Приложение

к приказу СПб ГБУЗ

«Детская городская поликлиника №11»

от \_\_\_\_\_\_\_\_\_\_\_\_ № \_\_\_\_\_

Политика информационной безопасности  
СПб ГБУЗ «Детская городская поликлиника №11»

2023

Санкт-Петербург

Содержание

[Определения](#bookmark2) 4

[Обозначения и сокращения](#bookmark3) 4

1. [Общие положения](#bookmark5) 5
2. [Цели и задачи обеспечения информационной безопасности](#bookmark8) 5
3. [Принципы обеспечения информационной безопасности](#bookmark10) 8
4. [Зоны ответственности участников процесса обеспечения информационной безопасности](#bookmark25) 10
5. [Основные требования по защите информации ограниченного доступа](#bookmark31) 12
6. [Основные требования к процессам обеспечения информационной безопасности](#bookmark35) 15
7. [Основные требования к процессам управления информационной   
   безопасностью](#bookmark51) 19
8. [Заключение](#bookmark58) 22

Определения

Защита информации - деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию;

Информация - сведения (сообщения, данные) независимо от формы их представления;

Информация ограниченного доступа - информация, доступ к которой ограничен федеральными законами;

Информационная система - совокупность содержащейся в базах данныхинформации и обеспечивающих ее обработку информационных технологий и технических средств;

Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

Обладатель информации - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким- либо признакам;

Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных).

Обозначения и сокращения

СПБ ГБУЗ «Детская городская поликлиника №11» - Санкт-Петербургское государственное бюджетное учреждение Здравоохранения «Детская городская поликлиника № 11»;

КИ - Конфиденциальная информация;

МЭ - Межсетевой экран;

НСД - Несанкционированный доступ;

СЗИ - Система защиты информации;

СКЗИ - Средство криптографической защиты информации;

СрЗИ - Средство защиты информации;

ФСБ России - Федеральная служба безопасности Российской Федерации;

ФСТЭК России - Федеральная служба по техническому и экспортному контролю.

1. **Общие положения**
   1. Настоящая Политика является документом, доступным всем сотрудникам СПБ ГБУЗ «Детская городская поликлиника №11» и всем пользователям его ресурсов. Представляет собой официально принятую руководством СПБ ГБУЗ «Детская городская поликлиника №11» систему взглядов на обеспечение информационной безопасности   
      в СПБ ГБУЗ «Детская городская поликлиника №11».
   2. Основной задачей в области информационной безопасности СПБ ГБУЗ «Детская городская поликлиника №11» признает совершенствование мер и средств обеспечения информационной безопасности информационных ресурсов СПБ ГБУЗ «Детская городская поликлиника №11» в контексте первичной медико-социальной помощи.
   3. В рамках своей деятельности СПБ ГБУЗ «Детская городская поликлиника №11» 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 СПБ ГБУЗ «Детская городская поликлиника №11».
   4. Требования информационной безопасности, которые предъявляются СПБ ГБУЗ «Детская городская поликлиника №11», соответствуют целям деятельности СПБ ГБУЗ «Детская городская поликлиника №11» и предназначены для снижения рисков, связанных с информационной безопасностью, до приемлемого уровня.
   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 СПБ ГБУЗ «Детская городская поликлиника №11» по информационной безопасности.
2. **Цели и задачи обеспечения информационной безопасности**
   1. Целями обеспечения информационной безопасности СПБ ГБУЗ «Детская городская поликлиника №11» являются:

* защита интересов СПБ ГБУЗ «Детская городская поликлиника №11», работников и иных субъектов информационных отношений, взаимодействующих с СПБ ГБУЗ «Детская городская поликлиника №11», от возможного нанесения ущерба   
  их деятельности посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования информационных систем СПБ ГБУЗ «Детская городская поликлиника №11», 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 СПБ ГБУЗ «Детская городская поликлиника №11» и предоставляемых сервисов;
* соблюдение правового режима использования массивов и программ обработки информации;
* предотвращение реализации угроз безопасности для деятельности СПБ ГБУЗ «Детская городская поликлиника №11».
  1. Объектами информационных правоотношений являются:
* информационные ресурсы, в том числе с ограниченным доступом;
* процессы обработки информации в информационных системах СПБ ГБУЗ «Детская городская поликлиника №11», информационные технологии, регламенты и процедуры сбора, обработки, хранения   
  и передачи информации;
* информационная инфраструктура, включающая системы обработки, хранения и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена   
  и телекоммуникации;
* системы и средства защиты информации, объекты и помещения, в которых размещены хранилища информации.
  1. Субъектами информационных отношений при использовании информационных систем СПБ ГБУЗ «Детская городская поликлиника №11», заинтересованными в обеспечении информационной безопасности, являются:
* СПБ ГБУЗ «Детская городская поликлиника №11», как собственник информационных ресурсов и оператор персональных данных;
* работники подразделений СПБ ГБУЗ «Детская городская поликлиника №11», как пользователи и поставщики информации в информационные системы;
* физические лица, сведения о которых накапливаются, хранятся и обрабатываются в информационных системах СПБ ГБУЗ «Детская городская поликлиника №11».
  1. Субъекты информационных отношений заинтересованы в обеспечении:
* конфиденциальности определенной части информации;
* целостности информации;
* своевременного доступа к необходимой им информации;
* защиты от навязывания им ложной (недостоверной, искаженной) информации;
* разграничения ответственности за нарушения законных прав (интересов) других субъектов информационных отношений и установленных правил обращения   
  с информацией;
* возможности осуществления непрерывного контроля и управления процессами обработки и передачи информации;
* защиты соответствующей части информации от незаконного   
  ее тиражирования и распространения.
  1. Для достижения целей защиты и обеспечения указанных свойств информации, система обеспечения информационной безопасности СПБ ГБУЗ «Детская городская поликлиника №11» должна обеспечивать решение следующих задач:
     1. Защиту от вмешательства в процесс функционирования информационных систем посторонних лиц (возможность использования системы и доступ к ее ресурсам должны иметь только зарегистрированные пользователи).
     2. Разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам информационных систем (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей).
     3. Регистрацию и периодический контроль действий пользователей   
        при использовании защищаемых ресурсов и периодический контроль корректности   
        их действий.
     4. Контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения.
     5. Защиту от несанкционированной модификации и контроль целостности используемых в СПБ ГБУЗ «Детская городская поликлиника №11» программных средств и данных, а также защиту   
        от несанкционированного внедрения вредоносных программ.
     6. Защиту информации ограниченного доступа, хранимой, обрабатываемой   
        в СПБ ГБУЗ «Детская городская поликлиника №11», от несанкционированного разглашения или искажения.
     7. Обеспечение аутентификации пользователей, участвующих   
        в информационном обмене (подтверждение подлинности отправителя и получателя информации), а также определение автора при создании и модификации информации.
     8. Обеспечение исправности применяемых в информационных системах СПБ ГБУЗ «Детская городская поликлиника №11» средств защиты информации.
     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.
     10. Создание условий для минимизации наносимого ущерба неправомерными действиями, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации в СПБ ГБУЗ «Детская городская поликлиника №11».
  2. Решение вышеперечисленных задач в СПБ ГБУЗ «Детская городская поликлиника №11» осуществляется:
     1. Учетом всех подлежащих защите информационных ресурсов (каналов связи, аппаратных и программных средств).
     2. Регламентацией процессов обработки подлежащей защите информации, действий работников СПБ ГБУЗ «Детская городская поликлиника №11» и персонала, осуществляющего обслуживание и модификацию программных и технических средств, на основе утвержденных организационно-распорядительных документов по вопросам обеспечения информационной безопасности.
     3. Назначением и подготовкой работников, ответственных за организацию   
        и осуществление мероприятий по обеспечению информационной безопасности в СПБ ГБУЗ «Детская городская поликлиника №11».
     4. Наделением каждого работника минимально необходимыми   
        для выполнения им своих функциональных обязанностей полномочиями   
        по доступу к информационным ресурсам.
     5. Знанием и строгим соблюдением всеми работниками, использующими   
        и обслуживающими аппаратные и программные средства, требований организационно-распорядительных документов по вопросам обеспечения информационной безопасности.
     6. Персональной ответственностью за свои действия каждого работника, участвующего в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющего доступ к ресурсам информационных систем.
     7. Реализацией технологических процессов обработки информации   
        с использованием комплексов организационно-технических мер защиты программного обеспечения, технических средств и данных.
     8. Принятием мер по обеспечению физической целостности технических средств информационных систем и поддержанием необходимого уровня защищенности их компонентов.
     9. Использованием физических и технических (программно-аппаратных) средств защиты ресурсов СПБ ГБУЗ «Детская городская поликлиника №11» и административной поддержкой их использования.
     10. Контролем соблюдения пользователями информационных систем требований по обеспечению информационной безопасности.
     11. Юридической защитой интересов СПБ ГБУЗ «Детская городская поликлиника №11» при взаимодействии с юридическими и физическими лицами от противоправных и несанкционированных действий со стороны этих лиц.
     12. Проведением анализа эффективности принятых мер и применяемых средств защиты информации в СПБ ГБУЗ «Детская городская поликлиника №11». Разработкой и реализацией предложений   
         по совершенствованию СЗИ в СПБ ГБУЗ «Детская городская поликлиника №11».

1. **Принципы обеспечения информационной безопасности**
   1. **Принцип законности**
      1. При выборе защитных мероприятий, реализуемых системой обеспечения информационной безопасности, должно соблюдаться действующее законодательство.
      2. Принятые меры защиты не должны препятствовать доступу к защищаемой информации со стороны государственных или правоохранительных органов, если такой доступ необходим в случаях, предусмотренных законодательством.
      3. Программно-технические средства, применяемые в СПБ ГБУЗ «Детская городская поликлиника №11», должны иметь соответствующие лицензии, официально приобретаться СПБ ГБУЗ «Детская городская поликлиника №11» у представителей разработчиков этих средств.
   2. **Принцип системности**

При построении системы обеспечения информационной безопасности необходимо применять системный подход, который предполагает взаимосвязь процессов организации защиты информационных ресурсов СПБ ГБУЗ «Детская городская поликлиника №11», согласованное применение методов и средств защиты информационных ресурсов СПБ ГБУЗ «Детская городская поликлиника №11».

* 1. **Принцип координации**
     1. При организации действий по обеспечению информационной безопасности руководство СПБ ГБУЗ «Детская городская поликлиника №11» обеспечивает четкую взаимосвязь соответствующих структурных подразделений между собой, с представителями сторонних организаций, оказывающих услуги в рамках договорных обязательств.
     2. При построении, внедрении и эксплуатации системы обеспечения информационной безопасности руководство СПБ ГБУЗ «Детская городская поликлиника №11» обеспечивает условия для эффективной координации действий всех лиц, обеспечивающих информационную безопасность.
  2. **Принцип дружественности и простоты**
     1. Система обеспечения информационной безопасности в СПБ ГБУЗ «Детская городская поликлиника №11» формируется таким образом, чтобы сделать максимально прозрачными для пользователей информационных систем СПБ ГБУЗ «Детская городская поликлиника №11» процессы ее функционирования.
     2. Система обеспечения информационной безопасности в СПБ ГБУЗ «Детская городская поликлиника №11» выстраивается таким образом, чтобы ограничения организационного и технического характера, налагаемые на сотрудников СПБ ГБУЗ «Детская городская поликлиника №11» в связи с реализацией защитных мер, существенно   
        не затрудняли работу с ресурсами информационных систем СПБ ГБУЗ «Детская городская поликлиника №11».
  3. **Принцип превентивности**

Меры, применяемые СПБ ГБУЗ «Детская городская поликлиника №11» с целью обеспечения информационной безопасности, должны носить упреждающий характер и не допускать реализацию соответствующих угроз и атак.

* 1. **Принцип оптимальности и многоуровневости**
     1. Выбор единых программно-технических средств с целью сокращения расходов на создание и поддержку функционирования компонентов системы обеспечения информационной безопасности.
     2. Применение разнородных программно-технических средств защиты,   
        с целью построения целостной системы обеспечения информационной безопасности   
        и устранения возможных уязвимостей.
     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.
  2. **Принцип экономической целесообразности**
     1. Осуществление оценки уровня затрат на обеспечение безопасности, ценности информационных ресурсов и величины возможного ущерба для СПБ ГБУЗ «Детская городская поликлиника №11» в случае нарушения конфиденциальности, целостности и доступности информационных ресурсов.
     2. Выбор необходимого и достаточного уровня защиты информационных ресурсов, при котором затраты, риск и размер возможного ущерба являются приемлемыми.
  3. **Принцип непрерывности и недопустимости открытого состояния**
     1. Система обеспечения информационной безопасности в СПБ ГБУЗ «Детская городская поликлиника №11» строится таким образом, чтобы процесс защиты информационных систем СПБ ГБУЗ «Детская городская поликлиника №11» осуществлялся непрерывно и целенаправленно на протяжении всего жизненного цикла информационных систем.
     2. Система обеспечения информационной безопасности в СПБ ГБУЗ «Детская городская поликлиника №11» при любых возникающих обстоятельствах либо полностью выполняет свои функции, либо полностью блокирует доступ.
  4. **Принцип профессионализма**
     1. Привлечение для разработки и внедрения системы обеспечения информационной безопасности, при необходимости, специализированных организаций, наиболее подготовленных к конкретному виду деятельности и имеющих соответствующие лицензии на выполнения работ и практический опыт в данной области.
     2. Организация профессиональной подготовки своих работников   
        для эксплуатации компонентов системы обеспечения информационной безопасности.
  5. **Принцип выбора решений защиты**
     1. Ориентация на применение современных высокотехнологичных решений   
        и программно-технических средств защиты, хорошо зарекомендовавших себя, интуитивно понятных и не сложных в эксплуатации.
     2. Использование оценки степени корректности функционирования   
        и исполнения защитных функций, отказоустойчивости, проверки согласованности конфигурации различных компонентов и возможности осуществления централизованного администрирования при выборе решений по защите информационных систем.
  6. **Принцип развития**
     1. Развитие и обновление на регулярной основе существующей системы обеспечения информационной безопасности.
     2. Ориентация на преемственность принятых ранее решений по защите,   
        на анализ функционирования информационных систем и самой системы обеспечения информационной безопасности.
  7. **Принцип персональной ответственности и разделения обязанностей**
     1. Руководство СПБ ГБУЗ «Детская городская поликлиника №11» определяет права и ответственность каждого конкретного работника (в пределах его должностных обязанностей) за обеспечение безопасности информационных ресурсов СПБ ГБУЗ «Детская городская поликлиника №11».
     2. Система обеспечения информационной безопасности СПБ ГБУЗ «Детская городская поликлиника №11» обеспечивает разделение полномочий в информационных системах, обязанностей и ответственности между работниками, исключающее возможность нарушения критически важных для СПБ ГБУЗ «Детская городская поликлиника №11» процессов или создания уязвимостей в защите информационных ресурсов.
  8. **Принцип минимизации привилегий пользователей**

Обеспечение пользователей привилегиями минимально достаточными   
для выполнения ими своих функций в СПБ ГБУЗ «Детская городская поликлиника №11», в соответствии со своими должностными обязанностями.

1. **Зоны ответственности участников процесса обеспечения информационной безопасности**

**4.1 Руководство СПБ ГБУЗ «Детская городская поликлиника №11»**

1. Создает условия, при которых каждый работник СПБ ГБУЗ «Детская городская поликлиника №11» знает свои обязанности и задачи в отношении информационных ресурсов и обеспечивает наличие необходимого разделения функций и полномочий в целях недопущения конфликта интересов.
2. Назначает работников, ответственных за создание и использование СЗИ, информации обрабатываемой в СПБ ГБУЗ «Детская городская поликлиника №11», реализацию процессов обеспечения информационной безопасности, а также их контроля.
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 СПБ ГБУЗ «Детская городская поликлиника №11».
4. Инициирует, осуществляет поддержку и контролирует выполнение всех процессов обеспечения информационной безопасности в СПБ ГБУЗ «Детская городская поликлиника №11».
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.
6. **Компетентные подразделения СПБ ГБУЗ «Детская городская поликлиника №11»**
7. Подготавливают предложения по доработке Политики информационной безопасности в части технического обеспечения информационных систем СПБ ГБУЗ «Детская городская поликлиника №11».
8. Разрабатывают процедуры эффективного управления техническими   
   и программными средствами информационных систем и применяют их в практической деятельности в отношении всех систем, действующих в СПБ ГБУЗ «Детская городская поликлиника №11».
9. Организуют проведение необходимого инструктажа работников структурных подразделений в части вопросов безопасной эксплуатации информационных систем.
10. Обеспечивают защиту доступа ко всему серверному и коммутационному оборудованию, носителям информации, которые используются в соответствующих структурных подразделениях.
11. Осуществляют мероприятия по поддержке сопровождения и использования информационных систем.
12. Обеспечивают отказоустойчивость всего программно-аппаратного комплекса и процедуру регламентированного восстановления работоспособности после отказов компонентов.
13. Регулярно обновляют программные и программно-аппаратные комплексы СЗИ в СПБ ГБУЗ «Детская городская поликлиника №11».
14. Осуществляют поддержку функционирования информационных систем   
    и принимают необходимые меры по конфигурированию систем для обеспечения необходимого уровня информационной безопасности СПБ ГБУЗ «Детская городская поликлиника №11».
15. Контролируют работоспособность устройств бесперебойного питания критичных для СПБ ГБУЗ «Детская городская поликлиника №11» информационных систем.
16. Обеспечивают физическую защиту помещений, в которых располагаются критичные для СПБ ГБУЗ «Детская городская поликлиника №11» информационные системы.
17. Обеспечивают сопровождение устройств контроля доступа в помещения СПБ ГБУЗ «Детская городская поликлиника №11».
18. Обеспечивают защиту информационных ресурсов СПБ ГБУЗ «Детская городская поликлиника №11» от случайного   
    или намеренного уничтожения, искажения, разглашения.
19. Контролируют выполнение установленных правил и процедур обеспечения информационной безопасности в СПБ ГБУЗ «Детская городская поликлиника №11».
20. **Руководители структурных подразделений СПБ ГБУЗ «Детская городская поликлиника №11»**
21. Обязаны соблюдать требования действующего законодательства Российской Федерации и внутренних документов СПБ ГБУЗ «Детская городская поликлиника №11» в части обеспечения информационной безопасности.
22. Обеспечивают контроль за соблюдением норм и правил обеспечения информационной безопасности в своем структурном подразделении и информируют компетентное подразделение о любых подозрительных событиях или нарушениях действующих правил обеспечения информационной безопасности.
23. Обеспечивают соответствие действий работников подразделения Политике информационной безопасности, внутренним документам по информационной безопасности и любым другим распоряжениям руководства СПБ ГБУЗ «Детская городская поликлиника №11» по вопросам информационной безопасности.
24. Организуют проведение необходимого инструктажа по вопросам выполнения правил информационной безопасности для всех работников своего структурного подразделения.
25. Контролируют выполнение работниками в своем структурном подразделении установленных правил в целях обеспечения физической безопасности компьютерного оборудования и носителей информации.
26. Своевременно информируют руководство о всех выявленных сбоях в работе информационных систем.
27. Контролируют доступ к необходимым информационными ресурсам работников своего структурного подразделения в соответствии с потребностью   
    в пределах служебных обязанностей.
28. **Работники СПБ ГБУЗ «Детская городская поликлиника №11»**
29. Соблюдают и выполняют требования Политики информационной безопасности, соответствующих локальных актов, документов СПБ ГБУЗ «Детская городская поликлиника №11» по вопросам информационной безопасности.
30. Соблюдают конфиденциальность данных, доступ к которым был ими получен.
31. Обеспечивают физическую безопасность всего технического оборудования и носителей информации, используемых в работе.
32. Не допускают самовольного подключения и использования   
    в автоматизированной информационной системе личного компьютерного и цифрового оборудования, а также носителей информации.
33. Не допускают самовольную установку программного обеспечения   
    на компьютеры, входящие в состав информационной системы.
34. Своевременно информируют руководителя своего структурного подразделения о всех случаях нарушения информационной безопасности и о всех выявленных сбоях в работе программных и программно-аппаратных средств.
35. Проявляют осмотрительность в отношении любых действий, которые могут повлечь за собой снижение уровня информационной безопасности.
36. **Сторонние физические и юридические лица**

Соблюдают и выполняют требования Политики информационной безопасности, соответствующих локальных актов и документов СПБ ГБУЗ «Детская городская поликлиника №11» и других распоряжений руководства по вопросам информационной безопасности при исполнении договорных обязательств

1. **Основные требования по защите информации ограниченного доступа**
   1. **Общие требования**
      1. В СПБ ГБУЗ «Детская городская поликлиника №11» 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.
      2. В СПБ ГБУЗ «Детская городская поликлиника №11» осуществляется обработка и хранение информации ограниченного доступа (доступ к которой ограничен федеральными законами и служебной необходимостью).
      3. В СПБ ГБУЗ «Детская городская поликлиника №11» должен быть разработан перечень информации ограниченного доступа.
      4. СПБ ГБУЗ «Детская городская поликлиника №11», как обладатель информации ограниченного доступа, при осуществлении своих прав обязана:

* соблюдать права и законные интересы иных лиц;
* принимать меры по защите информации;
* ограничивать доступ к информации, если такая обязанность установлена федеральными законами.
  + 1. СПБ ГБУЗ «Детская городская поликлиника №11», 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;
* передавать информацию другим лицам на установленном законом основании;
* защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;
* осуществлять иные действия с информацией или разрешать осуществление таких действий, если эти действия не противоречат федеральным законам и другим нормативно-правовым актам регуляторов.
  + 1. СПБ ГБУЗ «Детская городская поликлиника №11», являясь обладателем информации ограниченного доступа, в случаях, установленных законодательством РФ, обязана обеспечить:
* предотвращение НСД к информации и (или) передачи ее лицам,   
  не имеющим права на доступ к информации;
* своевременное обнаружение фактов НСД к информации;
* недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
* возможность регламентированного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
* постоянный контроль за обеспечением уровня защищенности информации.
  + 1. Защита информации ограниченного доступа представляет собой принятие правовых, организационных и технических мер, направленных на:
* соблюдение конфиденциальности информации (исключение неправомерного доступа, копирования, предоставления или распространения информации);
* обеспечение целостности информации (исключение неправомерного уничтожения или модифицирования информации);
* реализацию права на доступ к информации (исключение неправомерного блокирования информации).
  1. **Организация защиты конфиденциальной информации**
     1. При организации в СПБ ГБУЗ «Детская городская поликлиника №11» защиты информации ограниченного доступа, необходимо руководствоваться требованиями Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», которые регулируют отношения, связанные с установлением, изменением и прекращением режима обработки защищаемой информации.
     2. В СПБ ГБУЗ «Детская городская поликлиника №11» необходимо соблюдать режим защиты конфиденциальной информации (далее – КИ):
* ограничение доступа к КИ, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;
* учет лиц, получивших доступ к КИ, и (или) лиц, которым такая информация была предоставлена или передана;
* регулирование отношений по использованию КИ, с работниками   
  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.
  + 1. Для обеспечения защиты КИ СПБ ГБУЗ «Детская городская поликлиника №11» вправе применять средства и методы технической защиты, предпринимать другие, не противоречащие законодательству РФ, меры.
    2. 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 СПБ ГБУЗ «Детская городская поликлиника №11» режимом защиты КИ, а также мерами ответственности за его нарушение;
* создать работникам необходимые условия для соблюдения установленного режима защиты КИ.
  + 1. Работники СПБ ГБУЗ «Детская городская поликлиника №11», обязаны выполнять установленный в СПБ ГБУЗ «Детская городская поликлиника №11» режим защиты КИ, не разглашать информацию, составляющую КИ, и не использовать эту информацию   
       в личных целях.
  1. **Особенности защиты персональных данных**
     1. При организации в СПБ ГБУЗ «Детская городская поликлиника №11» 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.
     2. СПБ ГБУЗ «Детская городская поликлиника №11» 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.
     3. Перечень мер, выполнение которых обеспечивает СПБ ГБУЗ «Детская городская поликлиника №11» в качестве оператора персональных данных, должен включать:
* назначение в СПБ ГБУЗ «Детская городская поликлиника №11» ответственного за организацию обработки персональных данных;
* издание СПБ ГБУЗ «Детская городская поликлиника №11» 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 персональных данных», соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных»;
* ознакомление работников СПБ ГБУЗ «Детская городская поликлиника №11», непосредственно осуществляющих обработку персональных данных, с положениями законодательства РФ о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику СПБ ГБУЗ «Детская городская поликлиника №11» в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных и обучение,   
  при необходимости, указанных работников.
  + 1. СПБ ГБУЗ «Детская городская поликлиника №11» при обработке персональных данных обязана принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.
    2. Обеспечение безопасности персональных данных достигается, в частности:
* определением угроз и нарушителей безопасности персональных данных   
  при их обработке в информационных системах персональных данных (далее – ИСПДн);
* проведением классификации ИСПДн в соответствии с требованиями Постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований   
  к защите персональных данных при их обработке в информационных системах персональных данных», и определением класса защищенности для ИСПДн;
* применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн, необходимых   
  для выполнения требований к защите персональных данных, исполнение которых обеспечивает выбранные уровни защищенности персональных данных;
* применением прошедших в установленном порядке процедур оценки соответствия средств защиты информации;
* оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию ИСПДн;
* учетом машинных носителей персональных данных;
* обнаружением фактов НСД к персональным данным и принятием мер;
* восстановлением персональных данных, модифицированных   
  или уничтоженных вследствие НСД к ним;
* установлением правил доступа к персональным данным, обрабатываемым   
  в ИСПДн, а также обеспечением регистрации и учета всех действий, совершаемых   
  с персональными данными в ИСПДн;
* контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности ИСПДн.
  + 1. Работники СПБ ГБУЗ «Детская городская поликлиника №11» должны быть ознакомлены под роспись с документами СПБ ГБУЗ «Детская городская поликлиника №11», устанавливающими порядок обработки персональных данных, а также об их правах, обязанностях и ответственности.

1. **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 СПБ ГБУЗ «Детская городская поликлиника №11».

1. **Физическая безопасность и безопасность на рабочем месте**
2. Система защиты зданий и помещений СПБ ГБУЗ «Детская городская поликлиника №11», объектов и технических средств информационных систем СПБ ГБУЗ «Детская городская поликлиника №11» обеспечивает выполнение следующих функций:

* разграничение доступа работников в помещения СПБ ГБУЗ «Детская городская поликлиника №11» 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 СПБ ГБУЗ «Детская городская поликлиника №11»;
* 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.

1. Определяется перечень технических средств, находящихся в специальных контролируемых зонах.
2. 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 СПБ ГБУЗ «Детская городская поликлиника №11» системы и коммуникационное оборудование, обеспечивающее внешние коммуникации СПБ ГБУЗ «Детская городская поликлиника №11».

1. Контролируемые зоны защищаются соответствующими системами контроля и управления доступом, обеспечивая доступ только авторизованному персоналу.
2. Доступ в контролируемые зоны сторонних лиц или представителей других организаций возможен только в сопровождении уполномоченного работника СПБ ГБУЗ «Детская городская поликлиника №11».
3. Размещение и эксплуатация рабочих станций, серверов и сетевого оборудования СПБ ГБУЗ «Детская городская поликлиника №11» осуществляется в помещениях, оборудованных замками, средствами сигнализации и (при необходимости) постоянно находящихся под охраной или наблюдением.
4. Размещение технических средств вывода и отображения информации   
   в помещениях СПБ ГБУЗ «Детская городская поликлиника №11» производится с учетом исключения возможности визуального просмотра информации посторонними лицами и персоналом, не допущенным к работе с данной информацией.
5. Работники СПБ ГБУЗ «Детская городская поликлиника №11» на момент своего отсутствия на рабочем месте обязаны исключить возможность наличия на рабочем столе документов или носителей   
   с защищаемой информацией.
6. Технические средства и оборудование должны размещаться и храниться таким образом, чтобы сократить возможный риск его повреждения и угрозы несанкционированного доступа.
7. Помещения СПБ ГБУЗ «Детская городская поликлиника №11» должны быть оборудованы детекторами огня и дыма, огнетушителями, системами кондиционирования воздуха, средствами охранно-пожарной сигнализации.
8. Основное техническое оборудование СПБ ГБУЗ «Детская городская поликлиника №11» должно быть защищено от перебоев в подаче электроэнергии путем подключения к электросети с применением источников бесперебойного питания. Источники бесперебойного питания необходимо регулярно тестировать и проверять уполномоченным работникам СПБ ГБУЗ «Детская городская поликлиника №11» в соответствии с рекомендациями производителя.
9. Пользователи портативных технических средств не должны оставлять техническое оборудование и носители информации без присмотра.
10. Портативные технические средства не должны оставаться за пределами контролируемой зоны СПБ ГБУЗ «Детская городская поликлиника №11» дольше, чем того требует служебная необходимость, если иное не определено руководством СПБ ГБУЗ «Детская городская поликлиника №11».
11. **Безопасность при работе с носителями информации**
12. В СПБ ГБУЗ «Детская городская поликлиника №11» должны соблюдаться меры по безопасной работе с электронными носителями информации с целью контроля их использования, для предотвращения несанкционированного копирования и разглашения защищаемой информации, внесения изменений или уничтожения указанной информации, а также внесения изменений в работу информационных систем.
13. Работники СПБ ГБУЗ «Детская городская поликлиника №11» должны использовать электронные носители информации только для выполнения своих служебных обязанностей. Использование электронных носителей информации в СПБ ГБУЗ «Детская городская поликлиника №11» в иных целях строго запрещено.
14. Электронные носители информации в СПБ ГБУЗ «Детская городская поликлиника №11» должны быть учтены путем присвоения каждому носителю инвентаризационного номера и назначения владельца.
15. Электронные носители информации должны храниться в помещениях, исключающих получение к ним НСД, при этом должен быть обеспечен контроль доступа к носителям.
16. Для контроля процессов использования и хранения электронных носителей информации должен быть разработан порядок плановой инвентаризации носителей.
17. 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.
18. При снятии электронного носителя информации с эксплуатации, все данные, хранящиеся на нем, должны быть гарантированно стерты.
19. При утилизации электронных носителей информации должна быть обеспечена невозможность восстановления записанной на них информации.
20. Факт уничтожения информации и утилизации носителя информации фиксируется в соответствии с порядком, установленным в СПБ ГБУЗ «Детская городская поликлиника №11».
21. **Техническое обслуживание оборудования**
22. Технические средства всех систем СПБ ГБУЗ «Детская городская поликлиника №11» должны проходить на регулярной основе сервисное обслуживание в соответствии с рекомендациями производителей оборудования.
23. Ремонт и сервисное обслуживание оборудования должны выполняться только квалифицированным персоналом.
24. Техническое обслуживание оборудования и систем сторонними организациями не должно приводить к риску нарушения конфиденциальности защищаемой информации.
25. **Взаимодействие с третьими лицами**

В целях обеспечения информационной безопасности СПБ ГБУЗ «Детская городская поликлиника №11» 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 СПБ ГБУЗ «Детская городская поликлиника №11» 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 СПБ ГБУЗ «Детская городская поликлиника №11» 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 непосредственном обращении к ней.

6.6.3 При установке программного обеспечения на серверы информационных систем СПБ ГБУЗ «Детская городская поликлиника №11» или их обновлении должна автоматически выполняться предварительная проверка данного программного обеспечения на отсутствие вредоносного программного обеспечения.

6.6.4 Сигнатурные базы вредоносного программного обеспечения и антивирусные средства защиты должны регулярно обновляться.

6.6.5 Пользователи информационных систем СПБ ГБУЗ «Детская городская поликлиника №11» не должны иметь возможность получения доступа к конфигурации антивирусного средства защиты или его отключения.

6.6.6 В СПБ ГБУЗ «Детская городская поликлиника №11» необходимо определить процедуру для обработки и восстановления инфицированных данных и отслеживание источника заражения.

**6.7 Контроль доступа к информационным системам**

6.7.1 Все работники СПБ ГБУЗ «Детская городская поликлиника №11», допущенные к работе с информационными системами, несут персональную ответственность за нарушения установленного порядка обработки информации, правил хранения, использования и передачи, находящихся в их распоряжении защищаемых ресурсов системы.

6.7.2 Уровень полномочий пользователя в информационной системе СПБ ГБУЗ «Детская городская поликлиника №11» должен определяться в соответствии с его должностными обязанностями и производственной необходимостью.

6.7.3 Доступ пользователей к информационным системам СПБ ГБУЗ «Детская городская поликлиника №11» должен контролироваться администратором системы.

6.7.4 Осуществление регулярного контроля выполнения политик и иных документов, касающихся регламентации допуска работников СПБ ГБУЗ «Детская городская поликлиника №11» к информационным системам.

**6.8 Идентификация и аутентификация**

6.8.1 Доступ пользователей к информационным системам должен предоставляться только после успешного завершения процедур идентификации, аутентификации   
и авторизации.

6.8.2 Получение пользователем имени в системе и парольной информации, которые обеспечивают доступ пользователя к ресурсам системы, должно осуществляться   
по представлению руководителей структурных подразделений.

**6.9 Безопасность пароля**

6.9.1 С целью обеспечения защиты от несанкционированного доступа   
к информационным системам устанавливаются требования к выбору парольной информации, обеспечивающие достаточную степень стойкости паролей.

6.9.2 Для обеспечения конфиденциальности парольной информации пользователю запрещается хранить значения своих паролей на бумажном носителе в открытом виде   
и в свободном доступе.

6.9.3 Для обеспечения конфиденциальности парольной информации пользователям запрещается передавать значения своих паролей третьим лицам.

6.9.4 При вводе пароля пользователем для доступа к информационной системе СПБ ГБУЗ «Детская городская поликлиника №11» должно исключаться отображение парольной информации на экране монитора в открытом виде.

6.9.5 Процедура смены парольной информации в информационных системах СПБ ГБУЗ «Детская городская поликлиника №11» должна проводиться на регулярной основе.

**6.10 Регистрация событий**

Осуществление регистрации событий безопасности на всех компонентах информационных систем СПБ ГБУЗ «Детская городская поликлиника №11», 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 СПБ ГБУЗ «Детская городская поликлиника №11» в соответствии с законодательством Российской Федерации.

6.11.2 При эксплуатации СКЗИ и ключевой информации все сотрудники СПБ ГБУЗ «Детская городская поликлиника №11» должны выполнять требования нормативных правовых актов, издаваемых федеральным органом исполнительной власти в области обеспечения безопасности, документов СПБ ГБУЗ «Детская городская поликлиника №11»   
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 СПБ ГБУЗ «Детская городская поликлиника №11» для обеспечения защиты данных и защиты информационных систем СПБ ГБУЗ «Детская городская поликлиника №11» 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 СПБ ГБУЗ «Детская городская поликлиника №11» 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 СПБ ГБУЗ «Детская городская поликлиника №11» с целью организации обмена электронными сообщениями между работниками, а также между работниками СПБ ГБУЗ «Детская городская поликлиника №11» и внешними абонентами.

6.13.2 В СПБ ГБУЗ «Детская городская поликлиника №11» должны быть четко определены требования к использованию системы корпоративной электронной почты.

6.13.3 Предоставление и прекращение доступа к ресурсам корпоративной электронной почты должно осуществляться только на основе оформленной заявки.

6.13.4 В СПБ ГБУЗ «Детская городская поликлиника №11» должно быть установлено специальное программное обеспечение, осуществляющее контроль всех входящих сообщений на наличие вредоносного программного обеспечения.

6.13.5 В СПБ ГБУЗ «Детская городская поликлиника №11» должны быть предусмотрены механизмы архивирования и резервного копирования корпоративной электронной почты в автоматическом режиме.

**6.14 Резервное копирование и восстановление данных**

6.14.1 Осуществление резервного копирования для:

* файловых серверов и серверов приложений, критичных для деятельности СПБ ГБУЗ «Детская городская поликлиника №11»;
* операционных систем файловых серверов и прикладных программ;
* приложений, критичных для деятельности СПБ ГБУЗ «Детская городская поликлиника №11»;
* рабочих данных.

6.14.2 Частота и режим резервного копирования устанавливаются таким образом, чтобы обеспечить минимальную потерю данных и допустимое время восстановления.

6.14.3 Резервное копирование и восстановление ресурсов информационных систем СПБ ГБУЗ «Детская городская поликлиника №11» должны проводить уполномоченные работники СПБ ГБУЗ «Детская городская поликлиника №11».

6.14.4 Резервное копирование должно осуществляться в автоматическом режиме   
с применением специализированного программно-аппаратного комплекса.

1. **Основные требования к процессам управления информационной безопасностью**

**7.1 Управление рисками**

1. Выбор требований по информационной безопасности и защитных механизмов, применяемых в системе информационной безопасности, должен основываться на проведении анализа рисков нарушения основных свойств безопасности для наиболее критичных информационных ресурсов СПБ ГБУЗ «Детская городская поликлиника №11».
2. Основой оценки рисков должна быть оценка условий и факторов, которые могут стать причиной нарушения свойств целостности, конфиденциальности   
   и доступности для ресурсов информационной системы СПБ ГБУЗ «Детская городская поликлиника №11».
3. Результатом проведения анализа рисков должен быть комплекс мер, направленных на снижение возможного негативного влияния на основную деятельность СПБ ГБУЗ «Детская городская поликлиника №11» при реализации той или иной угрозы, и обеспечивающих достаточный уровень защищенности информационных систем СПБ ГБУЗ «Детская городская поликлиника №11».
4. **Управление инцидентами информационной безопасности**
5. Для обеспечения эффективного разрешения инцидентов информационной безопасности в СПБ ГБУЗ «Детская городская поликлиника №11», минимизации потерь и уменьшения риска возникновения повторных инцидентов должно осуществляться эффективное управление инцидентами информационной безопасности.
6. Для управления инцидентами информационной безопасности должна быть создана система учета произошедших инцидентов, которая представляет собой комплекс средств и мероприятий для сбора и консолидации информации об инцидентах.
7. В отношении каждого произошедшего инцидента должен выполняться   
   его анализ и разработка эффективных мер реагирования на данный инцидент.
8. **Мониторинг текущего уровня информационной безопасности**
9. Для обеспечения высокого уровня контроля в отношении системы обеспечения информационной безопасности в СПБ ГБУЗ «Детская городская поликлиника №11» на постоянной основе должен проводиться комплексный анализ существующих защитных механизмов и возникающих инцидентов информационной безопасности, а также периодический аудит всей системы обеспечения информационной безопасности.
10. Процесс мониторинга системы обеспечения информационной безопасности должен включать в себя контроль организационных и технических защитных мер, анализ параметров конфигурации и настройки защитных механизмов.
11. При проведении контрольных мероприятий, связанных с оценкой функционирования защитных мер в СПБ ГБУЗ «Детская городская поликлиника №11», уполномоченные работники должны придерживаться следующих принципов:

* не нарушать функционирование текущей деятельности СПБ ГБУЗ «Детская городская поликлиника №11»;
* действовать в соответствии с внутренними документами СПБ ГБУЗ «Детская городская поликлиника №11»   
  по информационной безопасности;
* не скрывать факты выявленных инцидентов и нарушений требований информационной безопасности;
* оформлять отчеты, подтверждающие выполнение мероприятий по обеспечению информационной безопасности.

1. 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.
2. 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 СПБ ГБУЗ «Детская городская поликлиника №11».
3. **Аудит системы обеспечения информационной безопасности**
4. В целях оценки текущего уровня информационной безопасности уполномоченные работники СПБ ГБУЗ «Детская городская поликлиника №11» на регулярной основе должны проводить аудит информационной безопасности.
5. Внутренние аудиты или самооценки должны выполняться, по возможности, работниками СПБ ГБУЗ «Детская городская поликлиника №11».
6. Результатом выполнения аудитов по информационной безопасности должны стать отчеты о выполненном аудите информационной безопасности, которые разрабатываются специалистами СПБ ГБУЗ «Детская городская поликлиника №11».
7. По результатам аудита уполномоченные работники и ответственные подразделения СПБ ГБУЗ «Детская городская поликлиника №11» должны определить действия, необходимые для устранения обнаруженных несоответствий в процессе аудита, и вызвавших их причины.
8. **Управление персоналом**
9. Организация такого процесса управления персоналом, который обеспечит доверительное отношение к работникам, а также организует комплексное противодействие угрозам информационной безопасности, исходящим от персонала СПБ ГБУЗ «Детская городская поликлиника №11».
10. Выполнение обязательных проверок при приеме новых работников   
    на работу с точки зрения достоверности сообщаемых ими данных и с позиции оценки   
    их профессиональных навыков.
11. Организация работы в направлении повышения осведомленности   
    и обучения в области информационной безопасности.
12. Повышение осведомленности работников СПБ ГБУЗ «Детская городская поликлиника №11»:

* по существующим в СПБ ГБУЗ «Детская городская поликлиника №11» политикам информационной безопасности;
* по применяемым в СПБ ГБУЗ «Детская городская поликлиника №11» защитным мерам;
* по правильному использованию защитных мер в соответствии   
  с внутренними документами СПБ ГБУЗ «Детская городская поликлиника №11».

1. **Заключение**
   1. Настоящая Политика является внутренним документом СПБ ГБУЗ «Детская городская поликлиника №11», общедоступной и подлежит размещению на официальном сайте СПБ ГБУЗ «Детская городская поликлиника №11».
2. Настоящая Политика подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке   
   и защите персональных данных, но не реже одного раза в три года. При внесении изменений в актуальной редакции указывается дата последнего обновления. Новая редакция Политики вступает в силу с момента ее размещения, если иное не предусмотрено новой редакцией Политики. Действующая редакция всегда находится на странице по адресу: https://dgp11.spb.ru/informaczionnaya-bezopasnost/.
3. Контроль исполнения требований настоящей Политики осуществляется ответственным лицом за обеспечение безопасности персональных данных СПБ ГБУЗ «Детская городская поликлиника №11».
4. Ответственность должностных лиц СПБ ГБУЗ «Детская городская поликлиника №11», имеющих доступ к конфиденциальной информации, за невыполнение требований норм, регулирующих обработку и защиту информации, определяется в соответствии с законодательством Российской Федерации и внутренними документами СПБ ГБУЗ «Детская городская поликлиника №11».