

# 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

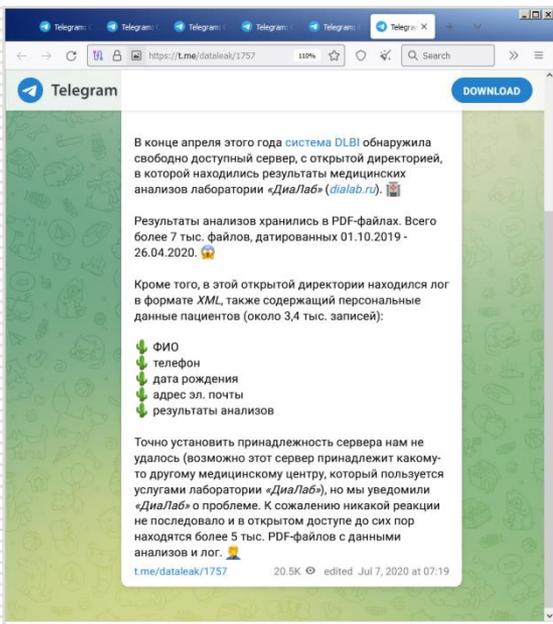
# Сервисы компании

---

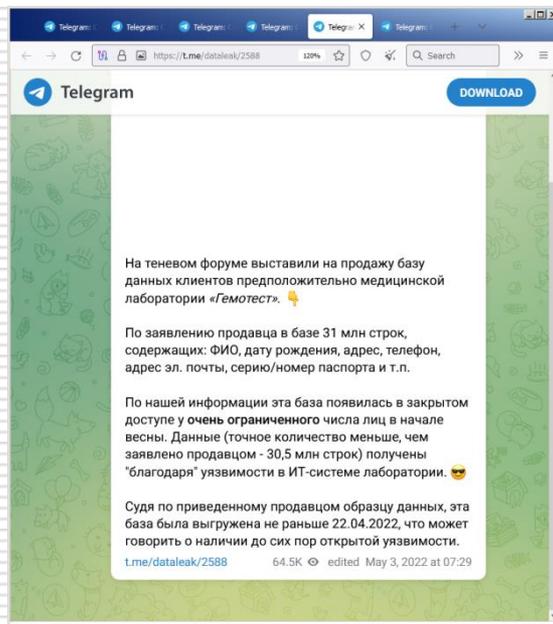
- Сертифицированные средства защиты информации и их сопровождение
  - Максимальный ассортимент
  - Обоснованный оптимальный выбор
  - Нормативное внедрение
  - Компетентная техническая поддержка
- PKI (ЭЦП, ЗЭД, TLS)
- VPN
- Подключение к ФГИС
- КИИ и ГосСОПКА
- Отечественное программное обеспечение

# Утечки в медицине

## □ ДиаЛаб, 2020



## □ Гемотест, апрель 2022



# Утечки в медицине

## СИТИЛАБ, май 2022

В субботу стало известно, что хакеры из группировки «UNG» «слили» данные предположительно из сети клинично-диагностических лабораторий «СИТИЛАБ» ([citilab.ru](https://citilab.ru)).

Нам на анализ предоставили несколько текстовых дампов, содержащих персональные данные:

- логин
- ФИО
- адрес эл. почты (483 тыс. уникальных адресов)
- телефон (435 тыс. уникальных номеров)
- хешированный пароль
- пол (не у всех)
- дата рождения (не у всех)
- дата регистрации (с 01.01.2007 по 18.05.2023)

Мы выборочно проверили случайные адреса эл. почты из этой утечки через форму восстановления пароля на сайте [my.citilab.ru/client/](https://my.citilab.ru/client/) и выяснили, что они действительные.

В данный момент в открытом доступе находится только 1,7 ТБ архив с отсканированными результатами анализов/исследований, договорами и чеками в PDF-файлах.

До этого «UNG» взламывали сервис по продаже билетов [kassy.ru](https://kassy.ru).

t.me/dataleak/2977 46.3K May 22 at 07:02

## Хеликс, июль 2023

Вчера в свободный доступ был выложен файл, содержащий персональные данные клиентов предположительно сети медицинских лабораторий «Хеликс» ([helix.ru](https://helix.ru)).

В этом файле содержится 7,344,919 строк:

- ФИО
- телефон (879 тыс. уникальных номеров)
- адрес эл. почты (779 тыс. уникальных адресов)
- дата рождения
- пол
- СНИЛС (не для всех)

Кроме этого файла, к нам на анализ попал другой дамп, содержащий записи 4,986,296 зарегистрированных пользователей:

- адрес эл. почты (4,9 млн уникальных адресов)
- хешированный (SHA-512 без соли) пароль
- IP-адрес и строка User-Agent
- дата регистрации и последнего захода в личный кабинет (с 17.07.2012 по 15.07.2023)

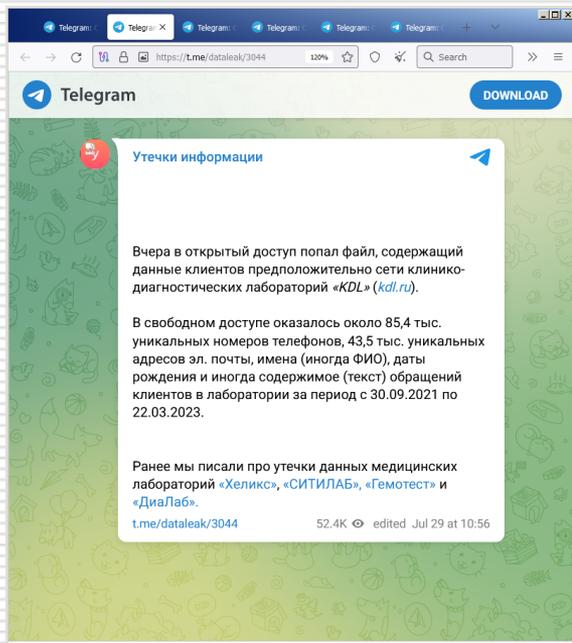
Оба дампа датируются 15.07.2023.

Ранее мы писали про утечки данных медицинских лабораторий «СИТИЛАБ», «Гемотест» и «ДиаЛаб».

t.me/dataleak/3036 48.5K edited Jul 20 at 05:30

# Утечки в медицине

## □ KDL, июль 2023



**Утечки информации**

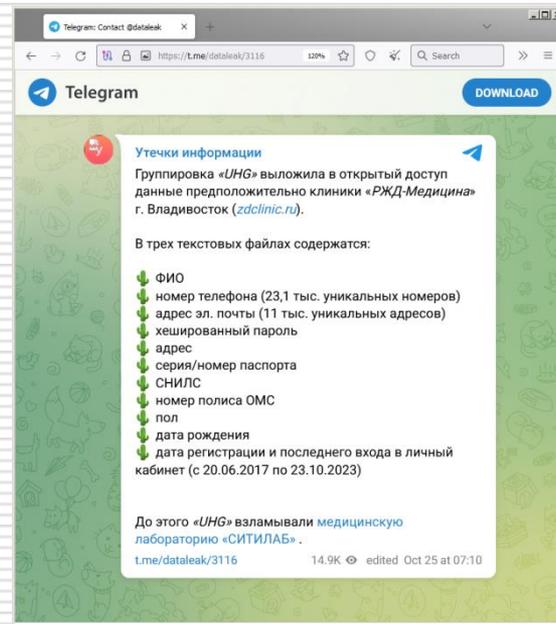
Вчера в открытый доступ попал файл, содержащий данные клиентов предположительно сети клинично-диагностических лабораторий «KDL» ([kdl.ru](https://kdl.ru)).

В свободном доступе оказалось около 85,4 тыс. уникальных номеров телефонов, 43,5 тыс. уникальных адресов эл. почты, имена (иногда ФИО), даты рождения и иногда содержимое (текст) обращений клиентов в лаборатории за период с 30.09.2021 по 22.03.2023.

Ранее мы писали про утечки данных медицинских лабораторий «Хеликс», «СИТИЛАБ», «Гемотест» и «ДиаЛаб».

[t.me/dataleak/3044](https://t.me/dataleak/3044) 52.4K edited Jul 29 at 10:56

## □ РЖД-Медицина, октябрь 2023



**Утечки информации**

Группировка «ИИГ» выложила в открытый доступ данные предположительно клиники «РЖД-Медицина» г. Владивосток ([zdclinic.ru](https://zdclinic.ru)).

В трех текстовых файлах содержатся:

- ↓ ФИО
- ↓ номер телефона (23,1 тыс. уникальных номеров)
- ↓ адрес эл. почты (11 тыс. уникальных адресов)
- ↓ хешированный пароль
- ↓ адрес
- ↓ серия/номер паспорта
- ↓ СНИЛС
- ↓ номер полиса ОМС
- ↓ пол
- ↓ дата рождения
- ↓ дата регистрации и последнего входа в личный кабинет (с 20.06.2017 по 23.10.2023)

До этого «ИИГ» взламывали медицинскую лабораторию «СИТИЛАБ».

[t.me/dataleak/3116](https://t.me/dataleak/3116) 14.9K edited Oct 25 at 07:10

# 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 Р (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 штампами»
  - «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 (КСЗ)
  - 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

---

- RSNет
- 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-КСЗ)
  - 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-ЗБ/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](http://www.infotrust.ru)
  - ❑ [mvv@infotrust.ru](mailto:mvv@infotrust.ru)
  - ❑ +7(3412) 918-100
-