|  |  |  |
| --- | --- | --- |
| **ЧАСТНОЕ ТЕХНИЧЕСКОЕ ЗАДАНИЕ**  **на создание системы защиты информации Медицинской системы**  На 74 листах | | |
|  |  |  |
|  |  |  |

Содержание

[1 Введение 3](#_Toc162304049)

[1.1 О документе 3](#_Toc162304050)

[2 Общие сведения 4](#_Toc162304051)

[2.1 Наименование системы 4](#_Toc162304052)

[2.2 Цели и задачи создания СЗИ 4](#_Toc162304053)

[2.3 Наименование заказчика и разработчика системы 4](#_Toc162304054)

[2.4 Нормативно-технические документы 4](#_Toc162304055)

[2.5 Этапы работ 6](#_Toc162304056)

[3 Описание объекта защиты 8](#_Toc162304057)

[3.1 Назначение и основные задачи 8](#_Toc162304058)

[3.2 Классификация медицинской системы 8](#_Toc162304059)

[3.3 Состав обрабатываемой информации 8](#_Toc162304060)

[3.4 Функциональная архитектура медицинской системы 8](#_Toc162304061)

[3.5 Категории и типы доступа к информационным ресурсам и техническим средствам медицинской системы 8](#_Toc162304062)

[4 Требования к СЗИ 9](#_Toc162304063)

[4.1 Требования к СЗИ в целом 9](#_Toc162304064)

[4.2 Требования к структуре СЗИ 9](#_Toc162304065)

[4.3 Требования к функциям СЗИ 9](#_Toc162304066)

[4.4 Требования к средствам защиты информации 61](#_Toc162304067)

[4.5 Требования к подсистемам СЗИ 62](#_Toc162304068)

[4.6 Требования к видам обеспечения 65](#_Toc162304069)

[5 Порядок контроля и приемки системы 67](#_Toc162304070)

[6 Порядок внесения изменений в техническое задание 68](#_Toc162304071)

[7 Требования к документированию 69](#_Toc162304072)

[8 Перечень принятых сокращений 70](#_Toc162304073)

# Введение

## О документе

Настоящий документ содержит частное техническое задание на создание системы защиты информации медицинской системы.

Формирование требований к системе защиты информации медицинской системы осуществляется на основе на основе категорий защищаемой информации, модели нарушителя и угроз безопасности информации в соответствии с положениями законодательных актов и нормативных документов уполномоченных федеральных органов исполнительной власти.

# Общие сведения

## Наименование системы

Полное наименование системы: Система защиты информации медицинской системы.

Краткое наименование системы: СЗИ.

## Цели и задачи создания СЗИ

Целью создания СЗИ является обеспечение защиты информации, обрабатываемой в медицинскую систему.

Организационные и технические меры защиты информации, реализуемые в рамках СЗИ, направлены на обеспечение:

* конфиденциальности (предотвращение неправомерного доступа, копирования, предоставления или распространения информации);
* целостности (предотвращение неправомерного уничтожения или модифицирования информации);
* доступности (предотвращение неправомерного блокирования информации).

Критериями оценки достижения поставленных целей по созданию СЗИ являются:

* нейтрализация актуальных угроз безопасности информации;
* соответствие медицинской системы требованиям по обеспечению безопасности информации, установленным законодательством Российской Федерации и нормативными правовыми актами;
* выполнение требований настоящего частного технического задания.

## Наименование заказчика и разработчика системы

Заказчик: АО «неКУЛИКОВА» (далее – Заказчик)

Юридический адрес: 127051, г. Москва, Цветной б-р, д. 30, корпус 2

Исполнитель: ФГУП «НПП «точноКУЛИКОВА» (далее – Исполнитель).

## Нормативно-технические документы

При разработке настоящего ЧТЗ использовалась следующая нормативно-правовая и методическая документация:

* Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
* Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
* Постановление Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
* Методический документ «Методика оценки угроз безопасности информации» (утвержден ФСТЭК России 05.02.2021);
* «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности» (утверждены руководством 8 Центра ФСБ России 31 марта 2015 года № 149/7/2/6-432);
* Приказ ФСТЭК от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
* «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных правительством российской федерации требований к защите персональных данных для каждого из уровней защищенности» (утверждены ФСБ России 10 июля 2014 г. N 378).

## Этапы работ

Состав и содержание работ по созданию системы защиты информации медицинской системы приведены в таблице (Таблица 1).

Таблица 1 – Состав и содержание работ по созданию СЗИ

| Наименование работ | Результат выполнения работ |
| --- | --- |
| Определение требований к системе защиты информации | * Акт категорирования медицинской системы * Модель угроз и модель нарушителя безопасности информации; * Частное техническое задание на создание системы защиты информации. |
| Разработка организационно-распорядительной документации для системы защиты информации | Комплект организационно-распорядительной документации |
| Разработка системы защиты информации | Комплект документов технического проекта СЗИ:   * Ведомость технического проекта на систему защиты информации; * Пояснительная записка к техническому проекту на систему защиты информации; * Схема структурная комплекса технических средств; * Ведомость покупных изделий. |
| Внедрение системы защиты информации | * Протокол приемочных испытаний; * Акт перевода системы в промышленную эксплуатацию; * Проект технического паспорта информационной системы. |
| Аттестационные испытания медицинской системы | * Программа и методики аттестационных испытаний; * Протокол аттестационных испытаний; * Заключение по результатам аттестационных испытаний; * Аттестат соответствия требованиям защиты информации (в случае отсутствия замечаний в заключении по результатам аттестационных испытаний). |

# Описание объекта защиты

Медицинская система содержит чувствительную информацию о пациентах, медицинских процедурах, лекарствах и прочих данных, требующих особой защиты от несанкционированного доступа и утечки.

## Назначение и основные задачи

Назначение:

Медицинская информационная система (МИС) предназначена для автоматизированной обработки медицинских данных пациентов с целью обеспечения безопасности информации в медицинской сфере.

Основные задачи:

1. Управление медицинскими данными: обеспечение хранения, передачи и анализа информации о пациентах, диагнозах, лечении и результатах обследований.

2. Обеспечение безопасности данных: защита от несанкционированного доступа к медицинской информации, предотвращение утечек и сохранение конфиденциальности пациентов.

3. Автоматизация процессов: упрощение работы медицинского персонала за счет автоматизации записей, отчетности, назначений лекарств и процедур.

4. Повышение качества медицинской помощи: обеспечение доступа к актуальным медицинским данным, улучшение координации между специалистами и оптимизация процессов диагностики и лечения.

5. Мониторинг и аналитика: сбор и анализ данных для выявления тенденций заболеваемости, эффективности лечения, оптимизации ресурсов и принятия информированных решений в области здравоохранения.

6. Интеграция с другими системами: обеспечение взаимодействия МИС с другими информационными системами в медицинском учреждении (лабораториями, фармацией, страховыми компаниями и т.д.) для обмена данными и согласованной работы..

## Классификация медицинской системы

В соответствии с актом классификации информационной системы обрабатывающей ПДн, класс медицинской информационной системы — УЗ2.

## Состав обрабатываемой информации

1. ФИО пациента.

2. Дата рождения.

3. Адрес проживания.

4. Контактная информация (телефон, электронная почта).

5. Номер медицинского полиса.

6. Результаты анализов и обследований.

7. Диагнозы и история болезни.

8. Информация о лечении и назначенных препаратах.

9. Данные о визитах к врачу (дата, время, причина обращения).

10. Интимная информация о здоровье пациента (сексуальная ориентация, ВИЧ-статус).

## Функциональная архитектура медицинской системы

Медицинская информационная система (МИС) представляет собой клиент-серверную информационную систему. Она состоит из серверов баз данных, клиентских приложений, сетевого оборудования и систем мониторинга безопасности.

## Категории и типы доступа к информационным ресурсам и техническим средствам медицинской системы

Категории доступа:

1. Администраторы;
2. Врачи;
3. Медсестры;
4. пациенты.

Типы доступа:

1. Чтение;
2. Запись;
3. Исполнение.

Режим работы пользователей в медицинской информационной системе (МИС): многопользовательский с разными правами доступа.

Пользователи подключаются к серверам МИС посредством веб-браузера, установленного на рабочем месте пользователя (АРМ), с использованием протокола HTTPS по каналам связи сети "Интернет".

# Требования к СЗИ

## Требования к СЗИ в целом

СЗИ медицинской системы должна обеспечивать целостность, конфиденциальность и доступность данных, обрабатываемых в медицинской системы, за счет нейтрализации актуальных угроз безопасности информации.

СЗИ должна обеспечивать:

* реализацию организационных и технических мер по обеспечению безопасности персональных данных, определенных Приказом ФСБ России № 378 для третьего уровня защищенности персональных данных;
* Приказ ФСТЭК от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
* нейтрализацию актуальных угроз безопасности обрабатываемой информации.

При использовании СКЗИ в целях решения задач обеспечения безопасности информации, должны выполняться технические и организационные меры обеспечения безопасности для СКЗИ, предъявляемые ФСБ России.

## Требования к структуре СЗИ

В рамках создания СЗИ медицинской системы должны быть реализованы следующие меры защиты информации:

* технические меры, представляющие собой комплекс установленных и настроенных средств защиты, отвечающих установленным требованиям, а также направленных на нейтрализацию актуальных угроз безопасности;
* организационные меры, представляющие собой комплекс организационных и методических мероприятий по обеспечению безопасности информации.

Технические средства в составе СЗИ медицинской системы должны обеспечивать реализацию технических мер, предусмотренных требованиями законодательства в области защиты информации.

## Требования к функциям СЗИ

### Требования к перечню мер защиты информации

Согласно Приказу ФСТЭК от 18 февраля 2013 №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» выбор мер по обеспечению безопасности информации включает:

* определение базового набора мер по обеспечению безопасности информации для установленного уровня защищенности персональных данных и установленного класса защищенности информационной системы;
* адаптацию базового набора мер по обеспечению безопасности персональных данных с учетом структурно-функциональных характеристик информационной системы, информационных технологий, особенностей функционирования информационной системы (в том числе исключение из базового набора мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе);
* уточнение адаптированного базового набора мер по обеспечению безопасности информации с учетом не выбранных ранее мер, в результате чего определяются меры по обеспечению безопасности информации, направленные на нейтрализацию всех актуальных угроз безопасности для конкретной информационной системы;
* дополнение уточненного адаптированного базового набора мер по обеспечению безопасности персональных данных мерами, обеспечивающими выполнение требований о защите информации, установленными иными нормативными правовыми актами в области защиты информации, в том числе в области защиты персональных данных.

### Определение адаптированного базового набора мер защиты информации

СЗИ медицинской системы должна обеспечить реализацию мер безопасности для 2 класса защищенности информационной системы при их обработке в информационной системе.

Базовый набор мер защиты информации, выбранный в соответствии с классом защищенности медицинской системы, подлежит адаптации применительно к структурно-функциональным характеристикам и особенностям функционирования информационной системы, уточнению в зависимости от угроз безопасности информации и при необходимости дополнению мерами защиты информации.

Адаптированный базовый набор мер для СЗИ медицинской системы представлен в Таблице (Таблица 2).

Таблица 2 – Адаптированный базовый набор мер защиты информации в медицинской системе

| **Мера** | **Содержание мер по обеспечению безопасности персональных данных** | **Базовый перечень для УЗ2** | **Адаптированный перечень** |
| --- | --- | --- | --- |
| ИАФ.1 | Идентификация и аутентификация пользователей, являющихся работниками оператора | + | + |
| ИАФ.2 | Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных | + | + |
| ИАФ.3 | Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов | + | Неприменимо.  ИСПДН предполагает работу в закрытых сетях, где доступ к данным осуществляется через проводные каналы связи. |
| ИАФ.4 | Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации | + | + |
| ИАФ.5 | Защита обратной связи при вводе аутентификационной информации | + | + |
| ИАФ.6 | Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей) | + | Неприменимо.  ИСПДН требует строгого контроля доступа к данным и исключения возможности несанкционированного доступа. Технологии беспроводного доступа могут создать риски безопасности, такие как возможность перехвата данных или несанкционированного подключения к сети. |
| УПД.1 | Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей | + | + |
| УПД.2 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа | + | + |
| УПД.3 | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами | + | Неприменимо.  ИСПДН требует строгого контроля доступа к данным и исключения возможности несанкционированного доступа. Технологии беспроводного доступа могут создать риски безопасности, такие как возможность перехвата данных или несанкционированного подключения к сети. |
| УПД.4 | Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы | + | + |
| УПД.5 | Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы | + | + |
| УПД.6 | Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) | + | + |
| УПД.7 | Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры по обеспечению безопасности персональных данных, и о необходимости соблюдения установленных оператором правил обработки персональных данных |  |  |
| УПД.8 | Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему |  |  |
| УПД.9 | Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы |  |  |
| УПД.10 | Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу | + | + |
| УПД.11 | Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации | + | + |
| УПД.12 | Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки |  |  |
| УПД.13 | Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети | + | + |
| УПД.14 | Регламентация и контроль использования в информационной системе технологий беспроводного доступа | + | + |
| УПД.15 | Регламентация и контроль использования в информационной системе мобильных технических средств | + | + |
| УПД.16 | Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) | + | + |
| УПД.17 | Обеспечение доверенной загрузки средств вычислительной техники | + | + |
| ОПС.1 | Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения |  |  |
| ОПС.2 | Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения | + | + |
| ОПС.3 | Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов |  | + |
| ОПС.4 | Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов |  | + |
| ЗНИ.1 | Учет машинных носителей персональных данных | + | + |
| ЗНИ.2 | Управление доступом к машинным носителям персональных данных | + | + |
| ЗНИ.3 | Контроль перемещения машинных носителей персональных данных за пределы контролируемой зоны |  |  |
| ЗНИ.4 | Исключение возможности несанкционированного ознакомления с содержанием персональных данных, хранящихся на машинных носителях, и (или) использования носителей персональных данных в иных информационных системах |  |  |
| ЗНИ.5 | Контроль использования интерфейсов ввода (вывода) информации на машинные носители персональных данных |  |  |
| ЗНИ.6 | Контроль ввода (вывода) информации на машинные носители персональных данных |  |  |
| ЗНИ.7 | Контроль подключения машинных носителей персональных данных |  |  |
| ЗНИ.8 | Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания | + | + |
| РСБ.1 | Определение событий безопасности, подлежащих регистрации, и сроков их хранения | + | + |
| РСБ.2 | Определение состава и содержания информации о событиях безопасности, подлежащих регистрации | + | + |
| РСБ.3 | Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения | + | + |
| РСБ.4 | Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти |  |  |
| РСБ.5 | Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них | + | + |
| РСБ.6 | Генерирование временных меток и (или) синхронизация системного времени в информационной системе |  |  |
| РСБ.7 | Защита информации о событиях безопасности | + | + |
| АВЗ.1 | Реализация антивирусной защиты | + | + |
| АВЗ.2 | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) | + | + |
| СОВ.1 | Обнаружение вторжений | + | + |
| СОВ.2 | Обновление базы решающих правил | + | + |
| АНЗ.1 | Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей | + | + |
| АНЗ.2 | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации | + | + |
| АНЗ.3 | Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации | + | + |
| АНЗ.4 | Контроль состава технических средств, программного обеспечения и средств защиты информации | + | + |
| АНЗ.5 | Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе | + | + |
| ОЦЛ.1 | Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации | + | + |
| ОЦЛ.2 | Контроль целостности персональных данных, содержащихся в базах данных информационной системы |  |  |
| ОЦЛ.3 | Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций |  |  |
| ОЦЛ.4 | Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама) | + | + |
| ОЦЛ.5 | Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и (или) контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из информационной системы |  |  |
| ОЦЛ.6 | Ограничение прав пользователей по вводу информации в информационную систему |  |  |
| ОЦЛ.7 | Контроль точности, полноты и правильности данных, вводимых в информационную систему |  |  |
| ОЦЛ.8 | Контроль ошибочных действий пользователей по вводу и (или) передаче персональных данных и предупреждение пользователей об ошибочных действиях |  |  |
| ОДТ.1 | Использование отказоустойчивых технических средств |  |  |
| ОДТ.2 | Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы |  |  |
| ОДТ.3 | Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование |  |  |
| ОДТ.4 | Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных | + | + |
| ОДТ.5 | Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала | + | + |
| ЗСВ.1 | Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации | + | + |
| ЗСВ.2 | Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин | + | + |
| ЗСВ.3 | Регистрация событий безопасности в виртуальной инфраструктуре | + | + |
| ЗСВ.4 | Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры |  |  |
| ЗСВ.5 | Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией |  |  |
| ЗСВ.6 | Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных | + | + |
| ЗСВ.7 | Контроль целостности виртуальной инфраструктуры и ее конфигураций | + | + |
| ЗСВ.8 | Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры | + | + |
| ЗСВ.9 | Реализация и управление антивирусной защитой в виртуальной инфраструктуре | + | + |
| ЗСВ.10 | Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей | + | Неприменимо.  ИСПДН требует строгого контроля доступа к данным и исключения возможности несанкционированного доступа. Изолирование виртуальной инфраструктуры с помощью сегментации может быть сложным и затратным процессом, особенно в случае медицинской информационной системы (МИС) |
| ЗТС.1 | Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам |  |  |
| ЗТС.2 | Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования |  |  |
| ЗТС.3 | Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены | + | Неприменимо.  ИСПДН требует строгого контроля доступа к данным и исключения возможности несанкционированного доступа. Постоянный контроль и ограничение физического доступа к техническим средствам и информационным ресурсам может затруднить работу медицинского персонала и замедлить процессы обслуживания пациентов. |
| ЗТС.4 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр | + | Неприменимо.  ИСПДН требует строгого контроля доступа к данным и защиты информации от несанкционированного доступа. Использование технологий беспроводного доступа может создать уязвимости в системе безопасности, так как данные могут быть перехвачены или скомпрометированы через беспроводные каналы связи. |
| ЗТС.5 | Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов) |  |  |
| ЗИС.1 | Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты персональных данных, функций по обработке персональных данных и иных функций информационной системы |  |  |
| ЗИС.2 | Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом |  |  |
| ЗИС.3 | Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи | + | + |
| ЗИС.4 | Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации) |  |  |
| ЗИС.5 | Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств |  |  |
| ЗИС.6 | Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с персональными данными, при обмене ими с иными информационными системами |  |  |
| ЗИС.7 | Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода |  |  |
| ЗИС.8 | Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи |  |  |
| ЗИС.9 | Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации |  |  |
| ЗИС.10 | Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам |  |  |
| ЗИС.11 | Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов | + | + |
| ЗИС.12 | Исключение возможности отрицания пользователем факта отправки персональных данных другому пользователю |  |  |
| ЗИС.13 | Исключение возможности отрицания пользователем факта получения персональных данных от другого пользователя |  |  |
| ЗИС.14 | Использование устройств терминального доступа для обработки персональных данных |  |  |
| ЗИС.15 | Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных | + | + |
| ЗИС.16 | Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер или внутри разрешенных сетевых протоколов |  |  |
| ЗИС.17 | Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы | + | + |
| ЗИС.18 | Обеспечение загрузки и исполнения программного обеспечения с машинных носителей персональных данных, доступных только для чтения, и контроль целостности данного программного обеспечения |  |  |
| ЗИС.19 | Изоляция процессов (выполнение программ) в выделенной области памяти |  |  |
| ЗИС.20 | Защита беспроводных соединений, применяемых в информационной системе | + | + |
| ИНЦ.1 | Определение лиц, ответственных за выявление инцидентов и реагирование на них | + | + |
| ИНЦ.2 | Обнаружение, идентификация и регистрация инцидентов | + | Не применимо.  ИСПДН недостаточно понимание процессов и методов обнаружения инцидентов; отсутствие соответствующих процедур и политик безопасности; недостаточное финансирование и ресурсы; технические ограничения. |
| ИНЦ.3 | Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами | + | Неприменимо.  ИСПДН необходимо обеспечить высокий уровень конфиденциальности пациентов, соответствие регуляторным требованиям и избежать негативного воздействия на доверие пациентов. |
| ИНЦ.4 | Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий | + | Неприменимо.  ИСПДН требует обеспечения высокой степени защиты данных, а беспроводные технологии могут быть уязвимыми для несанкционированного доступа и атак. |
| ИНЦ.5 | Принятие мер по устранению последствий инцидентов | + | Неприменимо.  ИСПДН требует превентивного подхода к защите данных, в то время как технологии беспроводного доступа ориентированы на реакцию на события. |
| ИНЦ.6 | Планирование и принятие мер по предотвращению повторного возникновения инцидентов | + | + |
| УКФ.1 | Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных | + | + |
| УКФ.2 | Управление изменениями конфигурации информационной системы и системы защиты персональных данных | + | + |
| УКФ.3 | Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных | + | + |
| УКФ.4 | Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных | + | + |

### Уточнение адаптированного базового набора мер защиты информации

Уточнение адаптированного базового набора мер защиты производится путём сопоставления адаптированного базового набора мер с актуальными угрозами (см. – Модель угроз безопасности информации).

В случае, если адаптированный базовый набор мер защиты информации не обеспечивает блокирование (нейтрализацию) всех угроз безопасности информации, в него дополнительно включаются иные, предусмотренные Приказами ФСТЭК России № 21, и не выбранные ранее меры, для возможности нейтрализовать все актуальные угрозы безопасности информации.

Выбор мер по нейтрализации актуальных угроз безопасности информации для медицинской системы представлен в таблице (Таблица 3).

Таблица 3 – Меры по нейтрализации актуальных угроз безопасности информации

| **Угроза (группа угроз)** | **Угрозы, входящие в группу** | **Меры по нейтрализации** |
| --- | --- | --- |
| Угрозы внедрения вредоносного кода | УБИ.006, УБИ.041, УБИ.042, УБИ.044, УБИ.073, УБИ.145, УБИ.167, УБИ.172, УБИ.186, УБИ.188, УБИ.189, УБИ.190, УБИ.191, УБИ.192, УБИ.198, УБИ.217 | 1. Установка антивирусного программного обеспечения.  2. Ограничение прав доступа.  3. Мониторинг сетевого трафика.  4. Обновление программного обеспечения.  5. Обучение персонала.  6. Резервное копирование данных.  7. Проведение аудитов безопасности.  8. Использование белых списков. |
| Угрозы воздействия на BIOS/UEFI | УБИ.009, УБИ.032, УБИ.039, УБИ.045, УБИ.072, УБИ.123, УБИ.129, УБИ.144, УБИ.150, УБИ.154 | 1. Установка защиты паролем.  2. Включение Secure Boot.  3. Обновление BIOS/UEFI.  4. Физическая защита.  5. Мониторинг изменений.  6. Использование Trusted Platform Module (TPM).  7. Обучение персонала.  8. Резервное копирование конфигурации BIOS/UEFI. |
| Угрозы недоступности ПО | УБИ.022, УБИ.095, УБИ.109, УБИ.114, УБИ.152, УБИ.155, УБИ.166 | 1. Резервное копирование данных.  2. Использование отказоустойчивых решений.  3. Мониторинг доступности системы.  4. Обновление и патчи ПО.  5. Управление ресурсами.  6. Разработка плана восстановления после кризиса.  7. Обучение персонала.  8. Установка защиты от DDoS-атак. |
| Угрозы отказа в обслуживании на устройстве | УБИ.014, УБИ.022, УБИ.051, УБИ.059, УБИ.076, УБИ.121, УБИ.140, УБИ.143, УБИ.153, УБИ.155, УБИ.171, УБИ.173 | 1. Регулярное техническое обслуживание.  2. Мониторинг состояния оборудования.  3. Замена изношенных деталей.  4. Обучение персонала.  5. Разработка плана аварийного восстановления.  6. Резервирование оборудования.  7. Использование сертифицированных поставщиков.  8. Обновление программного обеспечения. |
| Угрозы блокирования (уничтожения) защищаемых данных | УБИ.091, УБИ.113, УБИ.152, УБИ.156, УБИ.158, УБИ.170, УБИ.205 | 1. Регулярное резервное копирование данных.  2. Использование защиты от вредоносного ПО.  3. Установка системы мониторинга безопасности.  4. Обучение персонала по безопасности данных.  5. Установка системы резервирования данных.  6. Шифрование данных.  7. Управление доступом к данным.  8. Аудит безопасности данных. |
| Угрозы несанкционированного ознакомления с защищаемой информацией и (или) несанкционированного копирования или распространения защищаемых данных | УБИ.003, УБИ.015, УБИ.016, УБИ.017, УБИ.028, УБИ.034, УБИ.037, УБИ.067, УБИ.071, УБИ.088, УБИ.093, УБИ.111, УБИ.115, УБИ.151, УБИ.156, УБИ.159, УБИ.168, УБИ.174, УБИ.175, УБИ.200, УБИ.203, УБИ.209 | 1. Шифрование данных.  2. Управление доступом.  3. Мониторинг активности пользователей.  4. Обучение персонала по безопасности данных.  5. Использование системы аудита.  6. Физическая безопасность.  7. Регулярное обновление систем безопасности. |
| Угрозы несанкционированной модификации защищаемой информации | УБИ.027, УБИ.049, УБИ.124, УБИ.130, УБИ.179 | 1. Цифровая подпись.  2. Контроль целостности данных.  3. Разграничение доступа.  4. Журналирование событий.  5. Обучение персонала по безопасности.  6. Автоматизированные системы контроля доступа.  7. Обновление систем безопасности. |
| Угрозы внесения несанкционированных изменений в конфигурацию защищаемой системы | УБИ.012, УБИ.023, УБИ.025, УБИ.026, УБИ.061, УБИ.062, УБИ.063, УБИ.068, УБИ.073, УБИ.089, УБИ.090, УБИ.094, УБИ.102, УБИ.121, УБИ.149, УБИ.198, УБИ.211, УБИ.212 | 1. Установка механизмов контроля целостности.  2. Ограничение доступа к конфигурационным файлам.  3. Мониторинг изменений.  4. Использование цифровых подписей.  5. Регулярное обновление системы.  6. Обучение персонала.  7. Резервное копирование конфигурационных данных. |
| Угрозы нецелевого использования ресурсов защищаемой системы | УБИ.171, УБИ.208 | 1. Мониторинг ресурсов.  2. Управление доступом.  3. Установка ограничений.  4. Автоматизация процессов.  5. Регулярное обновление и мониторинг.  6. Обучение персонала.  7. Журналирование событий. |
| Угрозы воздействия на СрЗИ | УБИ.003, УБИ.185, УБИ.187, УБИ.214 | 1. Шифрование данных.  2. Установка брандмауэра и системы обнаружения вторжений.  3. Регулярное обновление программного обеспечения.  4. Организация обучения персонала по безопасности информации.  5. Резервное копирование данных.  6. Мониторинг активности пользователей.  7. Установка антивирусного ПО. |
| Угрозы деструктивного воздействия на аппаратное обеспечение устройства | УБИ.113, УБИ.143 | 1. Физическая безопасность.  2. Резервное копирование данных.  3. Использование защиты от перенапряжений и скачков напряжения.  4. Регулярное техническое обслуживание.  5. Мониторинг температуры и влажности.  6. Обучение персонала по правилам эксплуатации оборудования. |
| Угрозы изменения конфигурации сети | УБИ.019, УБИ.069, УБИ.131 | 1. Управление доступом.  2. Аудит настроек сети.  3. Шифрование данных.  4. Резервное копирование конфигурации.  5. Обновление программного обеспечения.  6. Обучение персонала. |
| Угрозы несанкционированного доступа к аутентификационной информации | УБИ.008, УБИ.030, УБИ.074, УБИ.086, УБИ.123, УБИ.168, УБИ.174, УБИ.175, УБИ.181, УБИ.197, УБИ.201 | 1. Многофакторная аутентификация.  2. Строгая политика паролей.  3. Шифрование данных.  4. Мониторинг доступа.  5. Обучение персонала.  6. Регулярное обновление системы. |
| Угрозы сбора информации о защищаемой системе | УБИ.036, УБИ.037, УБИ.098, УБИ.099, УБИ.103, УБИ.104, УБИ.116, УБИ.132, УБИ.151 | 1. Шифрование данных.  2. Сегментация сети.  3. Мониторинг сетевой активности.  4. Обновление системы безопасности.  5. Обучение персонала.  6. Управление доступом. |
| Угрозы повышения привилегий | УБИ.007, УБИ.031, УБИ.100, УБИ.117, УБИ.118, УБИ.122, УБИ.162, УБИ.163, УБИ.209 | 1. Принцип наименьших привилегий.  2. Многоуровневая аутентификация.  3. Мониторинг активности пользователей.  4. Регулярное обновление системы.  5. Обучение персонала.  6. Журналирование и аудит. |
| Угрозы подмены доверенных пользователей | УБИ.127, УБИ.128 | 1. Идентификация и аутентификация.  2. Управление доступом.  3. Мониторинг активности.  4. Шифрование данных.  5. Обучение сотрудников.  6. Резервное копирование данных. |
| Угрозы со стороны смежных систем | УБИ.215 | 1. Сегментация сети.  2. Установка брандмауэров.  3. Шифрование данных.  4. Мониторинг активности.  5. Обновление программного обеспечения.  6. Проведение аудита безопасности.  7. Обучение персонала. |
| Угрозы использования отладочных механизмов | УБИ.169 | 1. Отключение отладочных механизмов.  2. Управление доступом.  3. Мониторинг активности.  4. Шифрование данных.  5. Обучение персонала.  6. Обновление и патчи.  7. Резервное копирование данных. |
| Угрозы несанкционированного доступа в виртуальной среде | УБИ.044, УБИ.078, УБИ.079, УБИ.080, УБИ.084, УБИ.085 | 1. Установка многофакторной аутентификации.  2. Сегментация сети.  3. Шифрование данных.  4. Регулярное обновление ПО и патчей.  5. Мониторинг сетевой активности.  6. Обучение персонала.  7. Управление доступом.  8. Резервное копирование данных. |
| Угрозы деструктивного воздействия на виртуальную среду | УБИ.010, УБИ.046, УБИ.048, УБИ.076, УБИ.077, УБИ.084, УБИ.108, УБИ.119, УБИ.120 | 1. Регулярное резервное копирование данных.  2. Установка систем мониторинга и обнаружения инцидентов.  3. Использование антивирусного ПО и брандмауэров.  4. Обучение сотрудников безопасности информации.  5. Установка систем резервирования электропитания.  6. Аудит безопасности системы.  7. Разработка и реализация плана восстановления после инцидента. |
| Угрозы мобильным устройствам | УБИ.184 | 1. Установка политики использования мобильных устройств.  2. Шифрование данных на мобильных устройствах.  3. Установка удаленного управления устройствами.  4. Обновление программного обеспечения и антивирусов.  5. Обучение сотрудников по безопасности мобильных устройств.  6. Мониторинг активности на мобильных устройствах.  7. Регулярные аудиты безопасности мобильных устройств. |
| Угрозы сбоя в работе обеспечивающих систем | УБИ.180 | 1. Резервное копирование данных.  2. Использование резервных источников питания.  3. Мониторинг состояния оборудования.  4. Регулярное обновление и техническое обслуживание оборудования.  5. Установка систем автоматизированного управления.  6. Обучение персонала по восстановлению работоспособности систем.  7. Планы действий при сбоях. |
| Угрозы сбоя в работе аппаратного и программного обеспечения | УБИ.165 | 1. Регулярное обновление программного обеспечения.  2. Установка антивирусного ПО.  3. Мониторинг работы оборудования.  4. Резервное копирование данных.  5. Обучение персонала по безопасности информации.  6. Физическая защита оборудования.  7. Планы аварийного восстановления. |
| Угрозы ошибочных действий | УБИ.177, УБИ.178 | 1. Обучение персонала.  2. Разделение доступа.  3. Использование двойной проверки.  4. Использование чек-листов и стандартов.  6. Обратная связь и анализ инцидентов.  7. Постоянное обновление процедур. |

Таким образом, адаптированный базовый набор мер для медицинской системы должен быть уточнён (дополнен) следующими мерами защиты, не включенными в базовый набор мер:

1. Мониторинг активности пользователей: Внедрить систему мониторинга активности пользователей в медицинской системе, которая позволит отслеживать действия сотрудников и выявлять подозрительную активность или несанкционированный доступ.

2. Шифрование данных: Обеспечить шифрование всех данных, хранящихся и передаваемых в медицинской системе, чтобы предотвратить утечку конфиденциальной информации и защитить данные от несанкционированного доступа.

3. Резервное копирование и восстановление данных: Регулярно создавать резервные копии данных медицинской системы и разработать план восстановления данных в случае аварийной ситуации или кибератаки, чтобы минимизировать потерю информации.

3. Обновление программного обеспечения: Проводить регулярное обновление программного обеспечения медицинской системы и её компонентов для закрытия уязвимостей и обеспечения безопасности данных.

4. Обучение пользователей по кибербезопасности: Проводить обучающие программы по кибербезопасности для всех пользователей медицинской системы, чтобы повысить осведомленность о возможных угрозах и улучшить практики безопасности.

5. Аудит безопасности: Проводить регулярные аудиты безопасности медицинской системы для выявления слабых мест, уязвимостей и потенциальных угроз, а также для проверки соответствия стандартам безопасности.

### Результаты определения состава мер по защите информации

Итоговый (дополненный уточненный адаптированный базовый) набор мер по защите информации медицинской системы с указанием средств защиты, с помощью которых выполняется реализация мер, приведен в таблица (Таблица 4).

Таблица 4 – Итоговый перечень мер по защите информации медицинской системы

| **Мера** | **Содержание** | **Способ реализации мер защиты** |
| --- | --- | --- |
| ИАФ.1 | Идентификация и аутентификация пользователей, являющихся работниками оператора | 1. Использование уникальных идентификаторов.  2. Сильные пароли.  3. Двухфакторная аутентификация.  4. Биометрическая идентификация.  5. Ограничение прав доступа.  6. Логирование действий пользователей.  7. Обучение персонала.  8. Регулярная проверка и обновление прав доступа. |
| ИАФ.2 | Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных | 1. Использование уникальных идентификаторов устройств.  2. Сертификаты и цифровые подписи.  3. Механизмы шифрования.  4. Блокировка и удаленное управление.  5. Сетевые механизмы безопасности.  6. Обновление программного обеспечения.  7. Мониторинг и обнаружение инцидентов.  8. Обучение пользователей. |
| ИАФ.4 | Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации | 1. Хранение средств аутентификации.  2. Выдача и инициализация средств аутентификации.  3. Блокирование средств аутентификации.  4. Принятие мер в случае утраты и (или) компрометации средств аутентификации.  5. Мониторинг и аудит.  6. Обучение и осведомленность пользователей. |
| ИАФ.5 | Защита обратной связи при вводе аутентификационной информации | 1. Шифрование трафика.  2. Многофакторная аутентификация.  3. Защита от перехвата и подмены данных.  4. Отображение маскированных символов.  5. Аудит ввода информации.  6. Обучение пользователей. |
| УПД.1 | Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей | 1. Создание политики управления учетными записями.  2. Развертывание системы управления доступом (IAM).  3. Установка строгих правил и процедур.  4. Регулярный мониторинг и аудит.  5. Обучение сотрудников. |
| УПД.2 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа | 1. Разработка матрицы доступа.  2. Внедрение системы управления доступом (IAM).  3. Применение дискреционного контроля доступа.  4. Использование ролевого управления доступом.  5. Установка правил и политик безопасности.  6. Обучение пользователей. |
| УПД.4 | Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы | 1. Определение ролей и полномочий.  2. Разработка матрицы доступа.  3. Внедрение системы управления доступом (IAM).  4. Применение принципа минимальных привилегий.  5. Аудит и мониторинг доступа.  6. Обучение и осведомление пользователей. |
| УПД.5 | Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы | 1. Анализ полномочий.  2. Создание политики безопасности.  3. Реализация принципа нулевого доверия.  4. Использование IAM системы.  5. Регулярный аудит прав доступа.  6. Обучение сотрудников.  7. Мониторинг и реагирование. |
| УПД.6 | Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) | 1. Настройка блокировки учетных записей.  2. Использование CAPTCHA.  3. Мониторинг журналов аудита.  4. Внедрение двухфакторной аутентификации.  5. Обучение пользователей.  6. Уведомление об аномальной активности.  7. Регулярное обновление ПО. |
| УПД.10 | Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу | 1. Установка времени бездействия.  2. Механизм отслеживания активности.  3. Блокирование сеанса.  4. Возможность блокирования по запросу.  5. Логирование действий. |
| УПД.11 | Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации | 1. Определение разрешенных действий.  2. Блокировка недоступных функций.  3. Интерфейс для ввода учетных данных.  4. Проверка учетных данных.  5. Логирование попыток доступа. |
| УПД.13 | Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети | 1. Идентификация и аутентификация.  2. Шифрование данных.  3. Управление доступом.  4. Мониторинг и регистрация.  5. Обновление и обучение. |
| УПД.14 | Регламентация и контроль использования в информационной системе технологий беспроводного доступа | 1. Политики и процедуры.  2. Аутентификация и шифрование.  3. Мониторинг и контроль.  4. Сегментация сети.  5. Обновление и обучение. |
| УПД.15 | Регламентация и контроль использования в информационной системе мобильных технических средств | 1. Политики и процедуры.  2. Управление устройствами.  3. Аутентификация и доступ.  4. Шифрование данных.  5. Обновление и мониторинг.  6. Обучение пользователей. |
| УПД.16 | Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) | 1. Оценка рисков.  2. Установление правил и политик.  3. Соглашения и контракты.  4. Механизмы защиты данных.  5. Мониторинг и аудит.  6. Обучение персонала. |
| УПД.17 | Обеспечение доверенной загрузки средств вычислительной техники | 1. Проверка целостности и подлинности загрузочного образа.  2. Использование безопасных загрузочных сред.  3. Защита BIOS и UEFI.  4. Ограничение доступа к загрузочным устройствам.  5. Обучение пользователей.  6. Мониторинг и аудит.  7. Регулярное обновление. |
| ОПС.2 | Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения | 1. Идентификация и классификация компонентов программного обеспечения.  2. Настройка параметров установки компонентов.  3. Контроль за установкой компонентов программного обеспечения.  4. Управление доступом к установке компонентов программного обеспечения.  5. Обучение сотрудников по правилам управления установкой.  6. Регулярное обновление и аудит безопасности. |
| ЗНИ.1 | Учет машинных носителей персональных данных | 1. Идентификация и классификация машинных носителей данных.  2. Физическая безопасность машинных носителей.  3. Шифрование данных на машинных носителях.  4. Управление доступом к машинным носителям.  5. Регулярное обновление и аудит политики безопасности.  6. Обучение сотрудников. |
| ЗНИ.2 | Управление доступом к машинным носителям персональных данных | 1. Разработка политики доступа.  2. Идентификация и аутентификация пользователей.  3. Установка привилегий доступа.  4. Мониторинг и аудит доступа.  5. Обучение сотрудников.  6. Регулярное обновление политики безопасности. |
| ЗНИ.8 | Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания | 1. Политика уничтожения данных.  2. Обучение сотрудников.  3. Использование специализированного оборудования.  4. Документирование процесса.  5. Контрольный аудит. |
| РСБ.1 | Определение событий безопасности, подлежащих регистрации, и сроков их хранения | 1. Анализ угроз и уязвимостей.  2. Определение критических событий.  3. Разработка политики регистрации событий.  4. Внедрение системы регистрации.  5. Обучение персонала.  6. Мониторинг и анализ данных. |
| РСБ.2 | Определение состава и содержания информации о событиях безопасности, подлежащих регистрации | 1. Анализ требований и стандартов.  2. Создание каталога событий безопасности.  3. Установление правил регистрации.  4. Интеграция с системой мониторинга.  5. Обучение персонала.  6. Аудит и контроль. |
| РСБ.3 | Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения | 1. Определение информации для сбора и хранения.  2. Разработка процесса сбора данных.  3. Установление времени хранения.  4. Защита данных.  5. Резервное копирование.  6. Мониторинг и анализ данных.  7. Обучение персонала. |
| РСБ.5 | Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них | 1. Настройка мониторинга.  2. Установка пороговых значений.  3. Реагирование на события.  4. Анализ и отчетность.  5. Обучение персонала. |
| РСБ.7 | Защита информации о событиях безопасности | 1. Настройка журналирования событий.  2. Шифрование журналов.  3. Установка прав доступа.  4. Резервное копирование журналов.  5. Мониторинг и анализ журналов.  6. Обучение персонала. |
| АВЗ.1 | Реализация антивирусной защиты | 1. Выбор надежного антивирусного ПО.  2. Установка и настройка антивирусного ПО.  3. Регулярные обновления.  4. План реагирования на инциденты.  5. Обучение персонала.  6. Мониторинг и анализ. |
| АВЗ.2 | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) | 1. Выбор и установка антивирусного ПО.  2. Настройка автоматических обновлений.  3. Планирование регулярных проверок.  4. Мониторинг процесса обновлений.  5. Обучение персонала.  6. Резервное копирование. |
| СОВ.1 | Обнаружение вторжений | 1. Установка системы мониторинга безопасности.  2. Настройка правил и оповещений.  3. Регулярное обновление базы данных угроз.  4. Анализ данных и реагирование.  5. Обучение персонала.  6. Аудит системы безопасности. |
| СОВ.2 | Обновление базы решающих правил | 1. Выбор системы управления доступом.  2. Создание базы решающих правил.  3. Регулярное обновление правил.  4. Автоматизация процесса обновления.  5. Мониторинг и анализ эффективности правил.  6. Обучение персонала. |
| АНЗ.1 | Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей | 1. Проведение регулярного сканирования уязвимостей.  2. Анализ результатов сканирования.  3. Планирование и приоритизация действий.  4. Оперативное устранение уязвимостей.  5. Мониторинг и повторное сканирование.  6. Обучение персонала. |
| АНЗ.2 | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации | 1. Создание плана обновлений.  2. Автоматизация процесса обновлений.  3. Мониторинг состояния обновлений.  4. Тестирование перед установкой.  5. Резервное копирование данных.  6. Обучение персонала.  7. Регулярное аудитирование процесса обновлений. |
| АНЗ.3 | Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации | 1. Создание системы мониторинга.  2. Установка агентов мониторинга.  3. Анализ данных мониторинга.  4. Реагирование на инциденты.  5. Обновление параметров настройки.  6. Обучение персонала.  7. Регулярное тестирование. |
| АНЗ.4 | Контроль состава технических средств, программного обеспечения и средств защиты информации | 1. Инвентаризация.  2. Документирование.  3. Мониторинг изменений.  4. Аудит безопасности.  5. Контроль доступа.  6. Обновление и патчи.  7. Обучение персонала. |
| АНЗ.5 | Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе | 1. Политика безопасности.  2. Сложные пароли.  3. Механизм авторизации.  4. Аудит аккаунтов.  5. Разграничение доступа.  6. Мониторинг доступа.  7. Обучение персонала.  8. Регулярные проверки. |
| ОЦЛ.1 | Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации | 1. Установка программного обеспечения из официальных и проверенных источников.  2. Регулярное обновление программного обеспечения.  3. Использование цифровых подписей.  4. Мониторинг целостности файлов.  5. Резервное копирование данных.  6. Обучение персонала.  7. Аудит и контроль доступа. |
| ОЦЛ.4 | Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама) | 1. Установка и настройка антивирусного программного обеспечения.  2. Использование фильтров спама на почтовых серверах.  3. Обучение сотрудников.  4. Мониторинг и анализ входящей почты.  5. Обновление программного обеспечения.  6. Резервное копирование данных. |
| ОДТ.4 | Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных | 1. Определение периодичности.  2. Выбор резервных носителей.  3. Настройка программного обеспечения.  4. Шифрование и защита данных.  5. Тестирование восстановления.  6. Мониторинг и аудит. |
| ОДТ.5 | Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала | 1. Установление временного интервала.  2. Регулярное резервное копирование.  3. Хранение резервных копий.  4. Документирование процедур восстановления.  5. Тестирование восстановления данных.  6. Мониторинг и аудит. |
| ЗСВ.1 | Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации | 1. Использование многофакторной аутентификации.  2. Установление строгих политик паролей.  3. Ограничение привилегий доступа.  4. Аудит и мониторинг доступа.  5. Обучение и осведомленность пользователей.  6. Регулярное обновление систем безопасности. |
| ЗСВ.2 | Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин | 1. Разделение доступа на роли и права.  2. Применение принципа минимальных привилегий.  3. Использование управления доступом на уровне объектов.  4. Автоматизация процессов управления доступом.  5. Мониторинг и аудит доступа.  6. Обучение и осведомленность пользователей. |
| ЗСВ.3 | Регистрация событий безопасности в виртуальной инфраструктуре | 1. Выбор подходящей системы регистрации событий.  2. Настройка мониторинга событий.  3. Установка правил и оповещений.  4. Хранение и анализ журналов.  5. Интеграция с другими системами безопасности.  6. Обучение персонала. |
| ЗСВ.6 | Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных | 1. Шифрование данных.  2. Управление доступом.  3. Мониторинг перемещения данных.  4. Аудит действий.  5. Ограничение перемещения.  6. Обучение персонала. |
| ЗСВ.7 | Контроль целостности виртуальной инфраструктуры и ее конфигураций | 1. Централизованное управление конфигурациями.  2. Использование систем мониторинга целостности.  3. Регулярное обновление и патчи.  4. Резервное копирование конфигураций.  5. Разделение обязанностей.  6. Аудит целостности. |
| ЗСВ.8 | Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры | 1. Планирование и создание резервных копий.  2. Автоматизация процесса резервного копирования.  3. Шифрование резервных копий.  4. Тестирование процесса восстановления.  5. Резервирование технических средств.  6. Мониторинг состояния технических средств.  7. Резервирование каналов связи. |
| ЗСВ.9 | Реализация и управление антивирусной защитой в виртуальной инфраструктуре | 1. Выбор антивирусного программного обеспечения.  2. Установка и настройка антивирусного ПО.  3. Регулярное обновление антивирусных баз данных.  4. Мониторинг и управление антивирусной защитой.  5. Обучение персонала.  6. Анализ инцидентов.  7. Регулярные аудиты безопасности. |
| ЗИС.3 | Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи | 1. Шифрование данных.  2. Использование виртуальных частных сетей (VPN).  3. Установка брандмауэров и антивирусов.  4. Аутентификация и авторизация.  5. Обучение персонала.  6. Регулярное обновление программного обеспечения.  7. Мониторинг и аудит безопасности. |
| ЗИС.11 | Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов | 1. Использование протокола TLS/SSL.  2. Использование цифровых сертификатов.  3. Настройка брандмауэра и IPS/IDS.  4. Механизмы аутентификации.  5. Мониторинг сетевого трафика.  6. Обновление программного обеспечения. |
| ЗИС.15 | Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных | 1. Создание резервной копии данных.  2. Шифрование данных.  3. Разграничение прав доступа.  4. Мониторинг активности.  5. Обновление программного обеспечения.  6. Обучение персонала. |
| ЗИС.17 | Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы | 1. Сегментирование сети.  2. Настройка брандмауэров.  3. Установка правил фильтрации.  4. Аутентификация и авторизация.  5. Мониторинг и аудит.  6. Обучение персонала.  7. Обновление систем. |
| ИНЦ.6 | Планирование и принятие мер по предотвращению повторного возникновения инцидентов | 1. Анализ инцидентов.  2. Разработка плана действий.  3. Внедрение мер безопасности.  4. Обучение персонала.  5. Мониторинг и аудит.  6. Проверка и корректировка. |
| УКФ.1 | Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных | 1. Определение ролей и ответственности.  2. Обучение персонала.  3. Установление контроля доступа.  4. Мониторинг и аудит.  5. Документирование.  6. Регулярная проверка. |
| УКФ.2 | Управление изменениями конфигурации информационной системы и системы защиты персональных данных | 1. Определение процесса управления изменениями.  2. Оценка рисков.  3. Плановая документация.  4. Тестирование.  5. Обратная связь.  6. Обучение персонала.  7. Мониторинг и аудит. |
| УКФ.3 | Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных | 1. Оценка рисков.  2. Анализ потенциального воздействия.  3. Согласование изменений.  4. Документирование.  5. Тестирование.  6. Обратная связь.  7. Обучение персонала.  8. Мониторинг и аудит. |
| УКФ.4 | Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных | 1. Определение формата документации.  2. Создание базы данных.  3. Внесение изменений в документацию.  4. Архивирование документов.  5. Доступ к документации.  6. Контроль доступа.  7. Регулярное обновление. |

## Требования к средствам защиты информации

Применяемые в СЗИ медицинской системы программные и программно-аппаратные средства защиты информации, должны быть обеспечены гарантийной и (или) технической поддержкой.

При реализации СЗИ медицинской системы должно использоваться только лицензионное программное обеспечение. В составе СЗИ медицинской системы должны применяться только серийно выпускаемые программные и аппаратные средства.

Должны применяться следующие СрЗИ:

* средства вычислительной техники не ниже 2 класса;
* средства защиты информации не ниже не ниже 5 класса и 5 уровня доверия, а также средства вычислительной техники не ниже 5 класса защиты, соответствующие стандартам безопасности в здравоохранении.

В соответствии с Моделью угроз безопасности информации для нейтрализации атак нарушителей безопасности информации допускается применение СКЗИ, соответствующих «Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну» по классу КС1 и выше.

## Требования к подсистемам СЗИ

### Требования к подсистеме защиты от НСД

Подсистема защиты от НСД предназначена для защиты информационных ресурсов и защищаемой информации медицинской системы от несанкционированного доступа.

Подсистема защиты от несанкционированного доступа должна включать следующие компоненты:

* программно-аппаратные и/или программные средства защиты от несанкционированного доступа;
* программно-аппаратные и/или программные средства доверенной загрузки.

Подсистема защиты от НСД должна реализовывать следующий функционал:

* обеспечение доверенной загрузки АРМ и серверного оборудования;
* реализацию правил разграничения доступа;
* идентификацию пользователей при запросах на доступ;
* проверку подлинности идентификации – аутентификацию;
* запрет доступа к защищаемым ресурсам не прошедших идентификацию пользователей и пользователей, подлинность идентификации которых при аутентификации не подтвердилась;
* регистрацию событий (результат идентификации и аутентификации, запрос на доступ к защищаемому ресурсу, создание и уничтожение объекта и т.д);

Подсистема защиты от НСД должна строиться на базе решений, прошедших процедуру оценки соответствия ФСТЭК России.

### Требования к подсистеме контроля и анализа защищенности

Подсистема контроля и анализа защищенности создается с целью проведения анализа защищенности и управления информационной безопасностью в медицинской системы.

Подсистема контроля и анализа защищенности должна обеспечивать выполнение следующий функций:

* поиск уязвимостей в установленном программном обеспечении с использованием баз известных уязвимостей;
* контроль установки обновлений программного обеспечения, в том числе программного обеспечения, входящего в состав СЗИ;
* анализ сетевой активности;
* инвентаризация ресурсов сети.

Подсистема контроля и анализа защищенности должна включать следующие компоненты:

* программные средства анализа защищенности.

Подсистема контроля и анализа защищенности должна строиться на базе решений, прошедших процедуру оценки соответствия ФСТЭК России.

### Требования к подсистеме обнаружения вторжений

Подсистема обнаружения вторжений создается с целью организации защиты сетей организации от сетевых атак.

Подсистема обнаружения вторжений должна обеспечивать выполнение следующий функций:

* обнаружение сетевых атак (вторжений) на основе анализа сетевого трафика стека протоколов TCP/IP;
* анализ данных с целью обнаружения вторжений с использованием сигнатурного и эвристического методов;
* регистрация фактов обнаружения атаки (вторжения);
* обновление базы решающих правил в автоматизированном режиме.

Подсистема обнаружения вторжений должна включать следующие компоненты:

* программно-аппаратные и/или программные средства обнаружения вторжений;
* программно-аппаратные и/или программные средства для централизованного управления компонентами подсистемы.

Подсистема обнаружения вторжений должна строиться на базе решений, прошедших процедуру оценки соответствия ФСТЭК России.

### Требования к подсистеме защиты каналов связи

Подсистема защиты каналов связи создается с целью организации защищенных каналов связи, выходящих за границы контролируемой зоны.

Подсистема защиты каналов связи должна обеспечивать выполнение следующий функций:

* предоставление пользователям медицинской системы возможности защищенного удаленного доступа к информационным ресурсам медицинской системы через информационно-телекоммуникационную сеть общего пользования;
* обеспечение целостности, предаваемой по каналам связи информации.

Подсистема защиты каналов связи должна включать следующие компоненты:

* программно-аппаратные и/или программные средства криптографической защиты информации, передаваемой по каналам связи (криптошлюзы);
* программно-аппаратные и/или программные средства для централизованного управления компонентами подсистемы.

Подсистема должна строиться на базе решений, обладающих сертификатом соответствия по требованиям безопасности ФСБ России для защиты информации, не содержащей сведений, составляющих государственную тайну, по классу не ниже КС1.

### Требования к подсистеме защиты среды виртуализации

Подсистема защиты среды виртуализации создается с целью обеспечения безопасности виртуальной инфраструктуры, на базе которой развернута медицинской системы .

Подсистема защиты среды виртуализации должна обеспечивать выполнение следующий функций:

* идентификация и аутентификация администраторов виртуальной инфраструктуры;
* идентификация узлов виртуальной инфраструктуры по логическим именам;
* контроль доступа к защищаемым информационным ресурсам в виртуальной инфраструктуре;
* централизованное управление идентификаторами и аутентифицирующей информацией администраторов виртуальной инфраструктуры;
* контроль целостности конфигурации виртуальных машин и их доверенная загрузка;
* очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти виртуальной инфраструктуры;
* регистрация событий ИБ в виртуальной инфраструктуре;
* регистрация изменений полномочий доступа субъектов на АРМ и серверах медицинской системы ;
* проверка конфигурации хостов виртуальной среды на предмет соблюдения необходимых требований безопасности по заданным шаблонам.

Подсистема защиты среды виртуализации должна включать следующие компоненты:

* программные средства защиты среды виртуализации;
* программные средства для централизованного управления компонентами подсистемы.

Подсистема защиты среды виртуализации должна строиться на базе решений, прошедших процедуру оценки соответствия ФСТЭК России.

## Требования к видам обеспечения

### Требования к организационному обеспечению

Перечень организационных мер по защите информации в медицинской системы уточняется на этапе технического проектирования СЗИ медицинской системы .

### Требования к математическому обеспечению

Математические методы и алгоритмы, используемые для криптографических операций в СЗИ медицинской системы , должны соответствовать следующим криптографическим стандартам:

* ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования»;
* ГОСТ 34.12-2018 «Информационная технология. Криптографическая защита информации. Блочные шифры».

### Требования к информационному обеспечению

Совместимость СЗИ медицинской системы со смежными подсистемами медицинской системы и внешними информационными системами должна достигаться путем совместимости средств защиты информации, используемых в СЗИ медицинской системы , со следующими стандартами:

* протокол TCP/IP v.4 для обеспечения сетевого взаимодействия всех компонентов медицинской системы ;
* протокол HTTP, HTTPS (RFC 1945, RFC 2068 «Hypertext Transfer Protocol», RFC 2818 «HTTP Over TLS»);
* протокол TLS (RFC 2246 «The TLS Protocol. Version 1.0», RFC 5246 «The Transport Layer Security (TLS) Protocol. Version 1.2»).

### Требование к защите обеспечивающей инфраструктуры

Должна быть определена контролируемая зона, в пределах которой постоянно размещаются средства обеспечения функционирования медицинской системы . Должен обеспечиваться контроль и управление физическим доступом к средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обеспечения функционирования медицинской системы и помещения и сооружения, в которых они установлены, в том числе:

* определен перечень лиц, допущенных к средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены;
* обеспечено санкционирование физического доступа к средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены;
* обеспечено ведение учета физического доступа к средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены.

Помещения, в которых расположены сегменты и средства, обеспечивающие функционирование медицинской системы , должны быть оснащены системами автоматической охранной и пожарной сигнализации.

Технические средства обеспечения функционирования медицинской системы должны соответствовать ГОСТ Р 50628-2000 «Совместимость машин электронных вычислительных персональных электромагнитная. Устойчивость к электромагнитным помехам. Технические требования и методы испытаний».

# Порядок контроля и приемки системы

Контроль и приемка работ осуществляются на основании настоящего частного технического задания.

В целях проверки качества результатов выполненных работ и его соответствия требованиям частного технического задания производятся аттестационные испытания СЗИ медицинской системы. Аттестационные испытания проводятся на площадке объекта автоматизации в соответствии с Программой и методикой аттестационных испытаний, разрабатываемой органом по аттестации. Результаты испытаний фиксируются в Протоколе аттестационных испытаний.

Сроки приемки работ определяются календарными планами и сроками проведения соответствующих этапов в соответствии с техническими требованиями на создание СЗИ.

# Порядок внесения изменений в техническое задание

Настоящее частное техническое задание может корректироваться в соответствии с установленным порядком по взаимному соглашению между Заказчиком и Исполнителем.

# Требования к документированию

При разработке отчетной документации Исполнитель должен руководствоваться ГОСТ 34.201-2020, а также ГОСТ Р 59795-2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов» (далее – ГОСТ Р 59795-2021).

Требования по полному формальному соответствию ГОСТ Р 59795-2021 и ГОСТ 34.201-2020 по составу и структуре разделов не предъявляются.

Комплект документации представляется Заказчику Исполнителем в печатном виде (оригинал), а также в электронном виде. Электронный вариант предоставляемых документов должен соответствовать форматам программного пакета Microsoft Office.

# Перечень принятых сокращений

В настоящем документе приняты следующие сокращения:

|  |  |  |
| --- | --- | --- |
| АРМ | – | автоматизированное рабочее место |
| ИС | – | информационная система |
| ИБ | – | информационная безопасность |
| ЛВС | – | локальная вычислительная сеть |
| МЭ | – | межсетевой экран |
| НСД | – | несанкционированный доступ |
| ОС | – | операционная система |
| ПДн | – | персональные данные |
| ПО | – | программное обеспечение |
| СЗИ | – | система защиты информации |
| ТС | – | технические средства |
| ФСТЭК России | – | Федеральная служба по техническому и экспортному контролю Российской Федерации |
| ЧТЗ | – | частное техническое задание |
|  |  |  |