VIII СЪЕЗД МЕДИЦИНСКИХ СТАТИСТИКОВ ГОРОДА МОСКВЫ

МОСКОВСКАЯ МЕДИЦИНА

НИИ ОРГАНИЗАЦИИ ЗДРАВООХРАНЕНИЯ И МЕДИЦИНСКОГО МЕНЕДЖМЕНТА

Безопасность витрин данных: требования регуляторов и меры защиты

Королев Андрей Игоревич, начальник управления информатизации
НИИ организации здравоохранения и медицинского менеджмента

Содержание

1 **Роль витрин данных в современной архитектуре здравоохранения**
Понятие, источники данных, риски

2 **Нормативно-правовая база и требования регуляторов**
149-ФЗ, 152-ФЗ, 323-ФЗ, ПП № 1119, приказ ФСТЭК № 117

3 **Основные угрозы и уязвимости**
Нарушители, типовые уязвимости

4 **Меры защиты**
Организационно-правовые, технические, криптографические

5 **Заключение**
Выводы и рекомендации

РАЗДЕЛ 1 ИЗ 5

Роль витрин данных в современной архитектуре здравоохранения

Что такое витрина данных

Пример: Единый цифровой контур здравоохранения

Хранилище (Единый цифровой контур)

Данные из медицинских систем (МИС МО, ЛИС, РИС)

→

Витрина

Данные отобраны под конкретную задачу, например «Заболеваемость по району» или «Нагрузка на врачей»

→

Пользователь (врач, аналитик, руководитель)

Получает готовые показатели и отчёты для принятия клинических и управленческих решений

Примеры использования витрин в здравоохранении

Статистическая отчётность

Данные для форм статистического наблюдения (№ 12, № 14, № 30 и др.)

Регистры и мониторинг

Пациенты с онкологическими заболеваниями, диабетом; диспансерное наблюдение

Панели руководителя на базе витрин

Загрузка коек и врачей, сроки ожидания, выполнение плановых показателей

Аналитика и ИИ

Наборы данных для научных исследований и обучения моделей

Почему витрина требует отдельной защиты

В витрине сведены данные из различных систем, которые составляют информацию ограниченного доступа, поэтому она в приоритете у злоумышленников

Концентрация данных

Данные из медицинских систем

Широкий круг пользователей

Статистики, аналитики, руководители, подрядчики, аналитические панели и ИИ-сервисы

Регулярные выгрузки

Пользователи постоянно выгружают данные в Excel, это основной канал утечек

Витрину защищаем как отдельную систему: свой класс, модель угроз и меры

РАЗДЕЛ 2 ИЗ 5

Нормативно-правовая база и требования регуляторов

Витрина данных — это информационная система или её часть

Определение информационной системы (149-ФЗ, ст. 2 п. 3)

База данных/СУБД + **Программное обеспечение** + **Серверы и сети** = **Информационная система**

«совокупность содержащейся в базах данных информации и обеспечивающих её обработку информационных технологий и технических средств»

Самостоятельная система

Свой оператор, свой акт классификации, своя система защиты

Часть другой системы

Сегмент ГИС или регионального хранилища; сегменту можно присвоить свой класс (п. 9 прил. к приказу № 117)

Часть государственной платформы

Витрины единой платформы управления данными (ПП № 733); защита по 149-ФЗ

Вывод: на витрину распространяются все требования: оператор, класс защищенности, модель угроз, меры по приказу № 117, уровень защищенности ПДн по ПП № 1119. Если данные получены из ГИС, получатель тоже обязан выполнять требования (п. 2 приказа № 117).

Нормативные правовые акты

Уровень	Документы	Что определяют для витрины
Федеральные законы	149-ФЗ (ст. 16), 152-ФЗ, 323-ФЗ (ст. 13), 187-ФЗ	Обязанность защищать информацию; персональные данные и врачебная тайна; критическая информационная инфраструктура
Правительство РФ	ПП № 1119, ПП № 676	Уровни защищенности ПДн; порядок создания и работы ГИС
ФСТЭК России	Приказ № 117 (ред. № 137), методический документ от 12.04.2026; приказы № 21, 239, 77	Классы защищенности, обязательные мероприятия и меры; ПДн в негосударственных системах; КИИ; аттестация
ФСБ России, Роскомнадзор	Приказ ФСБ № 378, приказ РКН № 140	Шифрование данных и каналов связи; требования и методы обезличивания

С 01.03.2026 действует приказ ФСТЭК № 117 вместо № 17; методический документ от 12.04.2026 заменил «Меры защиты информации в ГИС» 2014 г. Для ПДн в ГИС одновременно применяются ПП № 1119 и приказ № 117 (п. 5).

Требования приказа ФСТЭК России № 117

Требование	Содержание	Пункты
Организовать защиту	Утвердить политику, стандарты и регламенты; назначить ответственного и подразделение ИБ (не менее 30 % сотрудников с профильным образованием)	**пп. 13–27**
Определить класс и угрозы	Оформить акт классификации (К1–К3) и модель угроз на основе банка данных угроз ФСТЭК	**п. 36; прил.**
Выполнять 21 мероприятие	Управление уязвимостями и обновлениями, контроль настроек, мониторинг, резервное копирование, обучение, подрядчики, ИИ и др.	**пп. 34–61**
Внедрить 17 групп мер	Учётные записи и доступ, журналы событий, антивирус, обнаружение атак, разделение сети, защита каналов связи, веб-сервисов и API	**пп. 62–64**
Применять сертифицированные средства	Средства защиты с сертификатом ФСТЭК: класс 4 для К1, 5 для К2, 6 для К3; поддержка в РФ; без средств из недружественных стран (Указ № 250)	**пп. 71–72**
Подтвердить соответствие	Аттестация государственной информационной системы до начала работы с данными (приказ ФСТЭК № 77)	**п. 65**
Измерять и отчитываться	Расчёт Кзи раз в полгода, проверка защищенности раз в 3 года, отчёты в ФСТЭК	**пп. 32, 49, 67**
Если мера невыполнима	Разработать и обосновать компенсирующие меры, подтвердить их эффективность	**п. 69**

Сроки и показатели по приказу № 117

КЗИ

Показатель защищённости информации – раз в 6 месяцев расчёт и отправка отчёта в ФСТЭК

п. 32

Не более 24 ч / 7 дн.

Устранение уязвимостей критического и высокого уровня опасности

п. 38

30 %

Сотрудников ИБ с профильным образованием или переподготовкой

п. 20

3 года

Проверка защищенности не реже, а также после каждого инцидента

пп. 66–67

УЗИ

Показатель уровня зрелости - раз в 2 года

п. 32 в ред. приказа № 137

ИИ

Отдельные требования к защите при использовании ИИ

пп. 34 «т», 60–61

Приказ ФСТЭК России от 11.04.2025 № 117 (действует с 01.03.2026; изменения — приказ от 08.05.2026 № 137)

Класс защищенности витрины и уровень защищенности ПДн

Класс по приказу № 117

УЗ \ масштаб	Федер.	Регион.	Объект.
УЗ 1	К1	**К1**	К1
УЗ 2	К1	К2	К2
УЗ 3	К2	К3	К3

УЗ — уровень значимости информации: степень возможного ущерба от утечки, искажения или недоступности данных. Масштаб: федеральный, региональный, объектовый.

Персональные данные: ПП № 1119

К1 обеспечивает УЗ-1, УЗ-2, УЗ-3, УЗ-4 ПДн

К2 обеспечивает УЗ-2, УЗ-3, УЗ-4 ПДн

К3 обеспечивает УЗ-3, УЗ-4 ПДн

Прил. 3 к методическому документу ФСТЭК от 12.04.2026

Пример: городская витрина МО

более 100 тыс. человек, угрозы 3-го типа → УЗ-3 ПДн → не ниже К2

Высокий ущерб, регион. масштаб → УЗ 1 → К1

На практике: чем серьёзнее возможный ущерб и шире охват системы, тем выше класс и больше обязательных мер. Для данных жителей города класс, как правило, высокий.

РАЗДЕЛ 3 ИЗ 5

Основные угрозы и уязвимости

Источники угроз для витрины данных

Внешний нарушитель

- Фишинговое письмо и кража пароля аналитика
- Взлом через уязвимости в программах
- Вирусы-шифровальщики блокируют работу

Внутренний нарушитель

- Лишние права и массовые выгрузки
- Передача и продажа данных

Подрядчики

- Доступ подрядчика к рабочей системе
- Тестирование на реальных данных пациентов
- Взлом через инфраструктуру подрядчика

Сервисы ИИ

- Выгрузки в публичных чат-ботах
- Вредоносные запросы к модели
- Утечка через ответы модели

Угрозы определяются по банку данных угроз ФСТЭК России и Методике оценки угроз (ФСТЭК, 05.02.2021); модель угроз — п. 36 приказа № 117

Типовые слабые места витрин и способы их устранения

Слабое место	К чему приводит	Чем закрываем
Лишние права, общие логины в аналитических системах	Доступ к любым данным, виновного не установить	**Модель доступа, личные учётные записи**
Бесконтрольная выгрузка в Excel/CSV	Массовая утечка	**Учёт выгрузок, система DLP (п. 40)**
Открытые подключения к базе и программным интерфейсам	Скачивание всей базы	**Проверка прав и лимиты на запросы**
Необновлённые базы данных и программы	Взлом через известные уязвимости	**Обновления: 24 ч / 7 дн. (п. 38)**
Тестирование на реальных данных пациентов	Утечка через подрядчика	**Только тестовые стенды (п. 58)**
Слабое обезличивание	Пациента можно узнать	**Регламент по приказу РКН № 140**
Нет журнала запросов и выгрузок	Утечку никто не заметит	**Журналы и мониторинг (п. 49)**

РАЗДЕЛ 4 ИЗ 5

Меры защиты

Организационно-правовые меры

Направление	Что сделать	Результат	Основание
Политика и регламенты	Утвердить политику ИБ и регламенты: доступ, выгрузка, обновления, резервные копии, инциденты	Приказ руководителя, пакет регламентов	**пп. 14, 25**
Ответственные	Назначить ответственное лицо, подразделение ИБ и владельца данных каждой витрины	Приказ о назначении, должностные инструкции	**пп. 17–20**
Класс и угрозы	Определить класс витрины и уровень защищенности ПДн, составить модель угроз	Акт классификации, модель угроз	**п. 36; ПП № 1119**
Допуск к данным	Определить, кто и к каким данным допущен; взять обязательства о неразглашении КИ	Перечень лиц и ролей, подписанные обязательства	**152-ФЗ, 323-ФЗ**
Обезличивание	Описать методы, проверку достаточности, раздельное хранение и учёт действий	Регламент обезличивания	**приказ РКН № 140**
Подрядчики	Включить в договор требования по защите и запрет копирования; оценить зрелость до допуска	Договор и ТЗ с разделом по ИБ	**п. 58**
Обучение	Памятки, занятия, учебные фишинговые рассылки; проверка знаний раз в 3 года и после инцидента	План обучения, результаты проверки	**пп. 56–57**
Инциденты	Порядок реагирования; уведомление РКН за 24 ч и 72 ч; взаимодействие с ГосСОПКА	Регламент реагирования, журнал инцидентов	**ст. 21 152-ФЗ; п. 34**
Контроль	Кзи раз в полгода; проверка защищенности раз в 3 года; аттестация ГИС	Отчёты в ФСТЭК, аттестат соответствия	**пп. 32, 65, 67**

Технические меры защиты

Базовый набор для К1 при использовании всех технологий (разд. IV методического документа ФСТЭК России от 12.04.2026)

Группа мер	Что сделать для К1	Средства защиты	Меры
Идентификация и аутентификация	Личные учётные записи, двухфакторный вход для всех, пароль от 12 символов	СЗИ от НСД, средства аутентификации (токены)	**ИАФ.1, ИАФ.3**
Управление доступом	Ролевая модель, минимальные права, блокировка неиспользуемых учётных записей	Сертифицированные ОС и СУБД, СЗИ от НСД	**УПД.1–УПД.4, УПД.7–УПД.9**
Регистрация событий	Журналы СЗИ, серверов и СУБД; централизованный сбор; место удалённого входа	SIEM (средство управления событиями ИБ)	**РСБ.1–РСБ.5**
Среда виртуализации	Доверенная загрузка, еженедельный контроль целостности ВМ, разграничение доступа	Средства виртуализации и доверенной загрузки	**ЗСВ.1–ЗСВ.9**
Контейнерная среда	Изоляция контейнеров, контроль целостности образов, поиск уязвимостей раз в неделю	Сертифицированные средства контейнеризации	**ЗКО.1–ЗКО.8**
Электронная почта	Проверка вложений и ссылок, блокировка фишинга и спама, аудит почтовых ящиков	САВЗ для почты, средства защиты почты	**ЗЭП.1–ЗЭП.6**
Веб-приложения	Фильтрация запросов с анализом содержимого, проверка передаваемых файлов	МСЭ уровня веб-приложений (тип «Г»)	**ЗВТ.1–ЗВТ.5**
Программные интерфейсы (API)	Перечень API, контроль доступа, минимум сведений в ответах, пересмотр раз в год	МСЭ тип «Г», средства аутентификации	**ЗПИ.1–ЗПИ.3**
Конечные устройства (АРМ)	Доступ и целостность ПО на АРМ; при выходе в Интернет обнаружение атак на узле	СЗИ от НСД, САВЗ, средства EDR	**ЗКУ.1–ЗКУ.4, ЗКУ.6**

Технические меры (продолжение)

Средства защиты: сертификат ФСТЭК России, для К1 класс не ниже 4 (п. 72 приказа № 117); СКЗИ с сертификатом ФСБ России

Группа мер	Что сделать для К1	Средства защиты	Меры
Мобильные устройства	Пароль от 10 символов, контроль приложений, данные только в защищённой области	Система управления мобильными устройствами	**ЗМУ.1–ЗМУ.7, ЗМУ.9**
Интернет вещей	Идентификация и инвентаризация устройств, отключение лишних протоколов	МСЭ, отдельный сегмент сети	**ЗИВ.1–ЗИВ.5**
Беспроводной доступ	Аутентификация, отдельный сегмент, скрытый SSID, инвентаризация точек доступа	Защищённые точки доступа, МСЭ	**ЗБД.1–ЗБД.6**
Антивирусная защита	Серверы и АРМ, почта и сетевой трафик; проверка файлов из внешних источников	САВЗ (сертификат ФСТЭК)	**АВЗ.1–АВЗ.3**
Обнаружение вторжений	На периметре и в сегментах; собственные решающие правила под угрозы витрины	СОВ уровня сети, многофункциональные МСЭ	**СОВ.1, СОВ.2**
Сегментация сети	В отдельном сегменте, DMZ для внешних сервисов, микросегментация	МСЭ, многофункциональные МСЭ уровня сети	**МСЭ.1–МСЭ.3**
Защита от DDoS	Постоянная фильтрация входящего трафика, ограничение нагрузки, мониторинг сервисов	Средства защиты от DDoS-атак	**ЗОО.1–ЗОО.3, ЗОО.5, ЗОО.6**
Каналы связи	Защита данных за пределами контролируемой зоны, контроль доступа во внешние сети	СКЗИ, МСЭ	**ЗКС.1–ЗКС.3**

Мероприятия (процессы) защиты

Мероприятие	Что сделать	Средства защиты	Основание
Управление уязвимостями (КУ)	Мониторинг уязвимостей; критические закрыть за 24 ч, высокие за 7 дней	Средство анализа защищённости (сканер)	**КУ; п. 38**
Управление обновлениями (КО)	Обновления с проверкой подлинности и целостности, сначала на тестовом стенде	Тестовый стенд, выделенный источник обновлений	**КО**
Данные ограниченного доступа (ОД)	Доступ по списку, контроль и регистрация каждой выгрузки, учтённые носители	DLP, СЗИ от НСД, учтённые носители	**ОД; п. 40**
Привилегированный доступ (ПД)	Учётные записи за работниками, строгая аутентификация, запись действий	Средства контроля администраторов (PAM)	**ПД; ИАФ.3**
Удалённый доступ (УД)	Только по необходимости, двухфакторный вход, защищённый канал	СКЗИ (VPN), средства аутентификации	**УД**
Мониторинг ИБ (МБ)	Сбор и анализ событий, контроль действий пользователей и потоков данных	SIEM, СОВ	**МБ; п. 49**
Непрерывность и резервирование (НФ)	Копии данных и настроек на разных носителях, сроки восстановления, тренировки	Система резервного копирования	**НФ; пп. 52–55**
Искусственный интеллект (ИИ)	Оценка угроз, защита обучающих данных и модели, фильтрация запросов и ответов	Доверенные технологии ИИ	**ИИ; пп. 60–61**
Контроль защищённости (ПК)	Анализ уязвимостей или тест на проникновение раз в 3 года и после инцидента	Средства анализа защищённости	**ПК; пп. 66–67**

Криптографические меры

Где применяем	Что делаем	Требование
Каналы между МО и витриной	Шифрование трафика (VPN по ГОСТ)	**ЗКС.1; п. 7 приказа № 117**
Веб-доступ и API	Защищённое соединение (TLS по ГОСТ)	**ЗПИ.1, ЗКС.1**
Удалённый доступ	Только через СКЗИ; подрядчики только из РФ	**мероприятия УД, ЗП**
Базы данных и резервные копии	Шифрование, ключи хранятся отдельно от данных	**мероприятие ОД, усиление 1**
Вход администраторов	Строгая аутентификация: токен с неизвлекаемым ключом	**мероприятие ПД; ИАФ.3**
Обновления ПО	Проверка подлинности по сертификатам на ГОСТ	**мероприятие КО**
Журналы и модели ИИ	Целостность журналов; шифрование обучающих данных, целостность модели	**РСБ.4 ус. 5; ИИ ус. 2, 6**
Псевдонимы пациентов	Хэш с секретным ключом (по ГОСТ); хэш СНИЛС	**рекомендация**

Организационные правила: только сертифицированные ФСБ России средства шифрования; класс по приказу ФСБ № 378; поэкземплярный учёт средств и ключей (Инструкция ФАПСИ № 152); назначенный ответственный; плановая смена ключей

Обезличивание данных для статистики

Персонифицированные
Видно: ФИО, СНИЛС, диагноз
Кто: врачи и регистры, по списку

→ обезличиваем при загрузке →

Обезличенные
Видно: пациент под номером
Кто: статистики, аналитики

→ считаем итоги →

Агрегированные
Видно: только цифры
Кто: руководители, формы, публикации

Признак	Было	Стало
ФИО	Петрова А. В.	**ID 7F3A-91C2**
Дата рождения	12.03.1987	**35–39 лет**
Адрес	Профсоюзная, 12	**ЮЗАО**
Диагноз	E10.9	**E10**
Дата визита	14.05.2026	**05.2026**

Почему удалить ФИО недостаточно
Дата рождения, район и редкий диагноз вместе часто указывают на одного человека

Когда обезличиваем: автоматически при загрузке в витрину, внутри защищённого контура, а не вручную после выгрузки (п. 9 ч. 1 ст. 6 152-ФЗ)

Правила для регламента

1. Укрупнять возраст, адрес и даты
2. Скрывать ячейки с единичными случаями
3. Ключ «псевдоним — пациент» хранить отдельно
4. Проверять публикации на узнаваемость
5. Регламент и учёт действий (приказ РКН № 140)
6. Пока есть ключ, данные остаются персональными

Кейс 1. Украденный пароль аналитика

Модельная ситуация

Ситуация

Аналитик получил письмо «от службы поддержки» и ввёл пароль на поддельной странице.

Через два дня ночью с его учётной записи и с незнакомого устройства пошёл массовый запрос к витрине.

Итог: ПДн не пострадали, сработали разделение зон, мониторинг и лимиты

Как сработала защита

02:14 — Массовый запрос к витрине с нового устройства

↓

02:15 — SIEM поднимает тревогу: нетипичные время, объём и устройство

↓

02:22 — Дежурный блокирует учётную запись; выгрузку останавливает лимит объёма

↓

09:00 — Разбор: у аналитика был доступ только к обезличенной витрине, ПДн в системе не затронуты

Выводы и меры

- Ввести двухфакторный вход для всех пользователей витрин
- Учебные фишинговые рассылки и обучение
- Мониторинг с дежурством 24/7
- Разделение зон спасло персональные данные
- Инцидент зарегистрирован, сведения переданы в ГосСОПКА

Кейс 2. Учётная запись уволенного сотрудника

Модельная ситуация

Ситуация

Аналитик уволился, но его учётную запись в витрине не заблокировали: кадровая служба не сообщила в ИТ.

Через месяц кто-то вошёл под этой учётной записью и выгрузил 10 000 записей чувствительной информации.

Как это произошло

День 0 — Аналитик уволен, учётную запись не заблокировали

↓

День 30 — Вход под этой учётной записью и выгрузка 10 000 записей

↓

День 37 — Выгрузку замечают только при плановом просмотре журнала

↓

День 37 — Блокировка, расследование

Выводы и меры

- Блокировать доступ в день увольнения или перевода
- Кадровая служба сразу сообщает в ИТ и ИБ
- Раз в квартал сверять учётные записи с кадровыми приказами
- Тревога при входе в давно неиспользуемую учётную запись
- Включить двухфакторный вход

Что сделать в первую очередь

Руководителям и организаторам

- Назначить владельца данных каждой витрины
- Утвердить политику и регламенты по защите
- Выделить ресурсы на защиту и обучение
- Раз в полгода запрашивать показатель Кзи

Службе защиты информации

- Классификация витрин и модель угроз
- Настроить мониторинг выгрузок
- Проверять подрядчиков до допуска
- Обучение сотрудников, учебные рассылки

ИТ-службе

- Вести журналы запросов и выгрузок
- Вовремя устанавливать обновления
- Проверять восстановление из резервных копий

Статистикам и аналитикам

- Работать с обезличенными данными
- Выгружать только то, что нужно для задачи
- Не загружать данные в публичные чат-боты
- Сообщать о подозрительных письмах

Выводы

1

Витрина данных — это информационная система

Действуют приказ ФСТЭК № 117 и ПП № 1119: класс, модель угроз, меры защиты, аттестация для ГИС

2

Основные риски связаны с людьми и процессами

Украденные пароли, лишние права, бесконтрольные выгрузки, подрядчики и публичные ИИ-сервисы

3

Защита работает только в комплексе

Организационные, технические и криптографические меры; уровень защищенности оценивается по Кзи раз в полгода

4

Статистику ведём на обезличенных данных

Данные с ФИО остаются в защищённом сигменте, аналитики работают с обезличенными наборами

VIII СЪЕЗД МЕДИЦИНСКИХ СТАТИСТИКОВ ГОРОДА МОСКВЫ

МОСКОВСКАЯ МЕДИЦИНА

НИИ ОРГАНИЗАЦИИ ЗДРАВООХРАНЕНИЯ И МЕДИЦИНСКОГО МЕНЕДЖМЕНТА

Спасибо за внимание!