АЛМАТЫ ҚАЛАСЫ
ДЕНСАУЛЫҚ САҚТАУ БАСҚАРМАСЫ

ШАРУАШЫЛЫҚ ЖҮРГІЗУ ҚҰҚЫҒЫНДАҒЫ «№ 20 ҚАЛАЛЫҚ ЕМХАНАСЫ» МЕМЛЕКЕТТІК КОММУНАЛДЫҚ КӘСІПОРНЫ

УПРАВЛЕНИЕ ЗДРАВООХРАНЕНИЯ
ГОРОДА АЛМАТЫ

ГОСУДАРСТВЕННОЕ КОММУНАЛЬНОЕ ПРЕДПРИЯТИЕ НА ПРАВЕ ХОЗЯЙСТВЕННОГО ВЕДЕНИЯ «ГОРОДСКАЯ ПОЛИКЛИНИКА № 20»

БҰЙРЫҚ
«01» апреля 2019 г.
Алматы қаласы

ПРИКАЗ
№ 63/1п
город Алматы

Об утверждении
Программы информационной безопасности

В целях обеспечения информационной безопасности, недопущение нанесения материального, физического, морального или иного ущерба Поликлинике в результате информационной деятельности, оперативного восстановления информации в случае неавторизованного доступа, нарушения работоспособности информационных систем.

ПРИКАЗЫВАЮ:

1. Утвердить политику информационной безопасности
2. Контроль за исполнением настоящего приказа оставляю за собой.
3. Приказ вступает в силу со дня подписания.

Главный врач **Г. Кенжебекова**

Название документа	**Политика информационной безопасности**			
Разработчик	**Должность**	**Ф.И.О.**	**Подпись**	**Дата согласования**
	Старший программист	Искаков Д.Ж.		01.04.2019г.
Согласовано	И.о. заместитель главного врача по лечебно-профилактической работе	Алиева М.Б.		01.04.2019г.
	И.о. заместитель главного врача по организационной методической работе	Бегалиева Г.Е.		01.04.2019
	Главный медсестра	Бердибекова М.К.		01.04.2019
	Юрист	Кадирсизова Э.У		01.04.2019
Дата следующего пересмотра апрель 2021 г.				
Версия 1				
Код ПРГ-02-46				

Алматы 2019 г.

Содержание

Аннотация

Политика информационной безопасности Городской поликлиники №20 (далее – Политика) — комплекс превентивных мер по защите информации, в том числе информации с ограниченным распространением (служебная информация), информационных процессов и включает в себя требования в адрес пользователей информационных систем Городской поликлиники №20 (далее – Поликлиника). На основе Политики строится управление информационной безопасностью.

Список использованных сокращений:

ИС	Информационная система
ЗИ	Защита информации
КСПД	Корпоративная сеть передачи данных
НСД	Несанкционированный доступ
ПК	Персональный компьютер
ОС	Операционная система
СВТ	Средства вычислительной техники
ПО	Программное обеспечение
ИТ	Информационные технологии
ЛВС	Локально вычислительная сеть
УЗГС	Управление по защите государственных секретов

1. Термины и определения, используемые в данном документе

Основные термины и определения, используемые в политике информационной безопасности информационных ресурсов ГКП на ПХВ «Городская поликлиника №20» (далее - поликлиника), приведены согласно стандартам:

Закон Республики Казахстан от 23 января 2001 года № 148 «О местном государственном управлении и самоуправлении в Республике Казахстан» (с изменениями и дополнениями по состоянию на 09.02.2009 г.).

Закон Республики Казахстан 11 января 2007 года № 217-III «Об информатизации».

Закон Республики Казахстан от 15 марта 1999 года № 349-1 «О государственных секретах» (с изменениями и дополнениями по состоянию на 27.07.2007 г.).

Закон Республики Казахстан от 26 июня 1998 года № 233-1 «О национальной безопасности Республики Казахстан» (с изменениями и дополнениями по состоянию на 07.08.2007 г.).

Указ Президента Республики Казахстан от 14 марта 2000 г. № 359 «О Государственной программе обеспечения информационной безопасности Республики Казахстан на 2000-2003 годы».

Указ Президента Республики Казахстан от 10 октября 2006 года № 199 «О концепции информационной безопасности РК».

Международный стандарт ISO/IEC FDIS 17799.

1.2. При разработке данного документа использовались следующие понятия:

1) Поликлиника – ГКП на ПХВ «Городская поликлиника №20»;
2) Информационная безопасность - это процесс обеспечения конфиденциальности, целостности и доступности информации, все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации или средства ее обработки;
3) Информационная система (далее - ИС) - система, предназначенная для хранения, обработки, поиска, распространения, передачи и предоставления информации с применением аппаратно-программного комплекса;
4) Электронные информационные ресурсы - информация, хранимая в электронном виде (информационные базы данных), содержащаяся в информационных системах;
5) Информационные процессы - процессы создания, сбора, обработки, накопления, хранения, поиска, распространения и потребления информации;
6) Информационные услуги - услуги по предоставлению пользователям информационных ресурсов;
7) Корпоративная сеть - совокупность информационных систем, компьютеров, кабелей, сетевых адаптеров, объединенных в единую сеть и эксплуатируемых в государственном органе;
8) Конфиденциальные электронные информационные ресурсы - электронные информационные ресурсы, не содержащие государственных секретов, доступ к которым ограничен в соответствии с законами Республики Казахстан или их собственником либо владельцем в случаях, предусмотренных законодательством Республики Казахстан;
9) Информационно-коммуникационная сеть - совокупность технических и аппаратно-программных средств обеспечения взаимодействия между информационными системами или между их составляющими, а также передачи информационных ресурсов;
10) Аппаратно-программный комплекс - совокупность программных и технических средств, обеспечивающих информационные процессы;
11) Защита электронных информационных ресурсов, информационных систем - комплекс правовых, организационных и технических мероприятий, направленных на их сохранение, предотвращение неправомерного доступа к электронным информационным ресурсам, информационным системам, включая незаконные действия по получению, копированию, распространению, искажению, уничтожению или блокированию информации;
12) Средство(а) обработки информации - любая система обработки информации, сервис или инфраструктура, или их физические места размещения;

13) Структурированная кабельная система - набор коммутационных элементов, а также методика их совместного использования, позволяющие создавать регулярные, легко расширяемые структуры связей в вычислительных сетях;
14) Удаленный доступ - подключение к компьютеру по телефонной линии через модем;
15) Система управления сетью - система оборудования и программного обеспечения, используемая для администрирования, мониторинга и управления данными в сети;
16) Сервер - это обслуживающий компьютер или сеть компьютеров, предназначенные для обслуживания пользователей, которые обращаются к нему со своим запросом;
17) Администратор сервера или системный администратор - сотрудник, в обязанности которого входит создание оптимальной работоспособности компьютеров (серверов) и программного обеспечения для пользователей, связанных между собой;
18) Администратор сети - сотрудник, отвечающий за функционирование и использование ресурсов автоматизированной системы и/или вычислительной сети;
19) Модель нарушителя информационной безопасности - это набор предположений об одном или нескольких возможных нарушителях информационной безопасности, их квалификации, их технических и материальных средствах и т.д.;
20) Аутсорсинг - комплекс мероприятий, направленных на передачу предприятием определенных процессов и функций другой организации. Аутсорсинг - использование чужих ресурсов;
21) Локальная вычислительная сеть (далее - ЛВС) - это совокупность компьютеров и других средств вычислительной техники (активного сетевого оборудования, принтеров, сканеров и т.п.), объединенных с помощью кабелей и сетевых адаптеров и работающих под управлением сетевой операционной системы. Вычислительные сети создаются для того, чтобы группа пользователей могла совместно задействовать одни и те же ресурсы: файлы, принтеры, модемы, процессоры и т.п.;
22) Локальный администратор - это пользователь компьютера с правами администратора;
23) Автоматизированная система - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций;
24) Вычислительная сеть (компьютерная сеть) - это система, обеспечивающая обмен данными между вычислительными устройствами (компьютеры, серверы, маршрутизаторы и другое оборудование).

2. Введение

Политика информационной безопасности ГКП на ПХВ «Городской поликлиники №20» (далее - Поликлиника) - комплекс превентивных мер по защите информации, в том числе конфиденциальных данных, информационных процессов и включает в себя требования в адрес сотрудников, поставщиков и технических служб. На основе политики строится управление информационной безопасностью.

Настоящая политика учитывает современное состояние и ближайшие перспективы развития локально вычислительной сети Поликлиники, цели, задачи и правовые основы эксплуатации, режимы функционирования, а также анализ угроз безопасности для ее ресурсов.

Положения и требования политики распространяются на структурные подразделения Поликлиники, в которых осуществляется автоматизированная обработка информации, в том числе конфиденциальных сведений или персональных данных, а также специалистов и технических служб, осуществляющих обеспечение функционирования информационных систем Поликлиники.

3. Пользователи информационных систем

Пользователями информационных систем Поликлиники являются сотрудники, персонал, обеспечивающий информационную безопасность, системно-техническое обслуживание.

4. Модель нарушителя

Потенциальные нарушители делятся на внутренних и внешних. Внутренние нарушители - это практически все сотрудники Поликлиники, а также обслуживающий персонал по услугам аутсорсинга. Они делятся на следующие группы в зависимости от уровня доступа к информационным ресурсам корпоративной сети: лица, имеющие доступ к информации для служебного пользования и задействованные в технологии обработки, передачи и хранения информации; обслуживающий персонал по услугам аутсорсинга.

Чтобы построить реальную модель потенциального нарушителя необходимо принять во внимание виды выявленных нарушений, устремлений различных лиц и организаций к Поликлинике, а также имеющиеся в Поликлинике интересы других юридических лиц.

Классифицируются следующие виды нарушений: несанкционированное использование программ, которые негативно влияют на работоспособность локальной вычислительной сети (далее - ЛВС) Поликлиники, снижают ее производительность, мешают корректной работе ЛВС (сканеры сети, интенсивный широковещательный трафик и т.п.); использование прав локальных администраторов на рабочих станциях пользователей, что дает возможность установки обычному пользователю неограниченного количества

программ; нарушения сотрудниками вследствие незнания требований информационной безопасности и правовых актов Поликлиники.

Потенциальные внешние нарушители: бывшие сотрудники Поликлиники; посетители (приглашенные представители организаций, граждане РК и нерезиденты); представители поставщиков, поставляющих технику, программное обеспечение, услуги и т.п.

5. Политика информационной безопасности

5.1 Назначение, нормативная и правовая база Политики

Политика информационной безопасности Поликлиники является методологической базой: выработки и совершенствования комплекса согласованных нормативных, правовых, технологических и организационных мер, направленных на защиту информации; обеспечения информационной безопасности; координации деятельности структурных подразделений при проведении работ по соблюдению требований обеспечения информационной безопасности.

Научно-методической основой политики 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 положения политики базируются на качественном осмыслении вопросов информационной безопасности, не концентрируя внимание на экономическом (количественном) анализе рисков и обосновании необходимых затрат на защиту информации.

Нормативной правовой базой политики являются Конституция Республики Казахстан, Уголовный кодекс Республики Казахстан, Кодекс Республики Казахстан об административных правонарушениях, законы, указы, постановления и иные нормативные правовые акты Республики Казахстан, а также правовые акты Поликлиники, регламентирующие вопросы обеспечения информационной безопасности.

5.2 Цели и задачи политики информационной безопасности

Главной целью, на достижение которой направлены все положения политики, является надежное обеспечение информационной безопасности Поликлиники и, как следствие, недопущение нанесения материального, физического, морального или иного ущерба Поликлинике в результате информационной деятельности.

Указанная цель достигается посредством обеспечения и постоянного поддержания следующего состояния корпоративной вычислительной сети:
доступность обрабатываемой информации для зарегистрированных пользователей;

устойчивое функционирование ЛВС Поликлиники;
обеспечения конфиденциальности информации, хранимой, обрабатываемой на средствах вычислительной техники (далее - СВТ) и передаваемой по каналам связи;
целостность и аутентичность информации, хранимой и обрабатываемой в ЛВС Поликлиники, и передаваемой по каналам связи.

5.2.2. Задачи политики

Для достижения поставленных целей политика направлена на решение следующих задач:
защита от вмешательства посторонних лиц в процесс функционирования ЛВС Поликлиники;
разграничение доступа зарегистрированных пользователей к информации, а также к аппаратным, программно-аппаратным и программным средствам включая средства криптографической защиты информации, используемым в ЛВС Поликлиники;
регистрация действий пользователей при использовании ресурсов ЛВС Поликлиники в системных журналах;
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 вредоносных кодов, включая компьютерные вирусы;
защиту коммерческой тайны и персональных данных от утечки, несанкционированного разглашения или искажения при ее обработке, хранении и передаче по каналам связи;
обеспечение 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 для минимизации и локализации нанесенного ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации.

5.3. Меры по реализации политики

5.3.1. Средства и меры защиты от утечки информации по техническим каналам

Для выявления утечки информации необходим систематический контроль возможности образования каналов утечки и оценки их энергетической опасности на границах контролируемой зоны (территории, помещения). Закрытие и локализация каналов утечки обеспечивается организационно-техническими мерами.

В соответствии с используемыми каналами передачи информации в Поликлинике предусматриваются адекватные технические средства защиты. 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 Поликлиники, организуется пропускной режим для предотвращения доступа посторонних лиц в Поликлиника.

Защита информации от утечки по каналам их передачи в Поликлиника достигается путем применения комплексных программных, технических средств защиты и организационных мер.

5.4. Меры по защите средств вычислительной техники (далее - СВТ)

В результате возникновения аварий, стихийных бедствий и иных внештатных ситуаций могут возникнуть нарушения работоспособности СВТ, а также разрушение аппаратных, программных, информационных ресурсов в Поликлинике. На такие случаи в Поликлинике предусматриваются соответствующие меры защиты, согласно плану по обеспечению непрерывной деятельности информационных систем.

5.4.1.Защита от несанкционированного доступа (далее - НСД) к СВТ

Защита СВТ пользователей от несанкционированного доступа в Поликлиника строится по нескольким направлениям.

Определяются организационные меры по предотвращению НСД, в том числе в случае утраты/компрометации паролей и выхода из строя СВТ.

5.5. Защита от использования незарегистрированных носителей информации

Запись и копирование служебной и иной защищаемой информации, в том числе для передачи другим лицам, производится на зарегистрированные носители информации. За запись служебной и иной защищаемой информации на незарегистрированные в установленном порядке носители пользователь привлекается к дисциплинарной ответственности.

5.6. Защита от аппаратных спец вложений, нелегального внедрения и использования неучтенных программ

Для защиты от аппаратных спец вложений, нелегального внедрения и использования неучтенных программ в Поликлинике кроме мероприятий, включающих физическую защиту, проведение аудита обращения к СВТ и мониторинг системных журналов устанавливается базовый комплекс программного обеспечения, который необходимо устанавливать на рабочие станции пользователей. В базовый комплекс включается лицензионное ПО, необходимое для обеспечения работоспособности СВТ.

Использование для производственных целей прикладного ПО, не входящего в состав базового комплекса санкционируется руководством структурного подразделения Поликлиники.

5.7. Защита от несанкционированного копирования данных пользователем

Служебная и иная защищаемая информация, обрабатываемая и хранящаяся в ЛВС Поликлиники, подлежит копированию и передаче третьему лицу только с письменного разрешения руководителя структурного подразделения Поликлиники.

За копирование и передачу служебной и иной защищаемой информации третьему лицу без разрешения руководителя Поликлиники пользователь привлекается к дисциплинарной ответственности.

Примечание: Для пользователей категорированных объектов средств вычислительной техники в любых случаях информация, содержащая сведения, составляющие государственные секреты, передается только через Управление по защите государственных секретов (УЗГС).

5.8. Защита информации, отображаемой на мониторе СВТ

Защита достигается путем ограничения физического доступа к средствам отображения информации, исключения наблюдения за отображаемой информацией посторонними лицами, согласно Инструкции пользователя по эксплуатации средств вычислительной техники и программного обеспечения.

5.9. Защита от действий вредоносных программ, вирусов

В целях защиты от действий вредоносных программ и вирусов в Поликлинике используются «иммуностойкие» программные средства, защищенные от возможности несанкционированной модификации, специальные программы-анализаторы, осуществляющие постоянный контроль за возникновением отклонений в деятельности прикладных программных продуктов, периодическую проверку наличия возможных следов вирусной

активности, а также входной контроль новых программ перед их использованием.

Организационные меры, включают в себя разработку правовых актов Поликлиники, регламентирующие эту деятельность и проведение работ в соответствии с ними.

5.10. Защита от хищения носителей информации

В Поликлинике устанавливается определенный порядок учета, хранения и использования носителей информации, в том числе сведений в электронном виде. При передаче носителя цифровой информации для повторного использования за пределами Поликлиники проводится его очистка с целью исключения несанкционированного разглашения защищаемых сведений.

5.11. Защита информации в оперативной памяти

За каждым СВТ закрепляется сотрудник Поликлиники. На СВТ используется система аутентификации и идентификации сотрудника, работающего на нем. Передача СВТ в пользование другому сотруднику осуществляется с разрешения руководителя подразделения. Принимаются необходимые программно-технические средства защиты информации, обрабатываемой на СВТ.

5.12. Защита от умышленной модификации информации

Кроме средств регламентированного доступа к СВТ защита информации от модификации осуществляется программными, техническими и организационными мерами. Для своевременного выявления и обнаружения указанных посягательств используются журналы действий администратора.

5.13. Защита от ошибок программно-аппаратных средств

С целью проверки работоспособности, перед вводом в эксплуатацию программные продукты и аппаратные средства подлежат тестированию в условиях, приближенных к реальным условиям. Не пригодные к использованию программное обеспечение и аппаратные средства в эксплуатацию не принимаются.

5.14. Защита от некомпетентного использования, настройки или неправомерного отключения средств защиты

Средства защиты корпоративной вычислительной сети вводятся в эксплуатацию, сопровождаются и используются в соответствии с

установленным регламентом. Контроль за этим процессом осуществляет программист Поликлиники, обеспечивающий информационную безопасность.

5.15. Защита от частичного или полного отказа СВТ или разрушению аппаратных, программных, информационных ресурсов

Частичный, полный отказ СВТ, а также разрушение аппаратных, программных, информационных ресурсов в Поликлинике возникает в результате возникновения аварий, стихийных бедствий и иных внештатных ситуаций. На такие случаи в Поликлинике предусматриваются соответствующие меры защиты и План обеспечения непрерывной работы и восстановления.

5.16. Защита от атак типа «отказ в обслуживании» со стороны сети

В целях защиты от атак типа «отказ в обслуживании» враждебного мобильного кода проводятся организационные и технические мероприятия, включающие в себя разработку правовых актов Поликлиники, регламентирующие эту деятельность и проведение работ в соответствии с ними.

5.17. Меры по защите коммуникационных средств

Основные и резервные телекоммуникационные сервисы соответствующим образом отделяются друг от друга, чтобы не подвергаться одним и тем же угрозам.

5.18. Защита от незаконного подключения к линиям связи и к сетевому оборудованию

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 попытки незаконного подключения к линиям связи и сетевому оборудованию лица несут ответственность в соответствии с законодательством Республики Казахстан.

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

Повреждение, некорректное функционирование, частичный, полный отказ сетевого оборудования Поликлиники возникает, в первую очередь, в результате аварий, стихийных бедствий и иных внештатных ситуаций.

В Поликлинике принимаются меры, связанные с внедрением средств защиты, которые будут использоваться в случае стихийных бедствий (пожаров, наводнений, и землетрясений), а также в различных нештатных ситуациях.

Поликлиникой разрабатывается план обеспечения непрерывной работы и восстановления.

5.20. Защита от неправомерного включения, выключения оборудования

Сетевое оборудование корпоративной вычислительной сети Поликлиники вводится в эксплуатацию, сопровождается и используется в соответствии с установленным регламентом. Включение и отключение оборудования производится уполномоченным техническим персоналом, который работает в соответствии с указанием руководства Поликлиники.

5.21. 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. Для своевременного выявления, предупреждения и пресечения указанных посягательств используется аппаратура наблюдения и мониторинга.

5.22. Меры по защите системы архивирования

Поликлиникой определяется порядок резервного копирования, хранения и восстановления программных продуктов и информационных систем. Обеспечивается санкционированный доступ к хранилищу резервных копий для своевременного восстановления информации и информационных систем в случае сбоя, аварии и иных нештатных ситуациях.

Поликлиникой разрабатывается план обеспечения непрерывной работы и восстановления, в котором также определяются меры по защите архивов на случай возникновения аварий, стихийных бедствий и других нештатных ситуаций.

5.23. Меры по защите при выводе информации

К основным устройствам вывода информации являются мониторы, принтеры, средства записи информации на цифровые носители.

Следует принять исчерпывающие меры защиты информации на устройствах долговременной памяти при передаче СВТ на ремонт и сторонние организации.

5.24. Требования по обучению персонала вопросам информационной безопасности

Все сотрудники Поликлиники при необходимости проходят соответствующее обучение и получают на регулярной основе обновленные варианты политик и процедур информационной безопасности, принятых в Поликлинике, в соответствии с их должностными функциями. Подготовка в области осведомленности начинается с процесса введения предназначенного для ознакомления с политиками информационной безопасности и ожиданиями Поликлиники перед предоставлением доступа к информации или службам. Подготовка включает в себя изучение требований безопасности, юридических обязательств и мер контроля деловой деятельности, а также обучение правильному использованию средств обработки информации, например, процедуре регистрации учетной записи сотрудника в системах, применению пакетов программ, предоставление доступа к сети Интернет и информацию о дисциплинарном процессе.

Подготовка по улучшению осведомленности имеет целью дать возможность отдельным лицам распознавать проблемы информационной безопасности и инциденты ее нарушения и реагировать соответственно своим рабочим обязанностям.

5.25. Требования к анализу и оценке рисков по информационной безопасности

Оценки рисков идентифицируют, определяют количество рисков и их приоритеты по отношению к критериям принятия рисков и целям, подходящим Поликлинике.

Результаты направляют и определяют соответствующие действия руководства и приоритеты для управления рисками безопасности и для реализации мер контроля, выбранных для защиты от таких рисков. Требуется неоднократное повторение процесса оценки рисков и выбора мер контроля, чтобы охватить все информационные системы.

Оценка риска включает систематический подход определения величины рисков (анализ рисков) и процесс сравнения оцененных рисков с критериями рисков с целью определения значимости рисков (оценка степени рисков).

Оценки рисков проводятся периодически для реагирования на изменения в требованиях безопасности и в ситуации рисков, например, в активах, угрозах, уязвимостях, воздействиях, оценке степени рисков и при возникновении значительных изменений. В целях получения сравнимых и воспроизводимых результатов эти оценки рисков предпринимаются методическим образом.

Чтобы быть эффективной, оценка рисков безопасности информации имеет четко определенную область действия и включает взаимосвязь с оценками рисков в других областях, если это целесообразно.

Областью действия оценки риска являются Поликлиника, подразделения Поликлиники, отдельная информационная система, специфические

компоненты системы, или службы, где она осуществима, реалистична и полезна.

Перед рассмотрением проблемы обработки рисков Поликлиника определяет критерии определения принятия или неприятия рисков. Риски принимаются, если, например, сделана оценка, что риск незначителен или что стоимость обработки нерентабельна для Поликлиники. Подобные решения регистрируются.

Для каждого из идентифицированных рисков, следующих за оценкой рисков, необходимо принимать решение по обработке риска. Возможными вариантами для обработки риска включают:

применение подходящих мер контроля для уменьшения рисков;

сознательное и объективное принятие рисков при условии, что они соответствуют политике Поликлиники и критериям принятия рисков;

избежание рисков путем недопущения действий, вызывающих возникновение рисков;

передачу ассоциированных рисков другим сторонам (поставщикам).

5.26. Обязательные документы для обеспечения информационной безопасности

Обеспечение защищенности информационной среды Поликлиники, а также применения единой политики информационной безопасности достигается следующими документами по информационной безопасности: Правила инвентаризации и паспортизации средств вычислительной техники, телекоммуникационного оборудования и программного обеспечения, Правила разграничения прав доступа к электронным информационным ресурсам, Инструкцией о резервном копировании информации, Инструкцией о парольной защите, Правила использования Интернет и электронной почты, Правила организации процедуры аутентификации пользователей, Правила организации антивирусного контроля, , Правила использования мобильных устройств и носителей информации, Инструкцией администратора по сопровождению объекта информатизации, Инструкцией о порядке действий пользователей по реагированию на инциденты ИБ и во внештатных (кризисных) ситуациях, а также настоящей Политикой.

5.27. Пересмотр политики информационной безопасности

Соблюдение требований политики информационной безопасности обязательно для всех сотрудников Поликлиники. Проведение планового аудита информационной безопасности является одним из основных методов проверки эффективности мер по защите информации. Результаты аудита служат основанием для пересмотра некоторых положений политики и внесения в них необходимых корректировок.

Ежегодно проводится аудит информационной безопасности Поликлиники, на основании которого структурное подразделение, уполномоченное по обеспечению информационной безопасности совершенствует политику на предмет соответствия предъявляемым требованиям. В случае возникновения необходимости, при выявлении в процессе аудита несоответствия современным требованиям вносят изменения и дополнения.

Кроме этого, используемые информационные технологии и организация служебной деятельности непрерывно меняются, это приводит к необходимости корректировать существующие подходы к обеспечению информационной безопасности.

5.28. Меры по недопущению предоставления удаленного доступа к информационным ресурсам Поликлиники

В Поликлинике не допускается использование программных средств организации удаленного доступа из сети Интернет в информационно-коммуникационной среде Поликлиники.

Предоставление несанкционированного удаленного доступа к информационным ресурсам Поликлиники влекут за собой ответственность в соответствии с действующим законодательством Республики Казахстан.