Наименование структурного подразделения:	**Все структурные подразделения**		
Названия документа:	**СОП «Правила информационной безопасности»**		
Утвержден:	Руководитель ГКП на ПХВ «ЛГП» Чалкаров А.Б.		
Дата утверждения:			
Разработчик:	*Должность*	*Ф.И.О.*	*Подпись*
	Заместитель гл.врача по лечебному делу	Анаркулова У.О.	
	Заведующий отделением	Садыков Г.Б.	
Согласовано:	Заместитель гл.врача по ОМД	Кабылбеков Г.К.	
	Заместитель гл.врача по контролю качества мед.услуг	Рысбаев С.Т.	
	Врач эксперт		
Дата согласования:	04.01.2024г.		
Дата введения в действие	04.01.2024г.		
Версия №	**Копия №_____**	04_____/ _01_____/ 2024г. Ф.И.О. _____ Подпись _____	

Дата последнего пересмотра «_04_» «_____01_____» 2024г
Дата следующего пересмотра «_____» «_____» 2027г

СОП «Правила информационной безопасности»

1. **Цель:** обеспечение информационной безопасности в Медицинской организации.
2. **Область применения:** политика распространяется на всех работников Медицинской организации.
3. **Ответственность:**

1) Главный врач или лицо, назначенное главным врачом, обеспечивает контроль за выполнением всех пунктов данной Политики.
2) Специалисты, отвечающие за информационную безопасность, должны обеспечить контроль за использованием информации информационной системы в соответствии с постановлением Правительства Республики Казахстан от 24 июня 2022 года № 429 «Об утверждении Правил отнесения сведений к служебной информации ограниченного распространения и работы с ней».
3) Главный врач, и/или лицо назначенное Главным врачом должен обеспечить четкое управление и зримую поддержку инициатив в области поддержки информационной безопасности информационной системы Медицинской организации.
4) Специалисты, отвечающие за информационную безопасность должны обеспечивать координацию мер контроля в эксплуатируемых информационных системах.
5) Специалисты, отвечающие за информационную безопасность должны предоставлять ресурсы для обеспечения мер информационной безопасности.
6) Главный врач, и/или лицо, назначенное главный врачом должен утверждать распределение специфических ролей и обязанностей по информационной безопасности.
7) Обслуживающий персонал при нарушении требований пунктов Политики информационной безопасности будет привлекаться к административной или иной ответственности, в соответствии с действующим законодательством Республики Казахстан.
8) Специалисты, отвечающие за информационную безопасность должны обеспечить контроль издания и доведения до сведения утвержденных документов по информационной безопасности до обслуживающего персонала и пользователей информационных систем Медицинской организации.
9) Специалисты, отвечающие за информационную безопасность должны инициировать планы и программы по поддержанию осведомленности об информационной безопасности.
10) Ответственность на администраторов информационных систем возлагается в соответствии с зонами их ответственности согласно «Инструкции по закреплению функций и полномочий администратора сервера».
11) Администраторы информационных систем обязаны:

– обеспечивать обязательность процедуры идентификации и аутентификации для доступа к ресурсам информационных систем;
– не допускать получения права доступа к информационным системам неавторизированным пользователям и представлять пользователям входные имена и начальные пароли только после заполнения установленных регистрационных форм;
– обеспечивать защиту оборудования, в том числе специальных межсетевых программных средств;
– оперативно и эффективно реагировать на события, содержащие угрозу, принимать меры по отражению угрозы и выявлению нарушителей, фиксировать и информировать специалистов, отвечающие за информационную безопасность о попытках нарушения защиты.

4. Определения, термины и сокращения:

1) Настоящая политика информационной безопасности (далее - Политика) является внутренним нормативным документом Медицинской организации.
2) Политика устанавливает требования к обеспечению информационной безопасности для информационных систем, эксплуатируемых в Медицинской организации, определяет основные принципы, направления и требования по защите информации, является основой для обеспечения режима информационной безопасности, служит руководством при разработке соответствующих Положений, Правил, Инструкций.
3) Под обеспечением информационной безопасности или защитой информации понимается сохранение ее конфиденциальности, целостности и доступности. Конфиденциальность информации обеспечивается в случае предоставления доступа к данным только авторизованным лицам, целостность – в случае внесения в данные исключительно авторизованных изменений, доступность – обеспечении возможности получения доступа к данным авторизованным лицам в нужное для них время.
4) В настоящей Политике приведены следующие определения, обозначения и сокращения:

Аутентификация	Подтверждение подлинности субъекта или объекта доступа путем определения соответствия предъявленных реквизитов доступа, реализованных в системе
Авторизация	Предоставление прав на выполнение определенных действий; а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий.
Государственные секреты	Защищаемые государством сведения, составляющие государственную и служебную тайны, распространение которых ограничивается государством с целью осуществления эффективной медицинской, военной, экономической, научно-технической,

	внешнеэкономической, внешнеполитической, разведывательной, контрразведывательной, и иной деятельности, не вступающей в противоречие с общепринятыми нормами международного права
Доступность	Состояние информации (ресурсов автоматизированной информационной системы), при котором субъекты, имеющие право доступа, могут реализовывать их беспрепятственно
Информационная безопасность (далее - ИБ)	Состояние защищенности информационных ресурсов и систем, обеспечение конфиденциальности, целостности и доступности информации.
ИС	Информационные системы
Инфраструктура ИС	Каналы связи, оборудование, программное обеспечение, сотрудники и пользователи, документация, информация информационных систем.
Конфиденциальность информации	Обеспечение предоставления информации только авторизированным лицам по уровням доступа
ОС	Операционная система
ПО	Программное обеспечение
Пользователи ИС	Лица, работающие с ИС
ППРК	Постановления Правительства Республики Казахстан
СВТ	Средства вычислительной техники
ИБП	Источник бесперебойного питания
Целостность информации	Состояние информации (ресурсов автоматизированной информационной системы), при котором ее (их) изменение осуществляется только преднамеренно субъектами, имеющими на него право

5. Ресурсы:

1) Серверное помещение, отвечающее всем требованиям;
2) Источник бесперебойного питания (ИБП) необходимой мощности;
3) Внутренние нормативные документы (см. п. 9.15).

6. Документирование: ежегодный анализ информационной безопасности информационных систем с результатом в виде отчета.

7. Общие положения

1) Целью обеспечения ИБ является минимизация экономического, финансового, социального, институционального и экологического ущербов от реализации угроз ИБ, а также повышение общего уровня конфиденциальности, целостности и доступности информации в ИС.

2) Политика ИБ распространяется на функционирование всей инфраструктуры Медицинской организации.

3) Политика ИБ обязательна для исполнения всеми лицами, работающими с инфраструктурой, в том числе для третьих лиц, выполняющих работы по сопровождению либо развитию ИС.
4) Исполнение требований политики ИБ обеспечивают все лица, работающие с инфраструктурой информационных систем.
5) Действия по обеспечению ИБ должны координироваться руководством и специалистами, ответственными за ИБ.
6) Координация ИБ должна осуществлять следующую деятельность:
– обеспечивать соответствие выполняемых действий по обеспечению ИБ политике ИБ;
– определение действий в случае несоответствия выполняемых действий по обеспечению ИБ политике по ИБ;
– утверждение методологии и процессов обеспечения ИБ, например, оценку рисков, классификацию информации;
– идентифицировать значительные изменения угроз и подвергание информации и средств обработки информации угрозам;
– оценивание адекватности и координирования реализации мер контролю ИБ;
– эффективное способствование обучению, подготовке по ИБ и осведомленности о ней;
– оценивание информации, полученной от мониторинга и пересмотра инцидентов ИБ, и внесение рекомендаций в ответ на идентифицированные инциденты ИБ.

8. Описание управления информационной безопасностью

Конфиденциальность

1) Главным требованием конфиденциальности является обеспечение предоставления информации только авторизированным лицам.
2) Информация, обрабатываемая и хранящаяся в ИС, подлежит копированию и передаче третьему лицу только с официального разрешения руководства.
3) При работе с ИС должна исключаться возможность наблюдения за отображаемой информацией посторонними лицами.
4) В ИС не должны размещаться документы, содержащие государственные секреты, коммерческую тайну и иную информацию с ограниченным доступом.
5) Запись и копирование служебной и иной защищаемой информации, в том числе для передачи другим лицам, производится на зарегистрированные в установленном порядке носители информации.
6) При работе с ИС должны использоваться специальные лицензионные программные или аппаратные средства, обеспечивающие защиту от вредоносных программ, вирусов и сетевых атак.
7) Информация должна классифицироваться с точки зрения ее ценности, правовых требований, секретности и критичности для ИС.

Соглашения о конфиденциальности

1) Требования по соглашениям о конфиденциальности или неразглашении, отражающие потребности по защите безопасности, должны быть определены и регулярно пересмотрены.
2) Для определения требований по соглашениям о конфиденциальности или неразглашении необходимо рассмотреть следующие элементы:
– определение информации, которая должна быть защищена (т.е. конфиденциальная информация или информация, содержащая коммерческую тайну);
– предполагаемая продолжительности соглашения, включая случаи, когда конфиденциальность должна поддерживаться бесконечно;
– требуемые действия по окончанию соглашения;
– обязанности и действия подписавших сторон во избежание несанкционированного разглашения информации (такого как «принцип необходимого знания»);
– собственность на информацию, коммерческие секреты и интеллектуальную собственность и то, как она связана с защитой конфиденциальной информации;
– разрешенное использование конфиденциальной информации и право подписавшей стороны использовать информацию;
– право аудита и мониторинга действий, в которых задействована конфиденциальная информация;
– процесс уведомления и сообщения о несанкционированном разглашении или нарушении конфиденциальности информации и коммерческой тайны;
– условия о возврате или уничтожении информации при прекращении действия соглашения;
– предполагаемые действия в случае нарушения данного соглашения.
В соглашении о конфиденциальности или неразглашении могут потребоваться другие элементы, основанные на требованиях безопасности. Соглашения о конфиденциальности и неразглашении должны соответствовать всем применяемым правовым нормам и правилам юрисдикции, которые применяются.

9. Требования

Требования к обучению и осведомленности в вопросах ИБ:

1) Обслуживающий персонал ИС, пользователи и администраторы ИС, должны быть ознакомлены с политикой ИБ.
2) Обслуживающий персонал ИС должен предоставить пользователям ИС рабочую документацию (Инструкция о парольной защите ИС).
3) Обслуживающий персонал ИС по запросу пользователей должен проводить первичный инструктаж по ИБ.
4) Обслуживающий персонал, обеспечивающий функционирование ИС должен проходить регулярно инструктаж по соблюдению ИБ.
5) Обслуживающий персонал ИС должны принять пользовательское соглашение о конфиденциальности.

6) В целях обеспечения ИБ необходимо согласовать и определить в соглашении с третьей стороной мероприятия по управлению ИС.
7) В целях обеспечения гарантированного уведомления подразделения ответственного за ИБ, обслуживающего персонала ИС и всех заинтересованных сторон об инциденте и слабости ИБ по отношению к ИС должны быть реализованы формальные процедуры по уведомлению об инциденте и появлении угроз. Для трансляции уведомлений должен быть избран способ, гарантированно позволяющий своевременно принять корректирующие меры.
8) Обслуживающий персонал ИС должен знать процедуры уведомления, а также располагать сведениями о различных типах событий или слабых местах, которые могут влиять на безопасность ресурсов, и о наступлении которых или предпосылках к таковому необходимо отправить уведомление.
9) Обслуживающий персонал и администраторы ИС обязаны как можно быстрее сообщать о любых событиях в сфере ИБ ответственным за ИБ лицам.

Требования по аутентификации ИС:

Администраторы и пользователи ИС должны проходить безопасную аутентификацию, идентифицирующую их и исключающую возможность подбора пароля и перехвата авторотационных данных.

Требования к пользовательским учетным записям и паролям:

Требования к пользовательским учетным записям и паролям приведены во внутреннем нормативном документе «Инструкция о парольной защите ИС».

Требования к серверному помещению. Серверное помещение, в котором размещаются сервера и активное сетевое оборудование, используемое для ИС, должно быть оборудовано следующим образом:
1) Система контроля управления доступа - система, предназначенная для предоставления санкционированного входа/выхода авторизованным лицам и запрещения входа/выхода неавторизованным лицам в контролируемых зонах с помощью электрических, электронных или механических средств. Контроль входа/выхода может включать также отчет и регистрацию всех событий и действий пользователей;
2) Система видеонаблюдения - система охранного видеонаблюдения предназначена для визуального наблюдения и фиксации текущей обстановки в помещениях серверной. Камеры необходимо разместить таким образом, чтобы контролировать входы и выходы в помещение, пространство возле технологического оборудования (ИБП, кондиционеры, серверные шкафы и телекоммуникационные стойки). Разрешения видеокамер должно быть достаточным, чтобы уверенно различать лица сотрудников, обслуживающих технологическое оборудование;
3) Фактическая холодильная мощность системы кондиционирования воздуха должна превышать суммарное тепловыделение всего оборудования и систем, размещенного в помещении серверной;

4) Система мониторинга микроклимата - система контроля параметров предназначена для контроля климатических и других параметров в серверных шкафах и телекоммуникационных стойках. В каждом шкафу устанавливаются датчики для контроля следующих параметров:

- температура воздуха;
- запыленность воздуха;
- скорость потока воздуха;
- задымленность воздуха;
- открытие/закрытие дверей шкафов;

5) Система пожарной сигнализации - система пожарной сигнализации помещения серверной должна быть выполнена отдельно от пожарной сигнализации здания (офиса). В помещении серверной должны быть установлены два типа извещателей: температурные и дымовые. Извещатели должны контролировать как общее пространство помещений, так и полости, образованные фальшполом и фальшпотолком. Сигналы оповещения подсистемы пожарной сигнализации выводятся на отдельный пульт в помещение круглосуточной охраны. Система пожарной сигнализации может быть объединена с подсистемой охранного видеонаблюдения серверной;

6) Система газового пожаротушения - серверная оборудуется автоматической установкой газового пожаротушения, независимой от системы пожаротушения здания. Модуль газового пожаротушения подсистемы газового пожаротушения размещается непосредственно в помещении серверной (или вблизи ее), в специально оборудованном для этого шкафу. Запуск подсистемы производится от датчиков раннего обнаружения пожара, реагирующих на появление дыма, а также от ручных извещателей, расположенных у выхода из помещения. Система должна иметь табло оповещения о срабатывании персонала серверной, размещаемые внутри и снаружи помещения. Система должна обеспечивать подачу команд на закрытие защитных клапанов системы вентиляции и отключение питания оборудования. Допускается использование переносных порошковых огнетушителей.

7) Система газо- и дымоудаления - обеспечивает отвод дыма и газа из помещения серверной после срабатывания подсистемы газового пожаротушения. Система выполняется отдельно от системы вентиляции здания с выводом воздуховода на крышу здания. Система должна обеспечивать отвод газовоздушной смеси в объеме, втрое превышающем объем серверной. Допускается использование переносных дымососов;

8) Система организации оборудования и кабельного хозяйства:

Телекоммуникационные шкафы и стойки

- все оборудование серверной размещается в закрытых шкафах или открытых стойках. Количество стоек (шкафов) определяется исходя из имеющегося оборудования и его типоразмеров, способов монтажа;

– для улучшения температурного режима размещение шкафов (стоек) организуют рядами, с образованием «горячих» и «холодных» коридоров. Промежутки между шкафами не допускаются;

– распределение оборудования по шкафам (стойкам) осуществляется с учетом совместимости (возможного взаимного влияния), оптимального распределения потребляемой мощности (а значит и тепловыделения), оптимальности коммуникаций, габаритам и массе оборудования;

– закрытые шкафы, в отличие от стоек, позволяют организовать дополнительные ограничения на доступ к оборудованию. Доступ внутрь таких шкафов может осуществляться с использованием подсистемы контроля доступа;

– закрытые шкафы нуждаются в дополнительных мерах по обеспечению требуемого температурного режима. Для этого применяются дополнительные вентиляторы, встраиваемые системы охлаждения, модули отвода горячего воздуха.

Организации коммуникаций

– все коммуникационные кабели внутри серверной должны быть организованы в лотки, проложенные в нишах фальшпола или фальшпотолка. Лотки электрических кабелей и сигнальных должны быть разнесены на расстояние до 50 см. Допускается пересечение трасс под углом 90 градусов;

– вводные каналы в телекоммуникационные шкафы и стойки должны обеспечивать свободную протяжку требуемого количества кабелей вместе с оконечными разъемами;

– коэффициент заполнения кабельных каналов и закладных не должен превышать 50-60%;

– внутри стоек и шкафов необходимо использовать кабельные организаторы, предотвращающие свешивание лишней длины кабеля;

– для упрощения коммуникаций и исключения поломки разъемов оборудования, необходимо применять патч-панели;

– все кабели, кроссовые коммуникации и патч-панели должны иметь маркировку, позволяющую однозначно идентифицировать каждый кабель (разъем, порт).

9) Система бесперебойного электроснабжения.

Система электроснабжения представляет собой технологическую систему, обеспечивающую безопасное и надежное функционирование инфокоммуникационных систем и инженерных систем здания. В свою очередь, система электроснабжения должна обеспечиваться средствами безопасности, и, кроме того, сама система электроснабжения является источником повышенной опасности. Важной задачей эксплуатации системы электроснабжения, наряду с электроснабжением потребителей, является ее безопасное функционирование.

Контроль обеспечения конфиденциальности

С целью контроля обеспечения конфиденциальности должны обеспечиваться следующие мероприятия:

– ежегодный анализ ИБ ИС на соблюдение требований ИБ, с результатом в виде отчета.

– постоянный мониторинг инструментальными средствами ИБ серверов ИС и сети, в которой они находятся.

Целостность

– главным требованием целостности является обеспечение изменения информации только авторизированными лицами по уровням доступа;

– новые программно-аппаратные средства, внедряемые должны быть соответствующим образом одобрены со стороны руководства и специалистов, ответственных за обеспечение ИБ;

– аппаратные средства и программное обеспечение перед внедрением следует проверять на совместимость с другими компонентами системы.

Требования к антивирусной безопасности

Требования к антивирусной защите приведены во внутреннем нормативном документе «Инструкция по организации антивирусной защиты».

Требования к применению электронной почты и Интернета

Требования по использованию электронной почты и Интернета приведены во внутреннем нормативном документе «Инструкция по использованию электронной почты и служб Интернет на подстанциях».

Доступность

1) Главным требованием доступности является обеспечение состояния информации (ресурсов автоматизированной информационной системы), при котором авторизированные лица могут работать с ней беспрепятственно.

2) В случае возникновения внештатных ситуаций, аварий, стихийных бедствий и иных ситуаций, которые могут повлиять, должны быть предусмотрены соответствующие меры защиты и обеспечения непрерывной работы и восстановления.

3) Аварии, стихийные бедствия и иные внештатные ситуации должны фиксироваться в полном и тщательном виде, с сохранением данной информации на срок не менее 2-х лет.

4) В случае возникновения инцидента ИБ или другой нештатной ситуации необходимо руководствоваться «Инструкцией о порядке действий пользователей во внештатных (кризисных) ситуациях».

Требования к отказоустойчивости

1) Отказоустойчивость серверного оборудования должна быть обеспечена путем его дублирования и балансировки нагрузки.

2) Отказоустойчивость каналов связи должна быть обеспечена путем использования наряду с основным резервного канала связи.

3) В случае возникновения внештатной ситуации, произошедшей с серверным оборудованием ИС восстановление данных должно быть произведено в течение не более 2 суток.

Требования по бесперебойному питанию

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

Требования по обеспечению резервирования и дублирования мощностей

1) 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.

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

Требования по обеспечению оперативного мониторинга состояния доступности

Мониторинг ИС производится ежедневно в течение рабочего дня с помощью специализированного программного обеспечения, в случае изменения состояния доступности ИС произойдет оповещение администратора в режиме «онлайн».

Управление инцидентами и несоответствиями требованиям ИБ

Кроме сообщений о случаях нарушения и слабых местах ИБ для обнаружения инцидентов нарушения ИБ должен применяться мониторинг систем, предупреждений и уязвимостей. Для процедур управления инцидентами нарушения ИБ должны рассматриваться следующие правила:

1) Для работы с различными типами инцидентов необходимо установить следующие процедуры:

- сбои информационных систем и утрата сервисов;
- вредоносный код;
- отказ в обслуживании;
- ошибки вследствие неполных или неточных данных;
- нарушения конфиденциальности и целостности;
- неправильное использование информационных систем;

2) Дополнение к обычным планам обеспечения непрерывности должны существовать процедуры касательно:

- анализа и идентификации причины инцидента;
- локализации;
- планирования и внедрения средств, предотвращающих повторное проявление
- инцидентов, при необходимости;
- взаимодействия с лицами, на которых инцидент оказал воздействие, или участвующих в устранении последствий инцидента;
- информирования о действиях соответствующих должностных лиц;
- действия по устранению сбоев систем и ликвидации последствий инцидентов нарушения ИБ должны быть под тщательными формализованным контролем.

3) Необходимо наличие процедур с целью обеспечения уверенности в том, что:

– только полностью идентифицированному и авторизованному персоналу предоставлен доступ к системам и данным в среде промышленной эксплуатации;
– все действия, предпринятые при чрезвычайных обстоятельствах, подробно документально оформлены;
– о действиях, предпринятых при чрезвычайных обстоятельствах, сообщено руководству, и они проанализированы в установленном порядке;
– целостность бизнес-систем и систем контроля подтверждена в минимальные сроки.
– цели управления инцидентами нарушения ИБ должны быть согласованы с руководством и лица, ответственные за управление инцидентами, должны знать приоритеты при работе с инцидентами нарушения ИБ.
Администраторы ИС должны оперативно устранять выявленные уязвимости.

Требования к документации

Обязательно требуемые к разработке внутренние нормативные документы:
1) Правила паспортизации средств вычислительной техники и использования информационных ресурсов;
2) Инструкция о парольной защите;
3) Инструкция о порядке действий пользователей во внештатных (кризисных) ситуациях;
4) Инструкция пользователя по эксплуатации компьютерного оборудования и программного обеспечения;
5) Инструкция по организации антивирусной защиты;
6) Инструкция по закреплению функций и полномочий администратора сервера;
7) Правила доступа пользователей и администраторов в серверные помещения;
8) Правила регистрации пользователей в корпоративной информационной сети;
9) Памятка для работы системных администраторов;
10) Памятка пользователю средств вычислительной техники;
11) Инструкция по использованию электронной почты и служб Интернет на рабочих станциях;
12) Инструкция о резервном копировании информации.

Требования к анализу и оценке рисков

1) Политика ИБ первоначально должна основываться на данных, полученных в результате анализа и оценки рисков ИБ.
2) С целью совершенствования политики ИБ должен проводиться ежегодный анализ и оценка рисков ИБ.
3) Анализ и оценка рисков должны проводиться в соответствии со стандартами, действующими на территории Республики Казахстан, а также внутренними нормативными документами.
4) При оценке рисков должно учитываться влияние реализации угроз ИБ на финансовое состояние. Стоимость принимаемых мер не должна превышать возможный ущерб, возникающий при реализации угроз.

5) Формализованная процедура проведений анализа рисков описана в Приложении.
6) На основе результатов анализа затрат и выгод рисков, руководство соответствующего СТП определяет, наиболее экономически эффективные меры для снижения риска. Выбранные меры должны объединить технические, эксплуатационные и управленческие меры для обеспечения надлежащей безопасности для ИС.
7) Уровень мониторинга конкретных средств обработки информации следует определять на основе оценки рисков.
8) При мониторинге следует обращать внимание на авторизованный доступ, включая следующие детали:
– пользовательский ID;
– даты и время основных событий;
– типы событий;
– файлы, к которым был осуществлен доступ;
– используемые программы/утилиты;
– все привилегированные действия, такие как:
– использование привилегированных учетных записей, например, корневого каталога, администратора;
– запуск и остановка системы;
– подсоединение/отсоединение устройства ввода/вывода;
– попытки несанкционированного доступа, такие как:
– неудавшиеся или отвергнутые действия пользователя;
– неудавшиеся или отвергнутые действия, затрагивающие данные и другие ресурсы;
– нарушения политики доступа и уведомления сетевых шлюзов и межсетевых экранов;
– предупреждения от собственных систем обнаружения вторжения.

Пересмотр политики ИБ

1) Политика ИБ должна быть закреплена за ответственным лицом, который имеет право утверждать административную ответственность за развитие, пересмотр и оценку политики безопасности. Пересмотр должен включать возможности оценки для улучшения политики ИБ ИС и подход к управлению ИБ в ответ на изменения в организационной среде, деловой ситуации, юридических условиях или технической среде.
2) При пересмотре политики ИБ необходимо учитывать результаты пересмотров управления. Здесь должны быть определены процедуры пересмотра, включая график или продолжительности пересмотра.
3) Входные данные для пересмотра управления должны включать информацию по:
– обратной связи от заинтересованных сторон;
– результатам независимых пересмотров;

– статусу превентивных и корректирующих действий;
– результатам предыдущих пересмотров;
– характеристикам процесса и соответствию политики безопасности информации;
– изменениям, которые могут повлиять на подход ССМП к управлению ИБ, включая изменения в организационной среде, деловой ситуации, наличии ресурсов, договорных, регулятивных или юридических условиях или в технической среде;
– тенденции, связанные с угрозами и уязвимостями;
– сообщенным инцидентам ИБ;
– рекомендациям, представленным соответствующими учреждениями.

4) Политика ИБ должна пересматриваться в случае появления существенных изменений в целях обеспечения конфиденциальности, целостности, доступности.

5) Пересмотр политики ИБ должен осуществляться в соответствии с руководством по реализации Государственного стандарта Республики Казахстан СТ РК ИСО/МЭК 17799-2006.

Контроль на соответствие требованиям ИБ

Контроль требований настоящей политики ИБ осуществляют специалисты, отвечающие за ИБ.

10. Рассылка

1) Структурным подразделениям – информационный ресурс Медицинской организации.

2) Медицинская организация в целом - информационный ресурс, электронно-сканированная версия.

3) Делопроизводитель – оригинал бумажного экземпляра, электронно-сканированная версия.

11. Ссылки:

1) Закон РК от 07.01.2003 № 370-II «Об электронном документе и электронной цифровой подписи»;

2) Приказ и.о. МЗ РК от 10.02.2014 № 75 «Об утверждении технической документации по вопросам электронного здравоохранения»;

3) Государственный стандарт Республики Казахстан СТ РК ИСО/МЭК 17799-2006 «Информационная технология. Методы обеспечения защиты. Свод правил по управлению защитой информации»;

4) СТ РК ISO/IEC 27001-2015 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасностью.

5) Стандарты аккредитации Международной объединенной комиссии (Joint Commission International Accreditation Standards for Hospital – 6th Edition) для больниц, 6-е издание, глава 14: Менеджмент информации, 2017;

6) Приказ и.о. МЗ РК от 05.11.2021 № КР ДСМ-111 «Об утверждении стандартов аккредитации медицинских организаций».

Приложение
(информационное)

Оценка возможных технических рисков

Вид риска	**Описание**	**Измерения и меры по снижению риска**
Выход из строя сервера	Сбой в работе аппаратного или ПО сервера.	Измеряется в процентной доле времени штатного функционирования. Предусматривать длительный срок гарантийного обслуживания при заключении договора, а по его окончании - резервирование серверов
Выход из строя рабочей станции	Сбой в работе аппаратного или ПО рабочей станции.	Измеряется в процентной доле времени штатного функционирования. Приобретение только у ведущих мировых производителей, имеющих сертифицированные сервис центры
Потеря или искажение данных при передаче	Частичная потеря или искажение данных при передаче по каналам связи из-за сбоев в телекоммуникационном оборудовании с учетом корректирующих свойств коммуникационных протоколов.	Измеряется в доле потерянных либо искаженных данных. Перевод на наземные каналы связи и резервирование каналов
Потеря или искажение данных при хранении	Риск вызван возможностью сбоев в файловой системе диска или физическими ошибками на	Измеряется в среднем времени между отказами в часах. Наращивание систем хранения информации, периодическое резервное копирование согласно

Вид риска	Описание	Измерения и меры по снижению риска
	накопителях, с учетом способа хранения данных в БД.	инструкции.
Быстрое моральное устаревание технологий	Неприятие ППО пользователями	Уточнение требований заявителя по платформенной независимости ППО
Приобретение морально-устаревшей техники	Отсутствие комплектующих материалов Отсутствие технической поддержки морально-устаревшего оборудования	Уточнение требований заявителя составлением детальных технических спецификаций на работы при подписании договоров с Поставщиками услуг
Снижение ИБ	Внешнее воздействие на информационные сети, в том числе атаки хакеров и компьютерных вирусов	Мониторинг и аудит системы обеспечения ИБ. Осуществление анализа эффективности принятых мер по защите информации с учетом изменений ИКТ-среды, появление новых угроз, инцидентов и проблем. Внедрение дополнительных мер защиты

1. Указание условии пересмотра СОП: Пересмотр СОП проводиться 1 раз в 3 года или при появлении новых требовании.

2. Нормативные ссылки:

- Приказ и.о. Министра здравоохранения Республики Казахстан от 30 октября 2020 года «Об утверждении форм учетной документации в области здравоохранения, а также инструкций по их заполнению» № ҚР ДСМ-175/2020;

-Приказ и.о. Министра здравоохранения Республики Казахстан от 5 ноября 2021 года «Об утверждении стандартов аккредитации медицинских организаций» « № ҚР ДСМ – 111.

- Приказ Министра здравоохранения Республики Казахстан от 24 августа 2021 года № «Об утверждении «Правил оказания первичной медико-санитарной помощи» ҚР ДСМ-90

Лист регистрации изменений

№	№ раздела, пункта стандарта, в которое внесено изменение	Дата внесения изменения	ФИО лица, внесшего изменения

Лист ознакомления

№	Фамилия И.О.	Должность	Дата	Подпись

	Сужикин А.А.	программист	04.01.2024	Сус.
	Сонов А.В	программист	04.01.2024	