026

УТВЕРЖДАЮ
Ректор АО «ЮКМА»
Ж.Сейтжанова
2026 г.

ПОЛОЖЕНИЕ
ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
АО «ЮЖНО-КАЗАХСТАНСКАЯ МЕДИЦИНСКАЯ АКАДЕМИЯ»

П 504 - 2026

Число	Копия	Издание
		Второе

г. Шымкент

1. **РАЗРАБОТАН И ВНЕСЕН** специалистом по кибербезопасности и защите информационных систем **АО «ЮКМА»**

2. **УТВЕРЖДЕНО** решением Совета по качеству **АО «ЮКМА»**

Периодичность проверки – 3 года

СОДЕРЖАНИЕ

ПАСПОРТ ДОКУМЕНТА

Наименование документа:	Положение по информационной безопасности АО «ЮЖНО-КАЗАХСТАНСКАЯ МЕДИЦИНСКАЯ АКАДЕМИЯ»
Краткое описание:	Положение по информационной безопасности АО «ЮЖНО-КАЗАХСТАНСКАЯ МЕДИЦИНСКАЯ АКАДЕМИЯ»
Тема:	Информационная безопасность
Статус:	Второй
Дата утверждения:	« ___ » _____20_____г.
Дата завершения действия:	« ___ » _____20_____г.
Дата аудита:	Ежегодно

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящее Положение по информационной безопасности (далее Положение) учитывает современное состояние и ближайшие перспективы развития корпоративной сети передачи данных (далее - КСПД) АО «Южно-Казахстанской Медицинской Академий (далее – АО «ЮКМА») цели, задачи и правовые основы эксплуатации, режимы функционирования, а также анализ угроз безопасности для ее ресурсов.

Требования Положения распространяются на структурные подразделения АО «ЮКМА», в которых осуществляется автоматизированная обработка информации, в том числе информации с ограниченным распространением (служебная информация) или персональных данных, а также осуществляющих сопровождение, обслуживание и обеспечение функционирования АО «ЮКМА». Положение распространяется также на другие организации и учреждения, осуществляющих взаимодействие с АО «ЮКМА» в качестве поставщиков и потребителей (пользователей) информации и услуг.

Ответственным дожностным лицом за непосредственную организацию (построение) и обеспечение эффективного функционирования системы защиты информации является сотрудник КТИЦ «Специалист по кибербезопасности и защите информационной системы».

Сотрудник КТИЦ «Специалист по кибербезопасности и защите информационной системы» проводит необходимые технические и организационные мероприятия для обеспечения информационной безопасности в АО «ЮКМА».

Сотрудник КТИЦ «Специалист по кибербезопасности и защите информационной системы» осуществляет организацию квалифицированной разработки (совершенствования) системы защиты информации и организационного (административного) обеспечения ее функционирования в АО «ЮКМА.

2. НОРМАТИВНАЯ ССЫЛКИ

Настоящие положение разработаны с учетом требований следующих нормативных документов:

- Закон Республики Казахстан «Об информатизации», № 418-V ЗРК от 24 ноября 2015 года, с изменениями и дополнениями;
- Государственная программа «Информационный Казахстан», Указ Президента Республики Казахстан от 14 ноября 2011 года № 174 «О Концепции

информационной безопасности Республики Казахстан до 2016 года»;

- Законы Республики Казахстан «О национальной безопасности Республики Казахстан», «О государственных секретах», «О противодействии терроризму», «Об электронном документе и электронной цифровой подписи», «Об информатизации», «О техническом регулировании», «О лицензировании», «О средствах массовой информации»;
- Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности» и иные акты Республики Казахстан и Университета, регламентирующие вопросы обеспечения информационной безопасности.
- К 121-2023 Кодекс академической честности;
- Е 507-2026 Правила применения искусственного интелекта и цифровых технологий в АО «ЮКМА».

3. ПРАВОВАЯ БАЗА ПОЛОЖЕНИЯ

Настоящее Положение детализирует требования по решению вопроса обеспечения информационной безопасности в единой информационной телекоммуникационной среде, объединяющей ИС АО «ЮКМА.

Положение информационной безопасности АО «ЮКМА является методологической базой:

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

Научно-методической основой Положения является системный подход, предполагающий проведение исследований, разработку системы защиты информации в процессе ее обработки в информационных системах с учетом всех факторов, оказывающих на нее влияние и комплексного применения различных мер и средств защиты.

Основные требования Положения базируются на качественном осмыслении вопросов информационной безопасности, не концентрируя внимание на экономическом (количественном) анализе рисков и обосновании необходимых затрат на защиту информации.

4. ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЕ

В настоящем документе применяют следующие термины с соответствующими определениями, сокращениями и обозначениями.

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.

Безопасность информации – защищенность информации от ее нежелательного разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности, а также незаконного ее тиражирования.

Доступность – возможность для авторизованного пользователя автоматизированной информационной системы за приемлемое время получить информационную услугу, предусмотренную функциональностью.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационная безопасность – комплекс административно-правовых, организационно-распорядительных и технических мер, направленные на обеспечение конфиденци - альности, целостности и санкционированной доступности информации в процессе ее сбора,обработки, передачи и хранения.

Конфиденциальность – защита от несанкционированного ознакомления.

Несанкционированное действие – действие субъекта в нарушение установленныхв системе правил обработки информации.

Пользователь – субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации.

Сеть (локальная сеть, ЛВС, LAN) – группа точек, узлов или других устройств, соединенных коммуникационным набором оборудования, обеспечивающих соединение станций и передачу между ними информации.

Риски информационной безопасности – реально или потенциально возможные действия по реализации опасных воздействующих факторов с целью преднамеренного или случайного нарушения режима функционирования объекта.

Уязвимость – любая характеристика автоматизированной системы, использование которой может привести к реализации угроз.

Целостность информации – свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому ее состоянию).

Шифрование – преобразование данных в нечитабельную форму, используя ключи шифрования-расшифровки.

Искусственный интеллект – функциональная способность имитировать когнитивные функции, присущие человеку, обеспечивающая результаты, сопоставимые с результатами интеллектуальной деятельности человека или превосходящие их.

Пользователь системы искусственного интеллекта – человек, использующий систему искусственного интеллекта для выполнения конкретной функции и (или) задачи.

Результат деятельности системы искусственного интеллекта – информация, решение или действия, включая работы и (или) услуги, производимые системой искусственного интеллекта, независимо от формы их представления.

Академическая честность — это соблюдение принципов искренности, справедливости и ответственности в процессе преподавания, обучения и научной работы, что обеспечивает профилактику и предотвращение коррупции.

Принципы академической честности и противодействия коррупции:

- честность - не брать взятки, не предоставлять ложную информацию;
- справедливость - предоставление равных возможностей для всех, отсутствие привилегий по знакомству;
- ответственность - отчет за свои действия, соблюдение законов и правил;
- доверие - формирование доверительной среды в обществе и учебном заведении;
- уважение - соблюдение прав и уважение к труду других лиц;
- открытость - прозрачность принимаемых решений и системы оценивания.

АО «ЮКМА» - Акционерное общество «Южно–Казахстанская медицинская академия»;

ИС - информационная система;

ИР - информационные ресурсы;

СВТ - средства вычислительной техники;

ОС- операционная система;

СУБД - система управления базами данных;

ПО - программное обеспечение;

НСД - несанкционированный доступ;

ЛВС - локальная вычислительная сеть;

КТИЦ - компьютерно-тестовый, издательский центр.

5. ЗАДАЧИ И ОБЯЗАНОСТИ

Основной целью, на достижение которой направлены все пункты Положения, является надежное обеспечение информационной безопасности и как следствие недопущение нанесения материального, физического, морального или

иного ущерба АО «ЮКМА в результате информационной деятельности.

Для достижения поставленной цели необходимо решить следующие **задачи**:

- защита от вмешательства посторонних лиц в процесс функционирования информационных ресурсов АО «ЮКМА;
- разграничение доступа зарегистрированных пользователей к информации, аппаратными, программными и криптографическими средствами защиты, используемыми в ИС;
- регистрация в системных журналах действий пользователей при использовании сетевых ресурсов;
- периодический контроль корректности действий пользователей системы путем анализа содержимого этих журналов специалистами информационной безопасности;
- контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения;
- защита информации от несанкционированной модификации, искажения;
- контроль целостности используемых программных средств, а также защиту системы от внедрения вредоносного программного обеспечения;
- защиту служебной тайны и персональных данных от утечки, несанкционированного разглашения или искажения при ее обработке, хранении и передаче по каналам связи;
- обеспечение авторизации и аутентификации пользователей, участвующих в информационном обмене;
- своевременное выявление угроз информационной безопасности, причин и условий, способствующих нанесению ущерба;
- создание механизма оперативного реагирования на угрозы информационной безопасности и негативные тенденции;
- создание условий и инструкций для минимизации и локализации нанесенного ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения информационной безопасности.
- создание и обеспечения бесперебойной работы электронного документооборота.
- постоянный аудит политики безопасности внутренним аудитом не реже 1 раза в год руководителем КТИЦ.

Сотрудник АО «ЮКМА» (независимо от должности и компетенций) обязан формировать культуру академической честности и противодействия коррупции среди обучающихся и коллег, а также строго придерживаться этих принципов.

Сотрудник обязан соблюдать требования внутренних нормативных документов, касающихся применения технологий искусственного интеллекта и

цифровых решений, включая принципы их безопасного, этичного и ответственного использования.

6. НАЗНАЧЕНИЕ И ОБЛАСТЬ ПРИМЕНЕНИЯ

Настоящее Положение может быть предоставлено официальным представителям любых органов и ведомств Республики Казахстан, представителям органов сертификационного аудита, партнерам АО «ЮКМА», подрядным организациям и частным лицам, выполняющим работы для АО «ЮКМА», а также другим заинтересованным организациям и лицам как на территории Республики Казахстан, так и за ее пределами. Настоящий документ разработан с учетом накопленного опыта в сфере обеспечения безопасности информационных технологий в АО «ЮКМА».

Настоящее Положение разработано с целью установления единого подхода в АО «ЮКМА» к управлению безопасностью информации.

Настоящий документ обязателен для применения во всех подразделениях и всеми должностными лицами в АО «ЮКМА», при обеспечении и управлении информационной безопасности АО «ЮКМА».

Положение распространяется на все аспекты деятельности АО «ЮКМА», тем или иным образом влияющие на информационную безопасность АО «ЮКМА».

Действие настоящего документа распространяется на деятельность всех подразделений АО «ЮКМА».

Требования настоящего документа распространяются на процессы предоставления сервисов в области информационных технологий, включая облачные сервисы, сервисы эксплуатации, технической поддержки, мониторинга и обслуживания сетевой инфраструктуры, вычислительных систем, комплексов и программного обеспечения, предоставляемых пользователям.

7. ПРИНЦИПЫ ИНФОРМАЦИОННОЙ ПОЛИТИКИ

Основными принципами построения системы обеспечения безопасности информации АО «ЮКМА» и ее функционирования являются:

1) законность – соблюдение законодательства по защите информации и законных интересов всех участников информационного обмена;

2) системность – подход к вопросам организации информационной безопасности должен быть логическим и последовательным: в первую очередь оценка риска информационной безопасности исходя из реальных угроз и уязвимости информационных ресурсов, затем создание комплекса организационных и технических мер и средств защиты, учитывающих специфику АО «ЮКМА»;

3) эффективность – реализуемые в разумно достаточном объеме меры и мероприятия по обеспечению информационной безопасности должны сводить риски к минимуму, при этом адекватность и эффективность защитных мер должна быть оцениваема на регулярной основе;

4) целесообразность – соблюдение соразмерности затрат на обеспечение защиты информации и потенциальных потерь при реализации угроз;

5) непрерывность – принцип функционирования системы информационной безопасности, обеспечивающий непрерывную работу технических и программных средств, а также включающий меры по постоянному контролю системы информационной безопасности;

6) взаимодействие и координация – осуществление мер обеспечения информационной безопасности на основе четкой взаимосвязи подразделения, в функции которого входит обеспечение функционирования IT инфраструктуры и информационных систем АО «ЮКМА» и подразделений-пользователей информационных ресурсов, сторонних специализированных организаций в области защиты информации и обслуживания информационных систем, координации их усилий для достижения поставленных целей, а также взаимодействия с с иными заинтересованными органами;

7) совершенствование – совершенствование мер и средств защиты информации на основе собственного опыта, появления новых технических средств с учетом изменений в методах и средствах атак информационных ресурсов, нормативно-технических требований, достигнутого отечественного и зарубежного опыта;

8) приоритетность – категорирование (ранжирование) всех информационных ресурсов АО «ЮКМА» по степени важности и оценка реальных, а также потенциальных угроз информационной безопасности;

9) информированность и персональная ответственность – пользователи информационных ресурсов должны знать о наличии системы контроля и защиты информации, информационные сервисы индивидуально идентифицируют пользователей и инициируемые ими процессы;

10) соответствие стандартам – система информационной безопасности соответствует международным стандартам в данной области;

11) обязательность контроля – контроль за деятельностью пользователей, а также мониторинг IT инфраструктуры должен осуществляться на основе применения средств оперативного контроля и регистрации, охватывать как несанкционированные, так и санкционированные действия.

8. ОБЪЕКТЫ ИНФОРМАЦИОННЫЕ БЕЗОПАСНОСТИ

Основными объектами защиты ИБ АО «ЮКМА» являются:

- информационные ресурсы 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.

Объекты информационной инфраструктуры включают:

- технологическое оборудование (СВТ, сетевое и кабельное оборудование);
- информационные ресурсы, 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.

9. СРЕДСТВА И МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ

Средства и меры защиты от утечки информации по каналам. Ответственное лицо за ИБ организует, выполняет, контролирует и координирует вопросы и работы, связанные с защитой информации в соответствии с требованиями.

Защита информации от утечки по каналам их передачи из/в АО «ЮКМА» достигается, путем применения комплексных программных, технических средств защиты и организационных мер.

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.

В соответствии с используемыми каналами передачи электронной информации в АО «ЮКМА» предусматриваются необходимые технические средства защиты (межсетевой экран и т.п.). Организуется система регистрации, передачи, приема и хранения носителей информации, предусматриваются надлежащие способы их уничтожения, с целью исключения возможности восстановления записанных на них сведений. Технические каналы передачи информации оснащаются соответствующими средствами защиты. Создается надежная система охраны зданий и сооружений, организуется пропускной режим в помещения АО «ЮКМА» (карты доступа RFID, турникет, Face-ID) для предотвращения доступа посторонних лиц.

Меры по защите средств вычислительной техники:

- защита СВТ от несанкционированного доступа в АО «ЮКМА» строится по нескольким направлениям. Создаются автоматизированные средства регистрации пользователей, система блокирования учетных записей и оповещения сотрудников об угрозе или проникновении в СВТ, согласно правилам регистрации пользователей в корпоративной сети передачи данных и Плану по обеспечению непрерывной деятельности информационных систем АО «ЮКМА»;
- определяются организационные меры по предотвращению несанкционированного доступа (далее НСД), в том числе в случае утраты/компрометации паролей и выхода из строя СВТ, согласно Политике организации парольной защиты;
- в случае обнаружения фактов НСД к информационным ресурсам и системам АО «ЮКМА» или выявления потенциальной угрозы информационной безопасности Сотрудник КТИЦ «Специалист по кибербезопасности и защите информационной системы» немедленно информирует руководство АО «ЮКМА»;
- защита от аппаратных спецвложений, нелегального внедрения и использования неучтенных программ;
- для предотвращения аппаратных спецвложений используются меры физической защиты, устанавливаются средства видеонаблюдения и контроля доступа в серверное помещение АО «ЮКМА»;
- использование для производственных целей прикладного ПО, внешних носителей информации не входящего в состав базового комплекса санкционируется управлением сервиса и информационной безопасности по согласованию ректором АО «ЮКМА»;
- защита от несанкционированного копирования данных пользователем;

- служебная и иная защищаемая информация, обрабатываемая и хранящаяся в информационных системах АО «ЮКМА», подлежит копированию и передаче третьему лицу только с разрешения ректора АО «ЮКМА»;
- за копирование и передачу служебной и иной защищаемой информации третьему лицу без разрешения, пользователь привлекается к дисциплинарной ответственности;
- защита информации, отображаемой на мониторе средств вычислительной техники;
- защита достигается путем ограничения физического доступа к средствам отображения информации, исключения наблюдения за отображаемой информацией посторонними лицами, согласно Правилам пользователя по эксплуатации средств вычислительной техники и программного обеспечения АО «ЮКМА»;
- защита от действий вредоносных программ, вирусов;
- организационные меры изложены в правилах по антивирусной защите компьютеров и серверов;
- защита от хищения носителей информации;
- в АО «ЮКМА» устанавливается определенный порядок хранения и использования носителей информации, согласно Правилам пользователя по эксплуатации средств вычислительной техники и программного обеспечения АО «ЮКМА»;
- при передаче носителя цифровой информации для повторного использования за пределами АО «ЮКМА» проводится его очистка с целью исключения несанкционированного разглашения защищаемых сведений;
- требования по организации защиты общедоступных ресурсов;
- общедоступные ресурсы (почтовые сервера, web-сервера, web- порталы и другие ресурсы) должны быть размещены в отдельном сегменте ЛВС АО «ЮКМА». При этом должны применяться межсетевые экраны и системы обнаружения и предотвращения вторжений (IDP, IPS, Anti-DDoS).

Для обеспечения ИБ Интернет-ресурсов необходимо применять систему управления содержимым, 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;
- постоянный мониторинг инструментальными, программными средствами ИБ информационно-коммуникационной инфраструктуры АО «ЮКМА».

Требования безопасности ИС при разработке, усовершенствовании и обслуживании:

- требования к элементам обеспечения ИБ до разработки ИС необходимо идентифицировать и согласовать с ответственным лицом за ИБ и внести на утверждение ректору АО «ЮКМА» ;
- разработка программных средств или изменение исходного кода в рамках сопровождения программных средств должно осуществляться в разработочной среде;
- 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;
- запуск программного средства в эксплуатационную среду должен осуществляться только при наличии протокола тестирования с положительным заключением;
- ребования безопасности должны учитывать ценность информационных активов, потенциальный ущерб бизнес-процессу.

Требования к применению электронной почты и Интернета. 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.

Меры по защите коммуникационных средств. Основные и резервные телекоммуникационные сервисы соответствующим образом отделяются друг от друга, чтобы не подвергаться одним и тем же угрозам, согласно мерам по обеспечению непрерывной деятельности информационных систем АО «ЮКМА» и правилам по резервному копированию информации.

Защита от незаконного подключения к корпоративной сети передачи данных. Защита коммуникаций от незаконного подключения кроме средств санкционированного электронного и физического доступа, осуществляется программными, техническими средствами и организационными мерами. Проводятся необходимые мероприятия для своевременного выявления, предупреждения и пресечения неправомерных действий лиц по получению доступа к коммуникациям. За незаконное подключение и попытка незаконного подключения к линиям связи и сетевому оборудованию лица несут ответственность в соответствии с законодательством Республики Казахстан.

Защита от повреждения, некорректного функционирования, частичного или полного отказа сетевого оборудования:

- повреждение, некорректное функционирование, частичный, полный отказ сетевого оборудования АО «ЮКМА» может быть, в первую очередь, в результате возникновения аварий, стихийных бедствий и иных внештатных ситуаций;

- в АО «ЮКМА» принимаются меры, связанные с внедрением средств защиты, которые будут использоваться в случае стихийных бедствий (пожаров, наводнений и землетрясений), а также в различных нештатных ситуациях;

- защита от неправомерного включения, выключения оборудования. Сетевое оборудование АО «ЮКМА» вводится в эксплуатацию, сопровождается и используется в соответствии с установленным регламентом. Включение и отключение оборудования производится ответстенными сотрудниками КТИЦ;

- защита от неправомерной модификации передаваемых данных, технической и служебной информации. Кроме средств санкционированного доступа к коммуникационным средствам и сетевому оборудованию, защита передаваемых данных от модификации осуществляется программно-техническими и организационными мерами;

Меры по защите системы архивирования. Определяется порядок резервного копирования, хранения и восстановления программных продуктов и информационных систем. Хранилище резервных копий размещается в помещении специально оборудованным согласно Плану по обеспечению непрерывной

деятельности информационных систем. Обеспечивается санкционированный доступ к хранилищу резервных копий для своевременного восстановления информации и информационных систем в случае сбоя, аварии и иных нештатных ситуациях.

Разрабатывается План по обеспечению непрерывной деятельности информационных систем, в котором также определяются меры по защите архивов на случай возникновения аварий, стихийных бедствий и других нештатных ситуаций, согласно правилам по резервному копированию информации.

Прочие меры по защите информации. Следует принять исчерпывающие меры защиты информации на всех запоминающихся устройствах при передаче СВТ на ремонт сторонним организациям.

10. ТРЕБОВАНИЯ И ОТВЕТСТВЕННОСТЬ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Соблюдение требований Положения информационной безопасности обязательно для всех пользователей информационных систем АО «ЮКМА». Проведение планового аудита информационной безопасности является одним из основных методов проверки эффективности мер по защите информации. Результаты аудита могут служить основанием для пересмотра некоторых пунктов Положения и внесения в них необходимых корректировок.

Аудит информационной безопасности АО «ЮКМА» целесообразно проводить ежегодно руководителем КТИЦ должен проводиться пересмотр Положения на предмет соответствия предъявляемым требованиям, в случае возникновения необходимости вносить изменения и дополнения.

Работник обеспечивает проверку достоверности результатов, полученных при использовании инструментов искусственного интеллекта, соблюдение требований конфиденциальности и защиты данных, принципов академической честности, а также несет личную ответственность за окончательные решения и материалы, подготовленные с применением данных технологий.

Несоблюдение порядка применения технологий искусственного интеллекта и цифровых решений рассматривается как действие, противоречащее принципам академической честности.

Настоящее Положение определяет требования в следующих областях обеспечения информационной безопасности:

- обучение и информированность персонала;
- парольная политика;
- политика резервного копирования;
- антивирусная политика;

- политика управления инцидентами по ИБ;
- политика использования не корпоративных почтовых адресов для обмена служебными сообщениями по электронной почте;
- политика по физической безопасности в АО «ЮКМА» ;
- политика использования и управления внешними съемными носителями информации (все виды носителей) и регламент эксплуатации данных носителей;
- правила доступа к сети Интернет;
- политика удаленного доступа;
- политика межсетевого экранирования.

Обучение и информированность персонала. Для обеспечения должного уровня ИБ, работники структурных подразделений АО «ЮКМА» должны быть хорошо информированы в данных вопросах и при необходимости дополнительно обучены. Для этого в АО «ЮКМА» должна быть организована эффективная система обучения и контроля знаний работников в области ИБ, включающая:

- обучение вопросам обеспечения ИБ в АО «ЮКМА» при найме на работу;
- ознакомление с действующими нормативными документами по вопросам ИБ;
- при необходимости периодический контроль знаний по вопросам ИБ, в части касающейся выполняемых работниками АО «ЮКМА» функций по защите информационных активов;
- при необходимости повышение квалификации лиц, выполняющих функции специалистов ИБ, сетевых администраторов, системных администраторов, путем обучения их на специализированных курсах по вопросам ИБ;
- организацию доступа работников АО «ЮКМА» к нормативным документам по вопросам ИБ для самостоятельного изучения.

Парольная Политика. Основным инструментом защиты информационных систем АО «ЮКМА» и информации хранящейся в них (далее - ИС), является персонализированная учетная запись, состоящая из идентификатора и пароля. Пароль должен выбираться пользователем ИС самостоятельно. Пароли должны соответствовать следующим требованиям:

- минимальная длина пароля пользователя должна быть не менее 7 символов;
- при смене пароля пользователь не должен повторно использовать предыдущие три пароля;
- минимальная длина пароля службы администрирования и системных учетных записей (root, administrator и т.п.) должна быть не менее 12 символов, история паролей при смене не менее 20 паролей;
- пароли должны быть сложными, состоять из комбинации цифр, букв в

верхнем и нижнем регистре;

- пароли не должны включать в себя легко вычисляемые сочетания символов (имена, фамилии, номера телефонов, словарные слова и т.п.) и какие либо сокращения;
- имена учетных записей запрещено использовать в качестве паролей.

Пользователь должен обеспечить конфиденциальность личного пароля. Передача пароля другим коллегам, работникам службы КТИЦ, руководству или другим третьим лицам строго запрещена. При работе с паролями должны выполняться следующие требования:

- новой учетной записи назначается временный пароль;
- первый вход в ИС пользователь должен осуществить с временным паролем;
- после аутентификации в ИС, пользователю должна быть предоставлена возможность смены пароля;
- пользователь должен сменить временный пароль после первого входа в ИС;
- пароли стандартных «по умолчанию» учетных записей ИС должны быть изменены;
- при вводе пароль не должен отображаться на экране в открытом виде;
- пользователь должен блокировать сеанс работы, если оставляет свое рабочее место на длительное время;
- сеансы работы, оставленные пользователем без присмотра, должны автоматически блокироваться по истечению 15 минут;
- записи о паролях в ИС должны храниться в зашифрованном виде и быть доступны только их владельцу;
- пользователям запрещено записывать, хранить свои пароли на бумажном носителе.

Политика резервного копирования. В целях защиты информации от преднамеренного или непреднамеренного ее уничтожения и фальсификации должно быть обеспечено обязательное резервирование всей информации, являющейся важной. При взаимодействии и по согласованию с владельцами информации должны быть выполнены следующие работы:

- классификация информации, подлежащей резервному копированию и/или архивированию;
- расчет объема информации, подлежащей резервному копированию и/или архивированию;
- составление расписания для системы резервного копирования;
- определение методов резервного копирования;
- определение ответственных лиц за хранение и резервирование

информации;

- определение и согласование сроков хранения резервных и/или архивных копий, схемы ротации носителей и их количество;
- определение требований к восстановлению и тестированию резервных копий ИС.

Антивирусная Политика. Для защиты ИС и своевременного блокирования вредоносных программ (далее - Вирусов), в АО «ЮКМА» должна применяться Система Антивирусной Защиты. Система Антивирусной Защиты должна основываться на клиент-серверной технологии. Клиентская часть должна быть установлена на всех рабочих станциях и ноутбуках. Серверная часть должна предоставлять возможность централизованного управления и обновления антивирусного приложения, установленного на рабочих станциях и ноутбуках, а также обеспечивать возможность мониторинга состояния антивирусного приложения и оповещения об этих событиях ответственных лиц. Система Антивирусной Защиты должна отвечать следующим требованиям:

- мониторинг возможных каналов проникновения Вирусов на всех средствах обработки информации, должен производиться в режиме реального времени;
- не реже одного раза в неделю должна производиться полная проверка средств обработки информации на предмет наличия Вирусов;
- пользователи средств обработки информации не должны иметь возможность отключения или изменения настроек антивирусного приложения;
- пользователи должны иметь возможность инициировать частичную или полную проверку средства обработки информации на предмет наличия Вирусов;
- обновление баз Вирусных сигнатур должно производиться регулярно, но не реже одного раза в сутки;
- обновление клиентских баз Вирусных сигнатур и приложения должно производиться незамедлительно после получения данных обновлений серверной частью.

Политика управления инцидентами по ИБ. Для инцидентов в области ИБ должны выполнятся следующие мероприятия:

- немедленное реагирование на инцидент (защита системы);
- предоставление информации об инциденте руководителю структурного подразделения;
- анализ инцидента;
- восстановление работоспособности ИС, возобновление учебного процесса и бизнес процессов АО «ЮКМА»;
- расследование причин инцидента, установление виновных;
- выработка корректирующих шагов (при необходимости) направленных на улучшение системы обеспечения ИБ;

- документирование инцидента.

Политика использования не корпоративных почтовых адресов для обмена служебными сообщениями по электронной почте. Работники не должны использовать внешнюю электронную почту как официальное средство связи. В тех случаях, когда нарушение настоящего положения повлекли за собой утечку конфиденциальной информации, несанкционированное копирование, модификацию, блокирование или уничтожение информации, а также в случаях создания ситуаций, которые потенциально могли бы привести к таким последствиям, необходимо выполнить мероприятия по управлению инцидентами в области ИБ, согласно положениям.

Политика по физической безопасности в АО «ЮКМА». Все объекты критичные с точки зрения информационной безопасности (все сервера баз данных, телефонная станция, маршрутизатор, файервол) должны находиться в отдельном помещении, доступ в которое разрешен только работникам, имеющими соответствующее разрешение от руководителя КТИЦ. Помещение должно быть оборудовано принудительной вентиляцией, пожарной сигнализацией и системой автоматического пожаротушения. Доступ в помещение посторонним лицам запрещен. Технический персонал, осуществляющий уборку помещения, ремонт оборудования, обслуживание кондиционера и т.п. может находится в помещении только в присутствии работников, имеющих право находится в помещении для выполнения своих должностных обязанностей.

Политика использования и управления внешними съемными носителями информации (все виды носителей) и регламент эксплуатации данных носителей. Внешние носители информации (USB флэш накопители, внешние жесткие диски, коммуникаторы, портативные компьютеры и т.д.) могут быть использованы с учетом следующих исключений:

- рекомендуется хранить информацию на зашифрованном внешнем съемном носителе;
- хранение служебной информации на личных внешних съемных носителях запрещено;
- запрещено передавать внешние съемные носители информации третьим лицам;
- запрещено оставлять внешние съемные носители информации без присмотра;

Правила доступа к сети Интернет. Доступ к развлекательным, вредоносным сайтам, а также к социальным сетям может быть заблокирован по инициативе руководства АО «ЮКМА». Руководителя КТИЦ определяются группы пользователей и список запрещенных им ресурсов сети Интернет. При работе в корпоративной сети АО «ЮКМА» и сети Интернет работникам запрещается:

- рассылать информацию коммерческого характера (SPAM);
- скачивать и устанавливать на компьютер программное обеспечение не входящее в список разрешенного к использованию;
- посещать интернет-ресурсы, не имеющие непосредственного отношения к работе и выполнению служебных обязанностей;
- осуществлять подписку на рассылку информации непроизводственного характера;
- сообщать адрес электронной почты в непроизводственных целях;
- использовать Интернет для получения материальной выгоды или непроизводственных целей, в том числе осуществляя торговлю через Интернет.

Политика удаленного доступа. Удаленный доступ к ИС через сеть Интернет или каналы связи, не находящиеся под контролем АО «ЮКМА», должен быть защищен посредством использования технологии VPN. Используемые в АО «ЮКМА» средства реализации технологии VPN должны обеспечивать выполнение следующих требований:

- наличие уникального идентификатора у каждого пользователя;
- шифрование среды передачи данных;
- при необходимости проверка соответствия конфигурации пользовательских устройств, требованиям корпоративных политик;
- ведение аудиторского следа удачных и неудачных попыток авторизации в процессе подключения;
- использование защищенных протоколов передачи данных.

Политика межсетевого экранирования. В АО «ЮКМА» должны быть реализованы межсетевые экраны, которые классифицируются по следующим признакам:

- по исполнению (аппаратно-программный и программный);
- по используемой технологии (контроль состояния протокола, на основе модулей посредников (proxy). Конфигурация межсетевого экрана должна быть полностью формализована. Межсетевые экраны должны управлять всем входящим и исходящим трафиком.

Требования к управлению инцидентами безопасности:

- о случаях нарушения ИБ следует сообщать незамедлительно ректору АО «ЮКМА» ;
- должны быть установлены зоны ответственности и процедуры, чтобы гарантировать быструю, результативную и упорядоченную реакцию на инциденты в системе защиты информации;
- должны быть приняты механизмы для ведения мониторинга инцидентов в системе защиты информации и постоянно их контролировать.

Требования к отказоустойчивости:

- аппаратно-программное обеспечение должно обеспечивать выполнение задач ИС АО «ЮКМА» со временем однократного простоя не более 10 часов и суммарным временем простоя не более 48 часов в год;
- в случае возникновения внештатной ситуации, произошедшей с производственным сервером ИС, восстановление ПО, системного ПО и ОС должно быть произведено в течение 9 часов;
- восстановление работоспособности и обеспечение непрерывной работы ИС АО «ЮКМА» 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;
- 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;
- 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.

Требование к анализу и оценке рисков:

- положение ИБ первоначально должно основываться на данных, полученных в результате анализа и оценки рисков ИБ;
- с целью совершенствования Положения ИБ должен проводиться ежегодный анализ и оценка рисков ИБ. Данный анализ основывается на данных ежегодного аудита ИБ и вносится ректору АО «ЮКМА» с целью принятия дальнейших организационно распорядительных мер;
- анализ и оценка рисков должны проводиться в соответствии с руководством по реализации Государственного стандарта Республики Казахстан;
- 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 АО «ЮКМА».

Работник при использовании инструментов искусственного интеллекта обеспечивает проверку достоверности полученных результатов, соблюдение требований конфиденциальности и защиты данных, принципов академической

добросовестности, а также несёт персональную ответственность за окончательные решения и материалы, подготовленные с использованием указанных технологий.

Несоблюдение порядка применения технологий искусственного интеллекта и цифровых решений рассматривается как действие, противоречащее принципам академической честности, и влечет за собой дисциплинарную ответственность в соответствии с законодательством Республики Казахстан и внутренними нормативными актами АО «ЮКМА»

11. ПОРЯДОК ПРИНЯТИЯ, УТВЕРЖДЕНИЯ И ИЗМЕНЕНИЯ ПОЛОЖЕНИЯ

Внесение изменений в действующий документ организует руководитель КТИЦ при наступлении одного из следующих условий:

-при необходимости по результатам анализа рисков, аудитов и проверок соответствия требованиям кибербезопасности;

-при получении сообщения о необходимости внесения изменений в документ от любого участника процесса, обнаружившего несоответствие в нем;

-при получении распоряжения Руководства АО «ЮКМА»;

-при проведении организационных и структурных изменений в АО «ЮКМА», затрагивающих процессы управления ИБ;

-в связи с внесением изменений в законодательство;

-в связи с внесением изменений во внутренние документы АО «ЮКМА».

В целях поддержания актуальности и эффективности действий по обеспечению ИБ данный документ должен пересматриваться не реже одного раза в год. Ответственный за соблюдение периода пересмотра документа является руководителя КТИЦ внесение изменений в положение, его утверждение и порядок принятия осуществляется приказом ректора АО «ЮКМА».

Разработал:

Должность	**Ф.И.О.**
Специалист по кибербезопасности и защите информационных систем.	Арынбаев С.А.

Проверил:

Должность	**Ф.И.О.**
Руководитель центра компьютерного тестирования и типографии	Уксикбаев М.Т.
Заведующий отделом обеспечения качества и мониторинга	Ержанов Н.А.
Руководитель Управления административного и правового обеспечения	Кабиштаев О.А.

Согласовал:

Должность	**Ф.И.О.**
Проректор по академической работе	Анартаева М.У.
Проректор по клинической работе	Нурмашев Б.Қ.
Проректор по научному и стратегическому развитию	Аукенов Н.Е.
Проректор по воспитательной работе и социальным вопросам	Сәлім Е.Қ.
Комплаенс офицер	Пернебаев Н.А.

Лист согласования и подписания

ФИО	Тип действия	Время и дата согласования или подписания	Замечания	Данные по ЭЦП
Арынбаев Сабыр	Разработано	14.05.2026, 15:02:36	Без замечаний	
Уксикбаев Максат Туларович	Проверено	14.05.2026, 15:04:20	Без замечаний	
Ержанов Нурлан Амирович	Проверено	28.05.2026, 14:57:07	Без замечаний	
Кабиштаев Орынбасар Абдукаримович	Проверено	15.05.2026, 17:11:24	Без замечаний	
Анартаева Мария Уласбековна	Согласовано	15.05.2026, 11:13:09	Без замечаний	
Нурмашев Бекайдар Калдыбаевич	Согласовано	14.05.2026, 18:46:16	Без замечаний	
Аукенов Нурлан Ерденович	Согласовано	14.05.2026, 15:33:55	Без замечаний	
Сәлім Ербол Қалтұрсынұлы	Согласовано	14.05.2026, 17:06:15	Без замечаний	
Пернебаев Нургали Алиханович	Согласовано	14.05.2026, 15:07:09	Без замечаний	
Сейтжанова Жанна Серикжановна	Подписано	29.05.2026, 14:40:47	Без замечаний	Издатель ЭЦП - ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (GOST) 2022, СЕЙТЖАНОВА ЖАННА, "Оңтүстік Қазақстан медицина академиясы" акционерлік қоғамы, BIN991040003556
Сейтжанова Жанна Серикжановна	Зарегистрировано	29.05.2026, 14:40:49	Без замечаний	Издатель ЭЦП - ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (GOST) 2022, СЕЙТЖАНОВА ЖАННА, "Оңтүстік Қазақстан медицина академиясы" акционерлік қоғамы, BIN991040003556