Информационная безопасность: современные задачи и решения

Майшев Вадим
ООО «КриптоСвязь»

ООО «КриптоСвязь»

- **Опыт работы на профессиональном рынке защиты информации с 2012 года**
  - Лицензии по защите информации в группе компаний «Ижинформпроект» с 2003 года

ООО «КриптоСвязь»

- Опыт работы на профессиональном рынке защиты информации с 2012 года
- **Лицензии ФСБ, ФСТЭК и Минобразования**
  - Криптографическая защита информации
  - Техническая защита конфиденциальной информации
  - Образовательная деятельность

ООО «КриптоСвязь» - лицензии

- Лицензия Управления **ФСБ России** по Удмуртской Республике № 122Н от 24.12.2018
- Лицензия Федеральной службы по техническому и экспортному контролю (**ФСТЭК России**) № 2347 от 30.07.2014
- Лицензия Министерства образования и науки Удмуртской Республики (**МОиН УР**) № 506 от 06.08.2015

ООО «КриптоСвязь»

- Опыт работы на профессиональном рынке защиты информации с 2012 года
- Лицензии ФСБ, ФСТЭК и Минобразования
- **Партнер ведущих российских производителей средств защиты информации**

ООО «КриптоСвязь» - партнеры

ООО «КриптоСвязь» - партнеры

- Золотой партнер
- Стратегический партнер по ПФО
- Сервисный партнер

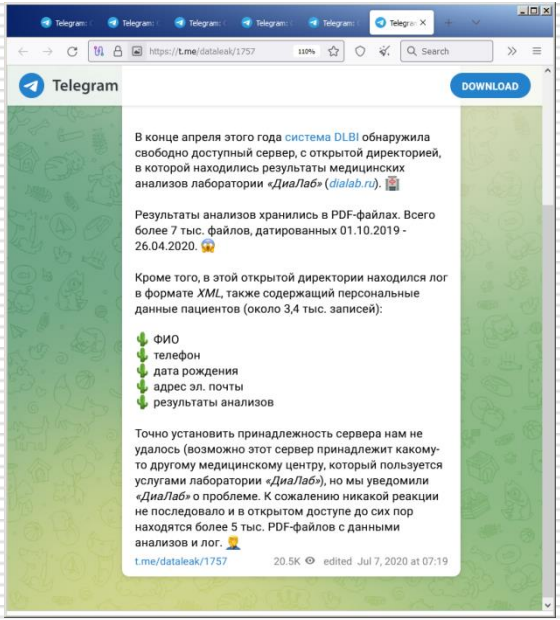
- Платиновый партнер

Сервисы компании

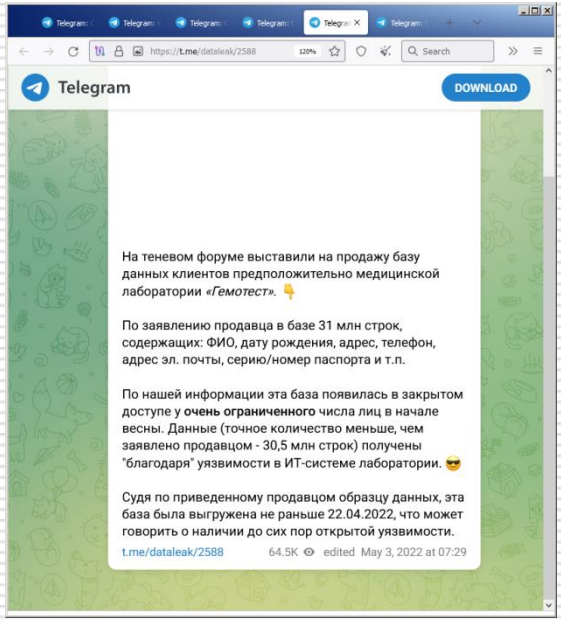
- Сертифицированные средства защиты информации и их сопровождение
  - Максимальный ассортимент
  - Обоснованный оптимальный выбор
  - Нормативное внедрение
  - Компетентная техническая поддержка
- PKI (ЭЦП, ЗЭД, TLS)
- VPN
- Подключение к ФГИС
- КИИ и ГосСОПКА
- Отечественное программное обеспечение

Утечки в медицине

- ДиаЛаб, 2020

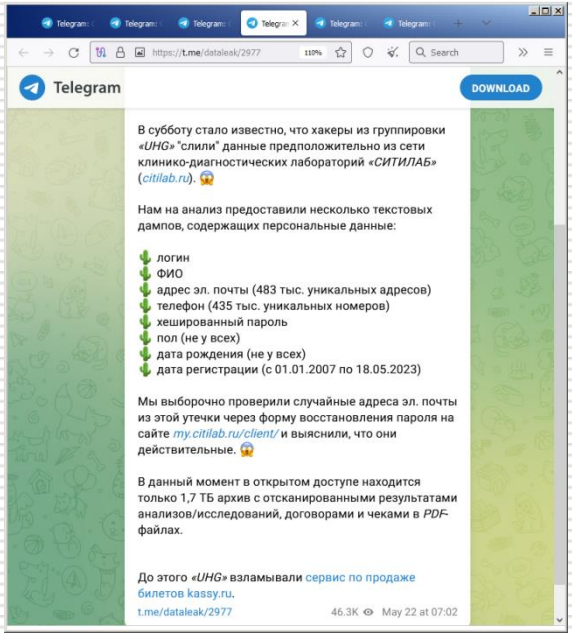


- Гемотест, апрель 2022

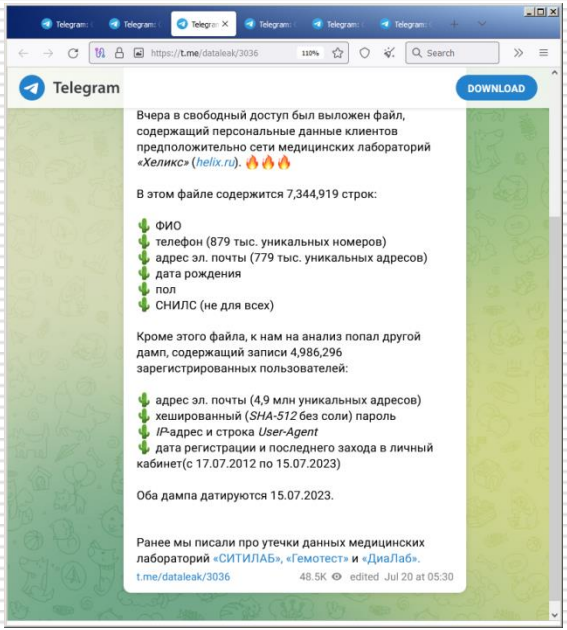


Утечки в медицине

- СИТИЛАБ, май 2022

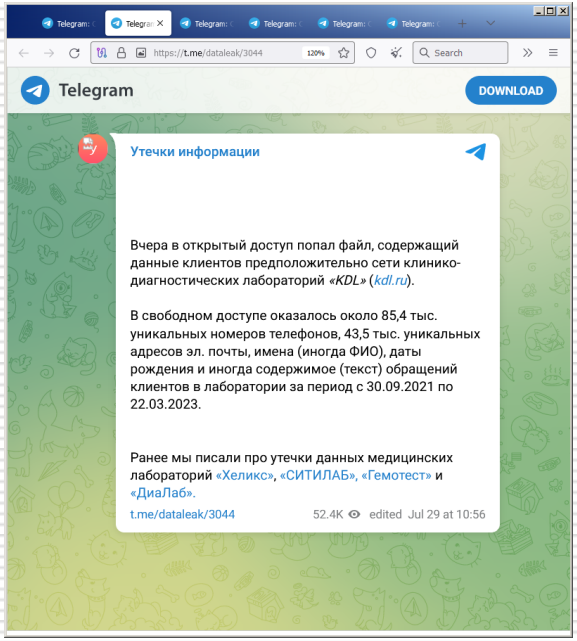


- Хеликс, июль 2023

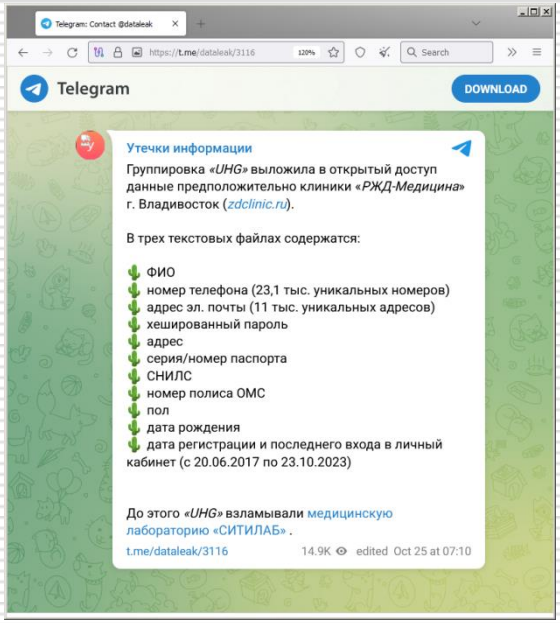


Утечки в медицине

- KDL, июль 2023



- РЖД-Медицина, октябрь 2023



Решения

- Удобно ИЛИ (И) Безопасно?
- Пароль (и OTPviaSMS тоже) ≠ защита информации!
- Вход в ИС с незащищенного терминала = данные в ИС не защищены

- Комплекс защитных мер (EPP/ЦОД + PKI/VPN)
  - Антивирус
  - СЗИ НСД (доверенная загрузка/идентификация/аутентификация/авторизация/контроль доступа)
  - МЭ (NGFW и WAF)
  - СКЗИ (шифрование и ЭЦП)
  - Обнаружение и предотвращение атак (IDS/IPS)
  - Анализ защищенности/DLP/Резервирование/…
  - Шифрование канала (с двусторонней криптографической аутентификацией) и/или данных

Госмеры: вектор развития ИБ

- Первомайский указ № 250
  - Субъекты КИИ:
    - Заместитель руководителя – полномочия по ИБ
    - Структурное подразделение ИБ - функции по ИБ
    - Привлечение к мероприятиям лицензиатов ТЗКИ
    - Привлечение аккредитованных центров ГосСОПКА
    - (Удаленный) доступ ФСБ к мониторингу защищенности ИР
    - Незамедлительная реализация мер, указанных ФСБ/ФСТЭК
  - Руководитель – персональная ответственность за ИБ
  - Типовые положения о заместителе руководителя и подразделении ИБ
    - ППРФ от 15.07.2022 № 1272
    - Заместитель руководителя – высшее образование по ИБ (специалитет/магистратура или профпереподготовка)
  - 01.01.2025 - запрет использовать СЗИ из «недружественных стран»

Public Key Infrastructure (ЭЦП)

- Революционные изменения 63-ФЗ (*по УКЭП*)
  - АУЦ: 1 000 000 000 ₽ (ФЛ + *временно ЮЛ-сотрудник)*
  - УЦ ФНС России (ЮЛ-руководитель и ИП)
    + УЦ ФК России (ДЛГО) + УЦ Банка России (банки)
- Машиночитаемая доверенность (МЧД)
  - Уникальное в мире и нестандартное решение
  - ПДн в МЧД в каждом ЭД + Реестр(ы) доверенностей
  - Некриптографическая суть (было: проверка ЭЦП+CER
    стало: проверка ЭЦП+CER + «юрстатус» МЧД)
- Промежуточные итоги:
  - Уничтожены все «бедные» аккредитованные УЦ
  - ~~МЧД промышленно нет ни в одной ИС~~ каждая ИС принимает «свою» МЧД
  - ЮЛ-сотрудник до ~~31.12.2021,~~ ~~31.12.2022,~~ 31.08.2023 («умрут» 01.09.2024)
  - Вместо оригиналов документов (ЭД с ЭЦП) или их скан-копий в стране начался повсеместный оборот «картинок ЭД со штампиками»
  - «Зарегулирование» УНЭП как УКЭП и популяризация Госключа

Public Key Infrastructure (ЗЭД)

- Расширение взаимодействия G2B и B2B (G2C/B2C - ?защита?)
- Сервисы отраслевого защищенного электронного документооборота
  - Отчетность
  - Регистрационный и миграционный учет (*7 регионов*)
  - Медицина труда (*20 регионов*)
- Комплекс средств защиты информации
  - СЗИ НСД/МЭ/АВС/…
  - Двусторонняя криптографическая аутентификация
  - Шифрование по ГОСТу канала связи и ДОКУМЕНТА

Public Key Infrastructure (TLS)

- Специализированные TLS шлюзы
- Различная криптография
  - ГОСТ (28147-89, Р 34.12-2015 + Р 34.13-2015)
  - RSA и ECDSA
- Функционал
  - Удобство сопряжения с некриптографическими ИС
  - Шифрование канала на прикладном уровне
  - Двусторонняя криптографическая аутентификация
- Нет шифрования документа

Virtual Private Network

- Защита сетей передачи данных и Межведомственное взаимодействие
- Услуги VPN на основе ViPNet (КС3)
  - Комплексная защита информации
    - Site-to-Site VPN
    - Remote access VPN/Point-to-Site VPN
    - Point-to-Point VPN
  - ПАК, VA, Windows, Linux, MacOS, Android, iOS, Аврора
  - Межсетевое взаимодействие:
    - ИД Пенсионного фонда Российской Федерации (314)
    - ОПФР по Удмуртской Республике (430)
    - Минсоцполитики Удмуртской Республики (577)
    - ФГУП «Почта России» (6474)
    - ЗАО «Перспективный мониторинг» (10253)
    - ООО «ЭлНетМед» (12848)
- + МЭ/IPS, промышленные шлюзы

Подключение к ФГИС

- RSNet
- ФГИС Росаккредитации
- ФИС ФРДО, ФИС ГИА (ЕГЭ) и Приема
- ЕИСУ КС
- ФГИС ЦС
- …

КИИ и ГосСОПКА

- Анализ и корректировка информационных процессов
- Разработка организационно-распорядительных документов
  - АльфаДок!
- Защита серверов/рабочих мест и сетей
  - СЗИ НСД/СКЗИ/МЭ/ЗСВ/АВС/САЗ
- Сетевые и узловые сенсоры
  - IDS/IPS NS/HS + опционально SIEM
- Центр мониторинга (АО «Перспективный мониторинг»)
- Взаимодействие с ГосСОПКА (НКЦКИ ФСБ России)
- Пилот
  - Отчеты о текущем состоянии инфраструктуры и наличии инцидентов ИБ
  - Рекомендации по актуализации системы защиты информации
  - Обоснование для руководства и планирование дальнейших действий

Отечественное ПО

- Операционные системы (cert!)

- Офисные пакеты и прикладные средства

Подключение к ГИС «РС ЕГИСЗ»

- Поставка, установка и настройка СЗИ
  - Криптошлюз или VPN-клиент (ФСБ-КС3)
  - Межсетевой экран (ФСБ-МЭ4+ФСТЭК-УД4/МЭА4/МЭБ4)
  - Средство антивирусной защиты (ФСТЭК-А2/Б2/В2/Г2 + ФСБ-А2/Б2/В2/Г2)
  - СКЗИ/СЭП (ФСБ-КС2)
  - СЗИ НСД (ФСТЭК-УД4/СВТ5/СКН4/САВЗВ4/МЭВ3/СОВУ4)
  - АПМДЗ/средство доверенной загрузки (ФСБ-АПМДЗ-3Б/ФСТЭК-СДЗПР2)
  - средство обнаружения вторжений (СОВ)/атак (СОА) (ФСТЭК-СОВУ4/УД4+ФСБ-СОАБ)
- Комплект шаблонов ОРД
- Организация оценки соответствия установленным требованиям
- Техподдержка и обслуживание

Спасибо за внимание!

Защищенные информационные технологии = Удобно И Безопасно

Решения есть! Обращайтесь, мы поможем

- Майшев Вадим
- ООО «КриптоСвязь»
- www.infotrust.ru
- mvv@infotrust.ru
- +7(3412) 918-100