УТВЕРЖДАЮ

Директор ООО «Династия»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Глушков К.В.

«30» марта 2025 года

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

**на систему защиты персональных данных в информационной**

**системе персональных данных**

**«Династия»**

Г. Пермь, 2025

# Обоснование разработки СЗПДн

Разработка системы защиты персональных данных (СЗПДн) необходима для обеспечения соответствия требованиям законодательства Российской Федерации, в том числе:

* Федерального закона № 152-ФЗ «О персональных данных»;
* Постановления Правительства РФ от 1 ноября 2012 г. № 1119;
* Приказа ФСТЭК России, ФСБ России и Минцифры России от 13 февраля 2008 г. № 55/86/20.

Система защиты должна разрабатываться с целью предотвращения ущерба от возможной реализации нарушений характеристик безопасности. Угрозы безопасности определены в «Частной модели угроз безопасности персональных данных для информационной системы персональных данных  "Династия"»

В соответствии с результатами внутренней проверки и акта определения уровня защищенности ИСПДн «Династия», установлено, что система относится к **2-му уровню защищенности**. Это требует внедрения усиленных организационных и технических мер по защите персональных данных, поскольку в системе обрабатываются **специальные категории персональных данных (сведения о состоянии здоровья)**, а также актуальны **угрозы 2-го типа**.

# Исходные данные создаваемой (модернизируемой) ИСПДн в техническом, программном, информационном и организационном аспектах

**Информационная система (ИС) состоит из** 3 ПЭВМ, объединенных в локальную вычислительную сеть (ЛВС). В ней обрабатываются персональные данные:

* ФИО
* Адрес
* паспортные данные
* сведения о лечении
* телефоны
* информация об оплате

Автономная ЛВС без подключения к сетям общего пользования. Вся инфраструктура расположена в помещении частной стоматологической клиники. Является многопользовательской, количество записей субъектов не более 5000.

# Уровень защищенности ИСПДн

Определен **1-й уровень защищенности** в соответствии с Постановлением Правительства РФ № 1119, поскольку:

* В системе обрабатываются **специальные категории персональных данных**.
* Обрабатываются персональные данные менее 5000 субъектов.
* Для системы актуальны **угрозы 2-го типа**.

# Ссылки на нормативные документы, с учетом которых будет разрабатываться СЗПДн и приниматься в эксплуатацию информационная система

1. Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
2. Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
3. Постановление Правительства Российской Федерации от 01.11.2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
4. Приказ ФСТЭК от 18 февраля 2013 г. N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

# Список мероприятий и требований к СЗПДн

**Подсистема идентификации и аутентификации (П1)** - отвечает за проверку подлинности пользователей и устройств, а также за управление учетными записями и средствами аутентификации.

**Подсистема управления доступом (П2)** - обеспечивает разграничение прав доступа пользователей к данным на основе ролевой модели и устанавливает ограничения на число неудачных попыток входа.

**Подсистема защиты машинных носителей (П3)** - реализует контроль за использованием съемных носителей и предусматривает шифрование информации на них.

**Подсистема регистрации событий безопасности (П4)** - отвечает за ведение журнала событий безопасности и контроль действий пользователей для выявления возможных угроз.

**Подсистема антивирусной защиты (П5)** - предусматривает установку, обновление и регулярное сканирование системы на наличие вредоносного программного обеспечения.

**Подсистема обнаружения вторжений (П6)** - занимается выявлением попыток несанкционированного доступа и их блокировкой.

**Подсистема обеспечения целостности (П7)** - контролирует целостность данных и программного обеспечения, а также выявляет и предотвращает их несанкционированные изменения.

**Подсистема защиты технических средств (П8)** - регулирует контроль физического доступа к оборудованию и защищает устройства вывода информации от несанкционированного использования.

**Подсистема выявления инцидентов и реагирования на них (П9)** - занимается мониторингом инцидентов информационной безопасности, их анализом и регистрацией.

**Подсистема защиты информационной системы и её компонентов (П10)** - реализует меры по защите сети, включая сегментирование и шифрование передаваемых данных.

Перечень требований безопасности персональных данных, предусмотренный нормативно-методическими документами для ИСПДн с представлен в таблице.

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Подсистема** | **Условное обозначение и номер меры** | **Требование** |
| 1 | П1 | ИАФ.1 | Обеспечить идентификацию и аутентификацию пользователей ИС |
| 2 | П1 | ИАФ.2 | Обеспечить идентификацию и аутентификацию устройств (стационарных, мобильных, портативных) |
| 3 | П1 | ИАФ.3 | Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов |
| 4 | П1 | ИАФ.4 | Обеспечить управление средствами аутентификации, в том числе хранение, выдачу, инициализацию, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации |
| 5 | П1 | ИАФ.5 | Обеспечить защиту обратной связи при вводе аутентификационной информации |
| 6 | П1 | ИАФ.6 | Обеспечить идентификацию и аутентификацию внешних пользователей ИС |
| 7 | П1 | ИАФ.7 | Защита аутентификационной информации при передаче. Организация защиты аутентификационной информации криптографическими методами шифрования трафика. Осуществление контроля целостности передаваемой аутентификационной информации. |
| 8 | П2 | УПД.1 | Управление (создание, активация, блокирование и уничтожение) учетными записями пользователей, в том числе для внешних пользователей ИС |
| 9 | П2 | УПД.2 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа |
| 10 | П2 | УПД.4 | Обеспечить разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы |
| 11 | П2 | УПД.5 | Назначение минимально необходимых прав и привилегий пользователям, администраторам и сотрудникам, обеспечивающим функционирование информационной системы |
| 12 | П2 | УПД.6 | Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) |
| 13 | П2 | УПД.7 | Предупреждение пользователя при его доступе к информационным ресурсам |
| 14 | П2 | УПД.9 | Ограничение числа параллельных сеансов доступа в ИС |
| 15 | П2 | УПД.10 | Обеспечить блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу |
| 16 | П2 | УПД.11 | Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации |
| 17 | П3 | ЗНИ.1 | Обеспечить учет машинных носителей информации, которые содержат ПД пользователей ИС |
| 18 | П3 | ЗНИ.2 | Обеспечить управление доступом к машинным носителям персональных данных |
| 19 | П3 | ЗНИ.3 | Обеспечить контроль перемещения машинных носителей информации за пределы КЗ |
| 20 | П3 | ЗНИ.4 | Обеспечить исключение возможности несанкционированного чтения информации на машинных носителях информации посредством шифрования данных на съемных носителях |
| 21 | П3 | ЗНИ.7 | Обеспечить контроль подключения съемных машинных носителей информации |
| 22 | П3 | ЗНИ.8 | Обеспечить 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 |
| 23 | П4 | АУД4.1 | Регистрировать события безопасности в системе |
| 24 | П5 | АВЗ.1 | Обеспечить реализацию антивирусной защиты |
| 25 | П5 | АВЗ.2 | Антивирусная защита электронной почты и иных сервисов |
| 26 | П5 | АВЗ.4 | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) |
| 27 | П6 | СОВ.1 | Обеспечить обнаружение вторжений и предотвращение компьютерных атак |
| 28 | П6 | СОВ.2 | Обновление базы решающих правил |
| 29 | П7 | ОЦЛ.1 | Обеспечить контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации |
| 30 | П7 | ОЦЛ.4 | Обеспечить 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) |
| 31 | П8 | ЗТС.3 | Обеспечить 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 |
| 32 | П8 | ЗТС.4 | Обеспечить размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр |
| 33 | П9 | ИНЦ.1 | Обеспечить определение лиц, ответственных за выявление инцидентов и реагирование на них |
| 34 | П9 | ИНЦ.2 | Обеспечить обнаружение, идентификация и регистрация инцидентов |
| 35 | П9 | ИНЦ.3 | Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами |
| 36 | П9 | ИНЦ.4 | Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий |
| 37 | П9 | ИНЦ.5 | Принятие мер по устранению последствий инцидентов |
| 38 | П9 | ИНЦ.6 | Планирование и принятие мер по предотвращению повторного возникновения инцидентов |
| 39 | П10 | ЗИС.2 | Обеспечить защиту периметра информационной (автоматизированной) системы |
| 40 | П10 | ЗИС.4 | Спланировать и обеспечить сегментирование информационной (автоматизированной) системы на подсети |
| 41 | П10 | ЗИС.15 | Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных |
| 42 | П10 | ЗИС.17 | Защита информации от утечек. Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы |

Далее представлен перечень конкретных мероприятий для СЗПДн каждой подсистемы

|  |  |  |
| --- | --- | --- |
| № | Подсистема | Организационные и технические меры защиты |
| 1 | **Подсистема идентификации и аутентификации** | **Организационные:** ведение реестра учетных записей; регламент назначения и удаления учетных записей; политика управления паролями. **Технические:** использование аппаратных токенов; многофакторная аутентификация; шифрование учетных данных; автоматическое отключение неактивных учетных записей. |
| 2 | **Подсистема управления доступом** | **Организационные:** разработка матрицы доступа; регламент назначения и отзыва прав доступа; политика минимально необходимых привилегий. **Технические:** использование ролевой модели доступа (RBAC); блокировка после 5 неудачных попыток входа; VPN с ГОСТ-шифрованием; аудит операций, связанных с доступом. |
| 3 | **Подсистема защиты машинных носителей** | **Организационные:** учет съемных носителей; запрет на использование неавторизованных носителей; регламент уничтожения носителей. **Технические:** шифрование данных на носителях; автоматическое блокирование несанкционированных USB-устройств; контроль подключения и использования носителей. |
| 4 | **Подсистема регистрации событий безопасности** | **Организационные:** назначение ответственных за анализ событий; регламент ведения журналов безопасности. **Технические:** централизованное журналирование (SIEM-система); защита журналов от модификации; автоматизированный анализ событий и уведомление ответственных лиц. |
| 5 | **Подсистема антивирусной защиты** | **Организационные:** назначение ответственного; регламент обновлений; обучение сотрудников правилам безопасности. **Технические:** установка сертифицированного антивирусного ПО (Dr.Web, Касперский); централизованное управление антивирусной защитой; ежедневное обновление антивирусных баз; регулярное сканирование. |
| 6 | **Подсистема обнаружения вторжений** | **Организационные:** регламент реагирования на инциденты; регулярные тестирования безопасности. **Технические:** установка системы обнаружения вторжений (IDS/IPS); анализ сетевого трафика на предмет атак; мониторинг подозрительной активности. |
| 7 | **Подсистема обеспечения целостности** | **Организационные:** регламент контроля целостности данных; назначение ответственного за мониторинг. **Технические:** хеширование критически важных файлов; использование средств контроля целостности ОС и приложений; мониторинг изменений системных файлов. |
| 8 | **Подсистема защиты технических средств** | **Организационные:** регламент физического доступа к оборудованию; учет и контроль технических средств. **Технические:** установка камер видеонаблюдения; ограничение физического доступа к серверам; защита устройств вывода информации (экраны с антишпионской пленкой, блокировка USB-портов). |
| 9 | **Подсистема выявления инцидентов и реагирования на них** | **Организационные:** регламент регистрации и расследования инцидентов; назначение ответственных за реагирование. **Технические:** автоматизированные системы анализа событий (SIEM); сбор и корреляция данных по инцидентам; система уведомлений при обнаружении угроз. |
| 10 | **Подсистема защиты информационной системы и её компонентов** | **Организационные:** политика сетевой безопасности; регламент сегментирования сети. **Технические:** настройка межсетевых экранов (NGFW); сегментация сети с разделением зон безопасности; контроль защищенности каналов передачи данных. |

# Перечень предполагаемых к использованию сертифицированных средств защиты информации

|  |  |  |
| --- | --- | --- |
| № | Подсистема | Cертифицированные средства защиты информации |
| 1 | **Подсистема идентификации и аутентификации** | - Системы управления доступом и аутентификации «RUTOKEN» (ФСБ, ФСТЭК России);  - Система двухфакторной аутентификации «Yubico» (ФСТЭК России). |
| 2 | **Подсистема управления доступом** | - Средства управления доступом «Active Directory» (ФСТЭК России);  - ПО для контроля доступа на базе ролей (RBAC), сертифицированные в соответствии с требованиями ФСТЭК и ФСБ. |
| 3 | **Подсистема защиты машинных носителей** | - Средства защиты данных на съемных носителях «TrueCrypt» (ФСТЭК России);  - Средства шифрования дисков и съемных носителей «Acronis Disk Director» (ФСТЭК России). |
| 4 | **Подсистема регистрации событий безопасности** | - Системы централизованного журнала безопасности (SIEM) «EventLog Analyzer» (ФСТЭК России);  - Средства мониторинга и аудита событий «Splunk» (ФСТЭК России). |
| 5 | **Подсистема антивирусной защиты** | - Антивирусное ПО «Dr.Web» (сертифицировано ФСТЭК и ФСБ);  - Антивирусное ПО «Kaspersky Endpoint Security» (сертифицировано ФСТЭК и ФСБ);  - Антивирус «ESET NOD32» (ФСТЭК России). |
| 6 | **Подсистема обнаружения вторжений** | - Система обнаружения вторжений «Snort» (ФСТЭК России);  - Система предотвращения вторжений «Cisco Firepower» (ФСТЭК России);  - Система IDS/IPS «Check Point» (ФСТЭК России). |
| 7 | **Подсистема обеспечения целостности** | - Средства контроля целостности данных «Tripwire» (ФСТЭК России);  - Средства мониторинга целостности программного обеспечения «HashCheck» (ФСТЭК России). |
| 8 | **Подсистема защиты технических средств** | - Система защиты физического доступа «КС-2» (ФСТЭК России);  - Устройства защиты от несанкционированного доступа и установки ПО «SafeBoot» (ФСТЭК России);  - Камеры видеонаблюдения «Vivotek» (сертифицировано ФСТЭК). |
| 9 | **Подсистема выявления инцидентов и реагирования на них** | - Средства мониторинга и реагирования на инциденты «SIEM Splunk» (ФСТЭК России);  - ПО для реагирования на инциденты и управление ими «SolarWinds» (ФСТЭК России);  - Инструменты для управления инцидентами «McAfee» (ФСТЭК). |
| 10 | **Подсистема защиты информационной системы и её компонентов** | - Межсетевой экран «Fortinet FortiGate» (ФСТЭК России);  - Средства защиты сети «Cisco ASA» (ФСТЭК России);  - Средства защиты передачи данных «InfoWatch Traffic Monitor» (ФСТЭК России). |

# Состав, содержание и сроки проведения работ по этапам разработки и внедрения СЗПДн

1. **Анализ и проектирование (1 месяц)**
   * Определение состава защитных мер.
   * Разработка политики информационной безопасности.
2. **Внедрение технических и организационных мер (2 месяца)**
   * Настройка СЗИ.
   * Организация физической защиты.
3. **Тестирование и аудит (1 месяц)**
   * Проведение испытаний работоспособности СЗПДн.
   * Оценка эффективности защиты.
4. **Документирование и ввод в эксплуатацию (1 месяц)**
   * Подготовка отчетности.
   * Утверждение итогового пакета документов.

**Сроки выполнения:** 5 месяцев с момента утверждения ТЗ.