

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ЗДРАВООХРАНЕНИЯ
"ГОРОДСКАЯ КЛИНИЧЕСКАЯ БОЛЬНИЦА № 1 ИМ. С.З. ФИШЕРА"

13.10.2025

ПРИКАЗ

№ 210

Волжский

Об утверждении Политики информационной безопасности
ГБУЗ "Городская клиническая больница № 1 им. С.З. Фишера"

В соответствии с нормами Федеральных законов от 27.07.2006 № 152-ФЗ «О персональных данных», от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», в целях формирования в ГБУЗ «ГКБ № 1 им. С.З. Фишера» системного подхода к защите информации, решения ключевых задач в области защиты информации, обеспечения конфиденциальности, целостности и доступности информации, п р и к а з ы в а ю:

1. Утвердить и ввести в действие Политику информационной безопасности государственного бюджетного учреждения здравоохранения "Городская клиническая больница № 1 им. С.З. Фишера" (далее - Политика) (приложение к приказу).

2. Заведующим лечебно-диагностических отделений, руководителям структурных подразделений в срок до 31.10.2025 обеспечить:

2.1. ознакомление вверенного персонала с положениями Политики;

2.2. предоставление листов ознакомления с Политикой в канцелярию учреждения.

2.3. Работникам ГБУЗ "ГКБ № 1 им. С.З. Фишера" принять к исполнению положения Политики.

3. Начальнику отдела информационных технологий Козлову М.В. организовать:

3.1. Размещение Политики на официальном сайте учреждения в сети интернет;

3.2. ознакомление с Политикой вновь принимаемых в ГБУЗ "ГКБ № 1 им. С.З. Фишера" работников.

4. Заведующему канцелярией Ущенко О.В. обеспечить направление приказа структурным подразделениям учреждения.

5. Контроль исполнения приказа возложить на заместителя главного врача по медицинской части Миронова Р.В., ответственного за организацию и реализацию в ГБУЗ «ГКБ № 1 им. С.З. Фишера» мероприятий, направленных на обеспечение информационной безопасности.

Главный врач

К.П.Позднышев

1. Общие положения

1.1 Настоящая Политика является документом, доступным всем сотрудникам ГБУЗ «ГКБ № 1 им. С.З. Фишера» и всем пользователям его ресурсов. Представляет собой официально принятую руководством ГБУЗ «ГКБ № 1 им. С.З. Фишера» систему взглядов на обеспечение информационной безопасности в ГБУЗ «ГКБ № 1 им. С.З. Фишера».

1.2 Основной задачей в области информационной безопасности ГБУЗ «ГКБ № 1 им. С.З. Фишера» признает совершенствование мер и средств обеспечения информационной безопасности информационных ресурсов ГБУЗ «ГКБ № 1 им. С.З. Фишера» в контексте медико-социальной помощи.

1.3 В рамках своей деятельности ГБУЗ «ГКБ № 1 им. С.З. Фишера» обязуется предпринимать все возможные меры для защиты информации от риска причинения вреда, убытков и ущерба, возникающих в результате реализации угроз информационной безопасности или других противоправных действий, связанных с нарушением информационной безопасности ГБУЗ «ГКБ № 1 им. С.З. Фишера».

1.4 Требования информационной безопасности, которые предъявляются ГБУЗ «ГКБ № 1 им. С.З. Фишера», соответствуют целям деятельности ГБУЗ «ГКБ № 1 им. С.З. Фишера» и предназначены для снижения рисков, связанных с информационной безопасностью, до приемлемого уровня.

1.5 Реализация и контроль исполнения требований, установленных настоящей Политикой, осуществляется работниками, ответственными за информационную безопасность, в соответствии со своими должностными инструкциями и другими внутренними документами ГБУЗ «ГКБ № 1 им. С.З. Фишера» по информационной безопасности.

2 Цели и задачи обеспечения информационной безопасности

2.1 Целями обеспечения информационной безопасности ГБУЗ «ГКБ № 1 им. С.З. Фишера» являются:

- защита интересов учреждения, работников и иных субъектов информационных отношений, взаимодействующих с ГБУЗ «ГКБ № 1 им. С.З. Фишера», от возможного нанесения ущерба их деятельности посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования информационных систем ГБУЗ «ГКБ № 1 им. С.З. Фишера», нарушения работы технических и программных средств, приводящего к недоступности информации, разглашению, искажению, уничтожению защищаемой информации и ее незаконному использованию;
- обеспечение устойчивого и корректного функционирования программных и аппаратных компонентов ГБУЗ «ГКБ № 1 им. С.З. Фишера» и предоставляемых сервисов;
- соблюдение правового режима использования массивов и программ обработки информации;
- предотвращение реализации угроз безопасности для деятельности ГБУЗ «ГКБ № 1 им. С.З. Фишера».

при использовании защищаемых ресурсов и периодический контроль корректности их действий.

2.5.4 Контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения.

2.5.5 Защиту от несанкционированной модификации и контроль целостности используемых в ГБУЗ «ГКБ № 1 им. С.З. Фишера» программных средств и данных, а также защиту от несанкционированного внедрения вредоносных программ.

2.5.6 Защиту информации ограниченного доступа, хранимой, обрабатываемой в ГБУЗ «ГКБ № 1 им. С.З. Фишера», от несанкционированного разглашения или искажения.

2.5.7 Обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации), а также определение автора при создании и модификации информации.

2.5.8 Обеспечение исправности применяемых в информационных системах ГБУЗ «ГКБ № 1 им. С.З. Фишера» средств защиты информации.

2.5.9 Своевременное выявление источников угроз безопасности информации, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, создание механизма оперативного реагирования на угрозы безопасности информации.

2.5.10 Создание условий для минимизации наносимого ущерба неправомерными действиями, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации в ГБУЗ «ГКБ № 1 им. С.З. Фишера».

2.6 Решение вышеперечисленных задач в ГБУЗ «ГКБ № 1 им. С.З. Фишера» осуществляется:

2.6.1 Учетом всех подлежащих защите информационных ресурсов (каналов связи, аппаратных и программных средств).

2.6.2 Регламентацией процессов обработки подлежащей защите информации, действий работников ГБУЗ «ГКБ № 1 им. С.З. Фишера» и персонала, осуществляющего обслуживание и модификацию программных и технических средств, на основе утвержденных организационно-распорядительных документов по вопросам обеспечения информационной безопасности.

2.6.3 Назначением и подготовкой работников, ответственных за организацию и осуществление мероприятий по обеспечению информационной безопасности в ГБУЗ «ГКБ № 1 им. С.З. Фишера».

2.6.4 Наделением каждого работника минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам.

2.6.5 Знанием и строгим соблюдением всеми работниками, использующими и обслуживающими аппаратные и программные средства, требований организационно-распорядительных документов по вопросам обеспечения информационной безопасности.

2.6.6 Персональной ответственностью за свои действия каждого работника, участвующего в рамках своих функциональных обязанностей в процессах

представителями сторонних организаций, оказывающих услуги в рамках договорных обязательств.

3.3.2 При построении, внедрении и эксплуатации системы обеспечения информационной безопасности руководство ГБУЗ «ГКБ № 1 им. С.З. Фишера» обеспечивает условия для эффективной координации действий всех лиц, обеспечивающих информационную безопасность.

3.4 Принцип дружелюбности и простоты

3.4.1 Система обеспечения информационной безопасности в ГБУЗ «ГКБ № 1 им. С.З. Фишера» формируется таким образом, чтобы сделать максимально прозрачными для пользователей информационных систем ГБУЗ «ГКБ № 1 им. С.З. Фишера» процессы ее функционирования.

3.4.2 Система обеспечения информационной безопасности в ГБУЗ «ГКБ № 1 им. С.З. Фишера» выстраивается таким образом, чтобы ограничения организационного и технического характера, налагаемые на сотрудников ГБУЗ «ГКБ № 1 им. С.З. Фишера» в связи с реализацией защитных мер, существенно не затрудняли работу с ресурсами информационных систем ГБУЗ «ГКБ № 1 им. С.З. Фишера».

3.5 Принцип превентивности

Меры, применяемые ГБУЗ «ГКБ № 1 им. С.З. Фишера» с целью обеспечения информационной безопасности, должны носить упреждающий характер и не допускать реализацию соответствующих угроз и атак.

3.6 Принцип оптимальности и многоуровневости

3.6.1 Выбор единых программно-технических средств с целью сокращения расходов на создание и поддержку функционирования компонентов системы обеспечения информационной безопасности.

3.6.2 Применение разнородных программно-технических средств защиты с целью построения целостной системы обеспечения информационной безопасности и устранения возможных уязвимостей.

3.6.3 Использование для создания разных рубежей обеспечения информационной безопасности средств, которые имеют схожие друг с другом функции, но разработанные различными производителями и имеющие различную логику построения защитных механизмов.

3.7 Принцип экономической целесообразности

3.7.1 Осуществление оценки уровня затрат на обеспечение безопасности, ценности информационных ресурсов и величины возможного ущерба для ГБУЗ «ГКБ № 1 им. С.З. Фишера» в случае нарушения конфиденциальности, целостности и доступности информационных ресурсов.

3.7.2 Выбор необходимого и достаточного уровня защиты информационных ресурсов, при котором затраты, риск и размер возможного ущерба являются приемлемыми.

3.8 Принцип непрерывности и недопустимости открытого состояния

3.8.1 Система обеспечения информационной безопасности в ГБУЗ «ГКБ № 1 им. С.З. Фишера» строится таким образом, чтобы процесс защиты информационных систем ГБУЗ «ГКБ № 1 им. С.З. Фишера» осуществлялся непрерывно и целенаправленно на протяжении всего жизненного цикла информационных систем.

4 Зоны ответственности участников процесса обеспечения информационной безопасности

4.1 Руководство ГБУЗ «ГКБ № 1 им. С.З. Фишера»

4.1.1 Создает условия, при которых каждый работник ГБУЗ «ГКБ № 1 им. С.З. Фишера» знает свои обязанности и задачи в отношении информационных ресурсов и обеспечивает наличие необходимого разделения функций и полномочий в целях недопущения конфликта интересов.

4.1.2 Назначает работников, ответственных за создание и использование СЗИ, информации обрабатываемой в ГБУЗ «ГКБ № 1 им. С.З. Фишера», реализацию процессов обеспечения информационной безопасности, а также их контроля.

4.1.3 Обеспечивает достаточную численность и квалификацию персонала, ответственного за построение и поддержание процессов обеспечения информационной безопасности, внедрение и управление СЗИ, а также контроль и мониторинг текущего состояния системы обеспечения информационной безопасности ГБУЗ «ГКБ № 1 им. С.З. Фишера».

4.1.4 Иницирует, осуществляет поддержку и контролирует выполнение всех процессов обеспечения информационной безопасности в ГБУЗ «ГКБ № 1 им. С.З. Фишера».

4.1.5 Анализирует результаты работ по обеспечению информационной безопасности и на их основе принимает решения о необходимости развития системы обеспечения информационной безопасности, ее развития, о возможности принятия остаточных рисков информационной безопасности, о выделении ресурсов, необходимых для реализации Политики информационной безопасности.

4.2 Компетентные подразделения ГБУЗ «ГКБ № 1 им. С.З. Фишера»

4.2.1 Подготавливают предложения по доработке Политики информационной безопасности в части технического обеспечения информационных систем ГБУЗ «ГКБ № 1 им. С.З. Фишера».

4.2.2 Разрабатывают процедуры эффективного управления техническими и программными средствами информационных систем и применяют их в практической деятельности в отношении всех систем, действующих в ГБУЗ «ГКБ № 1 им. С.З. Фишера».

4.2.3 Организуют проведение необходимого инструктажа работников структурных подразделений в части вопросов безопасной эксплуатации информационных систем.

4.2.4 Обеспечивают защиту доступа ко всему серверному и коммутационному оборудованию, носителям информации, которые используются в соответствующих структурных подразделениях.

4.2.5 Осуществляют мероприятия по поддержке сопровождения и использования информационных систем.

4.2.6 Обеспечивают отказоустойчивость всего программно-аппаратного комплекса и процедуру регламентированного восстановления работоспособности после отказов компонентов.

4.2.7 Регулярно обновляют программные и программно-аппаратные комплексы СЗИ в ГБУЗ «ГКБ № 1 им. С.З. Фишера».

получен.

4.4.3 Обеспечивают физическую безопасность всего технического оборудования и носителей информации, используемых в работе.

4.4.4 Не допускают самовольного подключения и использования в автоматизированной информационной системе личного компьютерного и цифрового оборудования, а также носителей информации.

4.4.5 Не допускают самовольную установку программного обеспечения на компьютеры, входящие в состав информационной системы.

4.4.6 Своевременно информируют руководителя своего структурного подразделения о всех случаях нарушения информационной безопасности и о всех выявленных сбоях в работе программных и программно-аппаратных средств.

4.4.7 Проявляют осмотрительность в отношении любых действий, которые могут повлечь за собой снижение уровня информационной безопасности.

4.5 Сторонние физические и юридические лица

Соблюдают и выполняют требования Политики информационной безопасности, соответствующих локальных актов и документов ГБУЗ «ГКБ № 1 им. С.З. Фишера» и других распоряжений руководства по вопросам информационной безопасности при исполнении договорных обязательств

5 Основные требования по защите информации ограниченного доступа

5.1 Общие требования

5.1.1 В ГБУЗ «ГКБ № 1 им. С.З. Фишера» необходимо соблюдать режим безопасности, предусматривающий реализацию организационно-технических мероприятий, направленных на обеспечение конфиденциальности информации, доступ к которой ограничен в соответствии с требованиями законодательства Российской Федерации.

5.1.2 В учреждении осуществляется обработка и хранение информации ограниченного доступа (доступ к которой ограничен федеральными законами и служебной необходимостью).

5.1.3 В ГБУЗ «ГКБ № 1 им. С.З. Фишера» должен быть разработан перечень информации ограниченного доступа.

5.1.4 Учреждение, как обладатель информации ограниченного доступа, при осуществлении своих прав обязан:

- соблюдать права и законные интересы иных лиц;
- принимать меры по защите информации;
- ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

5.1.5 ГБУЗ «ГКБ № 1 им. С.З. Фишера», как обладатель информации ограниченного доступа, если иное не предусмотрено федеральными законами, вправе:

- разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;
- использовать информацию, в том числе распространять ее, по своему усмотрению;

на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

- использование материальных носителей, содержащих КИ в соответствии с утвержденным порядком, исключающим несанкционированный доступ к ним.

5.2.3 Для обеспечения защиты КИ ГБУЗ «ГКБ №1 им.С.З.Фишера» вправе применять средства и методы технической защиты, предпринимать другие, не противоречащие законодательству РФ, меры.

5.2.4 В целях охраны КИ, в рамках трудовых отношений необходимо:

- ознакомить под расписку работников, доступ которых к КИ, необходим для выполнения ими своих служебных обязанностей, с перечнем КИ, и установленным в ГБУЗ «ГКБ № 1 им. С.З. Фишера» режимом защиты КИ, а также мерами ответственности за его нарушение;

- создать работникам необходимые условия для соблюдения установленного режима защиты КИ.

5.2.5 Работники ГБУЗ «ГКБ № 1 им. С.З. Фишера», обязаны выполнять установленный в ГБУЗ «ГКБ № 1 им. С.З. Фишера» режим защиты КИ, не разглашать информацию, составляющую КИ, и не использовать эту информацию в личных целях.

5.3 Особенности защиты персональных данных

5.3.1 При организации в ГБУЗ «ГКБ № 1 им. С.З. Фишера» защиты персональных данных необходимо руководствоваться требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», который регулирует отношения, связанные с обработкой и хранением персональных данных граждан и определяет требования по защите их конфиденциальности.

5.3.2 ГБУЗ «ГКБ № 1 им. С.З. Фишера» самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» или другими федеральными законами.

5.3.3 Перечень мер, выполнение которых обеспечивает ГБУЗ «ГКБ № 1 им. С.З. Фишера» в качестве оператора персональных данных, должен включать:

- назначение в ГБУЗ «ГКБ № 1 им. С.З. Фишера» ответственного за организацию обработки персональных данных;

- издание ГБУЗ «ГКБ № 1 им. С.З. Фишера» документов, определяющих ее политику в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений;

- применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

- оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27.07.2006 № 152-ФЗ «О

под роспись с документами ГБУЗ «ГКБ № 1 им. С.З. Фишера», устанавливающими порядок обработки персональных данных, а также об их правах, обязанностях и ответственности.

6 Основные требования к процессам обеспечения информационной безопасности

6.1 Общие положения

Методическое руководство, разработку конкретных требований по защите информации, согласование выбора средств вычислительной техники и связи, технических и программных средств защиты, организацию работ по выявлению возможностей и предупреждению утечки и нарушения целостности защищаемой информации осуществляют компетентные подразделения ГБУЗ «ГКБ №1 им.С.З.Фишера».

6.2 Физическая безопасность и безопасность на рабочем месте

6.2.1 Система защиты зданий и помещений ГБУЗ «ГКБ №1 им.С.З.Фишера», объектов и технических средств информационных систем ГБУЗ «ГКБ №1 им.С.З.Фишера» обеспечивает выполнение следующих функций:

- разграничение доступа работников в помещения ГБУЗ «ГКБ №1 им.С.З.Фишера» в соответствии с их полномочиями и функциональными обязанностями;
- регистрацию фактов входа работников в помещения с повышенными требованиями к режиму их посещения (серверные помещения, архивы и т.д.);
- регистрацию фактов входа посторонних лиц в здания ГБУЗ «ГКБ №1 им.С.З.Фишера»;
- предотвращение доступа посторонних лиц в помещения, где размещены аппаратные и сетевые ресурсы информационных систем;
- разрешительный режим вноса/выноса (ввоза/вывоза) компьютерного оборудования, средств записи и хранения информации.

6.2.2 Определяется перечень технических средств, находящихся в специальных контролируемых зонах.

6.2.3 К техническим средствам, которые выделяются в специальные контролируемые зоны необходимо отнести следующие группы ресурсов:

- основные информационные серверы и средства вычислительной техники, на которых осуществляется обработка и хранение информации ограниченного распространения;
- сетевое оборудование и серверы, обеспечивающие работу критических систем;
- файловые серверы, на которых хранятся данные, в том числе резервные;
- критичные для деятельности ГБУЗ «ГКБ №1 им.С.З.Фишера» системы и коммуникационное оборудование, обеспечивающее внешние коммуникации ГБУЗ «ГКБ №1 им.С.З.Фишера».

6.2.4 Контролируемые зоны защищаются соответствующими системами контроля и управления доступом, обеспечивая доступ только авторизованному персоналу.

номера и назначения владельца.

6.3.4 Электронные носители информации должны храниться в помещениях, исключающих получение к ним НСД, при этом должен быть обеспечен контроль доступа к носителям.

6.3.5 Для контроля процессов использования и хранения электронных носителей информации должен быть разработан порядок плановой инвентаризации носителей.

6.3.6 В случае кражи или потери электронных носителей информации, а также иных инцидентов, которые могут привести к разглашению защищаемой информации, должны проводиться мероприятия по расследованию указанных инцидентов.

6.3.7 При снятии электронного носителя информации с эксплуатации, все данные, хранящиеся на нем, должны быть гарантированно стерты.

6.3.8 При утилизации электронных носителей информации должна быть обеспечена невозможность восстановления записанной на них информации.

6.3.9 Факт уничтожения информации и утилизации носителя информации фиксируется в соответствии с порядком, установленным в ГБУЗ «ГКБ №1 им.С.З.Фишера».

6.4 Техническое обслуживание оборудования

6.4.1 Технические средства всех систем ГБУЗ «ГКБ №1 им.С.З.Фишера» должны проходить на регулярной основе сервисное обслуживание в соответствии с рекомендациями производителей оборудования.

6.4.2 Ремонт и сервисное обслуживание оборудования должны выполняться только квалифицированным персоналом.

6.4.3 Техническое обслуживание оборудования и систем сторонними организациями не должно приводить к риску нарушения конфиденциальности защищаемой информации.

6.5 Взаимодействие с третьими лицами

В целях обеспечения информационной безопасности ГБУЗ «ГКБ №1 им.С.З.Фишера» при взаимодействии с третьими лицами должны выполняться следующие мероприятия:

- заключение соглашения о неразглашении конфиденциальной информации;
- контроль за действиями третьих лиц;
- в договорах с третьими лицами предусматривать право ГБУЗ «ГКБ №1 им.С.З.Фишера» на проведение аудита обеспечения безопасности той информации, которая передается третьим лицам.

6.6 Антивирусная защита

6.6.1 В целях предупреждения, обнаружения и устранения вредоносных программ в ГБУЗ «ГКБ №1 им.С.З.Фишера» на постоянной основе должны использоваться средства антивирусной защиты.

6.6.2 Обязательному антивирусному контролю должна подлежать любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация, хранимая на подключаемых съемных носителях, при

6.9.5 Процедура смены парольной информации в информационных системах ГБУЗ «ГКБ №1 им.С.З.Фишера» должна проводиться на регулярной основе.

6.10 Регистрация событий

Осуществление регистрации событий безопасности на всех компонентах информационных систем ГБУЗ «ГКБ №1 им.С.З.Фишера», в которых обрабатывается, хранится или по средствам которых передается защищаемая информация.

6.11 Использование СКЗИ

6.11.1 Решение об использовании СКЗИ в интересах защиты собственных информационных ресурсов принимается руководством ГБУЗ «ГКБ №1 им.С.З.Фишера» в соответствии с законодательством Российской Федерации.

6.11.2 При эксплуатации СКЗИ и ключевой информации все сотрудники ГБУЗ «ГКБ №1 им.С.З.Фишера» должны выполнять требования нормативных правовых актов, издаваемых федеральным органом исполнительной власти в области обеспечения безопасности, документов ГБУЗ «ГКБ №1 им.С.З.Фишера» по обеспечению безопасности использования СКЗИ, а также эксплуатационной документации производителя СКЗИ.

6.12 Безопасность информационной сети

6.12.1 Установление надлежащего контроля в отношении локальной вычислительной сети и всех внешних информационных коммуникаций ГБУЗ «ГКБ №1 им.С.З.Фишера» для обеспечения защиты данных и защиты информационных систем ГБУЗ «ГКБ №1 им.С.З.Фишера» от НСД.

6.12.2 Должны быть определены цели использования сети Интернет и требования к процедуре использования ресурсов сети Интернет. Использование сети Интернет работников в личных целях должно быть строго запрещено.

6.12.3 Доступ к информационным сервисам сети Интернет предоставляется работникам ГБУЗ «ГКБ №1 им.С.З.Фишера» только в случае производственной необходимости.

6.12.4 Подключение к сети Интернет должно осуществляться только при организации защиты соединения путем установки МЭ и специальных программных средств защиты.

6.12.5 Разрешительные политики доступа в Интернет должны технически реализовываться специализированным программным обеспечением.

6.12.6 Контроль использования работниками ресурсов сети Интернет должен осуществляться уполномоченными работниками на постоянной основе.

6.13 Использование корпоративной электронной почты

6.13.1 Система корпоративной электронной почты должна использоваться в ГБУЗ «ГКБ №1 им.С.З.Фишера» с целью организации обмена электронными сообщениями между работниками, а также между работниками ГБУЗ «ГКБ №1 им.С.З.Фишера» и внешними абонентами.

6.13.2 В ГБУЗ «ГКБ №1 им.С.З.Фишера» должны быть четко определены требования к использованию системы корпоративной электронной почты.

6.13.3 В ГБУЗ «ГКБ №1 им.С.З.Фишера» должно быть установлено специальное программное обеспечение, осуществляющее контроль всех входящих сообщений на наличие вредоносного программного обеспечения.

быть создана система учета произошедших инцидентов, которая представляет собой комплекс средств и мероприятий для сбора и консолидации информации об инцидентах.

7.2.3 В отношении каждого произошедшего инцидента должен выполняться его анализ и разработка эффективных мер реагирования на данный инцидент.

7.3 Мониторинг текущего уровня информационной безопасности

7.3.1 Для обеспечения высокого уровня контроля в отношении системы обеспечения информационной безопасности в ГБУЗ «ГКБ №1 им.С.З.Фишера» на постоянной основе должен проводиться комплексный анализ существующих защитных механизмов и возникающих инцидентов информационной безопасности, а также периодический аудит всей системы обеспечения информационной безопасности.

7.3.2 Процесс мониторинга системы обеспечения информационной безопасности должен включать в себя контроль организационных и технических защитных мер, анализ параметров конфигурации и настройки защитных механизмов.

7.3.3 При проведении контрольных мероприятий, связанных с оценкой функционирования защитных мер в ГБУЗ «ГКБ № 1 им. С.З. Фишера», уполномоченные работники должны придерживаться следующих принципов:

- не нарушать функционирование текущей деятельности ГБУЗ «ГКБ № 1 им. С.З. Фишера»;
- действовать в соответствии с внутренними документами ГБУЗ «ГКБ № 1 им. С.З. Фишера» по информационной безопасности;
- не скрывать факты выявленных инцидентов и нарушений требований информационной безопасности;
- оформлять отчеты, подтверждающие выполнение мероприятий по обеспечению информационной безопасности.

7.3.4 Информация, полученная в ходе проведения контролирующих мероприятий о действиях, событиях и параметрах, имеющих отношение к функционированию защитных мер, должна консолидироваться и храниться в местах, исключающих получение к ней несанкционированного доступа.

7.3.5 Мониторинг данных о зарегистрированных событиях информационной безопасности должен проводиться, по возможности, с использованием встроенных механизмов настройки и аудита событий в программных и программно-технических средствах, используемых в информационных системах ГБУЗ «ГКБ № 1 им. С.З. Фишера».

7.4 Аудит системы обеспечения информационной безопасности

7.4.1 В целях оценки текущего уровня информационной безопасности уполномоченные работники учреждения на регулярной основе должны проводить аудит информационной безопасности.

7.4.2 Внутренние аудиты или самооценки должны выполняться, по возможности, работниками учреждения.

7.4.3 Результатом выполнения аудитов по информационной безопасности должны стать отчеты о выполненном аудите информационной безопасности, которые разрабатываются специалистами ГБУЗ «ГКБ № 1 им. С.З. Фишера».