УТВЕРЖДЕНО
приказом ГБУ РО «МИАЦ»
от 19.12. 2024 г. № 141-од

# Политика информационной безопасности государственного бюджетного учреждения Ростовской области «Медицинский информационно-аналитический центр»

# 1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая Политика государственного бюджетного учреждения Ростовской области «Медицинский информационно-аналитический центр» (далее – Учреждение) является документом, определяющим направления деятельности в области обеспечения информационной безопасности и представляет собой систематизированное изложение целей и задач информационной безопасности, как одно или несколько правил, процедур, практических приемов и руководящих принципов, которыми руководствуется Учреждение, а также организационных, технологических и процедурных аспектов обеспечения информационной безопасности.

Положения настоящей Политики не распространяются на обеспечение информационной безопасности сведений, составляющих государственную тайну.

Основной задачей в области информационной безопасности Учреждение признает совершенствование мер и средств обеспечения защиты информации информационных ресурсов Учреждения в контексте развития законодательства Российской Федерации и норм регулирования информационной деятельности в текущих условиях функционирования информационных ресурсов Учреждения.

При разработке Политики учитывались основные принципы создания систем защиты информации, характеристики и возможности организационно-технических мер и современных программных и аппаратно-программных средств защиты информации.

В рамках своей деятельности Учреждение обязуется предпринимать все возможные меры для защиты информации от угроз безопасности информации.

Требования информационной безопасности, соответствуют целям деятельности Учреждения и предназначены для снижения рисков, связанных с реализацией угроз безопасности информации.

Политика доступна всем работникам Учреждения и всем пользователям его ресурсов.

# 2. ЦЕЛИ И ЗАДАЧИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

## 2.1. Субъекты информационный отношений

Субъектами при обеспечении информационной безопасности в Учреждении являются:

- кандидаты для приема на работу;
- работники (в том числе уволенные);
- члены семьи работников;
- физические лица, представители контрагентов в рамках исполнения договорных обязательств;
- физические лица, подавшие обращение в адрес Учреждения;
- юридические лица, в рамках исполнения договорных обязательств или во исполнении требований со стороны законодательства Российской Федерации;
- органы государственной власти.

## 2.2. Объекты информационных отношений

Объектами информационных отношений являются:

- информационные ресурсы Учреждения;
- государственные информационные системы Оператором которых является Учреждение;
- процессы обработки информации в информационных системах Учреждения, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации;
- информационная инфраструктура, включающая системы обработки, хранения и анализа информации, программные и программно-аппаратные средства, в том числе каналы связи и телекоммуникации;
- системы и средства защиты информации, объекты и помещения, в которых размещены средства обработки информации.

## 2.3. Цели обеспечения информационной безопасности

Основной целью обеспечения информационной безопасности Учреждения являются:

- действия, направленные на достижение защиты субъектов информационных отношений от возможного нанесения им материального,

физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, в том числе:

а) обеспечения отказоустойчивого функционирования программных и аппаратно-программных средств Учреждения и предоставляемых сервисов;

б) соблюдения правового режима использования массивов и средств обработки информации;

в) предотвращения реализации угроз безопасности информации при осуществлении деятельности Учреждения.

**2.4. Задачи обеспечения информационной безопасности**

Достижение целей обеспечения информационной безопасности и свойств информации Учреждения решается следующими задачами:

- защиты от несанкционированного доступа к информационным ресурсам; разграничения доступа пользователей к информационным, аппаратным, программным и иным ресурсам;

- регистрации и периодического контроля действий пользователей при обработке защищаемой информации и периодический контроль корректности их действий;

- контроля целостности среды исполнения программ и ее восстановление в случае нарушения;

- обеспечения аутентификации и идентификации пользователей, участвующих в информационном обмене;

- обеспечения исправности применяемых в информационных системах Учреждения средств защиты информации;

- своевременного выявление источников угроз безопасности информации, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений;

- созданием службы мониторинга и реагирования на угрозы безопасности информации и негативные последствия;

- созданием условий для минимизации наносимого ущерба неправомерными действиями, и устранение последствий нарушения информационной безопасности в Учреждении.

Решение вышеперечисленных задач в Учреждении осуществляется посредством:

- учета всех подлежащих защите информационных ресурсов;

- регламентации процессов обработки информации, действий работников Учреждения, осуществляющих эксплуатацию программных и программно-аппаратных средств, на основе утвержденных организационно-распорядительных документов по защите информации;

- назначения и подготовкой работников, ответственных за организацию и осуществление мероприятий по обеспечению информационной безопасности в Учреждении;

- наделения каждого работника минимально необходимыми правами при работе в информационной инфраструктуре согласно их должностным обязанностям;

- соблюдения всеми работниками, эксплуатирующими и обслуживающими программные и программно-аппаратные средства, требований организационно-распорядительных документов по вопросам обеспечения информационной безопасности;

- персональной ответственностью каждого работника за свои действия, участвующего в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющего доступ к ресурсам информационных систем;

- реализацией технологических процессов обработки информации с использованием комплексов организационно-технических мер защиты программного обеспечения,

- программно-аппаратных средств;

- принятия мер по обеспечению физической целостности программно-аппаратных средств информационных систем и поддержанием необходимого уровня защищенности компонентов;

- контроля соблюдения пользователями информационных систем требований по обеспечению информационной безопасности;

- проведения анализа эффективности принятых мер защиты информации и применяемых средств защиты информации в Учреждении;

- разработки и реализации предложений по совершенствованию систем защиты информации в Учреждении.

## 3. ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Обеспечение информационной безопасности осуществляется в соответствии со следующими основными принципами:

**Принцип законности**

При выборе мероприятий по защите информации соблюдаются действующее законодательство Российской Федерации в сфере защиты информации.

Все работники проинформированы об ответственности за правонарушения в сфере защиты информации. Программно-аппаратные средства, применяемые в Учреждении, имеют соответствующие лицензии, официально приобретаются у представителей разработчиков этих средств.

**Принцип системности**

При создании системы защиты учитываются актуальные угрозы безопасности информации, возможные объекты и направления атак на нее со стороны нарушителей.

Система защиты строится с учетом не только известных каналов утечки информации, но и с учетом возможности появления новых уязвимостей в программном обеспечении.

**Принцип комплексности**

Комплексное использование средств защиты информации предполагает согласованное применение при построении целостной системы защиты, перекрывающей все существенные угрозы безопасности информации. Защита строится эшелонировано. Физическая защита обеспечивается физическими средствами и организационными мерами.

При построении, внедрении и эксплуатации системы защиты информации руководство Учреждения обеспечивает условия для эффективной координации действий всех лиц, обеспечивающих информационную безопасность.

**Принцип преемственности**

Постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационных систем и системы ее защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите информации.

**Принцип достаточности**

Соответствие уровня затрат на обеспечение информационной безопасности и ценности информационных ресурсов на величину возможного ущерба от их разглашения, уничтожения и искажения.

Используемые меры и средства защиты информации не должны ухудшать эргономические показатели компонентов информационных систем.

**Принцип ответственности**

Возложение ответственности за обеспечение безопасности информации и ее обработки на каждого работника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей работников строится таким образом, чтобы в случае любого нарушения был известен нарушитель.

**Принцип обоснованности и технической реализуемости**

Информационные технологии, программные и программно-аппаратные средства, меры защиты информации реализованы по современным решениям, обоснованы с точки зрения достижения заданного уровня защищенности информации и экономической целесообразности, а также соответствовать установленным нормам и требованиям по безопасности информации.

**Принцип минимизации привилегий пользователей**

Обеспечение пользователей привилегиями минимально достаточными для выполнения ими своих должностных обязанностей в Учреждении.

## 4. ОСНОВНЫЕ ТРЕБОВАНИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА

Система защиты информации предусматривает комплекс организационных, программных и программно-аппаратных средств и мер по защите информации в процессе ее обработки.

Выполнение требований достигается за счет реализации на объектах информатизации мер по защите информации:

- идентификации и аутентификации субъектов доступа и объектов доступа;
- управлению доступом субъектов доступа к объектам доступа;
- ограничению программной среды;
- защите машинных носителей персональных данных;
- регистрации событий безопасности;
- антивирусной защите;
- обнаружению вторжений;
- контролю (анализу) защищенности персональных данных;

- обеспечению целостности информационной системы и персональных данных;

- обеспечению доступности персональных данных;

- защиты среды виртуализации;

- защиты технических средств;

- защиты информационной системы, ее средств, систем связи и передачи данных;

- выявлению инцидентов и реагирование на них;

- управлению конфигурацией информационной системы и системы защиты персональных данных.

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

- соблюдать права и законные интересы иных лиц;

- принимать необходимые меры по защите информации;

- ограничивать доступ к информации, если такая обязанность установлена законодательством Российской Федерации.

В том числе, Учреждение вправе, если иное не предусмотрено законодательством Российской Федерации:

- 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 законодательством Российской Федерации основании;

- защищать установленными законодательством Российской Федерации 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 Российской Федерации.

Защита информации ограниченного доступа представляет собой принятие 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).

Средства защиты информации внедряются по результатам проведения оценки рисков информационной безопасности.

**Организация защиты информации**

При организации в Учреждении защиты информации, выполняются требования:

Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», которые регулируют отношения, связанные с установлением, изменением и прекращением режима обработки защищаемой информации.

В том числе требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах утвержденные приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» для государственных информационных систем по которым Учреждение является Оператором.

В Учреждении, помимо реализации основных мер защиты информации, осуществляется:

- регулярная оценка и управление рисками информационной безопасности в соответствии с установленными процедурами в области управления рисками;

- информирование, обучение и повышение квалификации работников Учреждения в сфере информационной безопасности;

- методическая помощь работникам в вопросах обеспечения информационной безопасности;

- анализ и поиск возможностей по повышению уровня защищенности информации.

Для организации защиты информации, Учреждение вправе применять средства и методы технической защиты, предпринимать другие, не противоречащие законодательству Российской Федерации, меры.

В рамках обеспечения защиты информации, в рамках трудовых отношений работники Учреждения ознакомлены под роспись, доступ

которых к информации ограниченного доступа, необходим для выполнения ими своих должностных обязанностей, с перечнем информации ограниченного доступа, и принятыми в Учреждении мерами защиты информации

**Особенности защиты персональных данных**

При организации обработки в Учреждении персональных данных Учреждение руководствуется требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

Перечень мер, которые обеспечивает Учреждение в качестве оператора персональных данных, включает:

- назначен ответственный за организацию обработки персональных данных;

- разработаны документы, определяющие правила в отношении обработки персональных данных в Учреждении, локальные акты по вопросам обработки персональных данных;

- применены организационные и технические меры по обеспечению безопасности персональных данных в соответствии со статьей 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

- выполнены требования по составу и содержанию организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных утверждённых Приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- проведена оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона № 152-ФЗ, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ;

- ознакомлены работники Учреждения, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, документами, определяющими требования Учреждения в отношении обработки

персональных данных и обучение, при необходимости, указанных работников.

Обеспечение безопасности персональных данных в Учреждении достигается, в частности:

- определены угрозы и нарушители безопасности персональных данных при их обработке в информационных системах персональных данных;

- определен уровень защищенности персональных данных в соответствии с требованиями Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- проведена оценка эффективности принимаемых мер по защите персональных данных до ввода в эксплуатацию информационных систем персональных данных;

- определены меры по восстановлению персональных данных, вследствие получения несанкционированного доступа к ним;

- установлены правила доступа к персональным данным, обрабатываемым в информационных системах персональных данных;

- осуществляется контроль за принимаемыми мерами по защите персональных данных и определенного уровня защищенности информационных систем персональных данных в процессе ее эксплуатации.

## 5. ОСНОВНЫЕ ТРЕБОВАНИЯ К ПРОЦЕССАМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Методическое руководство, разработку решений по защите информации, согласование выбора средств вычислительной техники, программных и программно-аппаратных средств защиты информации, организацию работ по выявлению возможностей и предупреждению утечки защищаемой информации, аттестацию объектов информатизации осуществляют организации имеющие лицензии на право оказания услуг в этой области.

**Физическая безопасность**

Принятые организационные и технические меры по защите помещений Учреждения, серверного и коммутационного оборудования,

автоматизированных рабочих мест пользователей информационных систем Учреждения, обеспечивают реализацию следующих мер по:

- разграничению доступа работников в помещения Учреждения в соответствии с их полномочиями и должностными обязанностями;

- контролируемому пребыванию посторонних лиц в Учреждении в помещения, в которых ведется обработка информации ограниченного доступа и размещены аппаратные средства информационной системы;

- организации режима контролируемого вноса/выноса средств обработки информации.

Помещения Учреждения оборудованы детекторами огня и дыма, огнетушителями, средствами охранно-пожарной сигнализации.

Основное серверное и коммутационное оборудование Учреждения 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 Учреждения в соответствии с рекомендациями производителя.

Портативные технические средства не должны оставаться за пределами контролируемой зоны Учреждения без контроля со стороны работников Учреждения.

**Безопасность на рабочем месте**

Работникам Учреждения запрещено вести запись паролей в открытом виде на материальных носителях, за исключением случаев, регламентированных методов хранения.

Документы и носители с информацией ограниченного доступа по окончанию рабочего времени убираются в опечатываемые места (сейфы, шкафы и т.п.).

Документы, содержащие информацию ограниченного доступа, сразу изымаются из печатающих устройств. Утилизация конфиденциальных документов в Учреждении осуществляется в соответствии с действующими требованиями и правилами. При использовании мобильных технических средств соблюдаются дополнительные меры по регламентации и контролю использования в информационной системе мобильных технических средств.

Нахождение представителей юридических лиц в рамках исполнения договорных обязательств в помещениях в которых ведется обработка информации ограниченного доступа информационной системы,

осуществляется только в сопровождении работника Учреждения допущенного до обработки такой информации.

Размещение технических средств вывода информации в помещениях Учреждения производится с учетом исключения возможности визуального просмотра информации посторонними лицами и работниками, не допущенным к работе с данной информацией.

Технические средства размещены и храниться таким образом, чтобы сократить возможный риск повреждения и угрозы несанкционированного доступа.

**Техническое обслуживание оборудования**

Технические средства Учреждения проходят на регулярной основе сервисное обслуживание в соответствии с рекомендациями производителей оборудования.

**Взаимодействие с третьими лицами**

В целях обеспечения информационной безопасности Учреждение, при взаимодействии с третьими лицами, выполняет следующие мероприятия по:

- заключению соглашения о неразглашении информации ограниченного доступа полученной в ходе исполнения договорных обязательств;

- осуществлению контроля за действиями представителей контрагентов в пределах контролируемой зоны Учреждения.

**Управление жизненным циклом информационных систем**

Мероприятия в процессе жизненного цикла информационных систем Учреждения направлены на обеспечение защиты информации при вводе в действие, эксплуатации, сопровождении и модернизации, вывода из эксплуатации.

Работы по модернизации информационных систем, в том числе по установке программного обеспечения и обновлений, проводятся в нерабочее время или время наименьшей рабочей нагрузки.

Все процедуры обеспечения защиты информации, установленные в Учреждении в отношении информационных систем, выполняются и контролируются ответственными лицами за организацию работ по защите информации.

**Контроль доступа к информационным системам**

Все работники Учреждения, допущенные к работе с информационными системами, несут персональную ответственность за нарушения установленного порядка обработки информации.

Уровень полномочий Пользователей в информационных системах Учреждения определяется в соответствии с его должностными обязанностями.

Доступ пользователей к информационным системам Учреждения контролируется администраторами информационных систем.

Осуществляется регулярный контроль выполнения организационно-распорядительных документов, касающихся регламентации допуска работников Учреждения к информационным системам.

**Идентификация и аутентификация**

Доступ пользователей к информационным системам предоставляется только после успешного завершения идентификации, аутентификации.

Получение пользователем логина и пародля для доступа информационных системам осуществляется по представлению руководителя структурного подразделения.

**Управление доступом**

В Учреждении осуществляется управление доступом к информационным системам посредством реализации необходимых методов, типов и правил разграничения доступа пользователям информационных систем Учреждения.

**Безопасность при работе с носителями информации**

Работники Учреждения используют только учтенные съемные машинные носители информации для выполнения своих должностных обязанностей. Использование съемных машинных носителей информации в Учреждении в иных целях строго запрещено.

Съемные машинные носители информации хранятся в опечатываемых шкафах, в помещениях в которых предусмотрена обработка информации ограниченного доступа.

В случае кражи или потери съемного машинного носителя информации, а также иных инцидентов, которые могут привести к нарушению свойств информации ограниченного доступа, предусмотрено проведение мероприятий по расследованию таких инцидентов.

При выводе из эксплуатации съемного машинного носителя информации, все данные, хранящиеся на нем, удаляются средством гарантированного уничтожения информации.

Факт уничтожения информации на съемном машинном носителе информации фиксируется в акте об уничтожении информации со съемного машинного носителя информации.

**Регистрация событий**

В Учреждении осуществляется регистрации событий безопасности на всех компонентах информационных систем Учреждения, в которых обрабатывается защищаемая информация.

**Антивирусная защита**

В целях обнаружения и устранения вредоносных программ в Учреждении используются средства антивирусной защиты информации.

Обязательному контролю средством антивирусной защиты информации подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по локальной вычислительной сети в том числе и сетям общего пользования, а также информация, хранимая на съемных машинных носителях информации.

При установке программного обеспечения или его обновления на северное оборудование автоматически выполняться предварительная проверка данного программного обеспечения на отсутствие вредоносного программного обеспечения.

Обновление баз сигнатур для средства антивирусной защиты информации обновляются ежедневно.

Пользователи, без прав администратора информационной системы Учреждения, не имеют возможность получения доступа к конфигурации антивирусного средства защиты или его отключения.

**Контроль защищенности персональных данных**

В целях исключения эксплуатации уязвимостей программного обеспечения на постоянной основе проводятся работы по выявлению, анализу уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей. В том числе организация контроля установки обновления программного обеспечения включая средств защиты информации.

**Использование средств криптографической защиты информации**

Обеспечение защиты информации ограниченного доступа от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны обеспечивается применением средств криптографической защиты информации.

Приобретение средств криптографической защиты информации в Учреждении осуществляется на основании договоров и контрактов с лицами имеющими действующую лицензию ФСБ России на осуществление деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).

**Использование электронной почты**

Электронная почта используется в Учреждении с целью организации обмена электронными сообщениями между работниками и субъектами информационной безопасности.

При использовании электронной почты запрещается:

- обмен информацией для служебного пользования, а также информацией ограниченного доступа;

- предоставление доступа к электронной почте с использованием данных своей учетной записи третьим лицам;

- публикация своего служебного адреса электронной почты в электронных каталогах, на поисковых машинах и других ресурсах сети Интернет в целях, не связанных с исполнением своих должностных обязанностей;

- подписка по электронной почте на различные рекламные материалы, листы рассылки, электронные журналы и т.д., не связанные с выполнением пользователем должностных обязанностей;

- открытие (запуск на выполнение) файлов, полученных по электронной почте или из ресурсов сети Интернет, без предварительной проверки их антивирусным программным обеспечением.

**Работа в сетях общего пользования**

Учреждение оставляет за собой право блокировать или ограничивать доступ работникам к сетям связи общего пользования, в том числе сети Интернет, содержание которых не имеет отношения к исполнению должностных обязанностей, а также к информационным ресурсам, содержание и направленность которых запрещены законодательством Российской Федерации.

При использовании сети Интернет Пользователям запрещено:

- использовать предоставленный Учреждением доступ в сеть Интернет в личных целях;

- использовать несанкционированные программные и программно-аппаратные средства, позволяющие получить несанкционированный доступ к сети Интернет;

- публиковать, загружать и распространять материалы, содержащие недостоверную информацию о Учреждении, а также фальсифицировать свой IP-адрес.

**Резервное копирование и восстановление данных**

Осуществление резервного копирования осуществляется для информации обрабатываемой на файловом сервере и сервере приложений, информационных систем; рабочих мест администраторов информационных систем.

Настройка резервного копирования и восстановления ресурсов информационных систем Учреждения проводят уполномоченные работники Учреждения.

Резервное копирование осуществляется в автоматическом режиме с применением отечественного специализированного средства резервного копирования с действующим сертификатом соответствия по требованиям безопасности информации ФСТЭК России.

# 6. ОСНОВНЫЕ ТРЕБОВАНИЯ К ПРОЦЕССАМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

**Мониторинг информационной безопасности**

На постоянной основе проводится комплексный анализ функционирования информационной системы Учреждения и возникающих событий информационной безопасности.

Процесс мониторинга системы обеспечения информационной безопасности включает в себя контроль организационных и технических мер по защите информации, анализ параметров конфигурации и настройки средств защиты информации.

При проведении контрольных мероприятий, связанных с оценкой реализации мер по защите информации в Учреждении, уполномоченные работники придерживаются следующих принципов:

- не нарушают функционирование деятельности Учреждения;

- действуют в соответствии с утвержденными организационно-распорядительными документами Учреждения по защите информации;

- не скрывают факты выявленных событий информационной безопасности;

- оформляют отчеты, подтверждающие выполнение мероприятий по защите информации.

Информация, полученная в ходе проведения контролирующих мероприятий о действиях, событиях и параметрах, имеющих отношение к реализации мер по защите информации, консолидируется и хранится в местах, исключающих получение к ней несанкционированного доступа.

Мониторинг данных о зарегистрированных событиях информационной безопасности проводиться с использованием системы мониторинга инцидентов информационной безопасности или встроенных механизмов настройки и аудита событий в программных и программно-аппаратных средствах, используемых в информационной инфраструктуре Учреждения.

**Управление рисками**

Определение внутренних требований по защите информации, основаны на результатах проведения анализа рисков нарушения основных свойств безопасности для информационных ресурсов Учреждения.

Основой оценки рисков является оценка условий и факторов, которые могут стать причиной нарушения целостности, конфиденциальности и доступности для информационных ресурсов Учреждения.

Результатом проведения анализа рисков является разработка комплекса мер, направленных на снижение возможного негативного влияния на основную деятельность Учреждения при реализации той или иной угрозы безопасности информации и обеспечивающих в дальнейшем достаточный уровень защищенности информационных систем Учреждения.

**Управление инцидентами информационной безопасности**

Для обеспечения эффективного разрешения инцидентов информационной безопасности в Учреждении, минимизации потерь и уменьшения риска возникновения повторных инцидентов осуществляется управление инцидентами информационной безопасности.

**Аудит системы обеспечения информационной безопасности**

В целях оценки текущего уровня информационной безопасности в Учреждении на регулярной основе проводится аудит информационной безопасности.

Внутренние аудиты выполняются работниками Учреждения. В число задач, решаемых при проведении внутренних аудитов информационной безопасности, входят:

- сбор и анализ исходных данных об организационной и функциональной структуре информационных систем, необходимых для оценки состояния системы защиты информации;

- анализ утвержденных организационно-распорядительных документов по защите информации на предмет их полноты и эффективности, а также формирование рекомендаций по их доработке или разработки новых;

- обоснование финансовой эффективности вновь приобретаемых средств защиты информации;

- проверка правильности выбора и настройки средств защиты информации, формирование предложений по использованию имеющихся средств защиты информации для повышения уровня надёжности и безопасности информационных систем Учреждения;

- анализ отчетов по произошедшим инцидентам информационной безопасности и принятым мерам по их разрешению.

## 7. ЗАКЛЮЧЕНИЕ

При изменении действующего законодательства Российской Федерации в области защиты информации, а также организационно-распорядительных документов Учреждения настоящая Политика и изменения к ней применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам, а также внутренним документам Учреждения.

Все требования, установленные действующим законодательством Российской Федерации, подзаконными актами и договорными отношениями, а также подход Учреждения к обеспечению соответствия этим требованиям должны быть явным образом определены, документированы и поддерживаться в актуальном состоянии.

Учреждением в приоритетном направлении должен рассматриваться переход на программного обеспечение отечественного производителя, включенного в единый реестр российских программ для электронных вычислительных машин и баз данных. В том числе по части серверного, коммутационного оборудования и программно-аппаратных средств включенных в Единый реестр российской радиоэлектронной продукции.

Пересмотр и внесение изменений в настоящую Политику осуществляются на периодической и внеплановой основе.