УТВЕРЖДАЮ
Ректор АО «ЮКМА»
_____ Ж.Сейтжанова
«26» 02 2026 г.

ПОЛОЖЕНИЕ
ПО КИБЕРГИГИЕНЕ ДЛЯ КОРПОРАТИВНОГО СЕКТОРА АО «ЮЖНО-КАЗАХСТАНСКАЯ МЕДИЦИНСКАЯ АКАДЕМИЯ»

П 508- 2026

Число	Копия	Издание
		Первое

г. Шымкент

Копирование и/или передача третьим лицам запрещены.

1. **РАЗРАБОТАН И ВНЕСЕН** специалистом по кибербезопасности и защите информационных систем **АО «ЮКМА»**
протокол №7 02.03. 2026 г.

2. **УТВЕРЖДЕНО** решением Совета по качеству **АО «ЮКМА»**
протокол №4 26.03 2026 г.

Периодичность проверки – 3 года

Является интеллектуальной собственностью АО «ЮКМА». Копирование и/или передача третьим лицам запрещены.

СОДЕРЖАНИЕ

ПАСПОРТ ДОКУМЕНТА..... 4
1. НОРМАТИВНЫЕ ССЫЛКИ..... 5
2.ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ 5
3. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ..... 5
4. ОБЩИЕ ПОЛОЖЕНИЯ 6
5. ОСНОВНЫЕ ТРЕБОВАНИЯ К КИБЕРГИГИЕНЕ..... 8
6. УПРАВЛЕНИЕ ДОСТУПОМ 9
7. РЕАГИРОВАНИЕ НА КИБЕРИНЦИДЕНТЫ..... 10
8. ОБУЧЕНИЕ И ОСВЕДОМЛЕННОСТИ..... 10
9. ПОЛИТИКА ИСПОЛЬЗОВАНИЯ МОБИЛЬНЫХ УСТРОЙСТВ (BYOD)..... 11
10. ПОЛИТИКА ИСПОЛЬЗОВАНИЯ МЕССЕНДЖЕРОВ..... 12
11. ОТВЕТСТВЕННОСТЬ..... 12

Является интеллектуальной собственностью АО «ЮКМА». Копирование и/или передача третьим лицам запрещены.

ПАСПОРТ ДОКУМЕНТА

Наименование документа:	Положение по кибергигиене для корпоративного сектора АО «Южно-казахстанская медицинская академия»
Краткое описание:	Положение по кибергигиене для корпоративного сектора АО « Южно-казахстанская медицинская академия »
Тема:	Информационная безопасность
Статус:	Первый
Дата утверждения:	« ___ » _____20_____г.
Дата завершения действия:	« ___ » _____20_____г.
Дата аудита:	Ежегодно

Является интеллектуальной собственностью АО «ЮКМА». Копирование и/или передача третьим лицам запрещены.

1. НОРМАТИВНЫЕ ССЫЛКИ

Настоящее положение разработано с учетом требований следующих нормативных документов:

— Закон Республики Казахстан «О персональных данныхи их защите», № 94-V ЗРК от 21 мая 2013 года;

— П 504 – 2026 Положение по информационной безопасности АО «Южно – Казахстанская медицинская академия»;

— 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.

2. ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

В настоящем положении использованы следующие обозначения и сокращения:

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

— ИС - информационные системы;

— ПО – программное обеспечение;

— ИБ – информационная безопасность.

3. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем Положении используются следующие термины с соответствующими определениями:

кибергигиена — совокупность правил безопасного поведения пользователей в информационной среде;

информационная безопасность — состояние защищенности информации от внутренних и внешних угроз;

киберинцидент — событие, нарушающее безопасность

Является интеллектуальной собственностью АО «ЮКМА». Копирование и/или передача третьим лицам запрещены.

информационных систем (далее - ИС) ;

персональные данные — сведения, относящиеся к определённому физическому лицу;

кибератака – это преднамеренное воздействие на ИС, сети или устройства с целью нарушения их работы, получения несанкционированного доступа, кражи, изменения или уничтожения данных;

конфиденциальная информация — информация ограниченного доступа;

учетные данные — логин и пароль пользователя;

фишинг — способ получения данных путём обмана;

социальная инженерия — психологическое воздействие на пользователя;

кибербуллинг — цифровое преследование;

цифровые активы — информационные ресурсы организации;

ЭЦП — электронная цифровая подпись;

BYOD (Bring Your Own Device) — использование личных устройств в служебных целях.

4. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящее Положение определяет единые требования по обеспечению кибергигиены в АО «Южно-Казахстанская медицинская академия» (далее — АО «ЮКМА»).

Положение направлено на защиту информационных ресурсов АО «ЮКМА», снижение киберрисков и предотвращение утечек данных. Требования настоящего Положения являются обязательными для всех сотрудников, обучающихся и иных лиц, имеющих доступ к ИС АО «ЮКМА».

Настоящее Положение вступает в силу с момента его официального утверждения и является обязательным для исполнения всеми сотрудниками, обучающимися и иными пользователями ИС АО «ЮКМА».

Пересмотр и актуализация настоящего Положения осуществляются не реже одного раза в год, а также при необходимости внесения изменений в законодательство Республики Казахстан, внутренние нормативные документы или при изменении требований информационной безопасности (далее - ИБ).

Контроль за соблюдением и исполнением требований настоящего Положения возлагается на специалиста по кибербезопасности и ИС АО «ЮКМА», который осуществляет мониторинг, координацию и контроль выполнения установленных норм.

Является интеллектуальной собственностью АО «ЮКМА». Копирование и/или передача третьим лицам запрещены.

Цели и задачи.

Основная цель - обеспечение комплексной защиты информационных ресурсов АО «Южно-Казахстанская медицинская академия» от внутренних и внешних угроз, снижение уровня киберрисков, предотвращение утечек данных и обеспечение непрерывности функционирования ИС, а также формирование устойчивой культуры ИБ среди сотрудников и обучающихся.

Для достижения поставленной цели необходимо решить следующие:

— обеспечение комплексной защиты от внутренних и внешних угроз, включая несанкционированный доступ, утечку, уничтожение и искажение данных информационных ресурсов АО «ЮКМА»;

— снижение уровня киберрисков за счёт внедрения организационных и технических мер ИБ, направленных на предотвращение кибератак и минимизацию их последствий;

— формирование устойчивой культуры ИБ среди сотрудников и обучающихся, основанной на осознанном и ответственном отношении к защите информации;

—обеспечение непрерывности функционирования информационных систем и сервисов АО «ЮКМА»;

— защита персональных данных, служебной и иной конфиденциальной информации в соответствии с требованиями законодательства Республики Казахстан и внутренних нормативных документов;

—повышение уровня доверия к цифровой инфраструктуре АО «ЮКМА» со стороны сотрудников, обучающихся;

— внедрение и поддержание эффективной системы кибергигиены, включающей регламенты, инструкции и стандарты безопасной работы с информационными системами;

— обеспечение регулярного обучения, инструктажей и повышения осведомлённости сотрудников и обучающихся по вопросам ИБ и кибергигиены;

— организация и проведение профилактических мероприятий, направленных на предотвращение киберинцидентов, включая фишинг-симуляции и тестирование знаний пользователей;

—выявление, анализ и минимизация потенциальных уязвимостей в информационных системах и процессах АО «ЮКМА»;

— обеспечение соблюдения требований ИБ при использовании корпоративных и личных устройств (в рамках политики BYOD);

— контроль соблюдения пользователями установленных требований кибергигиены и применение мер реагирования при выявлении нарушений;

— организация эффективного процесса реагирования на

Является интеллектуальной собственностью АО «ЮКМА». Копирование и/или передача третьим лицам запрещены.

киберинциденты, включая своевременное обнаружение, локализацию и устранение последствий;

— обеспечение защиты цифровых активов АО «ЮКМА», включая базы данных, ИС и сетевую инфраструктуру;

— обеспечение взаимодействия между структурными подразделениями АО «ЮКМА» по вопросам кибербезопасности.

5. ОСНОВНЫЕ ТРЕБОВАНИЯ К КИБЕРГИГИЕНЕ

Основные требования к кибергигиене устанавливают обязательные правила безопасного поведения пользователей при работе с ИС и цифровыми ресурсами АО «ЮКМА», направленные на предотвращение несанкционированного доступа, утечек данных и иных киберинцидентов. Данные требования включают соблюдение политики управления учетными данными, использование только разрешённого ПО и устройств, внимательное отношение к электронным коммуникациям, а также неукоснительное выполнение установленных мер защиты информации и своевременное уведомление о любых подозрительных действиях или угрозах.

Пользователи обязаны:

— использовать сложные и уникальные пароли для каждой ИС, включающие не менее установленного количества символов, а также комбинации букв, цифр и специальных знаков, с целью предотвращения несанкционированного доступа;

— осуществлять регулярную смену паролей не реже одного раза в 90 календарных дней, а также незамедлительно изменять пароль в случае подозрения на его компрометацию;

— обеспечивать конфиденциальность учетных данных (логинов, паролей, кодов подтверждения), не передавать их третьим лицам, не записывать в открытом виде и не хранить в небезопасных местах;

— блокировать рабочие станции, ноутбуки и иные устройства при каждом случае временного отсутствия пользователя, в том числе с использованием автоматической блокировки экрана;

— использовать в служебной деятельности исключительно разрешённое и лицензированное ПО, утверждённое в установленном порядке;

— соблюдать требования информационной безопасности при работе с электронной почтой, интернет-ресурсами и корпоративными системами;

— использовать антивирусное ПО и иные средства защиты информации, установленные на рабочих устройствах, не отключать их без

Является интеллектуальной собственностью АО «ЮКМА». Копирование и/или передача третьим лицам запрещены.

разрешения;

— немедленно уведомлять специалиста по кибербезопасности и защите информационных систем о любых подозрительных действиях, сообщениях, попытках доступа или возможных инцидентах.

Пользователям запрещается:

— открывать электронные письма, вложения и переходить по ссылкам из неизвестных или подозрительных источников, а также выполнять файлы, полученные от непроверенных отправителей;

— устанавливать, загружать или использовать нелицензионное, несанкционированное или вредоносное ПО, а также ПО, не прошедшее согласование со специалистом по кибербезопасности и ИС;

— подключать к рабочим устройствам неизвестные или неавторизованные внешние носители информации (USB-накопители, жёсткие диски и др.), а также использовать личные устройства без разрешения;

— предпринимать попытки обхода установленных средств защиты информации, включая системы аутентификации, антивирусной защиты, межсетевые экраны и иные средства безопасности;

— передавать служебную, конфиденциальную или персональную информацию через незащищённые каналы связи или сторонние сервисы без соответствующего разрешения;

— использовать корпоративные информационные ресурсы в личных целях, если это может привести к угрозе ИБ или нарушению политики АО «ЮКМА»;

— самостоятельно изменять настройки безопасности устройств и программного обеспечения без согласования с ответственными подразделениями.

6. УПРАВЛЕНИЕ ДОСТУПОМ

Доступ к ИС АО «ЮКМА» предоставляется на основе принципа минимально необходимых привилегий, при котором пользователю предоставляются только те права и уровни доступа, которые необходимы для выполнения его должностных обязанностей.

Каждому пользователю в обязательном порядке назначается индивидуальная учетная запись, обеспечивающая персонализацию доступа и возможность идентификации действий в системе.

Все действия пользователей в ИС подлежат обязательной регистрации в журналах событий с обеспечением возможности их последующего анализа

Является интеллектуальной собственностью АО «ЮКМА». Копирование и/или передача третьим лицам запрещены.

и контроля, выявления подозрительной активности и проведения последующего анализа в случае инцидентов.

Предоставленные права доступа подлежат регулярному пересмотру, а также обязательному и своевременному отзыву при увольнении сотрудника, переводе на другую должность либо изменении его функциональных обязанностей, исключая возможность несанкционированного использования информационных ресурсов.

7. РЕАГИРОВАНИЕ НА КИБЕРИНЦИДЕНТЫ

Требования к реагированию на киберинциденты устанавливают обязанность пользователей своевременно информировать о любых подозрительных событиях и строго соблюдать установленный порядок действий при их выявлении. Пользователям запрещается самостоятельно предпринимать меры по устранению инцидентов, поскольку это может привести к искажению информации, утрате доказательств и усложнению расследования.

Пользователей незамедлительно сообщить о любом подозрительном событии, связанном с возможным нарушением ИБ включая получение подозрительных писем, обнаружение неизвестных программ, попытки несанкционированного доступа, утрату устройства или иные признаки киберинцидента, но не позднее 15 минут с момента его выявления. Уведомление должно быть направлено специалисту по кибербезопасности и ИС либо в ответственное подразделение с предоставлением максимально полной и достоверной информации о характере события, времени его обнаружения и предпринятых действиях (если таковые имели место).

Самостоятельные действия по устранению киберинцидента, включая удаление файлов, отключение оборудования, изменение настроек системы или запуск сторонних программ, строго запрещаются, за исключением случаев, когда такие действия прямо предписаны внутренними регламентами или получены соответствующие указания от специалиста по кибербезопасности и ИС. Данное требование направлено на предотвращение усугубления последствий инцидента и обеспечение корректного проведения расследования.

8. ОБУЧЕНИЕ И ОСВЕДОМЛЕННОСТЬ

Все сотрудники и обучающиеся АО «ЮКМА» проходят обязательное ежегодное обучение по вопросам кибергигиены и информационной безопасности, направленное на формирование устойчивых навыков безопасного поведения в цифровой среде, а также снижение уровня

Является интеллектуальной собственностью АО «ЮКМА». Копирование и/или передача третьим лицам запрещены.

киберрисков. Обучение может проводиться в различных форматах, включая очные занятия, дистанционные курсы и самообучение с использованием специализированных образовательных платформ, в том числе портала кибергигиены и кибербезопасности **citizensec.kz**, разработанного казахстанскими специалистами в области кибербезопасности.

В рамках системы повышения осведомлённости также регулярно проводятся тестирования уровня знаний пользователей с целью оценки усвоения материалов, выявления пробелов в знаниях и последующего их устранения. Результаты тестирования используются для совершенствования программ обучения и повышения общей культуры информационной безопасности АО «ЮКМА».

9. ПОЛИТИКА ИСПОЛЬЗОВАНИЯ МОБИЛЬНЫХ УСТРОЙСТВ (BYOD)

Политика использования мобильных устройств **(BYOD — Bring Your Own Device)** определяет порядок допуска, использования и защиты личных мобильных устройств сотрудников и обучающихся при доступе к информационным ресурсам АО «ЮКМА».. Данная политика направлена на обеспечение безопасности корпоративных данных при использовании персональных смартфонов, ноутбуков и других устройств, а также на минимизацию рисков утечки информации, несанкционированного доступа и киберугроз. Использование личных устройств допускается только при соблюдении требований ИБ, наличии базовых средств защиты (пароль, биометрическая аутентификация, антивирусное ПО) и обязательном соблюдении правил подключения к корпоративным системам через защищённые каналы связи.

В рамках данной политики пользователи обязаны соблюдать следующие правила:

- разрешается использование только защищённых мобильных устройств,
- обязательным является наличие пароля или биометрической защиты,
- запрещается использование устройств с root-доступом или jailbreak,
- доступ к корпоративным ресурсам допускается только через защищённые каналы связи,
- при утере устройства пользователь обязан незамедлительно уведомить специалиста по кибербезопасности и информационным системам,
- АО «ЮКМА», имеет право ограничивать доступ или удалённо удалять корпоративные данные (MDM).

Является интеллектуальной собственностью АО «ЮКМА». Копирование и/или передача третьим лицам запрещены.

10. ПОЛИТИКА ИСПОЛЬЗОВАНИЯ МЕССЕНДЖЕРОВ

Политика использования мессенджеров устанавливает правила безопасного и контролируемого применения средств мгновенного обмена сообщениями в служебной деятельности АО «ЮКМА». Данная политика направлена на обеспечение защиты конфиденциальной информации, предотвращение утечек, данных и снижение рисков киберугроз при цифровой коммуникации между сотрудниками и обучающимися.

Разрешается:

- служебная коммуникация использование официальных корпоративных чатов.

Запрещается:

- передача конфиденциальной информации пересылка служебных документов в личные аккаунты переход по подозрительным ссылкам.

Требования безопасности:

- использование двухфакторной аутентификации (2FA) проверка отправителей сообщений использование только утверждённых корпоративных платформ.

11. ОТВЕТСТВЕННОСТЬ

За нарушение требований настоящего Положения работники, обучающиеся и иные пользователи ИС АО «ЮКМА» несут установленную ответственность в соответствии с действующим законодательством Республики Казахстан и внутренними нормативными документами. В зависимости от характера, степени тяжести и последствий допущенного нарушения могут применяться различные меры воздействия, направленные на восстановление нарушенного порядка и предотвращение повторных инцидентов.

В первую очередь может быть применена дисциплинарная ответственность, включающая замечание, выговор, строгий выговор либо иные меры дисциплинарного взыскания в соответствии с трудовым законодательством и внутренними правилами АО «ЮКМА».

В случаях, предусмотренных законодательством, нарушение требований ИБ может повлечь административную ответственность, включая штрафные санкции, предусмотренные нормативными правовыми актами Республики Казахстан.

При причинении материального ущерба АО «ЮКМА» вследствие неправомерных действий пользователя может наступать материальная ответственность в порядке, установленном законодательством, с

Является интеллектуальной собственностью АО «ЮКМА». Копирование и/или передача третьим лицам запрещены.

возмещением причинённого ущерба в полном объёме или частично, в зависимости от обстоятельств нарушения.

Является интеллектуальной собственностью АО «ЮКМА». Копирование и/или передача третьим лицам запрещены.

Разработал:

Должность	Ф.И.О.	Дата	Подпись
Специалист по кибербезопасности и защите информационных систем.	Арынбаев С.А.	02.03.2026г.	

Проверили:

Должность	Ф.И.О.	Дата	Подпись
Руководитель центра компьютерно тестового и издательского центра	Уксикбаев М.Т.	02.03.2026г.	
Заведующий отделом обеспечения качества и мониторинга	Ержанов Н.А.	05.03.2026г.	
Руководитель Управления административного и правового обеспечения	Кабиштаев О.А.	12.03.2026г.	

Согласовали:

Должность	Ф.И.О.	Дата	Подпись
Проректор по академической работе	Анартаева М.У.	17.03.2026г.	
Проректор по клинической работе	Нурмашев Б.Қ.	17.03.2026г.	
Проректор по научному и стратегическому развитию	Аукенов Н.Е.	18.03.2026г.	
Проректор по воспитательной работе и социальным вопросам	Сәлім Е.Қ.	18.03.2026г.	
Комплаенс офицер	Пернебаев Н.А.	18.03.2026г.	

Является интеллектуальной собственностью АО «ЮКМА». Копирование и/или передача третьим лицам запрещены.