Министерство здравоохранения
Удмуртской Республики

Проблемы и задачи по обеспечению информационной безопасности в медицинских организациях Удмуртской Республики.

Проблемы и задачи по обеспечению информационной безопасности в медицинских организациях Удмуртской Республики

Определения

- **ЗСПД -** Защищенная сеть передачи данных Министерства здравоохранения Удмуртской Республики №2070
- **ЕГИСЗ –** Единая государственная информационная система в сфере здравоохранения Удмуртской Республики
- **КИИ –** Критическая информационная инфраструктура, совокупность объектов КИИ
- **Объекты КИИ –** совокупность объектов КИИ, информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов КИИ
- **Субъекты КИИ –** любой орган власти, юридическое лицо, организация которому принадлежит хотя бы одна информационная система, используемая в этих отраслях

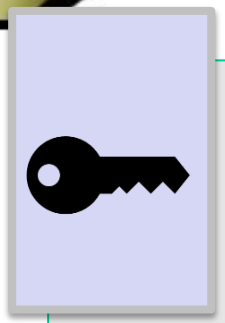
Проблемы и задачи по обеспечению информационной безопасности в медицинских организациях Удмуртской Республики

Информационные угрозы сегодня

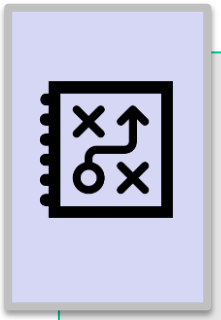
- **Внешние угрозы:**
- деятельность иностранных спец. служб
- деятельность преступных групп или злоумышленников
- промышленный шпионаж
- стихийные бедствия, аварии

- **Внутренние угрозы:**
- неправомерные действия должностных лиц
- преднамеренные действия персонала
- непреднамеренные действия персонала
- отказы технических средств

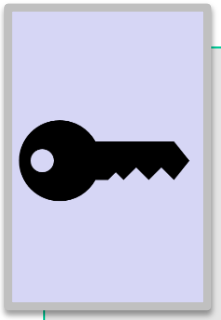
Угрозы информационной безопасности



Нарушение конфиденциальности (утечка, разглашение)



Нарушение работоспособности (дезорганизация работы)



Нарушение целостности и достоверности информации

Основные нормативные документы для реализации требований законодательства в области информационной безопасности в медицинских организациях Удмуртской Республики

- Федеральный закон "О персональных данных" от 27.07.2006 № 152-ФЗ
- Приказ ФСТЭК России от 11.02.2013 № 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"
- Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 № 187-ФЗ

Организация защищенной сети передачи данных Минздрава Удмуртии

ФЦОД ЕГИСЗ

Прикладные сервисы и БД (Сервис записи на прием)

АРМ Адм. без-ти ФЦОД (VPN-Сеть ФЦОД ЕГИСЗ МО ФП)

Сервер без-ти ФЦОД ПАК ViPNet HW 2000 в кластере (VPN-Сеть ФЦОД ЕГИСЗ)

Региональный сегмент ЕГИСЗ

ЦОД / МИС МО Субъекта

АРМ-ы/ Терминалы

ЛВС

Главный сервер без-ти МО Субъекта ПАК ViPNet HW 1000 (VPN-Сеть МО Субъекта)

АРМ Адм. без-ти МО Субъекта на базе ViPNet Administrator (VPN-Сеть МО Субъекта)

Сервер мониторинга МО Субъекта на базе ViPNet StateWatcher (VPN-Сеть МО Субъекта)

Сеть передачи данных Оператора

УД Оператора СПД

Сервер без-ти МО Субъекта ПАК ViPNet HW 1000/HW 2000 в кластере (VPN-Сеть МО Субъекта)

Шлюз без-ти МО Субъекта ПАК ViPNet HW 1000 в кластере (VPN-Сеть ФЦОД ЕГИСЗ)

Сеть передачи данных МО Субъекта РФ

Шлюз без-ти МО Субъекта на базе ПАК ViPNet (VPN-Сеть МО Субъекта

ЛВС МО

АРМ-ы/ Терминалы

МО Субъекта РФ

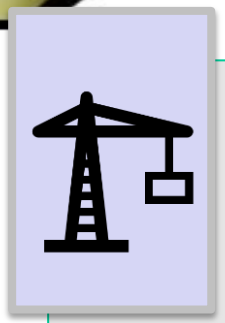
АРМ МО Субъекта ПО ViPNet Client (VPN-Сеть МО Субъекта)

МО Субъекта РФ

Терминал МО Субъекта ПАК ViPNet Terminal (VPN-Сеть МО Субъекта)

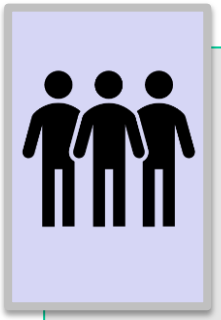
МО Субъекта РФ

Цели и задачи защищенной сети Минздрава Удмуртии



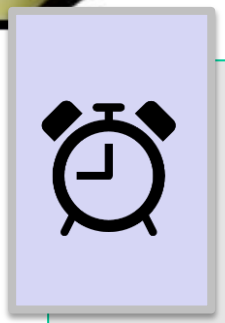
Организация единого информационного поля для обмена информацией, относящейся к категории персональных данных и врачебной тайны, по защищенным каналам связи

Сопровождение федеральных и региональных регистров с персональными данными (федеральный регистр медицинских работников, федеральный регистр медицинских организаций и т.д.)

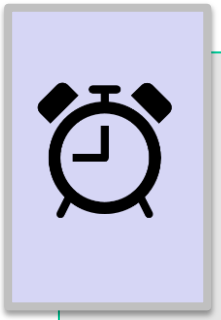


Предоставление государственных услуг на региональном портале государственных услуг (РПГУ), едином портале государственных услуг (ЕПГУ)(запись на прием к врачу и т.д.)

Обновление узлов защищенной сети передачи данных Министерства здравоохранения Удмуртской Республики № 2070 до версии 4.x



Необходимость обновления версии программно-аппаратных средств, входящих в состав защищенной сети передачи данных (ЗСПД) Министерства Здравоохранения Удмуртской Республики №2070 до версии 4.x



Срок действия сертификатов соответствия для ViPNet 3.x истек

Обновление до версии 4.x в 2019 году по программе «Развитие информационного общества»

Антивирусный контроль в медицинских организациях Удмуртской Республики

Оснащенность рабочих мест и серверов в мед. организациях Удмуртской Республики антивирусным ПО Dr.Web

По данным на 30 ноября 2018 года в Удмуртской Республике было обезврежено 1 163 513 угроз

Антивирусный контроль в медицинских организациях Удмуртской Республики

Причины оснащения всех рабочих мест и серверов государственных медицинских организаций антивирусным ПО Dr.Web предоставляемым АУ УР «РИЦ УР»

- Экономия средств организации
- Запрет на приобретение или продление иного антивирусного ПО (Нецелевое расходование средств)
- Часть проекта подключения информационных систем Удмуртской Республики к Государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) в соответствии с 187-ФЗ

Федеральный закон от 26.07.2017 № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"

Федеральный закон от 26.07.2017 № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"

Критическая информационная инфраструктура

Все информационные системы в следующем перечне:

- **Здравоохранение**
- Наука
- Транспорт
- Связь
- Энергетика
- Атомная энергетика
- Банковская и иные сферы финансового рынка
- Топливно-энергетический комплекс
- Оборонная промышленность
- Ракетно-космическая отрасль
- Горнодобывающая, металлургическая и химическая промышленность

Федеральный закон от 26.07.2017 № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"

Обязанности субъекта КИИ

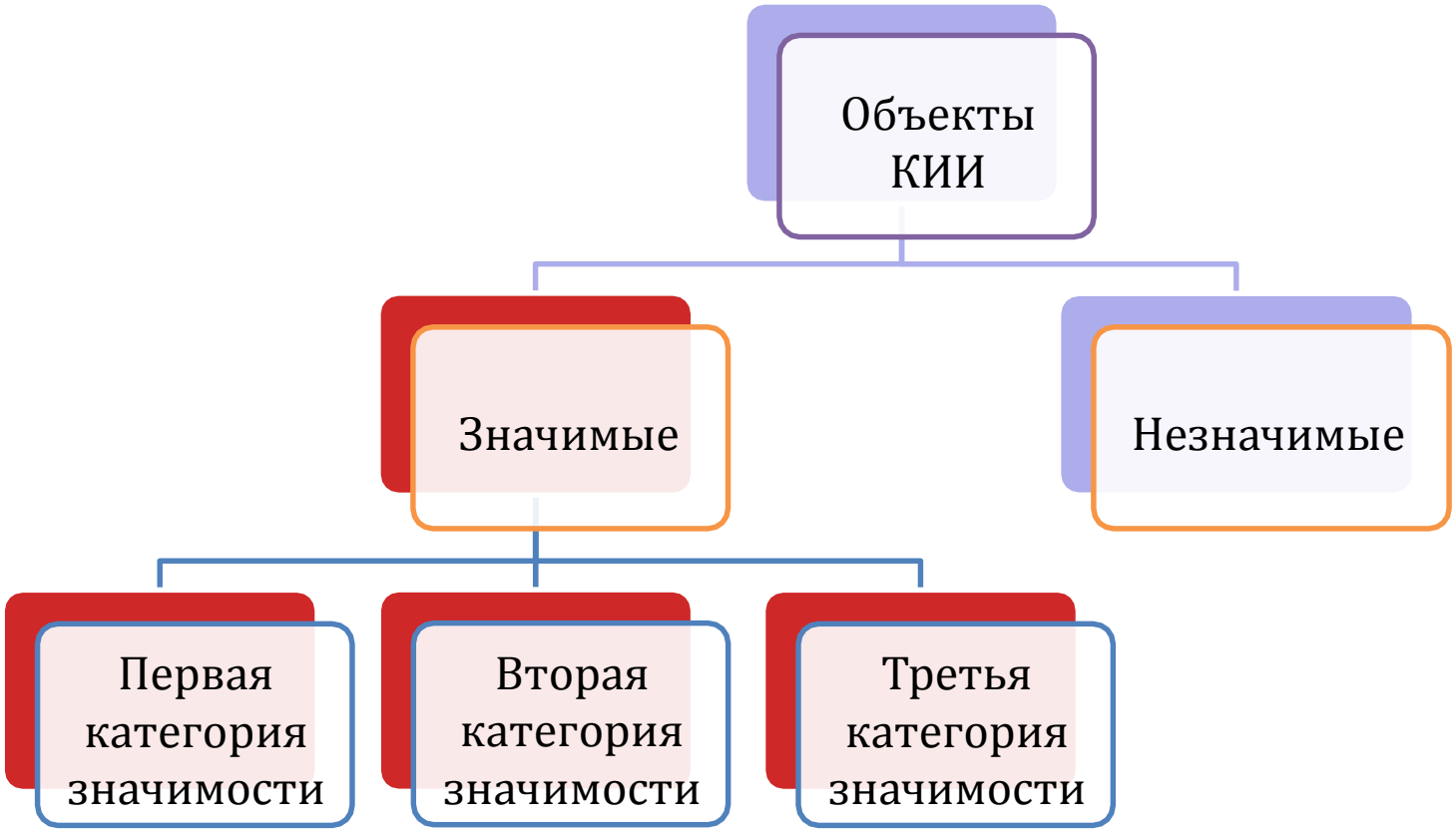
- Обязан незамедлительно информировать ФСБ об инцидентах
- Обязан оказывать содействие должностным лицам ФСБ в деятельности, связанной с предупреждением, обнаружением и ликвидацией последствий инцидентов
- Обязан соблюдать требования ФСТЭК по обеспечению безопасности значимых объектов КИИ
- Обязан выполнять предписания ФСТЭК об устранении выявленных нарушений
- Обязан реагировать на инциденты в порядке, утвержденном ФСБ
- Обязан обеспечить доступ должностным лицам ФСТЭК к значимым объектам КИИ для проведения надзорных действий

Федеральный закон от 26.07.2017 № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"

Выбор категории объектов КИИ

- Субъект КИИ сам определяет категории значимости своих объектов
- Серьезные требования предъявляются только к значимым объектам КИИ
- Невыполнение требований грозит уголовным преследованием

Федеральный закон от 26.07.2017 № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"



Федеральный закон от 26.07.2017 № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"

Ответственность субъекта КИИ

- **Глава 28 УК РФ Статья 274.1**

- Нарушение правил эксплуатации, если оно повлекло причинение вреда критической информационной инфраструктуре Российской Федерации:
- принудительные работы на срок до пяти лет с лишением права занимать определенные должности;
- лишение свободы на срок от трех до восьми лет (группой лиц по предварительному сговору);
- Лишение свободы насрок от пяти до десяти лет (тяжкие последствия).

• Следствие по уголовным делам по этим статьям передаётся в ведение ФСБ

Федеральный закон от 26.07.2017 № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"

Распоряжение МЗ УР №967 от 10.08.2018

«По обеспечению безопасности объектов КИИ в государственных медицинских организациях УР»

- Создать комиссию по категорированию объекта (До 15.08.2018)
- Разработать, утвердить и направить в управление ФСТЭК России и управление ФСТЭК России по ПФО перечень объектов КИИ (До 30.08.2018)
- Провести категорирование объектов КИИ, результаты направить в управление ФСТЭК России и управление ФСТЭК России по ПФО (До 01.01.2019)

Создание единого цифрового контура в здравоохранении Удмуртской Республики на основе государственной информационной системы здравоохранения

Задачи проекта в области защиты информации

- **Создание и внедрение концепции типовых организационно-технических мер в области ИБ для медицинских организаций;**
- Приобретение в рамках проекта для медицинских организаций средств защиты информации с целью реализации технических мер защиты информации в соответствии с требованием законодательства;
- Создание системы обнаружения вторжений с последующим подключением к Государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА);
- Подключение новых и дооснащение имеющихся площадок криптографическими шлюзами ViPNet
- Аттестация информационных систем в мед. организациях.

Спасибо за внимание!