### Оглавление

1. **Введение**  
   1.1. Цели и задачи информационной политики

1.2. Область применения

1.3. Определения и термины

2. **Обязанности и ответственность**

2.1. Ответственность руководства

2.2. Ответственность сотрудников

2.3. Ответственные лица и органы

3. **Права доступа и защита данных**

3.1. Правила доступа

3.2. Защита конфиденциальности данных

3.3. Хранение и передача данных

4. **Процедуры обработки и защиты данных**

4.1. Сбор и обработка данных

4.2. Хранение данных

4.3. Уничтожение данных

5. **Мониторинг и контроль**

5.1. Контроль исполнения

5.1.1. Механизмы контроля за выполнением информационной политики

5.1.2. Регулярные отчеты

5.1.3. Внедрение систем контроля

5.1.4. Обратная связь и корректирующие действия

5.2. Аудит и проверка

5.2.1. Регулярные проверки и аудит

5.2.2. Оценка результатов

5.3. Выявление и устранение нарушений

5.3.1. Анализ нарушений

5.3.2. Корректирующие действия

5.3.3. Мониторинг исправлений

5.4. Отчетность и улучшение

5.4.1. Отчеты о результатах аудита

5.4.2. Периодический пересмотр

6. **Обучение и повышение квалификации**

6.1. Разработка и внедрение программ обучения

6.1.1. Основные курсы

6.1.2. Специальные тренинги

6.1.3. Методические материалы

6.1.4. Обучение по новым технологиям

6.2. Форматы обучения

6.2.1. Очное обучение

6.2.2. Дистанционное обучение

6.2.3. Практические занятия

6.3. Оценка и сертификация

6.3.1. Оценка знаний

6.3.2. Сертификация

6.4. Повышение квалификации

6.4.1. Мероприятия по повышению квалификации

6.4.2. Индивидуальное развитие

6.4.3. Оценка и улучшение

7. **Права и обязанности**

7.1. Доступ к данным

7.1.1. Определение прав

7.1.2. Права на доступ

7.2. Использование информации

7.2.1. Цели использования

7.2.2. Ограничения

7.3. Запросы и отчеты

7.3.1. Запрос информации

7.3.2. Отчеты

7.4. Обязанности сотрудников

7.4.1. Соблюдение Политики

7.4.2. Доклады о проблемах и предложениях

**8.Использование ресурсов**

8.1. Правильное использование

8.2. Отчетность.

9. **Мероприятия при обнаружении нарушений в сфере сохранности информации**

9.1. Определение видов нарушений

9.1.1. Нарушение конфиденциальности

9.1.2. Нарушение процедур обработки данных

9.1.3. Необоснованный доступ

9.1.4. Неисполнение требований безопасности

9.1.5. Нарушение общих правил безопасности

9.2. Меры ответственности

9.2.1. Дисциплинарные последствия

9.2.2. Юридические последствия

9.2.3. Проведение расследования

9.2.4. Документирование

9.2.5. Процедура обжалования

9.3. Корректирующие действия

9.3.1. Устранение последствий

9.3.2. Обучение и повышение квалификации

10. **Обновление и пересмотр политики**

10.1. Основания для обновления

10.1.1. Изменения в законодательстве

10.1.2. Изменения в организационной структуре

10.1.3. Технологические новшества

10.1.4. Анализ инцидентов и нарушений

10.1.5. Предложения работников

10.1.6. Ответственные работники

10.1.7. Плановое обновление и пересмотр Политики

10.2. Аудит и процедура обновления Политики организации

10.2.1. Внеплановые обновления Политики

10.2.2. Плановое обновление Политики

10.2.3. Оценка необходимости изменений

10.2.4. Разработка изменений

10.2.5. Утверждение изменений

10.3. Документирование и внедрение

10.3.1. Обновление документации

10.3.2. Обучение и информирование

* 1. **Введение**

Настоящая Положение об информационной политики Санкт-Петербургского государственного бюджетного учреждения здравоохранения "Медицинский информационно-аналитический центр" (далее — СПб ГБУЗ МИАЦ, Положение) разработана в соответствии с требованиями законодательства Российской Федерации в сфере здравоохранения и информационной безопасности. Положение направлена на обеспечение конфиденциальности, доступности и актуальности медицинской информации, а также на повышение качества медицинской помощи и достижение целей и задач СПб ГБУЗ МИАЦ.

* 1. **Цели и основные задачи СПб ГБУЗ МИАЦ**

**Цели:**

а) Повышение качества медицинской помощи:

Создание условий для улучшения качества и доступности медицинской помощи через формирование единого информационного пространства в сфере здравоохранения.

б) Интеграция информационных систем:

Участие в создании и эксплуатации единой государственной информационной системы в сфере здравоохранения для эффективного обмена данными между медицинскими организациями.

в) Обеспечение управленческих решений:

Организационно-методическое обеспечение доступа к данным и ресурсам для поддержки управленческих решений в области здравоохранения.

г) Развитие цифровых технологий: Реализация политики цифровой трансформации, включая внедрение новых технологий и обеспечение безопасности информационных систем.

д) Анализ и улучшение:

Постоянный мониторинг данных, анализ больших данных и внедрение инновационных технологий для достижения целей и задач в области здравоохранения.

**Основные задачи:**

а) Формирование единого информационного пространства:

Создание и развитие инфраструктуры для интеграции медицинских данных на территории субъекта Российской Федерации.

б) Поддержка федеральных проектов:

Участие в реализации федерального проекта по созданию единого цифрового контура в здравоохранении.

в) Методическое обеспечение:

Организационно-методическое сопровождение внедрения и эксплуатации информационных систем и технологий в медицинских организациях.

г) Доступ к данным:

Обеспечение доступа к необходимой информации для принятия управленческих решений и мониторинга эффективности системы здравоохранения.

д) Внедрение новых технологий:

Участие в проектировании и разработке программного обеспечения для автоматизации процессов в медицинских учреждениях.

е) Обучение и поддержка:

Проведение обучающих мероприятий и техническая поддержка пользователей информационных систем.

ж) Анализ данных:

Сбор, обработка, хранение и анализ данных в сфере здравоохранения, включая медицинскую статистику и демографическую информацию.

з) Сотрудничество и координация:

Организация взаимодействия между медицинскими организациями, государственными органами и другими участниками системы здравоохранения.

и) Обеспечение безопасности:

Разработка и внедрение мер по защите информации и обеспечению безопасности значимых объектов критической информационной инфраструктуры.

* 1. **Цели и задачи Положения**

**Цель:** Создание условий для эффективного использования информационных ресурсов и технологий в интересах достижения целей и задач СПб ГБУЗ МИАЦ.

**Задачи:**

а) Законность и защищенность: Обработка и хранение данных осуществляется строго в соответствии с законодательством Российской Федерации, регулирующим сбор, хранение, обработку, защиту и уничтожение как конфиденциальной, так и другой информации, включая медицинскую. Данная задача описана в Положении о политике информационной безопасности СПб ГБУЗ МИАЦ.

б) Доступность:

Обеспечение доступа к информации для уполномоченных сотрудников и посетителей в рамках их полномочий и с соблюдением требований законности. Используются современные технологии для автоматизации процессов сбора, обработки и анализа данных, что позволяет своевременно получать необходимую информацию.

в) Интегрированность:

Объединение информационных систем и ресурсов в единую информационную систему, что улучшает взаимодействие между различными подразделениями и организациями здравоохранения для повышения качества обслуживания пациентов в медучреждениях города и посетителей, а также для достижения других целей СПб ГБУЗ МИАЦ.

г) Актуальность:

Обеспечение своевременного обновления и актуализации данных для принятия обоснованных управленческих решений. Постоянный мониторинг и анализ информации позволяют выявлять и устранять проблемные области, способствуя достижению целей СПб ГБУЗ МИАЦ.

* 1. **Управление и защита информационных ресурсов**

**Классификация и учет информации в СПб ГБУЗ МИАЦ:**

**1. Классификация информации**

1.1 Типы конфиденциальна информации: обрабатываемой в СПб ГБУЗ МИАЦ:

а) Медицинская информация (Приложение № 1. Положение о медицинской информации **в** СПб ГБУЗ МИАЦ):

б) Персональные данные (Приложение № 2. Общее положение о персональных данных в СПб ГБУЗ МИАЦ).

в) Коммерческая информация (Приложение № 3 Общее положение о коммерческой данных в СПб ГБУЗ МИАЦ ).

г) Открытая информация:

Информация, которая не содержит конфиденциальных данных и доступна для общего использования (например, общие статистические данные, публикации).

1.2 Категории информации:

а) Чувствительная информация:

Данные, требующие повышенной защиты, такие как информация о заболеваниях, результаты лабораторных исследований.

б) Критическая информация:

Информация, важная для функционирования организации, включая данные, связанные с выполнением ключевых задач и процессов.

в) Обычная информация:

Информация, не требующая специальной защиты, например, организационные объявления, внутренние регламенты.

**2. Методы учета информации:**

2.1 Регистрация и документация:

а) Регистрация:

Ведение реестров и журналов учета информации для отслеживания ее движения и изменений. Регистрация может включать дату создания, изменения, доступа и удаления данных.

б) Документация:

Оформление документов, связанных с управлением информацией, включая протоколы, отчеты и служебные записки.

2.2 Хранение и архивирование:

а) Хранение:

Определение мест хранения информации в зависимости от ее категории и уровня конфиденциальности. Это может быть, как физическое хранение (в сейфах, шкафах), так и электронное хранение (в базах данных, на серверах).

б) Архивирование: Процедуры по архивированию устаревших данных для обеспечения их сохранности и упрощения доступа к ним в будущем. Архивирование должно соответствовать требованиям законодательства и внутренним регламентам.

2.3 Актуализация и обновление:

а) Актуализация данных: Регулярное обновление информации для поддержания ее актуальности. Это может включать проверку и корректировку данных, добавление новых сведений.

б) Обновление регистров:

Обновление записей в регистрах учета информации при изменении данных или поступлении новых сведений.

2.4 Контроль доступа и безопасность:

а) Контроль доступа:

Установление правил и процедур для доступа к информации, включая права и обязанности сотрудников по работе с данными.

б) Безопасность: Применение мер по защите информации, включая физическую, техническую и организационную безопасность, для предотвращения несанкционированного доступа и утечек данных.

2.5 Отчетность и аудит:

а) Отчетность: Регулярное предоставление отчетов о состоянии и движении информации в рамках внутренних и внешних требований.

б) Аудит: Проведение регулярных проверок и аудитов для оценки состояния учета информации и соблюдения установленных процедур и стандартов.

**3. Меры защиты:** Положения и процедуры по обеспечению безопасности информации, включая физическую, техническую и организационную защиту.

**4. Порядок доступа:** Правила доступа к информационным ресурсам, определение прав и обязанностей пользователей.

**4. Обработка и хранение данных**

**4.1. Сбор данных**

**Методики сбора:**

Использование структурированных форм и анкет, автоматизированных систем сбора данных, медицинских информационных систем (МИС) и других источников, таких как электронные медицинские карты и результаты лабораторных исследований.

**Технологии сбора:**

Внедрение инструментов для автоматического ввода данных, интеграция с другими информационными системами и платформами для обеспечения комплексного сбора информации.

**4.2. Анализ данных**

**Методики анализа:**

Применение статистических методов, алгоритмов машинного обучения и искусственного интеллекта для анализа медицинских данных, выявления тенденций и паттернов.

**Технологии анализа:**

Использование аналитических платформ и программного обеспечения, инструментов для визуализации данных, и специализированных медицинских аналитических решений.

**4.3. Систематизация данных**

**Методики систематизации:**

Классификация данных по категориям и типам, создание и поддержка структурированных баз данных, разработка и внедрение справочников и классификаторов.

**Технологии систематизации:**

Разработка и поддержка информационных систем и баз данных, использование средств для управления метаданными, и внедрение стандартов и протоколов для структурирования информации.

**4.4. Обработка данных**

**Методики обработки:**

Обработка данных включает их очистку, трансформацию и интеграцию в единую информационную систему. Процессы могут включать обработку текстовых и числовых данных, преобразование данных из различных форматов и объединение информации из разных источников.

**Технологии обработки:**

Использование программного обеспечения для обработки данных, и платформы для обработки больших данных.

**4.5. Хранение данных**

**4.5.1. Правила хранения данных**

**Требования к надежности:**

Хранение данных должно обеспечивать их доступность и целостность. Внедрение резервного копирования и восстановления данных для защиты от потерь или повреждений.

**Требования к сохранности:**

Обеспечение физической и логической безопасности данных. Использование защищенных серверов, баз данных и систем хранения информации, а также регулярное тестирование систем резервного копирования.

**4.5.2. Категории хранения**

**Физическое хранение:**

Организация и поддержка физической инфраструктуры для хранения данных, включая серверные комнаты и архивные хранилища. Применение системы контроля доступа к физическим объектам хранения.

**Электронное хранение:**

Использование облачных решений и локальных серверов для хранения электронных данных. Обеспечение защиты данных через шифрование, контроль доступа и другие меры безопасности.

**4.5.3. Продолжительность хранения данных**

**Регламент хранения:**

Установление сроков хранения данных в зависимости от их типа и назначения. Учет требований законодательства, медицинских стандартов и внутренних регламентов СПб ГБУЗ МИАЦ.

**Удаление данных:**

Процедуры безопасного удаления данных, которые больше не требуются для обработки или хранения. Включает методы удаления, такие как физическое уничтожение носителей или полное удаление данных с дисков.

**4.5.4. Доступ и управление данными**

**Контроль доступа:**

Установка уровней доступа для различных категорий данных. Определение прав доступа для сотрудников, исходя из их полномочий и необходимости в работе с конкретными данными.

**Управление данными:**

Разработка и внедрение процедур управления данными, включая процессы для их обновления, изменения и удаления. Ведение документации по всем действиям с данными.

**4.6. Раскрытие и предоставление информации**

**4.6.1. Условия раскрытия информации**

**Случаи раскрытия информации:**

а) Законодательные требования: Информация раскрывается в соответствии с федеральными законами и нормативными актами, которые обязывают предоставлять данные в определенных случаях. Это может включать запросы от государственных органов, судебные запросы или в рамках государственных и федеральных программ.

б) Договорные обязательства: Информация может быть раскрыта в рамках договоров и соглашений, заключенных с другими медицинскими учреждениями или организациями, если это предусмотрено условиями таких соглашений.

в) Потребности в управленческих решениях: Для принятия обоснованных управленческих решений информация может быть раскрыта внутренним заинтересованным сторонам, если это необходимо для выполнения их должностных обязанностей.

**4.6.2. Порядок раскрытия информации**

**Процедура запроса:**

Все запросы на раскрытие информации должны быть оформлены в письменной форме, с указанием цели запроса и оснований для его подачи. Запросы от уполномоченных органов должны быть официальными и сопровождаться соответствующими документами.

**Проверка запроса:**

Каждый запрос на раскрытие информации должен быть проверен на соответствие законодательству и внутренним регламентам. Необходимо удостовериться, что запрос имеет законные основания и соблюдает требования конфиденциальности.

**Документирование:**

Вся информация о запросах и их удовлетворении должна быть задокументирована. Включает регистрацию запроса, результаты проверки и документы, подтверждающие предоставление информации.

**4.6.3. Требования к соблюдению конфиденциальности**

**Анализ информации:**

Перед раскрытием информации необходимо провести анализ на предмет наличия конфиденциальных данных. При необходимости, конфиденциальные сведения должны быть обезличены или анонимизированы.

**Соблюдение законодательства:**

Все действия по раскрытию информации должны соответствовать требованиям Федерального закона № 152-ФЗ "О персональных данных", а также другим нормативным актам, регулирующим защиту конфиденциальной информации.

**4.6.4. Взаимодействие с третьими сторонами**

**4.6.4.1. Правила предоставления информации государственным органам**

**Запросы от государственных органов:**

Информация предоставляется только по официальным запросам, сопровождаемым необходимыми документами. Запросы должны быть проверены на соответствие законодательству и полномочиям запрашивающего органа.

**Протоколирование:**

Все запросы от государственных органов и предоставленные ответы должны быть зафиксированы в документации. Это включает дату запроса, содержание запроса, дату предоставления информации и получателя.

**4.6.4.2. Правила предоставления информации контролирующим организациям**

**Аудиты и проверки:**

В случае проведения проверок и аудитов контролирующими организациями информация предоставляется в соответствии с установленными процедурами и требованиями, определенными в законодательстве и договорах.

**Документация и отчетность:**

Обеспечение надлежащей документации и отчетности по результатам взаимодействия с контролирующими организациями. Это включает составление отчетов и подготовку ответов на запросы.

**4.6.5. Правила предоставления информации другим заинтересованным сторонам**

**Согласие субъектов данных:**

При предоставлении информации третьим сторонам, не связанным с государственными органами или контролирующими организациями, необходимо учитывать согласие субъектов данных, если это применимо.

**Ограничение доступа:**

Информация предоставляется в рамках установленных полномочий и для целей, заранее согласованных с запрашивающими сторонами. Доступ к информации может быть ограничен в зависимости от ее категории и значимости.

**5.1. Контроль исполнения**

**5.1.1. Механизмы контроля за выполнением информационной Положения**

а) **Назначение ответственных лиц:** Назначаются ответственные сотрудники для контроля исполнения информационной политики, которые следят за выполнением всех установленных правил и процедур.

б) **Разработка регламентов:** Устанавливаются четкие внутренние регламенты и инструкции по выполнению информационной политики, включая процедуры контроля за обработкой данных, обеспечением конфиденциальности и раскрытием информации.

в) **Регулярные отчеты:** Ответственные лица обязаны регулярно предоставлять отчеты о соблюдении информационной политики, включая информацию о выявленных несоответствиях и принятых мерах по их устранению.

г) **Внедрение систем контроля:** Используются современные IT-системы для мониторинга доступа к информации, обработки данных и соблюдения требований безопасности. Эти системы помогают выявлять нарушения и обеспечивают оперативное реагирование.

д) **Обратная связь и корректирующие действия:** Установлена система для получения обратной связи от сотрудников и пользователей информационных систем. В случае выявления нарушений или несоответствий разрабатываются и реализуются корректирующие действия.

**5.2. Аудит и проверка**

**5.2.1. Регулярные проверки и аудит**

а) **Планирование аудита:** Проводится регулярное планирование аудитов информационных систем и процессов для проверки соответствия информационной Положения и требований законодательства. Аудиты могут проводиться как внутренними, так и внешними аудиторами.

б) **Проведение аудита:** Аудиты включают проверку выполнения всех установленных процедур и правил, оценку эффективности систем контроля и анализ соблюдения требований к защите данных и конфиденциальности. Проверяются записи о доступе, обработке и хранении данных.

в) **Оценка результатов:** По результатам аудита составляются отчеты, в которых отмечаются выявленные несоответствия, нарушения и рекомендации по их устранению. Эти отчеты предоставляются руководству СПб ГБУЗ МИАЦ для принятия необходимых мер.

**5.3. Выявление и устранение нарушений**

а) **Анализ нарушений:** При выявлении нарушений проводится детальный анализ причин и факторов, способствующих нарушению. Определяются меры по устранению нарушений и предотвращению их повторения - ответственный специалист по безопасности.

б) **Корректирующие действия:** Разрабатываются и внедряются план корректирующих действий для устранения выявленных проблем. Эти действия могут включать обновление процедур, усиление контроля или дополнительное обучение сотрудников – заместитель директора…….

в) **Мониторинг исправлений:** Осуществляется мониторинг выполнения корректирующих действий для оценки их эффективности и подтверждения устранения нарушений ответственные – начальники подразделений .

**5.4. Отчетность и улучшение**

а) **Отчеты о результатах аудита:** По завершению аудита составляются отчеты, которые предоставляются руководству для анализа и принятия решений. Эти отчеты могут включать рекомендации по улучшению информационной Положения и процедур.

б) **Периодический пересмотр:** Информационная Положение и связанные с ней процедуры регулярно пересматриваются и обновляются на основе результатов аудита и проверок, а также изменений в законодательстве и организационной структуре.

**6. Обучение и повышение квалификации**

**6.1. Разработка и внедрение программ обучения**

а) **Основные курсы:**

Включают обучение по основам информационной безопасности, управления данными, защиты персональных данных и соблюдения норм конфиденциальности. Программы направлены на обеспечение понимания ключевых принципов и процедур работы с информацией.

б) **Специальные тренинги:**

Организуются курсы по специфическим аспектам, таким как использование информационных систем, управление электронными медицинскими картами и работа с телемедицинскими технологиями.

в) **Методические материалы:**

Подготовка и предоставление обучающих материалов, включая инструкции, руководства и видеокурсы, доступные для сотрудников через внутренний портал СПб ГБУЗ МИАЦ.

г) **Обучение по новым технологиям:**

Организация тренингов по внедрению новых технологий и систем, включая обновления в области программного обеспечения и оборудования.

**6.2. Форматы обучения**

а) **Очное обучение:**

Проведение семинаров, лекций и мастер-классов с участием внешних экспертов и внутренних тренеров.

б) **Дистанционное обучение:**

Использование онлайн-курсов и вебинаров для обучения сотрудников в удобное для них время и месте.

в) **Практические занятия:**

Организация практических занятий и тренингов, направленных на применение полученных знаний в реальных условиях.

**6.3. Оценка и сертификация**

а) **Оценка знаний:**

Проведение тестов и экзаменов для проверки уровня знаний и понимания сотрудников по темам обучения.

б) **Сертификация:**

Выдача сертификатов и удостоверений о прохождении обучения, подтверждающих квалификацию сотрудников.

**6.4. Повышение квалификации**

**6.4.1. Мероприятия по повышению квалификации**

а) **Курсы повышения квалификации:**

Регулярное проведение курсов и тренингов для повышения квалификации сотрудников в области информационного управления и безопасности. Это может включать обучение новым методам работы и улучшение навыков анализа данных.

б) **Конференции и семинары:**

Участие сотрудников в профессиональных конференциях, семинарах и симпозиумах для обмена опытом и получения новых знаний о последних тенденциях и технологиях в области информационного управления.

в) **Мастер-классы:**

Организация практических мастер-классов для углубленного изучения специфических областей, таких как защита данных и управление информационными системами.

**6.4.2. Индивидуальное развитие**

а) **Планы развития:**

Разработка индивидуальных планов профессионального развития для сотрудников, включающих участие в курсах, тренингах и проектах по повышению квалификации.

б) **Менторство и коучинг:**

Назначение опытных сотрудников в качестве менторов и коучей для поддержки и обучения менее опытных коллег.

**6.4.3. Оценка и улучшение**

а) **Оценка эффективности:** Регулярная оценка эффективности мероприятий по повышению квалификации и их влияния на профессиональное развитие сотрудников.

б) **Обратная связь:** Сбор обратной связи от участников курсов и тренингов для улучшения программ обучения и повышения квалификации.

**7. Права и обязанности**

**7.1 Доступ к данным**

а) **Определение прав:**

Пользователи имеют доступ к информации в пределах их полномочий и функциональных обязанностей. Доступ к данным может быть разделен по уровням, в зависимости от роли пользователя (например, администратор, пользователь, оператор).

б) **Права на доступ:**

Доступ к информации предоставляется в соответствии с установленными требованиями безопасности и конфиденциальности. Права на доступ определяются в зависимости от потребностей работы и согласовываются с ответственными лицами.

**7.2. Использование информации**

а) **Цели использования:**

Пользователи могут использовать информацию только в рамках своих профессиональных обязанностей и в целях, для которых информация была предоставлена.

б) **Ограничения:**

Использование данных в личных целях или передача информации неавторизованным лицам строго запрещены.

**7.3. Запросы и отчеты**

а) **Запрос информации:**

Пользователи имеют право на получение необходимой информации для выполнения своих задач при условии соблюдения правил доступа и конфиденциальности.

б) **Отчеты:**

Пользователи могут предоставлять отчеты и обратную связь о работе информационных систем и качества данных в рамках своих полномочий.

**7.4. Соблюдение информационной безопасности**

Сотрудники, допущенные до работы с конфиденциальными данными, обязаны соблюдать Положения политики информационной безопасности СПб ГБУЗ МИАЦ, инструкции по пользованию информационными системами и другие инструкции и распоряжения по безопасности на территории (Положение о внутриобьектовом и объектовом режимах) СПб ГБУЗ МИАЦ.

**7.5. Соблюдение должностных обязанностей**

Сотрудники обязаны строго соблюдать свои должностные обязанности, докладывать руководству о выявленных проблемах и предложениях по улучшению информационных систем и процессов.

**8. Обучение и повышение квалификации**

**8.1. Обучение**

а) **Обучение:**

Проходить обучение по информационной безопасности и управлению данными, чтобы поддерживать свою квалификацию и соответствие актуальным требованиям.

б) **Участие в мероприятиях:**

Участвовать в мероприятиях по повышению квалификации и обучении, предоставляемых организацией.

**9. Использование ресурсов**

**9.5. Правильное использование информации:**

Использовать информационные ресурсы и системы только в рамках своей деятельности и в соответствии с установленными правилами и процедурами.

**9.6. Отчетность:**

Обеспечивать правильное ведение и отчетность по использованию ресурсов и данных в рамках своих полномочий.

**10. Мероприятия при обнаружении нарушений в сфере сохранности информации**

**10.1. Определение видов нарушений**

а) **Нарушение конфиденциальности:** Несанкционированное раскрытие, использование или передача конфиденциальной информации.

б) **Нарушение процедур обработки данных:** Нарушение установленных процедур сбора, хранения, обработки или уничтожения данных.

в) **Необоснованный доступ:** Получение доступа к информации или системам, не соответствующему полномочиям пользователя.

г) **Неисполнение требований безопасности:** Невыполнение требований по защите данных, включая меры по физической и логической безопасности информации.

д) **Нарушение правил общей безопасности:** Нарушение правил, которое может привести (привело) к повреждению или хищению информации и (или) физических носителей информации.

**10.2. Меры ответственности**

**10.2.1. Дисциплинарные последствия по ТК РФ или организационные меры**

а) **Замечание:** Официальное замечание за незначительные нарушения или первую регистрацию нарушения.

б) **Выговор:** Официальное дисциплинарное взыскание, предупреждение о необходимости устранения нарушений и соблюдения Положения в будущем, оформленное в соответствии с трудовым законодательством Российской Федерации.

в) **Ограничение доступа:** Временное или постоянное ограничение доступа к определенным информационным системам или данным.

г) **Перевод на другую должность:** Перевод на должность, не связанную с информационными системами или обработкой конфиденциальной информации.

д) **Увольнение:** В случае серьезных нарушений или повторяющихся нарушений трудового договора или законодательства РФ.

**10.2.2. Юридические последствия за несоблюдение Положения**

а) **Гражданско-правовая ответственность:**

Статья 1064 ГК РФ: Обязанность возмещения вреда.

б) **Административная ответственность:**

Статья 6.30 КоАП РФ: Нарушение прав в сфере охраны здоровья. Штраф за разглашение сведений, составляющих врачебную тайну.

Статья 13.11 КоАП РФ: Нарушение законодательства в области персональных данных.

Статья 13.12 КоАП РФ: Нарушение правил защиты информации.

в) **Уголовная ответственность:**

Статья 137 УК РФ: Нарушение неприкосновенности частной жизни.

Статья 272 УК РФ: Неправомерный доступ к компьютерной информации.

Статья 273 УК РФ: Создание, использование и распространение вредоносных программ для ЭВМ.

Статья 274 УК РФ: Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

**10.2.3. Проведение расследования по факту информационных инцидентов и нарушений**

а) **Служебное расследование:**

Проведение служебного расследования осуществляется специалистом по безопасности организации с привлечением специалиста (заместителя директора) по информационной безопасности (возможно привлечение сторонних организаций или специалистов). Расследование включает сбор доказательств, анализ ситуации и оценку последствий, а также предложения по недопущению подобных инцидентов в будущем.

б) **Привлечение компетентных органов:**

При обнаружении признаков деяний, попадающих под пункты 10.2.2, директор организации принимает решение о привлечении компетентных органов.

в) **Вынесение решения:**

Вынесение решения директором организации по итогам проведения мероприятий, описанных в пунктах а) и б), производится в соответствии с ТК РФ.

**10.2.4. Документирование**

Оформление и документирование всех фактов информационных инцидентов и нарушений, принятых решений и примененных санкций для обеспечения прозрачности, и учета.

**10.2.5. Процедура обжалования**

Установление процедуры для обжалования решений директора о мерах ответственности производится согласно законодательству РФ.

**10.3. Корректирующие действия в организации при обнаружении нарушений в сфере сохранности информации**

**10.3.1. Устранение последствий:**

Принятие мер для устранения последствий нарушений сохранности информации, включая корректировку бизнес-процессов и улучшение процедур защиты данных.

**10.3.2. Обучение и повышение квалификации:**

Проведение дополнительных обучений и повышения квалификации для сотрудников с целью предотвращения повторения нарушений в будущем.

**11. Обновление и пересмотр Положения**

**11.1. Основания для обновления**

а) **Изменения в законодательстве:**

Актуализация Положения в ответ на изменения в федеральных законах, подзаконных актах и других нормативных документах, касающихся информационной безопасности и защиты данных.

б) **Изменения в организационной структуре:**

Обновление Положения в связи с изменениями в структуре СПб ГБУЗ МИАЦ, добавлением новых подразделений или изменением их функций.

в) **Технологические новшества:**

Внесение изменений в связи с внедрением новых технологий, программного обеспечения или систем, которые требуют пересмотра процедур обработки и защиты информации.

### 11. Обновление и пересмотр Положения

#### 11.1. Основания для обновления

г) **Анализ инцидентов и нарушений:**

Корректировка Положения на основе анализа инцидентов, нарушений или угроз, выявленных в процессе мониторинга и контроля.

д) **Предложения работников:**

Рассмотрение предложений работников через их руководителей подразделений.

е) **Ответственные работники**

Ответственные за пункты а) – г) согласно пункту 7.5.

ж) **Плановое обновление и пересмотр Положения:**

Проведение обязательного регулярного мониторинга применения Положения на практике, анализ её влияния на процессы и результаты работы организации, а также её плановое обновление и (или) пересмотр не реже одного раза в год. Ответственный – заместитель по информационным технологиям.

#### 11.2. Аудит и процедура обновления Положения организации:

#### а) **Внеплановые обновления Положений** информационной политики:

#### Необходимости обновления может быть инициировано работниками организации через своих руководителей подразделений в качестве обратной связи с руководством, внешними аудиторами или на основании изменений в законодательстве и требований регуляторов сферы деятельности СПб ГБУЗ МИАЦ. Ответственный – заместитель по информационным технологиям.

б) **Плановое обновление Положения:**

Плановое обновление проводится не реже одного раза в год. Ответственный – заместитель по информационным технологиям.

в) **Оценка необходимости изменений:**

Анализ законодательства, ведомственных приказов и распоряжений, требований регуляторов в сфере деятельности СПб ГБУЗ МИАЦ, возможностей эксплуатируемой и новых технологий, предложений сотрудников организации и проведение оценки влияния предполагаемых изменений на существующую политику и бизнес-процессы организации. Обоснование – оценка стоимости внедрения и предполагаемые выгоды. Ответственные – члены комиссии по внесению изменений в Политику (Положение о Комиссии по внесению изменений в информационную политику – Приложение №1).

г) **Разработка изменений:**

Подготовка проекта обновлений, который включает пересмотр и корректировку существующих положений, добавление новых требований или исключение устаревших пунктов. Ответственный – заместитель по информационным технологиям.

д) **Утверждение изменений:**

Обсуждение и утверждение обновлений производится директором СПб ГБУЗ МИАЦ.

#### 11.3. Документирование и внедрение

а) **Обновление документации:**

Оформление и внесение изменений в официальные документы, регламентирующие информационную политику. Ответственный – заместитель по информационным технологиям.

б) **Обучение и информирование:**

Проведение обучающих мероприятий и информирование сотрудников о новых требованиях и изменениях в политике. Ответственный – обученный сотрудник, назначенный заместителем по информационным технологиям.

 **Положение о Комиссии по внесению изменений в информационную политику**

* **Пункт:** 11.1. е) Ответственные работники

 **Регламент по обработке и защите данных**

* **Пункт:** 5.1.1. б) Разработка регламентов

 **Инструкции по контролю и мониторингу**

* **Пункт:** 5.1.1. в) Регулярные отчеты
* **Пункт:** 5.1.1. г) Внедрение систем контроля

 **Шаблоны отчетов и аудиторских проверок**

* **Пункт:** 5.2.1. в) Оценка результатов
* **Пункт:** 10.2.4. Документирование

 **Положение управления доступом**

* **Пункт:** 7.1. а) Определение прав
* **Пункт:** 7.1. б) Права на доступ

 **Порядок проведения обучения и повышения квалификации**

* **Пункт:** 6.1. Разработка и внедрение программ обучения
* **Пункт:** 6.2. Форматы обучения
* **Пункт:** 6.4. Повышение квалификации

 **Формы запросов и обратной связи**

* **Пункт:** 7.3. а) Запрос информации
* **Пункт:** 7.3. б) Отчеты

 **План действий при инцидентах**

* **Пункт:** 10.3. Корректирующие действия в организации при обнаружении нарушений в сфере сохранности информации

 **Положение по использованию ресурсов**

* **Пункт:** 9. Использование ресурсов

 **Документы по юридическим последствиям**

* **Пункт:** 10.2.2. Юридические последствия за несоблюдение Положения

 **План по регулярному пересмотру и обновлению Положения**

* **Пункт:** 11.1 ж) Плановое обновление и пересмотр Положения

 **Руководство по работе с конфиденциальной информацией**

* **Пункт:** 7.2. Использование информации

 **Шаблоны для внутренней документации**

* **Пункт:** 10.2.4. Документирование