**Информационная политика СПб ГБУЗ МИАЦ**

**Оглавление**

1. Введение
2. **Основные цели и задачи СПб ГБУЗ МИАЦ**
3. Цели и задачи Политики

4. Управление и защита информационных ресурсов

* 1. Законность
  2. Конфиденциальность
  3. Доступность
  4. Интегрированность
  5. Актуальность

1. Основные задачи МИАЦ

Сбор и стандартизация медицинских данных

Анализ и оценка медицинских данных

Разработка информационных систем

Поддержка принятия решений

Значимость МИАЦ в здравоохранении

Организация и проведение научно-исследовательских работ

1. Стратегическое направление в области цифровой трансформации здравоохранения

3.1. Цели и задачи цифровой трансформации

3.2. Основные направления и проекты цифровой трансформации

3.3. Внедрение электронных медицинских систем и телемедицины

3.4. Совершенствование инфраструктуры информационных технологий

3.5. Инновации и исследовательские проекты в области здравоохранения

1. Организация информационной деятельности

4.1. Структура и функции подразделений, отвечающих за информационную деятельность

4.2. Порядок взаимодействия подразделений и сотрудников

4.3. Ведение и хранение документации

1. Управление и защита информационных ресурсов

5.1. Классификация и учет информационных ресурсов

5.2. Меры по защите информационных ресурсов

5.3. Порядок доступа к информационным ресурсам

5.4. Обеспечение безопасности персональных данных

1. Использование информационных технологий

6.1. Внедрение и использование электронных медицинских карт

6.2. Применение телемедицинских технологий

6.3. Использование автоматизированных систем управления

6.4. Поддержка и обслуживание информационных систем

1. Порядок предоставления и обмена информацией

7.1. Виды и категории информации

7.2. Порядок предоставления информации пациентам

7.3. Порядок обмена информацией с другими медицинскими организациями

7.4. Порядок взаимодействия с государственными органами

1. Обеспечение конфиденциальности и защиты персональных данных

8.1. Политика конфиденциальности

8.2. Порядок обработки персональных данных

8.3. Меры по предотвращению утечек информации

8.4. Ответственность за нарушение конфиденциальности

1. Обучение и повышение квалификации персонала

9.1. Программы обучения в области информационной безопасности

9.2. Повышение квалификации сотрудников в сфере информационных технологий

9.3. Организация внутреннего контроля и аудита

1. Мониторинг и контроль исполнения информационной политики

10.1. Системы и методы мониторинга

10.2. Порядок проведения проверок и аудитов

1. Приложение: Перечень использованных документов
2. **Введение**

Настоящая информационная политика Санкт-Петербургского медицинского информационно-аналитического центра (далее — СПб ГБУЗ МИАЦ, далее — **Политика**) разработана в соответствии с требованиями законодательства Российской Федерации в сфере здравоохранения и информационной безопасности. Политика 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. **Основные цели и 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 Политики**

**Целью политики**: является создание условий для эффективного использования информационных ресурсов и технологий в интересах достижения целей и задач СПб ГБУЗ МИАЦ.

**Задачи Политики** включают:

**Законность и защищенность** - обработки и хранения данных осуществляется строго в соответствии с законодательством Российской Федерации, регулирующим сбор, хранение, обработку, защиту и уничтожение как конфиденциальной, так и другой, включая медицинскую, информации. Данная задача описана в **Политики информационной безопасности**.

**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.

**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.

**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. **Типы информации**

**а) Медицинская информация**: Данные о состоянии здоровья пациентов, истории болезни, результаты диагностики, назначения и лечения.

**б) Персональные данные**: Личные данные пациентов, включая ФИО, контактную информацию, медицинскую историю и другие идентифицирующие данные.

**в) Конфиденциальная информация**: Информация, доступ к которой ограничен в силу закона или внутренней политики (например, данные, содержащиеся в отчетах о состоянии здоровья или внутренние рабочие документы).

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

* 1. **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**

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.

1. **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.

1. **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.

1. **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.

1. **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.

в) **Меры защиты**: Политики и процедуры по обеспечению безопасности информации, включая физическую, техническую и организационную защиту.

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

**4. Обработка и хранение данных**

**Процедуры обработки данных**

* 1. **Сбор данных**

**а) 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.

**б) Технологии сбора**: Внедрение инструментов для автоматического ввода данных, интеграция с другими информационными системами и платформами для обеспечения комплексного сбора информации.

* 1. **Анализ данных**

**а) Методики анализа**: Применение статистических методов, алгоритмов машинного обучения и искусственного интеллекта для анализа медицинских данных, выявления тенденций и паттернов.

**б) Технологии анализа**: Использование аналитических платформ и программного обеспечения, инструменты для визуализации данных, и специализированные медицинские аналитические решения.

* 1. **Систематизация данных**

а) **Методики систематизации**: Классификация данных по категориям и типам, создание и поддержка структурированных баз данных, разработка и внедрение справочников и классификаторов.

б) **Технологии систематизации**: Разработка и поддержка информационных систем и баз данных, использование средств для управления метаданными, и внедрение стандартов и протоколов для структурирования информации.

* 1. **Обработка данных**

а) **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.

б) **Технологии обработки**: Использование программного обеспечения для обработки данных, таких как ETL-инструменты (Extract, Transform, Load), и платформы для обработки больших данных.

**4.5. Хранение данных**

* + 1. **Правила хранения данных**

а) **Требования к надежности**: Хранение данных должно обеспечивать их доступность и целостность. Внедрение резервного копирования и восстановления данных для защиты от потерь или повреждений.

б) **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.

* + 1. **Категории хранения**

а) **Физическое хранение**: Организация и поддержка физической инфраструктуры для хранения данных, включая серверные комнаты и архивные хранилища. Применение системы контроля доступа к физическим объектам хранения.

б) **Электронное хранение**: Использование облачных решений и локальных серверов для хранения электронных данных. Обеспечение защиты данных через шифрование, контроль доступа и другие меры безопасности.

* + 1. **Продолжительность хранения данных**

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

б) **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.

* + 1. **Доступ и управление данными**

а) **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.

б) **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**

1. **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, но не ограничиваться, запросами от государственных органов, судебными запросами, 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.

* + 1. **Порядок раскрытия информации**

а) **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.

б) **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.

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

* + 1. **Требования к соблюдению конфиденциальности**

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

б) **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**

* + - 1. **Правила предоставления информации государственным органам**

а) **Запросы от государственных органов**: Информация предоставляется только по официальным запросам, сопровождаемым необходимыми документами. Запросы должны быть проверены на соответствие законодательству и полномочиям запрашивающего органа.

б) **Протоколирование**: Все запросы от государственных органов и предоставленные ответы должны быть зафиксированы в документации. Это включает в себя дату запроса, содержание запроса, дату предоставления информации и получателя.

**4.6.4.2. Правила предоставления информации контролирующим организациям**

а) **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.

б) **Документация и отчетность**: Обеспечение надлежащей документации и отчетности по результатам взаимодействия с контролирующими организациями. Это включает в себя составление отчетов и подготовку ответов на запросы.

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

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

**б) 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.

1. **Мониторинг и контроль**

**5.1. Контроль исполнения**

* + 1. **Механизмы контроля за выполнением информационной политики.**

а) **Назначение ответственных лиц:** Для контроля исполнения информационной политики назначаются ответственные сотрудники, которые будут следить за выполнением всех установленных правил и процедур.

б) **Разработка регламентов:** Установлены четкие внутренние регламенты и инструкции по выполнению информационной политики, которые включают 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**

* + 1. **Регулярные проверки и аудит.**

**а**) **Планирование аудита**: Проводится регулярное планирование аудитов информационных систем и процессов для проверки соответствия информационной политики 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.

* 1. **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.

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

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

* 1. **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 политики и процедур.

б) **Периодический пересмотр:** Информационная политика 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**

* 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**.**

* 1. **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.

* 1. **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**

* + 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.

* + 1. **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.

* + 1. **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**.**

1. **Права и обязанности**
   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 должен предоставляться в соответствии с установленными требованиями безопасности и конфиденциальности. Права на доступ определяются в зависимости от потребностей работы и согласовываются с ответственными лицами.

* 1. **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.

* 1. **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. Сотрудник, допущенный до работы с конфиденциальными данными**, обязан соблюдать положения **Политики информационной безопасности СПб ГБУЗ МИАЦ** , инструкции по пользованию информационными системами и другие инструкции и распоряжения по безопасности на территории СПб ГБУЗ МИАЦ.

* 1. **Сотрудник обязан строго соблюдать свои должностные обязанности** - докладывать руководству о выявленных проблемах и предложениях по улучшению информационных систем и процессов.

1. **Обучение и повышение квалификации**

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.

1. **Использование ресурсов**
   1. **Правильное использование:** Использовать информационные ресурсы и системы только в рамках своей деятельности и в соответствии с установленными правилами и процедурами.
   2. **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) Не соблюдение правил общий безопасности, которые могут привести (привели) к повреждению и (или) хищению информации и (или) физическим носителями информации.

**10.2. Меры ответственности.**

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

а)Замечание: официальное замечание в случае незначительных нарушений или первой регистрации нарушения.

б) Выговор: официальное дисциплинарное взыскание, включающее предупреждение о необходимости устранения нарушений и соблюдения **Политики** 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, не связанную с информационными системами или обработкой конфиденциальными информации.

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

**10.2.2. Юридические последствия за несоблюдение Политики**

**а) Гражданско-правовая ответственность**:

**ст. 1064 ГК РФ**: Обязанность возмещения вреда.

**б) Административная ответственность**:

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

**ст. 13.11 КоАП РФ**: Нарушение законодательства в области персональных данных.

**ст. 13.12 КоАП РФ**: Нарушение правил защиты информации.

**в) Уголовная ответственность**:

**ст. 137 УК РФ**: Нарушение неприкосновенности частной жизни.

**ст. 272 УК РФ**: Неправомерный доступ к компьютерной информации.

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

**ст. 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 деяния работника, попадающего под п. 10.2.2., директор организации принимает решение о привлечении компетентных органов.

**в) Вынесение решения**:

Вынесение решения директором организации по итогам проведения мероприятий по п. а) и б) в соответствии с п. 10.2.1. в отношении работника производится согласно 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 происходит 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.

1. **Обновление и пересмотр политики**

**11.1 Основания для обновления**

**а) Изменения в законодательстве**:

Актуализация Политики 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 Политики 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.

**г) Анализ инцидентов и нарушений**:

Корректировка Политики 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 Политики**:

Проведение обязательного регулярного мониторинга применения Политики 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 Политики организации**

а) **Внеплановые обновления Политики**:

Предложение о 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 Политики**:

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.