Информационная безопасность в медицинской организации

Реальные угрозы, последствия и здравый смысл

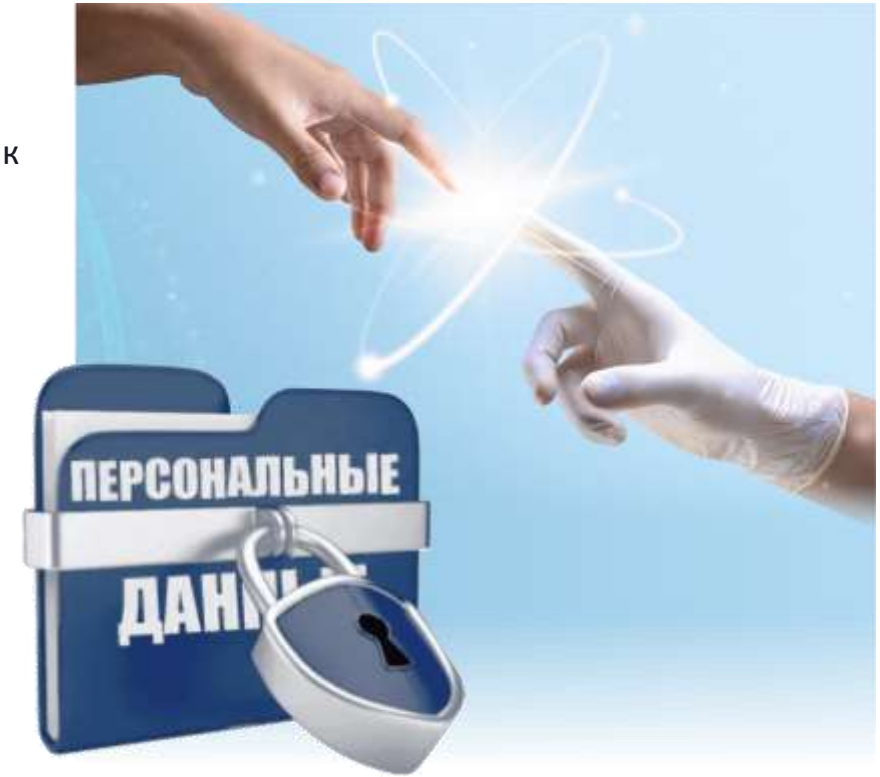
ариадна

XXVI Ежегодный всероссийский конгресс
"Информационные технологии в медицине".
Москва, 9-10 октября 2025

itmcongress.ru

О чём поговорим

- История краж и разрушения данных в медицине — к чему приводит беспечность.
- Почему защита информации в МО — это критично.
- Основные нормы РФ: 152-ФЗ, 323-ФЗ, ПП №1119, приказы ФСТЭК и др.
- Ответственность: административная, уголовная, гражданская.
- Реальная практика РФ: статистика и кейсы.
- Угрозы и типовые источники утечек.
- Удалённый доступ: что можно, а что нельзя
- Меры защиты и правильная последовательность работ.
- Выводы и чек-лист для руководителя.



Сентябрь 2025. Крупнейшая потеря данных в Корее

26 сентября пожар в дата-центре Национальной службы информационных ресурсов (NIRS).

Причина – возгорание заменяемой Li-Ion батареи.

Последствие:

- Утрата 96 критически-важных систем
- Отключение 647 государственных сервисов
- 585 терабайт данных, включая архивные сведения
- Самоубийство чиновника, ответственного за сохранность и восстановление данных.

История краж персональных данных (медицина, мир)

- **Anthem Insurance** (США, 2015): похищено ~78,8 млн записей; рекордные выплаты и штрафы.
- **WannaCry** (NHS, Великобритания, 2017): 60 медорганизаций парализованы, сорваны услуги, отменено ≈19 тыс. приёмов, ущерб 92 млн фунтов.
- **SingHealth** (Сингапур, 2018): похищены медицинские данные 1,5 млн пациентов, включая Премьера-министра.
- **Change Healthcare** (США, 2024): крупнейший инцидент, массовый сбой процессов, вынудил пациентов оплачивать лечение из собственных средств. Выкуп 22млн $

Крупнейшие хакерские атаки в РФ 2025

- **Сети аптек «Столички» и «Неофарм»** - утрата данных, нарушение логистики, закрытие розничных магазинов, сотни миллионов убытков от вынужденного простоя и складского хаоса.
- **Клиники «Семейный доктор»**
  - **ЕМИАС Московской области** – 17 ТБ документов (амбулаторные карты, истории болезни, назначения, схемы лечения, логины и технические ключи и многое другое)
  - **А еще**: Аэрофлот, Аэропорт Пулково, РЖД (DDoS-атаки), Ростелеком (~110 тыс телефонов и 154 тыс e-mail) и др.

Вывод: медицина — «сладкая цель» из-за ценности данных и критичности процессов.

Почему защита информации в здравоохранении важна

Репутационные риски и недоверие пациентов

Юридические последствия для организации и сотрудников

Срыв оказания помощи: простой регистратуры, ЛИС/МИС, телемедицины

Этическая сторона: врачебная тайна – базовое право пациента

Финансовые потери: штрафы, компенсации, восстановление ИТ, прямые потери

Утрата критически важных сведений о состоянии здоровья пациентов

Основные нормативные акты РФ (базовый минимум)

- **152-ФЗ** «О персональных данных»
  + **242-ФЗ** (локализация ПДн, трансграничная передача).
- **323-ФЗ (ст. 13)** — врачебная тайна и запрет разглашения.
- **ПП РФ №1119** — требования к защите ПДн в ИСПДн (определение уровней защищённости).
- **Приказ ФСТЭК №21** — состав мер защиты ПДн в ИСПДн.
- **187-ФЗ** и **ПП №127** — КИИ: категорирование, требования к безопасности.
- **Приказ ФСТЭК №77** — аттестация объектов информатизации; №117 (2025) — новые требования для ГИС/МИС (вступят 01.03.2026).

Ответственность за нарушения

КоАП РФ ст. 13.11 — штрафы за нарушения в области ПДн (в т.ч. за утечки).

КоАП РФ ст. 13.14 — разглашение информации с ограниченным доступом.

УК РФ ст. 137 — нарушение неприкосновенности частной жизни (в т.ч. врачебной тайны).

ГК РФ ст. 150–152, 151 — нематериальные блага и компенсация морального вреда.

Тенденция: ужесточение санкций и «оборотные» штрафы при повторных утечках.

Судебная практика РФ (кейсы)

1. Передача данных о пациентах третьим лицам (в т.ч. ритуальным службам) — крупные штрафы и запрет занимать должности.

2. Привлечение к ответственности медработников за разглашение врачебной тайны (ч. 2 ст. 137 УК РФ).

3. Административные дела по ст. 13.11 КоАП РФ в отношении операторов ПДн за утечки/несоблюдение режима, использование запрещенных методов удаленных подключений.

Вывод: персональная ответственность сотрудников реальна; организации несут финансовые и репутационные потери.

Типовые угрозы в медицине

- Фишинг/социнжиниринг (мессенджеры, письма «от руководства/поставщика»)
- Вредоносные программы/шифровальщики (блокировка ЛИС/МИС, пулемётное шифрование)
- Компрометация удалённого доступа (открытый RDP/VPN без СКЗИ и МФА)
- Ошибки настройки облачных хранилищ и резервных копий
- Инсайдеры: небрежность, умышленная передача данных
- Риски подрядчиков/ИТ-провайдеров (третьих сторон)

Типичная ситуация в безопасности МО

Купить средства защиты информации за десятки миллионов рублей, провести аттестацию ИСПДн и жестко следовать регламентам информационной безопасности

Оставить открытый RDP из дома с доступом до серверов и рабочих мест МО

Практика утечек в России (факты)

- За 2024 год РКН: 135 утечек баз, >710 млн записей о россиянах.
- Здравоохранение — одна из уязвимых отраслей: сочетание ПДн и медтайны.
- Тенденция к росту числа инцидентов в 2025 г. в медицине относительно II полугодия 2024 г.

Вывод: системная защита и дисциплина персонала — ключевые факторы снижения риска.

Запреты и допустимы разрешения при работе с ПДн

Нельзя: «голый» RDP из Интернета, «одноразовые» пароли, расшаренные учётки. AnyDesk/TeamViewer под строжайшим запретом.

Можно: сегментация сети (МИС/ЛИС/РМИС/АРМы), минимизация привилегий, контроль съёмных носителей.

Нельзя: хранить/обрабатывать ПДн пациентов в облаках за пределами РФ без соблюдения локализации и требований закона.

Для гос. МО: при закупках — ориентироваться на реестр отечественного ПО (ПП №1236) и реестр сертифицированных СЗИ (ФТСЭК).

Можно: VPN с сертифицированными СКЗИ (ФСБ/ФСТЭК), двухфакторная аутентификация, с ведением журналов доступа.

Меры ИБ: организационные

- Подписание соглашений об информационном обмене и межсетевом взаимодействии с допущенными вендорами ПО
- Назначение ответственных (оператор ПДн, ИБ-инженер), утверждение Положений/Политик.
- Классификация ИСПДн, модель угроз, определение уровня защищённости по ПП №1119.
- Обучение/тестирование персонала (врачебная тайна, фишинг-тренинги).
- Режим доступа: разграничение ролей, принцип «минимально необходимого».
- Регламенты реагирования на инциденты и уведомления (в т.ч. РКН, ФСБ при КИИ).

Меры ИБ: технические

- Сетевой периметр: межсетевые экраны, фильтрация, IDS/IPS, WAF (для веб-порталов).
- Защита рабочих мест/серверов: антивирус/EDR, контроль приложений, шифрование дисков.
- Управление уязвимостями и обновлениями (приоритет — интернет-экспонируемые сервисы).
- Резервное копирование с изоляцией (offline/immutable), регулярные проверки восстановления.
- Журналирование и корреляция событий (SIEM/SOC), контроль аномалий доступа (UEBA/DLP).
- MFA, парольная политика, запрет общих учёток.

Правильный порядок работ (ФСТЭК/КИИ)

- 1) Инвентаризация ИС и данных; 2) Составление модели угроз; 3) Выбор мер по ПП №1119 и Приказу №21.
- Закупка/внедрение СЗИ (сертифицированные средства по реестрам ФСТЭК/ФСБ при необходимости).
- Аттестация объектов информатизации по Приказу ФСТЭК №77 (при применимости).
- Оценка на предмет отнесения к КИИ, при наличии признаков — категорирование по ПП №127, выполнение Приказа №239.
- Подготовка к переходу на новые требования для ГИС/МИС (Приказ ФСТЭК №117, с 01.03.2026).

Что запрещено сотрудникам МО (и почему)

- Передавать ПДн/медтайну в мессенджеры/почту/облака.
- Использовать личные устройства без контроля безопасности.
- Подключаться к ИС МО из публичных Wi-Fi без защищённого канала.
- Снимать фото/скриншоты экранов с данными пациентов для личного использования.
- Делегировать пароли коллегам/подрядчикам; хранить их на стикерах или «под стеклом».
- Контактировать с третьими лицами и передавать им доступы, информацию, выписки, скриншоты, кем бы они не представлялись

Работа с подрядчиками и облачными сервисами

- Договором закреплять меры защиты ПДн, ответственность, порядок уведомления об инцидентах.
- Проверка локации хранения данных (локализация в РФ), реестры сертифицированных СЗИ.
- Регулярные аудиты/пентесты по согласованному периметру.
- Ограничение доступа подрядчикам по принципу «минимально необходимого», подписание соглашений и NDA.
- План непрерывности и восстановления бинзнес-процессов (BCP/DRP) для критичных сервисов.

Реагирование на инциденты

- Разработка плана реагирования: роли, контакты, сценарии (шифровальщик, утечка, DDoS).
- Отключение/изоляция, форензика (расследование инцидента), восстановление по резервным копиям.
- Уведомление РКН/ФСБ (в т.ч. о трансграничной передаче при необходимости), взаимодействие с правоохранительными органами.
- Коммуникации с пациентами: прозрачность, поддержка (горячая линия, информационные сообщения, анализ публичных сведений).
- Пост-инцидентный разбор и корректировка мер защиты, разработка превентивных мер с учетом полученного опыта.

Чек-лист руководителя МО

- Назначены ответственные, утверждены политики и реестр ИСПДн?
- Определён УЗ по ПП №1119, разработана модель угроз и план мер по Приказу №21?
- Закуплены/внедрены СЗИ, организовано резервное копирование и мониторинг?
- Настроен безопасный удалённый доступ (VPN с СКЗИ, МФА), проведена сегментация?
- Проведено обучение персонала и тренировки (включая фишинг-симуляции)?
- Проведена аттестация по №77 (при применимости) и проверка на КИИ (ПП №127)?

Выводы

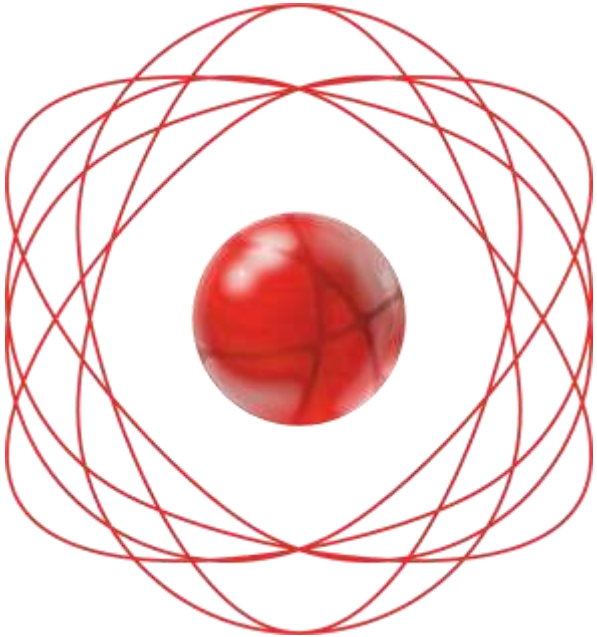
Медицина — критичная отрасль: цена ошибки - жизнь.

Выполнение требований 152-ФЗ, 323-ФЗ, ПП №1119 и приказов ФСТЭК — базовый минимум.

Главные факторы — дисциплина персонала и регулярная практика, в т.ч. при кадровой текучести.

Технические меры без процессов — недостаточны; процессы без техники — не работают.

Делаем защищённо и удобно: дорого, сложно, но не только возможно, а еще и необходимо.



«Путь в тысячу ли начинается с одного шага»…

ариадна

Контакты ООО «Решение»

190005, Санкт-Петербург,
Измайловский пр., д. 29, лит. А,
бизнес-центр «Маркс»
Тел. +7 (812) 337-70-07
info@reshenie-soft.ru

Богданов Алексей Александрович
Заместитель генерального директора
alexey@reshenie-soft.ru
https://t.me/AlexeyBogdanovSpb
+7 (921) 319-24-95