Введение.

1.Цели и основные задачи СПб ГБУЗ МИАЦ.

2. Цели и основные задачи информационная безопасность в СПб ГБУЗ МИАЦ.

* 1. Область применения.

2.2. Определения и термины.

2.3. Политики, положения и стратегии.

2.3.1. Политики

а) Политика защиты персональных данных.

б) Политика защиты медицинской тайны.

в) Политика защиты коммерческой тайне.

г) Политика защиты конфиденциальной информации.

д) Политика защиты служебной тайне.

е) Политика защиты профессиональной тайне.

ж) Политика защиты сведений с грифом "Для служебного пользования"

з) Политика обеспечения непрерывности бизнес-процессов в аспекте информационной безопасности

к) Политика по реагированию на нарушения информационной безопасности

2.3.2. Положения

а) Положение о обучение работников Организации по информационной безопасности.

б) Положение о службе безопас ности

в) Положение о реагировании на инциденты безопасности

г) Положение о проведения аудита информационной безопасности в Организации.

д). Положение о изменениях в Положения о информационной безопасности в Организации.

е) Положение об Организация и контроль за использованием информационных ресурсов

ж)Положение об взаимодействии со сторонними организациями по вопросам информационной безопасности.

2.3.3. Стратегии

а) Стратегия развития информационной безопасности

б) Стратегия защиты критической информационной инфраструктуры

в) Стратегия управления цифровыми рисками

г) Стратегия импортозамещения

3. Организационная структура информационной безопасности в Организации.

3. 3. Структура по обеспечению информационной безопасности в Организации.

3.1. Руководитель организации

3.2. Заместитель руководителя организации по информационной безопасности.

* + 1. Положение о Заместитель руководителя организации по информационной безопасности.
    2. Служебные обязанности Заместитель руководителя организации по информационной безопасности.
    3. Положение о привлечении внешними подрядчиками по информационной безопасности"
  1. Отдел по обеспечению информационной безопасность Организации.

Положение Отдел по обеспечению информационной безопасность

3.4. Отдел по обеспечению информационной безопасность Организации.

3.4.1. Положение Отдел по обеспечению информационной безопасность Организации.

3.4.2. Положение о привлечении внешними подрядчиками по информационной безопасности"

3.5. Положение It отдела по обеспечению информационной безопасность Организации.

Обязанности и ответственность

3.6. Служба безопасности.

3.7. Отдел АХО

3.8. Служба главного инженера

3.9. Ответственность по защите информации работников Организации

3.9.1. Ответственность руководителей Организации по защите информации

3.9.2. Ответственность работников Организации по защите информации.

Заключение.

5. Обновление и пересмотр политики

5.1. Основания для обновления

5.1.1. Изменения в законодательстве

5.1.2. Изменения в организационной структуре

5.1.3. Технологические новшества

5.1.4. Анализ инцидентов и нарушений

5.1.5. Предложения работников

5.2. Аудит и процедура обновления Политики

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

Регламенты и инструкции

13.1. Инструкция по порядку учета и хранению съемных носителей конфиденциальной информации

13.2. Инструкция по обеспечению физической безопасности

13.3. Инструкция по использованию антивирусного ПО

13.4. Регламент проведения внутреннего аудита информационной безопасности

13.5. Регламент реагирования на компьютерные инциденты

**Введение**

Настоящее Положение об информационной безопасности Санкт-Петербургского государственного бюджетного учреждения здравоохранения "Медицинский информационно-аналитический центр (далее - СПб ГБУЗ МИАЦ) " (далее — Положение) разработано в соответствии с требованиями законодательства Российской Федерации. Положение направлено на обеспечение конфиденциальности, доступности и актуальности информации, а также на повышение качества услуг и достижение стратегических целей и задач СПб ГБУЗ МИАЦ" и является частью Информационной политики 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 основные по**  **информационная безопасность в СПб ГБУЗ МИАЦ.**

**Цель**:

Обеспечение высокого уровня защиты информационных активов и инфраструктур в сфере здравоохранения, улучшение устойчивости к информационным угрозам через стратегические инициативы импортозамещения и укрепления критической информационной инфраструктуры.

**Задачи:**

**Законность и защищенность:**

Разработка и реализация мероприятий по укреплению информационной безопасности, соответствующих требованиям законодательства Российской Федерации. Это включает поддержание в актуальном состоянии категоризации объектов критической информационной инфраструктуры и информационных систем, обеспечивающих сбор, обработку, передачу и уничтожение данных, отнесенных законами РФ к персональным, конфиденциальным, врачебным, коммерческим, профессиональным и служебным данным, а также в документах, содержащих гриф «Для служебного пользования» (ДСП).

**Доступность:**

Обеспечение доступа к информационным ресурсам для уполномоченных пользователей при строгом соблюдении норм информационной безопасности. Включает создание защищенных автоматизированных рабочих мест и централизованное управление конфигурациями.

**Интегрированность:**

Интеграция всех информационных систем в единую структуру для облегчения взаимодействия между медицинскими учреждениями и органами управления. Поддержание актуальности всех информационных ресурсов, совершенствование архитектуры систем в соответствии с отраслевыми и технологическими стандартами. Внедрение и поддержание в рабочем состоянии типовых защищенных автоматизированных рабочих мест с централизованным управлением конфигурациями прикладного и общесистемного программного обеспечения, включая использование доверенных дистрибутивов.

**Актуальность:**

Постоянный контроль за обновлением информационных систем и ресурсов для обеспечения актуальности, и достоверности данных. Включает проведение аттестации объектов информатизации и реализацию мер по обнаружению и устранению последствий компьютерных атак.

**Обучение и развитие:**

Организация непрерывного обучения и повышения квалификации работников в области информационной безопасности. Реализация программ обучения с использованием современных образовательных технологий и методических материалов, учитывающих специфику медицинских данных и требования информационной безопасности.

**Внедрение политики импортозамещения:**

С акцентом на снижение зависимости от иностранных информационно-коммуникационных технологий и замену их отечественными аналогами.

**Мониторинг и реагирование:** Организация мониторинга, обнаружения и предупреждения компьютерных атак, а также ликвидация их последствий. Передача данных в отраслевой центр информационной безопасности для координации и анализа инцидентов.

**2.1 Область применения**

Положение применяется ко всем структурным подразделениям СПб ГБУЗ МИАЦ (далее – Организация), включая филиалы и представительства, а также к сотрудникам, подрядчикам, и третьим лицам, которые используют или управляют информационными ресурсами организации. Положение охватывает следующие аспекты:

1. **Информационные системы и технологии**, включая, но не ограничиваясь, корпоративные сети, серверные решения, облачные платформы и мобильные приложения.
2. **Персональные данные** всех сотрудников, клиентов, партнеров и других лиц, чьи данные обрабатываются организацией в соответствии с законодательством о защите персональных данных.
3. **Конфиденциальная информация**, включая коммерческие, служебные и профессиональные секреты, которые подлежат защите в соответствии с внутренними политиками и договорными обязательствами.
4. **Оборудование и программное обеспечение**, используемое для обработки, хранения и передачи защищаемой информации.
5. **Внешние и внутренние угрозы безопасности**, которые могут повлиять на информационные активы организации.
   1. **Определения и термины**

**Автоматизированная система (АС)** - система, состоящая из персонала и комплекса средств автоматизации деятельности, которая реализует информационные технологии для выполнения установленных функций.

**Аутентификация отправителя данных** - процесс подтверждения соответствия отправителя данных заявленному субъекту.

**Безопасность персональных данных** - состояние защищенности персональных данных, которое обеспечивается способностью системы защитить конфиденциальность, целостность и доступность данных.

**Биометрические персональные данные** - уникальные физиологические характеристики человека, используемые для его идентификации.

**Блокирование персональных данных** - временное прекращение обработки персональных данных, кроме хранения.

**Вирус** (компьютерный, программный) - исполняемый код, способный к несанкционированному распространению и самовоспроизведению.

**Вредоносная программа** - программа, созданная для осуществления несанкционированного доступа к данным или их уничтожения.

**Вспомогательные технические средства и системы** - техника и системы, поддерживающие функционирование основных систем обработки информации, но не участвующие в непосредственной обработке данных.

**Доступ в операционную среду компьютера** - возможность выполнения операций в рамках операционной системы, включая управление файлами и выполнение программ.

**Доступ к информации** - возможность получения и использования информации.

**Закладочное устройство** - скрытно внедренное устройство для несанкционированного съема информации.

**Защищаемая информация** - информация, подлежащая защите по закону или требованиям владельца.

**Идентификация** - процесс определения личности или объекта по уникальным признакам или идентификаторам.

**Информативный сигнал** - сигналы, несущие в себе данные, которые могут раскрыть конфиденциальную информацию.

**Информационная система персональных данных (ИСПДн)** - комплекс технических и программных средств для обработки персональных данных.

**Информационные технологии** - методы и процессы, связанные с обработкой и распространением информации.

**Использование персональных данных** - операции с персональными данными, выполняемые с целью их обработки.

**Источник угрозы безопасности информации** - фактор, способный вызвать угрозу для информационной безопасности.

**Контролируемая зона** - зона с ограниченным доступом, контролируемая для предотвращения несанкционированного доступа.

**Конфиденциальность персональных данных** - требование к операторам и другим лицам, имеющим доступ к персональным данным, не раскрывать их без согласия субъекта данных.

**Критическая информационная инфраструктура (КИИ)** - информационные системы и сети, жизненно важные для функционирования государства и общества.

**Обеспечение безопасности критической информационной инфраструктуры** - комплекс мер, направленных на защиту КИИ от угроз.

**Компьютерная атака** - действия, направленные на нарушение нормального функционирования информационной системы или сети.

**Мероприятия по обеспечению безопасности КИИ** - действия по укреплению защиты критической инфраструктуры, включая разработку политик, мониторинг угроз и обучение персонала.

**2.3. Политики, положения и стратегии**

**2.3.1. Политики.**

**а) Политика защиты персональных данных** - Определяет методы и процедуры защиты персональных данных сотрудников и клиентов. -

**Приложение 1**. **Политика защиты персональных данных.**

**б) Политика защиты медицинской тайны** - Устанавливает правила обработки и хранения медицинской информации для обеспечения её конфиденциальности

**Приложение 2**. **Политика защиты медицинской тайны**.

**в) Политика по коммерческой тайне** - Регулирует доступ, использование и распространение коммерческой информации.

**Приложение №3. Политика защиты коммерческой тайне.**

**г) Политика защиты конфиденциальной информации** - Охватывает меры по обеспечению защиты информации, требующей особого режима доступа.

**Приложение №4. Политика защиты конфиденциальной информации.**

**д) Политика защиты служебной тайне** - Управление доступом и защита информации, связанной со служебной деятельностью.

**Приложение №5. Политика защиты служебной тайне.**

**е) Политика защиты профессиональной тайне** - Защита информации, получаемой профессионалами в ходе их деятельности.

**Приложение №6. Политика защиты профессиональной тайне.**

**ж) Политика защиты сведений с грифом "Для служебного пользования"** - Описывает меры по обеспечению безопасности такой информации.

**Приложение №7. Политика защиты сведений с грифом "Для служебного пользования"**

**з) Политика обеспечения непрерывности бизнес-процессов в аспекте информационной безопасности.**

Политика по реагированию на нарушения информационной безопасности устанавливает чёткие процедуры для идентификации, документирования и реагирования на инциденты, модели угроз и методы (способы) нивелирования кибератак и хищение конфиденциальной

**Приложение № 8. Политик обеспечения непрерывности бизнес-процессов в аспекте информационной безопасности.**

**к) Политика по реагированию на нарушения информационной безопасности**

Политика по реагированию на нарушения информационной безопасности устанавливает чёткие процедуры для идентификации, документирования и реагирования на инциденты. Она включает описание видов нарушений, меры ответственности и корректирующие действия**.**

**Приложение № 9. Политика по реагированию на нарушения информационной безопасности**

**2.3.2. Положения**

**а) Положение Обучению и повышению квалификации Организации** - Описывает общие принципы и подходы к обучению работников по обеспечению информационной безопасности в Организации.

**Приложение №8. Положение о обучение работников Организации по информационной** **безопасности**

**б) Положение о службе безопасности** - Устанавливает структуру и задачи отдела безопасности, его права и обязанности.

**Приложение №9. Положение о службе безопасности**

**в) Положение о реагировании на инциденты безопасности** - Определяет процесс реагирования на инциденты безопасности и обязанности участников этого процесса.

**Приложение №10. Положение о реагировании на инциденты (информационной) безопасности.**

**г.)** **Положение о технической инфраструктуре и системах для обеспечения информационной безопасности Организации.**

В рамках настоящего положения описывается весь комплекс технических средств, задействованных для обеспечения информационной безопасности в организации. Ключевые элементы включают:

**Технический паспорт:**

Коммутационное оборудование - обеспечивает передачу данных между устройствами в сети.

Автоматизированные рабочие места - включают компьютеры и периферийные устройства, настроенные для выполнения специфических задач сотрудников.

Серверы - мощные компьютеры, предназначенные для обработки запросов и предоставления ресурсов в сети.

Системы контроля и управления доступом - технологии для ограничения и контроля доступа к физическим и информационным ресурсам.

Системы пожаротушения и пожарной сигнализации - автоматизированные системы для обнаружения и ликвидации огненных очагов.

Системы видеонаблюдения - оборудование для мониторинга и записи видео в целях безопасности.

Системы контроля микроклимата и вентиляции - обеспечивают оптимальные условия для работы технического оборудования и комфорта сотрудников.

Системы связи - включают телефонию, интернет и другие средства коммуникации.

Системы оповещения - используются для информирования сотрудников о чрезвычайных ситуациях.

Инструменты для сбора, анализа профилактирования и реагирования на события кибербезопасности (SIEM) - программные решения для мониторинга, анализа и реагирования на инциденты безопасности**.**

Приложение № 11 **Положение о технической инфраструктуре и системах для обеспечения информационной безопасности Организации**

**2.3.3. Стратегии**

а) **Стратегия развития информационной безопасности** - Определяет долгосрочные цели и мероприятия по улучшению информационной безопасности.

**Приложение №12**. **Стратегия развития информационной безопасности**

б) **Стратегия защиты критической информационной инфраструктуры** - Разрабатывает подходы к защите ключевых информационных активов, имеющих критическое значение для функционирования организации.

**Приложение №13 Стратегия защиты критической информационной инфраструктуры**

в) **Стратегия управления цифровыми рисками** - Устанавливает методы идентификации, анализа и минимизации рисков, связанных с цифровыми технологиями.

**Приложение №14. Стратегия управления цифровыми рисками.**

г) **Стратегия импортозамещения** - Планы по замене иностранных технологий на отечественные аналоги в рамках укрепления технологической независимости.

**Приложение №15.** **Стратегия импортозамещения.**

1. **Организационная структура по обеспечению информационной безопасности в Организации.**

Для организация эффективного построения и поддержание информационной безопасности в Организации нужно слаженная работа всех подразделений Организации и привлекаемых сторонних организаций.

**3.1. Руководитель организации**

Обязанности в сфере информационной безопасности:

Определяет, утверждает и контролирует выполнение политик, положений и стратегий в сфере информационной безопасности.

Несет ответственность за защиту информационных активов организации.

Утверждает бюджеты в сферу информационной безопасности.

**3.2. Заместитель руководителя организации по информационной безопасности.**

Непосредственный организатор защиты информации в Организации.

* + 1. **Положение о Заместитель руководителя организации по информационной безопасности.**

Положение о Заместитель руководителя организации по информационной безопасности определяет его роль, функции, обязанности и полномочия, связанные с управлением и координацией деятельности по обеспечению безопасности информации в организации, а также регулирует процедуры взаимодействия с другими отделами для эффективной реализации политик и стандартов информационной безопасности

**Приложение № 16.** **Положение о Заместитель руководителя организации по информационной безопасности.**

**3.2.2. Служебные обязанности Заместитель руководителя организации по информационной безопасности.**

Заместитель руководителя по информационной безопасности отвечает за разработки, согласование, утверждение и контроль политик, положений и стратегий в Организации в сфере информационной безопасности, координацию мер по защите данных и управление реагированием на инциденты безопасности

**Приложение № 17. Служебные обязанности Заместитель руководителя организации по информационной безопасности.**

**3.2. Отдел по обеспечению информационной безопасность Организации.**

* + 1. **Положение Отдел по обеспечению информационной безопасность Организации.**

Положение об отделе информационной безопасности определяет его структуру, функции, обязанности и полномочия, связанные с управлением и координацией деятельности по обеспечению безопасности информации и защите от киберугроз в организации.

Документ устанавливает методы и процессы, направленные на эффективную реализацию политик и стандартов информационной безопасности, а также регламентирует взаимодействие отдела с другими подразделениями организации для комплексного подхода к защите информационных ресурсов и предотвращению кибератак.

**Приложение № 18. Положение Отдел по обеспечению информационной безопасность Организации.**

* + 1. **Обязанности Специалистов по информационной безопасности**

3.2.2. 1. **Аудит и контроль соответствия**:

* Ответственный за проведение внутренних и внешних аудитов.
* Мониторинг соблюдения политик и стандартов ИБ в организации.

3.2.2.2. **Реагирование на инциденты безопасности**:

* Команда быстрого реагирования на инциденты ИБ.
* Анализ инцидентов и разработка мер по предотвращению повторения.

3.2.2.3. **Техническое обеспечение и защита инфраструктуры**:

* Обеспечение безопасности серверов, сетей и рабочих станций.
* Развертывание и настройка средств защиты, таких как антивирусы, фаерволы и системы обнаружения вторжений.

3.2.2.4.**Управление доступом и идентификация**:

* Контроль за системами управления доступом к ресурсам и данным.
* Поддержка и обновление систем идентификации и аутентификации.

3.2.2.5. . **Обучение и повышение осведомленности**:

* Разработка и проведение тренингов по ИБ для сотрудников.
* Информирование персонала о текущих угрозах и мерах защиты.

3.2.3.  **Положение о привлечении внешними подрядчиками по информационной безопасности"**

Положение о привлечении внешних организаций для мероприятий по информационной безопасности устанавливает процедуры отбора и сотрудничества с подрядчиками, специализирующимися на обнаружении и устранении киберугроз. Оно включает критерии квалификации подрядчиков, условия договоров, и методы контроля выполнения работ. Также определяется порядок взаимодействия между организацией и подрядчиками, включая обеспечение безопасности передаваемой информации. Положение регламентирует мониторинг исполнения и эффективность привлеченных ресурсов. Документ гарантирует соблюдение конфиденциальности и соответствие действий требованиям законодательства по защите данных.

**Приложение № 19.** **Положение о привлечении внешними подрядчиками по информационной безопасности"**

* 1. **Положение It отдела по обеспечению информационной безопасность Организации.**

Данное положение IT отдел по обеспечению том числе и информационной безопасности определяет действия по настройке и поддержанию безопасности информационных систем организации. Отдел отвечает за обновление защитных мер, мониторинг сетевых активностей и управление доступом к ресурсам. Также IT отдел участвует в реагировании на инциденты безопасности и восстановлении систем.

**Приложение № 20. Положение It отдела по обеспечению информационной безопасность**

* 1. **Служба главного инженера**

**а) Обеспечение электроснабжения** - поддержание надежной и стабильной работы всех систем питания, необходимых для функционирования серверов и другого критически важного оборудования.

**б) Освещение и отопление** - гарантия того, что все помещения, содержащие информационные системы, оборудованы адекватным освещением и поддержанием температурного режима, что особенно важно для серверных.

**в) Системы контроля и управления доступом (СКУД)** - разработка и реализация мер по контролю доступа к помещениям с критической информацией для предотвращения несанкционированного доступа.

**г) Видеонаблюдение** - установка и мониторинг систем видеонаблюдения для обеспечения визуального контроля за безопасностью объектов информационной инфраструктуры.

**д) Надежные двери и запорные устройства** - обеспечение защиты физических входов в помещения, содержащие информационные системы, использование сертифицированных замков и запорных систем.

**ж) Антивандальные меры** - защита от физического повреждения оборудования и информационных носителей.

**з) Системы противопожарной защиты** - обеспечение наличия и функционирования систем пожаротушения и сигнализации для предотвращения и быстрого реагирования на возможные пожары.

**и) Системы кондиционирования и вентиляции** - поддержание оптимального климата в помещениях с оборудованием для предотвращения перегрева и повреждения компонентов.

**к) Техническое обслуживание и аудит** - регулярная проверка и обслуживание всех инженерных систем и оборудования для гарантии их исправного состояния и соответствия современным требованиям безопасности.

* 1. **Отдел АХО**

а) **Обслуживание зданий и сооружений** - Обеспечивает техническое состояние и безопасность инфраструктуры организации, включая регулярные осмотры и ремонтные работы.

б) Организация **рабочих мест** - Гарантирует установку и расположение рабочих мест в соответствии с требованиями безопасности и эргономики, минимизируя риск несанкционированного доступа и повышая общую безопасность персонала.

в) Безопасность **и санитария** - Поддерживает чистоту и порядок в помещениях, следит за соблюдением санитарно-гигиенических норм и проводит необходимые дезинфекционные мероприятия для предотвращения распространения инфекционных заболеваний, что косвенно способствует поддержанию здорового и безопасного рабочего пространства.

* 1. **Служба безопасности.**

**Строгое соблюдение Положение об охране.**

**3.7. Ответственность по защите информации работников Организации**

Приложение № Ответственность

Заключение.