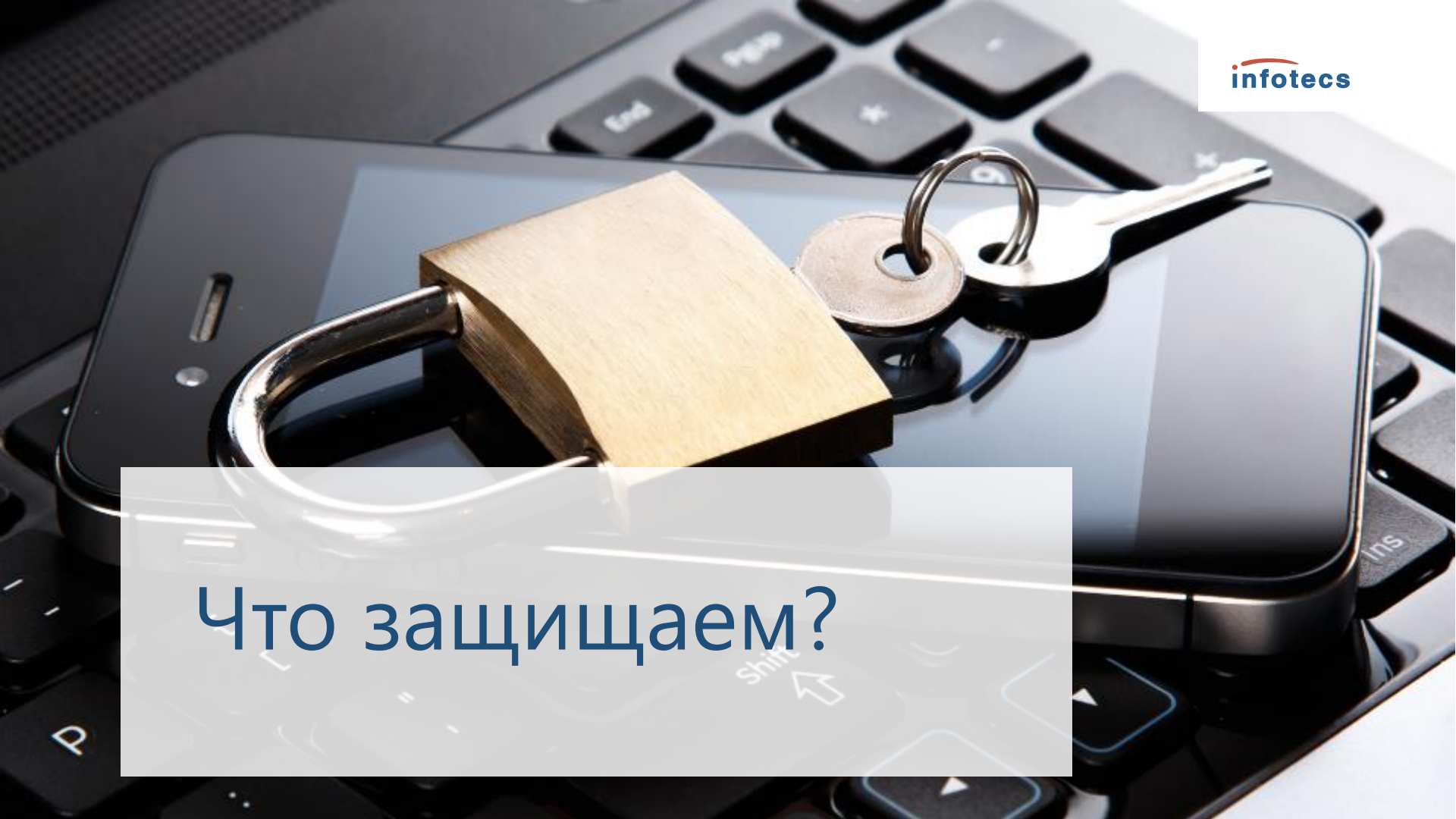
# Вводная базовая информация по продуктам ViPNet

Докладчик: Чефранова Анна

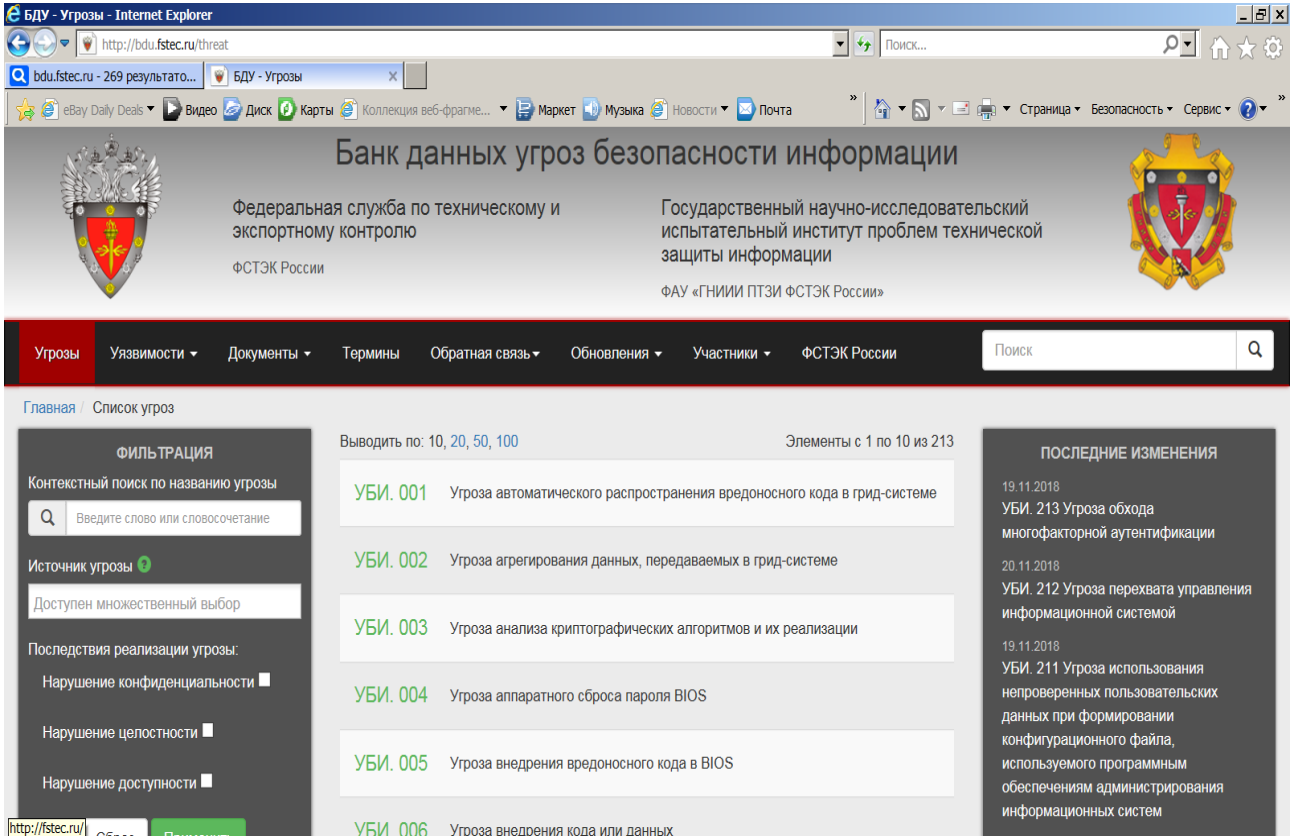
# Средства защиты

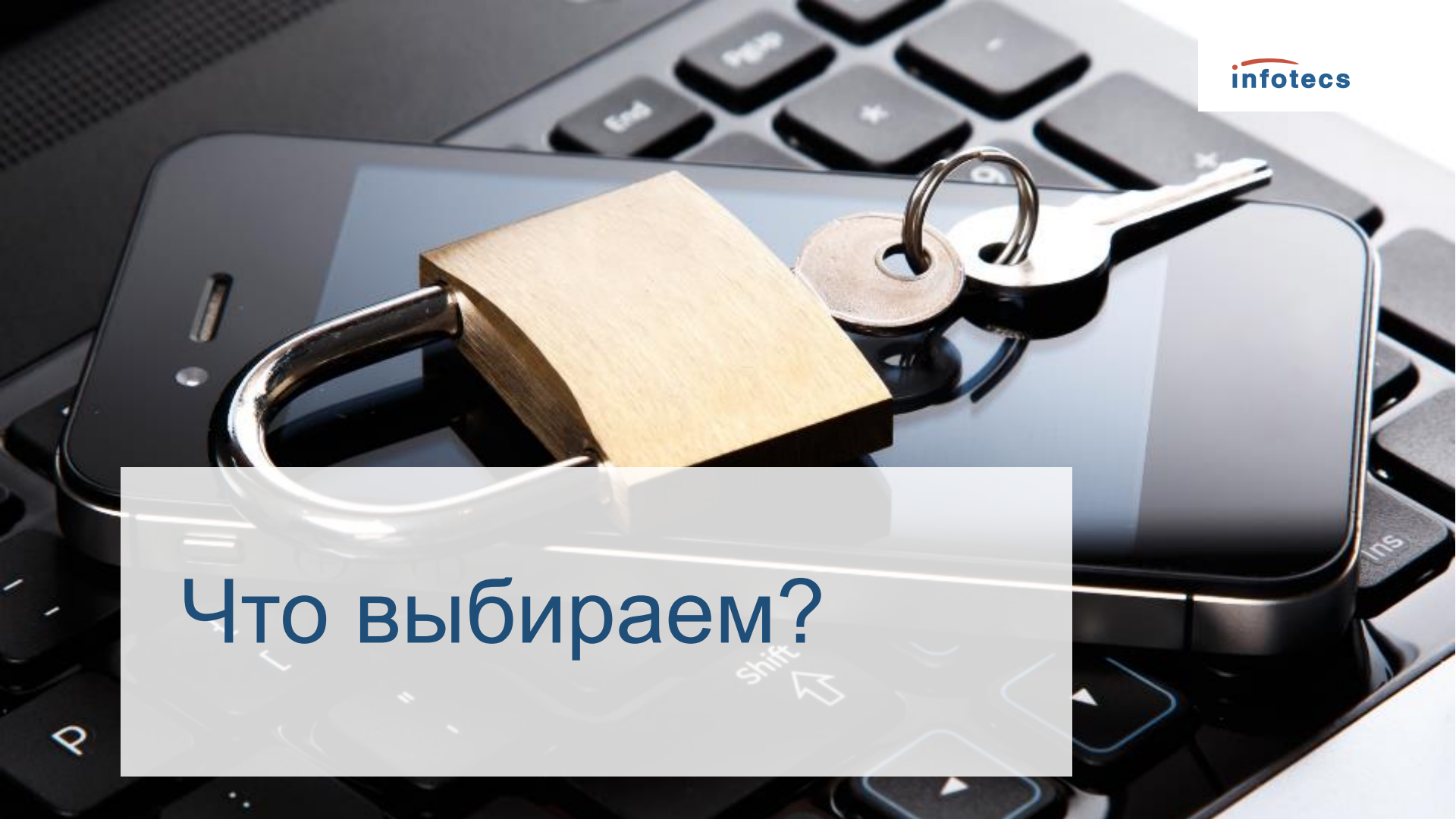


# Что защищаем?

# Вопросы

1. Какую информацию защищаем?
2. От кого защищаем?
3. Какими средствами защищаем и в какой мере?




infotecs
Что выбираем?

# СКЗИ (технологии VPN или PKI)

- средства шифрования,
- средства имитозащиты,
- средства электронной подписи,
- аппаратные шифровальные (криптографические) средства,
- программно-аппаратные шифровальные (криптографические) средства.

# МЕЖСЕТЕВЫЕ ЭКРАНЫ, IDS

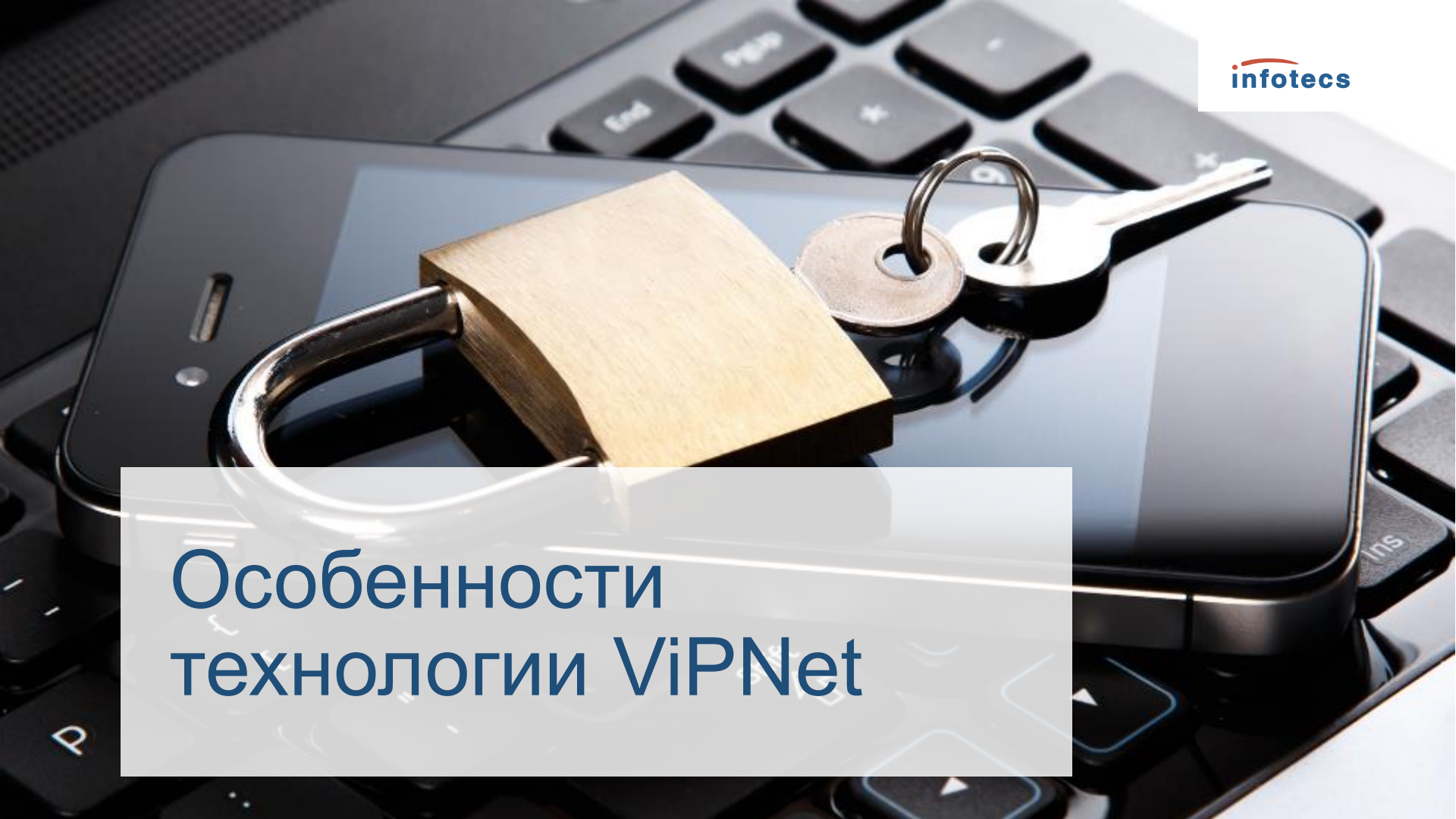
Какой уровень защиты, тип, класс?

IDS –сетевая или узловая?

# СРЕДСТВА ДОВЕРЕННОЙ ЗАГРУЗКИ, РАЗГРАНИЧЕНИЯ ДОСТУПА

# Для выбора должны быть критерии

- Выбор средства соответствует модели угроз
- Есть ли требуемые сертификаты для СЗИ
- Совместимость с другими средствами защиты
- Распространенность и тиражируемость
- Какие дополнительные сервисы и услуги есть
- Стоимость



# Особенности технологии ViPNet

# Технология ViPNet для защиты каналов связи, межведомственного электронного взаимодействия

Технология анализа и фильтрации трафика

Технология VPN

Технология PKI

Межсетевые экраны

Системы обнаружения вторжений

Криптографические средства защиты

# Технология ViPNet – защита конфиденциальной информации

**технологии идентификации и аутентификации**

- позволяют подтвердить личность пользователя и источник сетевого пакета

**технология межсетевого и персонального экранирования**

- обеспечивает фильтрацию любого вида трафика (входящего, исходящего, транзитного) на основе заданных правил

**технологии инкапсуляции и туннелирования**

- позволяют упаковать IP-пакет вместе со служебными полями в IP-пакет стандартного вида для сокрытия информации при ее передаче по открытым каналам связи

# Технология ViPNet – защита конфиденциальной информации

**технология создания виртуальных защищенных сетей (VPN)**

- позволяет соединить защищенными каналами связи компьютеры независимо от их месторасположения

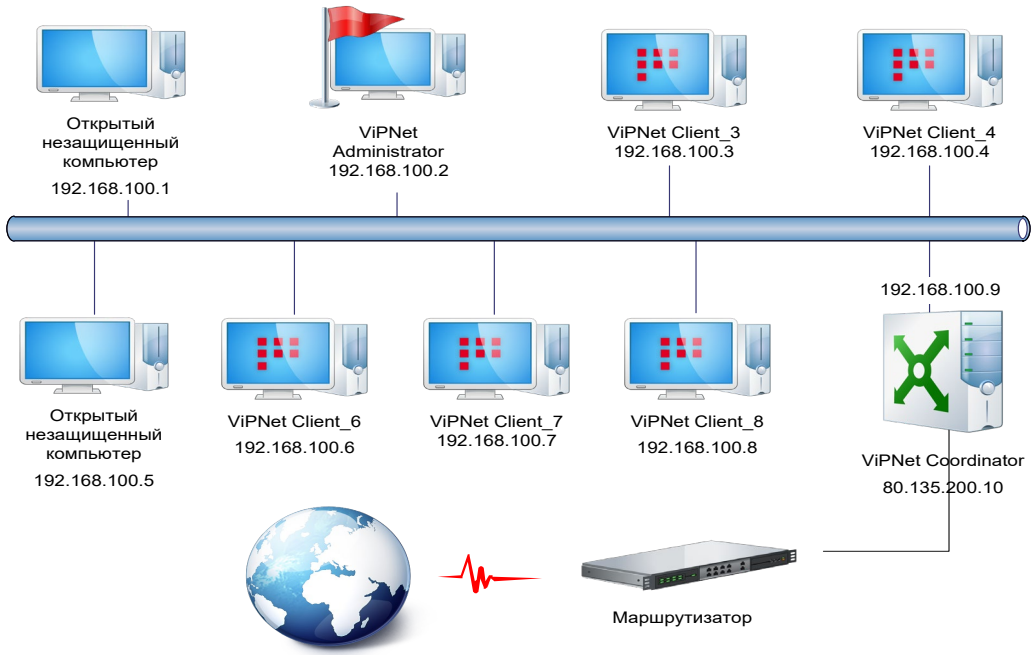
**технология криптографического преобразования данных**

- обеспечивает конфиденциальность информации при ее передачи и хранении

**технология работы с электронной подписью (ЭП)**

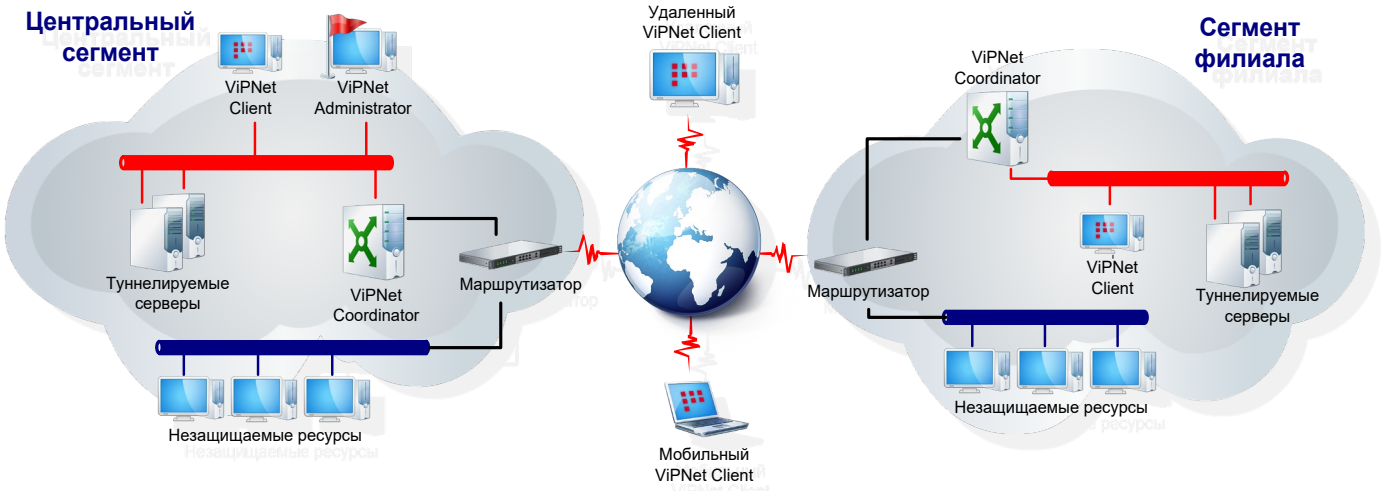
- обеспечивает целостности информации и позволяет установить ее авторство

# Технология ViPNet – защита конфиденциальной информации



# Типовая схема защиты

- С защищенным и незащищенным сегментами
- С удаленными пользователями
- С пользователями внутри корпоративной сети
- В корпоративной сети с удаленными пользователями

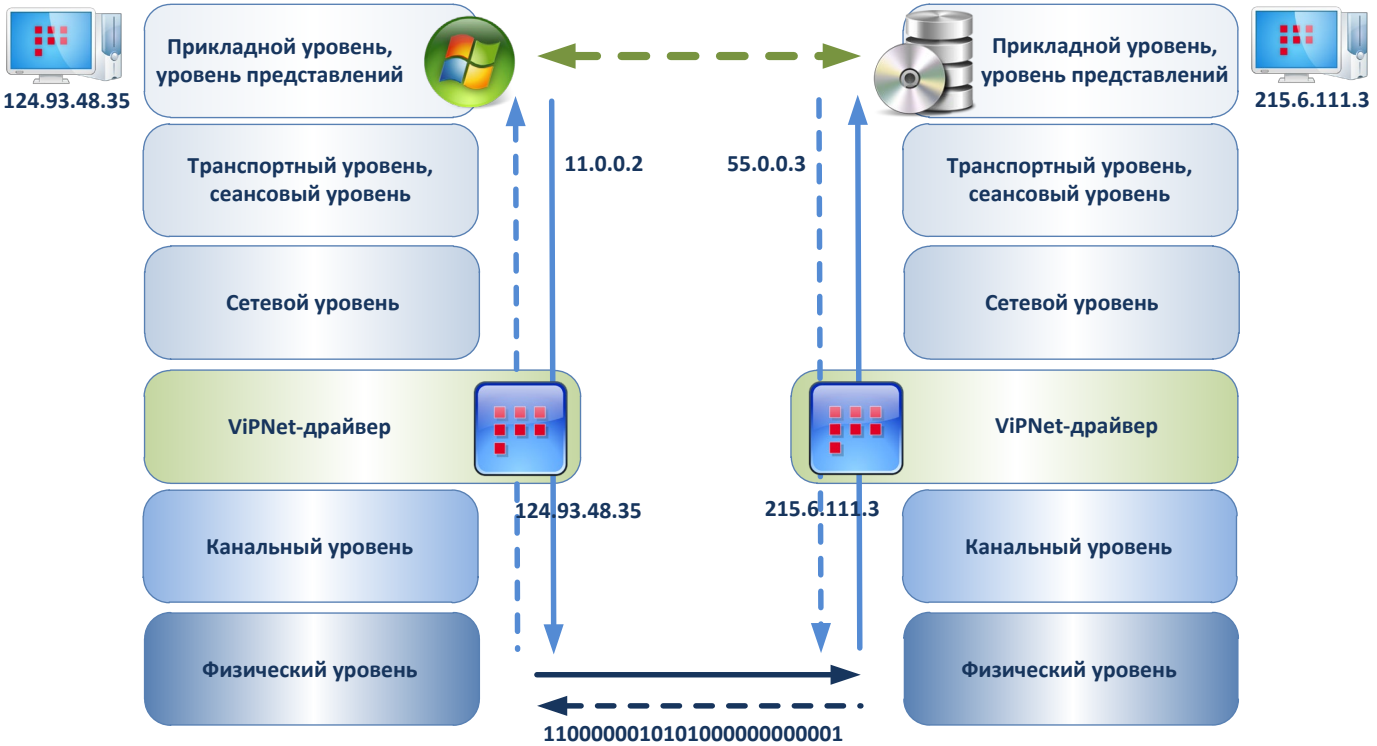


# «Сердце» технологии

**ViPNet-драйвер:**

- обеспечивает контроль всего IP-трафика, шифрование (расшифрование) трафика;
- работает между канальным и сетевым уровнем модели OSI;
- обрабатывает IP-пакеты до того как они будут обработаны стеком протоколов TCP/IP и переданы на прикладной уровень;
- активизируется только после авторизации в ПО ViPNet до загрузки прикладных сервисов и системных служб операционной системы.

# Принцип работы



# Программно-аппаратный комплекс ViPNet

**VPN ViPNet** — это линейка продуктов компании «ИнфоТеКС», предназначенных для защиты информации ограниченного доступа, в том числе персональных данных

Все программно-аппаратные комплексы, программные средства из состава ViPNet Network Security имеют сертификаты соответствия ФСТЭК России и ФСБ России

# Назначение  VPN ViPNet

**VPN ViPNet** позволяет организовывать защиту информации в различных информационных системах и нацелен на решение двух задач информационной безопасности:

- создание защищенной среды передачи данных с использованием публичных и выделенных каналов связи  путем организации сети VPN;
- развертывание инфраструктуры открытых ключей (PKI) и организация Удостоверяющего центра, что позволит использовать ЭП в прикладном ПО Заказчика (системах ЭДО, электронной почте, ЭТП и т.д.).

# Базовые модули ViPNet 4.x

**ViPNet Administrator**

- предназначен для создания и управления защищенной сетью ViPNet

**ViPNet Coordinator**

- предназначен для защиты сегментов IP-сетей, координации работы узлов защищенной сети

**ViPNet Client**

- предназначен для защиты отдельных компьютеров

# Состав VPN ViPNet 4.x

**ViPNet Administrator**
(Центр управления)

**ViPNet**
Центр управления сетью

**ViPNet**
Удостоверяющий и ключевой центр

**ViPNet Policy Manager**
(Управление политиками безопасности)

**ViPNet StateWatcher**
(Мониторинг сети)

**ViPNet Registration Point**
(Центр регистрации)

**ViPNet Publication Service**
(Публикация сертификатов)

**ViPNet TSP-OCSP Service**
(TSP/OCSP-сервер)

**ViPNet CA Web Service**
(Формирование запросов в удостоверящий центр)

**ViPNet CA Informing**
(Информирование о событиях, связанных с сертификатами)

**ПО для администрирования**

**ViPNet Coordinator**
(Сервер защищенной сети, криптошлюз и VPN-сервер)

**ViPNet Coordinator Linux**
(Сервер защищенной сети, криптошлюз и VPN-сервер для компьютеров с ОС Linux)

**ПАК ViPNet Coordinator HW** (Программно-аппаратный комплекс, выполняющий роли сервера защищенной сети, криптошлюза и VPN-сервера)

**Серверное ПО**

**ViPNet Client**
(Клиент защиенной сети)

**ViPNet CryptoService**
(Защита информации, передаваемой по незащищенным каналам)

**ViPNet Client for iOS,** ViPNet Client for Android
(VPN-клиент для мобильных устройств с ОС iOS и Android)

**ViPNet CSP**
(Криптопровайдер)

**ViPNet SafeDisk V**
(Защита информации на узле)

**ViPNet ThinClient**
(Терминальный клиент)

**Клиентское ПО**

# Аппаратные решения HW

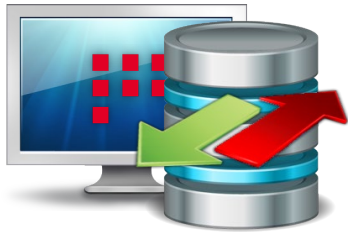
# ViPNet Administrator

**предназначен для:**

- создания VPN-сети на основе  технологии ViPNet;
- администрирования VPN-сети (добавление, удаление, изменение объектов сети, настройка параметров работы, контроль работоспособности и др.);
- обновления ПО ViPNet, установленного на узлах защищенной сети

**состоит из:**

- серверного приложения ЦУС;
- клиентского приложения ЦУС;
- базы данных SQL;
- удостоверяющего и ключевого центра.



# Состав ViPNet Administrator

**ViPNet Центр управления сетью**
выполняет следующие функции:

- создание и модификация структуры сети ViPNet;
- разграничение уровней полномочий пользователей сети ViPNet;
- отправка ключевой и справочной информации, обновлений ПО ViPNet на сетевые узлы.

**ViPNet Удостоверяющий и ключевой центр**
выполняет следующие функции:

- формирование и управление ключевой структурой сети;
- издание и управление сертификатами пользователей.

# ViPNet Coordinator

**Предназначен для:**

- защиты сегментов IP-сетей;
- защиты трафика, передаваемого по открытым каналам связи;
- координации работы узлов защищенной сети.

**Может быть установлен на:**

- стационарные компьютеры;
- серверные платформы;
- виртуальные машины.
- …

# Функции ViPNet Coordinator

- выполняет функции персонального и межсетевого экрана;
- создает туннели для организации защищенных соединений с открытыми узлами;
- осуществляет трансляцию адресов (NAT) для проходящего через координатор открытого трафика;
- позволяет разделить доступ защищенных узлов в Интернет и к ресурсам локальной сети;
- позволяет исключить любые атаки в реальном времени на компьютеры локальной сети.

# Функции ViPNet Coordinator

- обеспечивает обмен служебными и прикладными транспортными конвертами между узлами сети ViPNet;
- сообщает защищенным узлам информацию об IP-адресах и параметрах доступа других узлов;
- обеспечивает маршрутизацию транзитного VPN-трафика, проходящего через координатор на другие защищенные узлы.

# ViPNet Client

**предназначен:**

- для защиты рабочих компьютеров пользователей сети ViPNet.

**выполняет:**

- фильтрацию всего IP-трафика;
- шифрование соединений между защищенными узлами. Для шифрования трафика используются симметричные ключи, которые создаются и распределяются централизованно.

**может быть установлен:**

- на стационарные компьютеры,
- виртуальные машины,
- мобильные устройства…

# Поддерживаемые операционные системы

| ViPNet Client | ViPNet Coordinator | ViPNet Administrator |
|---|---|---|
| Windows XP 32-разрядная | Windows XP 32-разрядная | Windows 7 32/64-разрядная |
| Windows Server 2003 32-разрядная | Windows Server 2003 32-разрядная | Windows Server 2008 R2 64-разрядная |
| Windows Vista 32/64-разрядная | Windows Vista 32/64-разрядная | Windows 8 32/64-разрядная |
| Windows Server 2008 32/64-разрядная | Windows Server 2008 32/64-разрядная | Windows Server 2012 64-разрядная |
| Windows Server 2008 R2 64-разрядная | Windows Server 2008 R2 64-разрядная | |
| Windows 7 32/64-разрядная | Windows 7 32/64-разрядная | |
| Windows 8 32/64-разрядная | Windows 8 32/64-разрядная | |
| Windows Server 2012 64-разрядная | Windows Server 2012 64-разрядная | |
| ОС Android | ОС семейства Linux | |

# Дополнительные модули ViPNet Network Security 4.x

### ViPNet StateWatcher

- предназначен для централизованного мониторинга защищенных сетей и анализа событий, произошедших на узлах сети

### ViPNet Registration Point

- предназначен для регистрации и обслуживания внешних и внутренних пользователей ViPNet и хранения их регистрационных данных; является посредником между внешними пользователями и удостоверяющим центром

### ViPNet Policy Manager

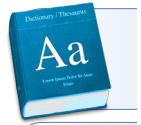
- предназначен для централизованного управления политиками безопасности на сетевых узлах ViPNet

# Новые возможности ViPNet Network Security 4.x

клиент-серверная архитектура ViPNet ЦУС

возможность многопользовательского режима работы с ViPNet ЦУС

**единая база данных SQL**, через которую происходит взаимодействие компонентов ViPNet Administrator




изменение в терминологии ViPNet

назначение права подписи и выбор узлов для рассылки СОС перенесено из ViPNet ЦУС в ViPNet УКЦ

упрощена организация межсетевого взаимодействия

# Новые возможности ViPNet Network Security 4.x

- настройки сетевых объектов можно выполнять непосредственно при их создании в ЦУС
- типы коллектива больше не используются
- появилась возможность объединять сетевые узлы и пользователей в группы
- связи задаются между сетевыми узлами и между пользователями
- отправка обновлений на узлы ViPNet осуществляется с помощью мастера обновления
- упрощена процедура создания ключей пользователей и ключей узлов

# Сетевой узел ViPNet

**Сетевой узел ViPNet:**

компьютер, на котором установлено программное обеспечение ViPNet

**Клиент:**

компьютер, на котором установлено клиентское ПО ViPNet

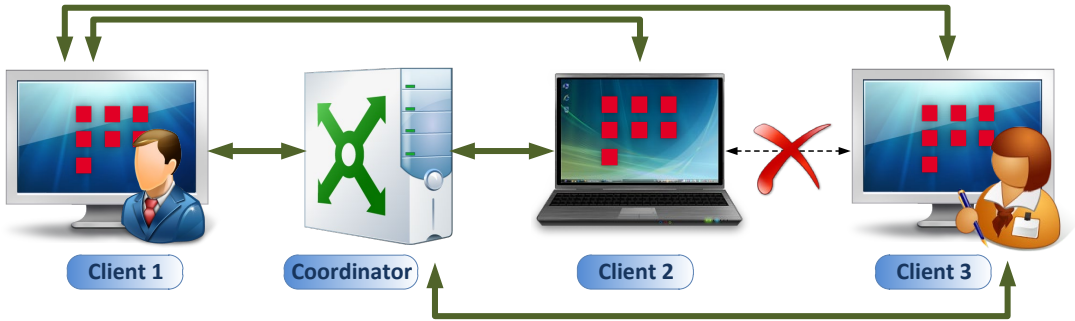
**Координатор:**

компьютер, на который установлено ПО ViPNet Coordinator или специальный программно-аппаратный комплек

# Связи между сетевыми узлами

**Связь:**

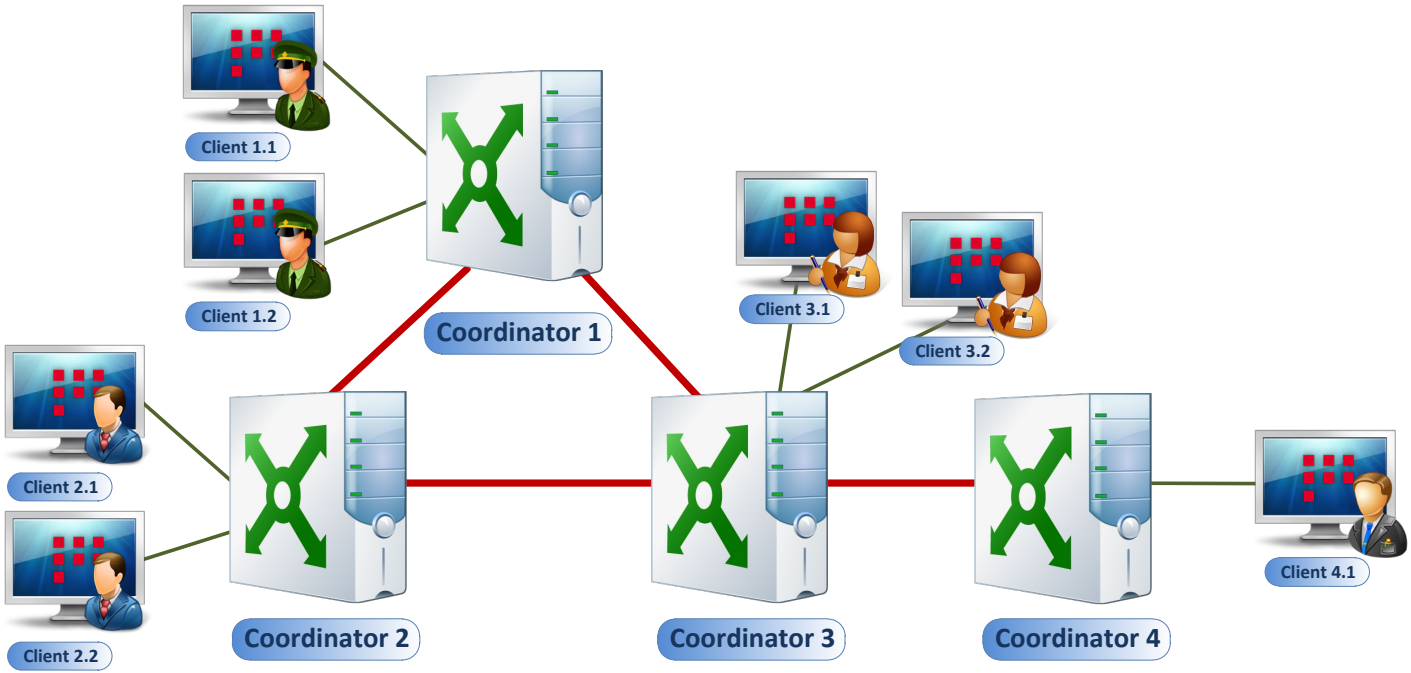
- обеспечивает возможность создания защищенного канала между узлами ViPNet;
- задается администратором ViPNet в клиентском приложении ЦУС;
- некоторые связи создаются автоматически и являются обязательным.



# Межсерверные каналы

- на основании межсерверных каналов выполняется маршрутизация управляющих, прикладных и транспортных конвертов между координаторами;
- межсерверные каналы могут быть организованы по любой схеме;
- если есть несколько маршрутов передачи конвертов между координаторами, будет использован кратчайший из них.

# Межсерверные каналы



# Идентификаторы объектов сети ViPNet

**Сеть ViPNet**
**1A0F**

уникальный 4-символьный шестнадцатеричный идентификатор (номер сети ViPNet)

**Сетевой Узел**
**1A0F0012**

уникальный 8-символьный шестнадцатеричный идентификатор: 1A0F – номер сети, 0012 – номер СУ

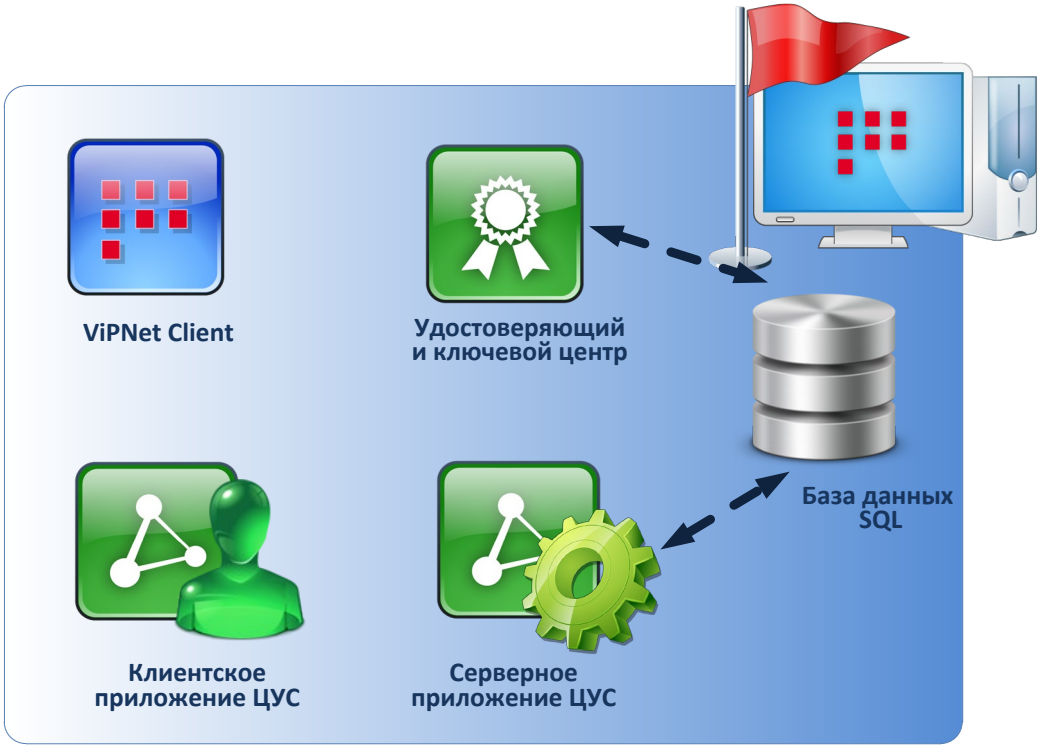
**Пользователь**
**1A0F00D**

уникальный 8-символьный шестнадцатеричный идентификатор: 1A0E – номер сети, 000D – номер пользователя

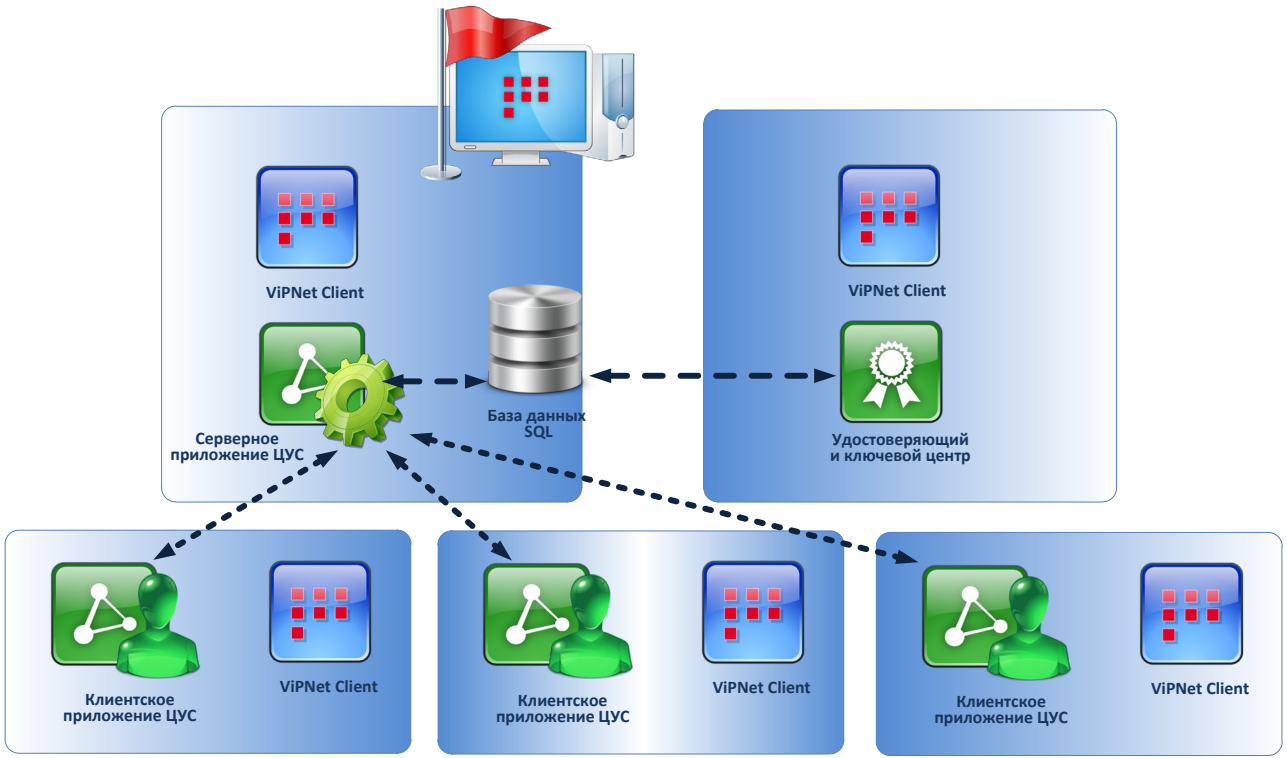
**Роль**
**001D**

уникальный 4-символьный шестнадцатеричный идентификатор

# Схемы размещения компонентов ViPNet Administrator



# Схемы размещения компонентов ViPNet Administrator



## Software solution

- ViPNet Client
- ViPNet CSP

## Mobile solution

- ViPNet Client Android
- ViPNet Client IOS
- ViPNet Connect

## Hardware based

- ViPNet Terminal

# Функции ViPNet Client

## VPN-клиент

- Обеспечивает защиту любого вида трафика между объектами защищенной сети ViPNet;
- Обеспечивает сохранение конфиденциальности, целостности и подлинности при помощи технологий:
  - шифрования;
  - хэширования;
  - электронной подписи;

## Персональный сетевой экран

- Обеспечивает надежную защиту от атак из локальных и внешних сетей посредством:
  - фильтрации IP-трафика по заданным параметрам;
  - контроля сетевой активности приложений;
  - обнаружения сетевых вторжений.

# Новые возможности ViPNet Client 4.x


реализована возможность создания групп объектов

реализована возможность автоматической смены конфигураций

изменился порядок применения сетевых фильтров

режимы безопасности больше не используются

ViPNet Деловая почта для хранения писем использует встроенную базу данных SQLite

# ViPNet Client 4.x

## Низкоуровневый драйвер сетевой защиты ViPNet-драйвер

- осуществляет шифрование и фильтрацию IP-трафика;
- перехватывает и контролирует весь IP-трафик, поступающий и исходящий из компьютера;
- взаимодействует непосредственно с драйверами сетевых интерфейсов компьютера;
- обеспечивает эффективный контроль IP-трафика во время загрузки операционной системы;

## ViPNet Монитор

- является интерфейсом для управления ViPNet-драйвером;
- позволяет настраивать параметры встроенного сетевого экрана;
- позволяет управлять параметрами обработки прикладных протоколов;
- предоставляет встроенные функции для защищенного обмена сообщениями, проведения конференций, файлового обмена;

# ViPNet Client 4.x

## Транспортный модуль ViPNet MFTP

- обеспечивает обмен управляющими конвертами, конвертами программы ViPNet Деловая почта и файлами с другими сетевыми узлами ViPNet;

## ViPNet Контроль приложений

- необязательный модуль ПО ViPNet Client;
- отслеживает сетевую активностью приложений, установленных на компьютере, а именно:
  - попытки создания исходящих соединений;
  - попытки открытия портов для входящих соединений;
  - отправку пакетов без предварительного создания соединения;
- ограничивает (разрешает или запрещает) доступ приложений к сети;
- ведет журнал событий по сетевой активности приложений;

# ViPNet Client 4.x

## ViPNet Деловая почта

- предназначена для организации электронного документооборота в защищенной сети ViPNet;
- обеспечивает работу защищенного почтового клиента;
- обеспечивает защищенный обмен почтовыми сообщениями посредством
  - подписания писем и вложений электронной подписью;
  - шифрования писем и файлов вложений;
- имеет мощную систему автоматической обработки входящих писем и исходящих файлов;
- обеспечивает передачу писем по защищенным каналам в сети ViPNet с помощью транспортного модуля MFTP;

## Криптопровайдер ViPNet CSP

- обеспечивает формирование и проверку электронной подписи;
- обеспечивает шифрование данных, в том числе сообщений электронной почты;
- обеспечивает аутентификацию и защиту соединений по протоколу TLS/SSL;

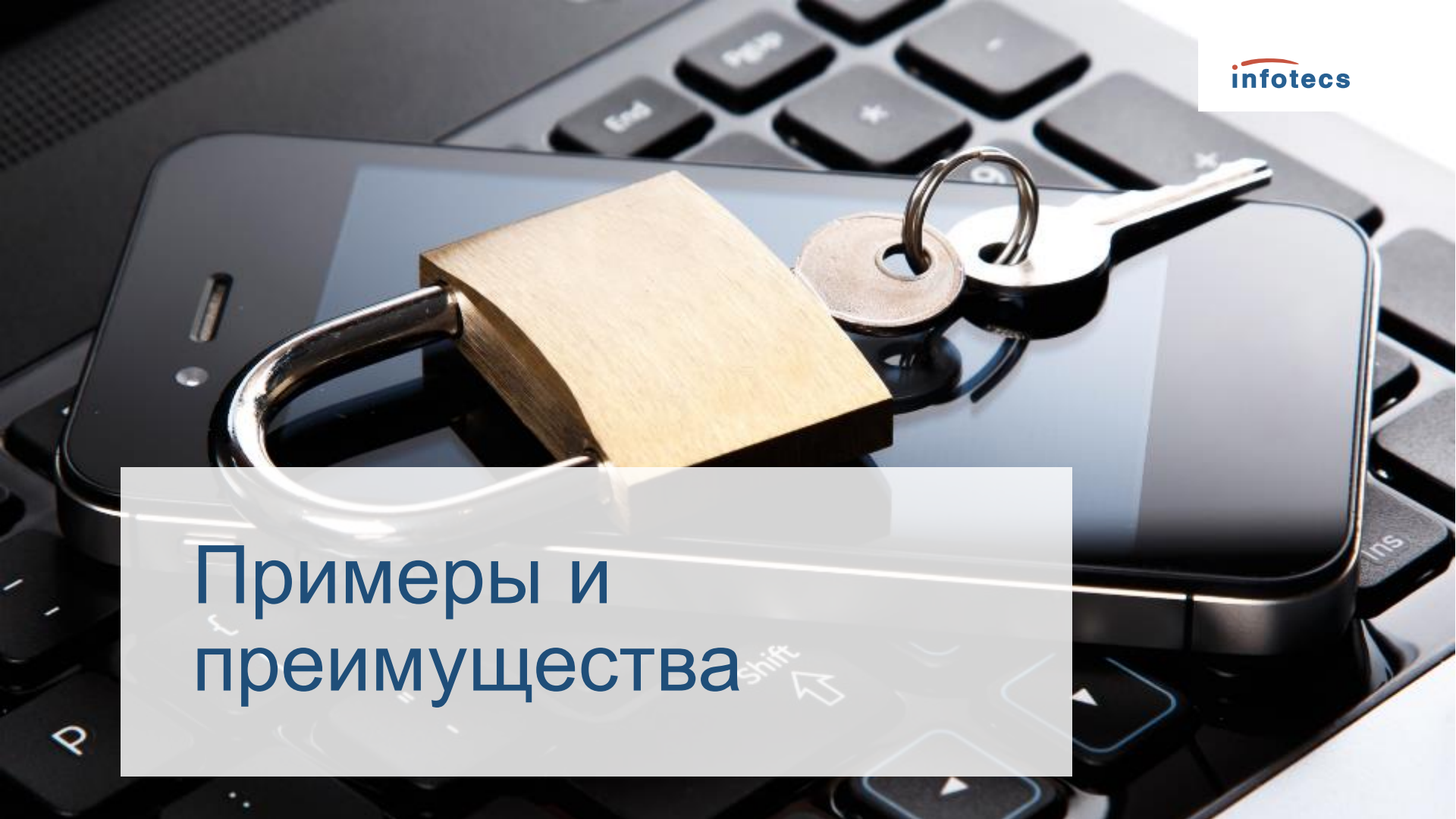
# Сертификаты ФСБ и ФСТЭК на продукты ViPNet

Продукты компании «ИнфоТеКС» проходят регулярную сертификацию в ФСБ и ФСТЭК России на соответствие требованиям безопасности для средств защиты конфиденциальной информации, включая персональные данные.



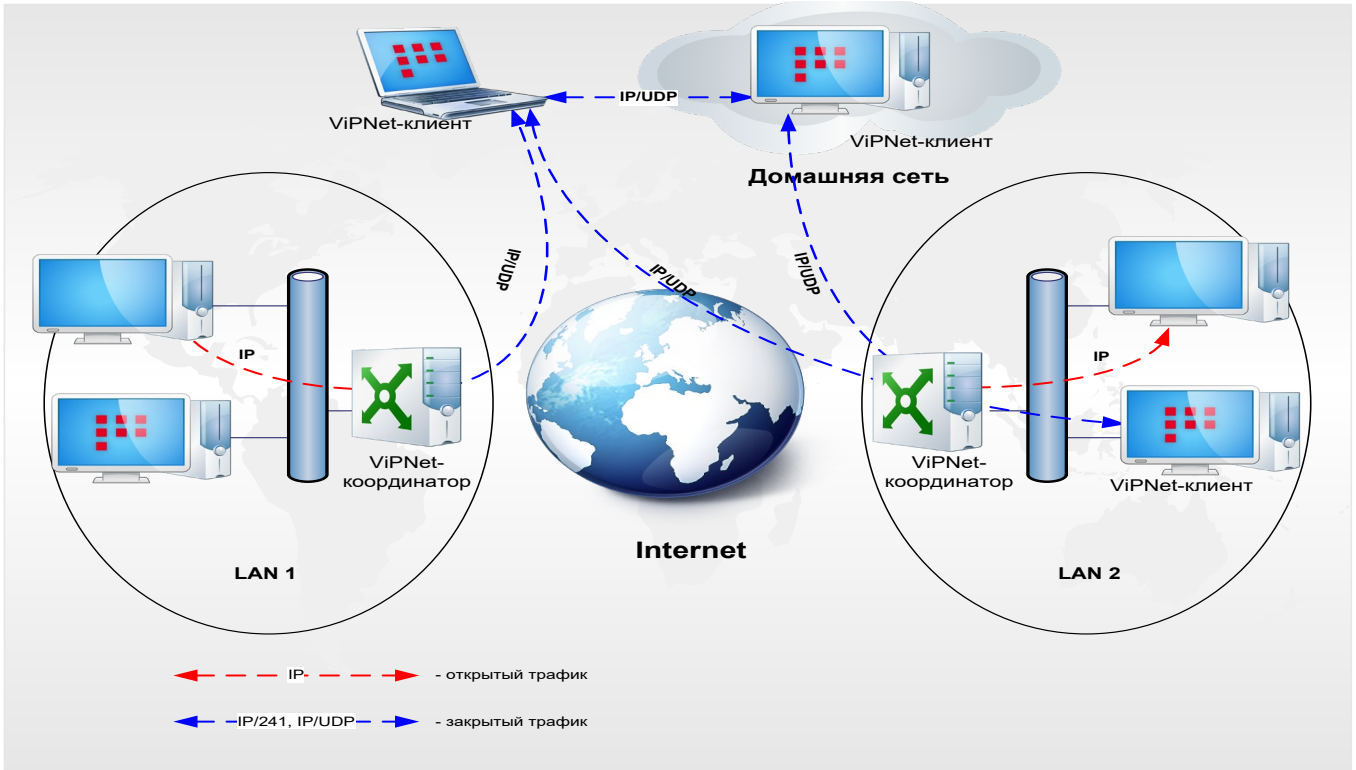


**https://www.infotecs.ru/about/sertificate/**

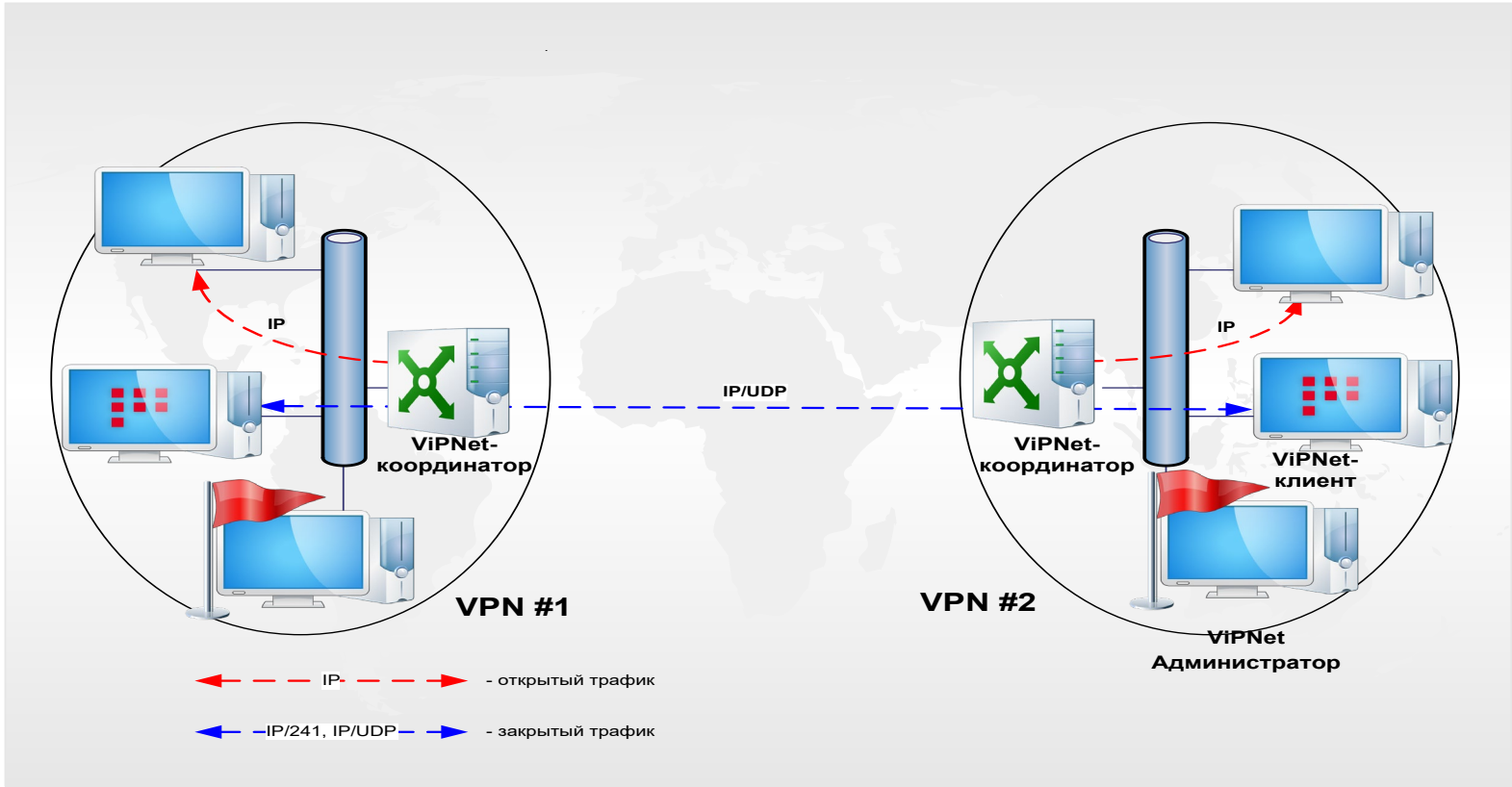


# Примеры и преимущества

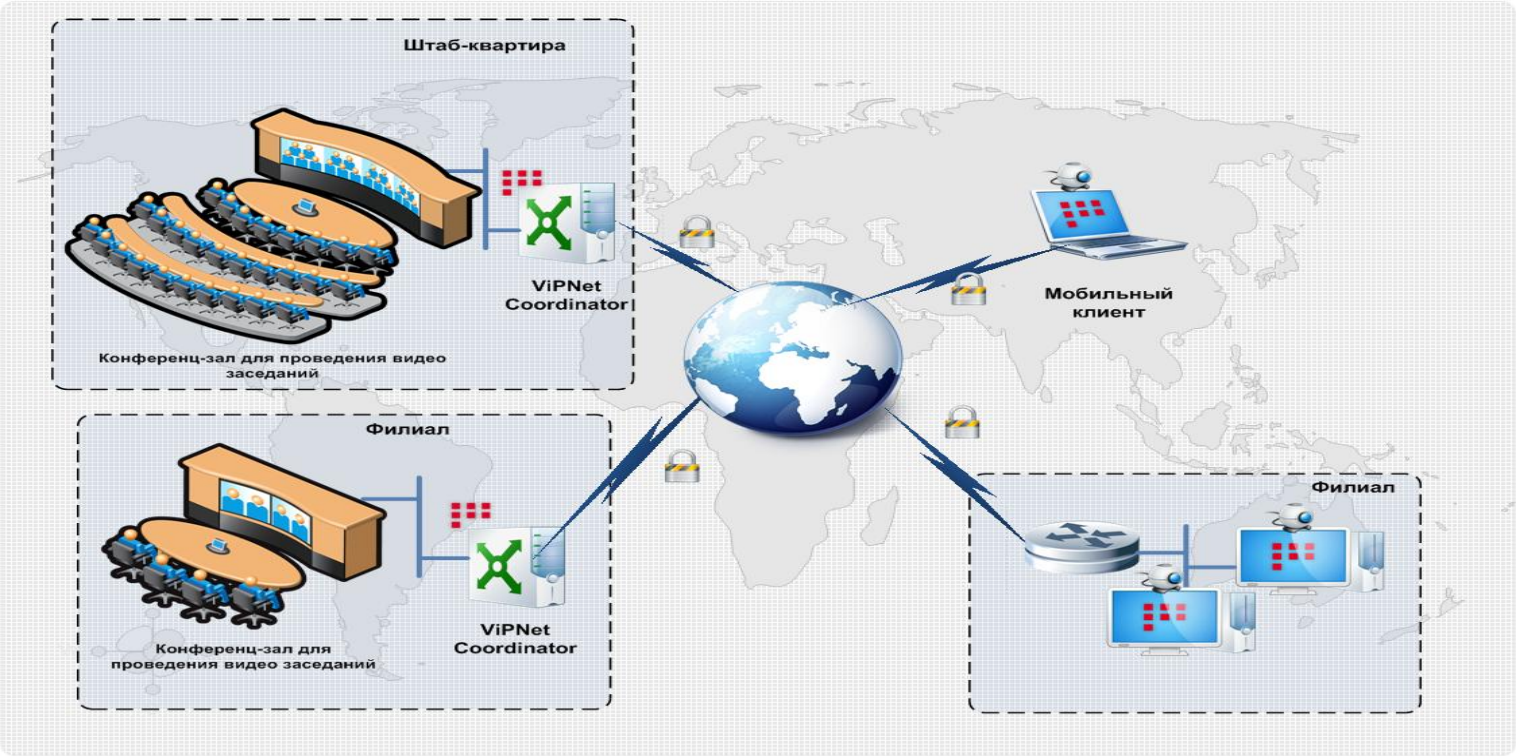
# Защищенный удаленный доступ



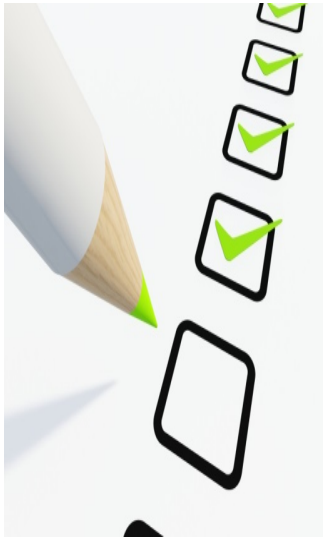
# Межсетевое взаимодействие



# Защита видеоконференцсвязи



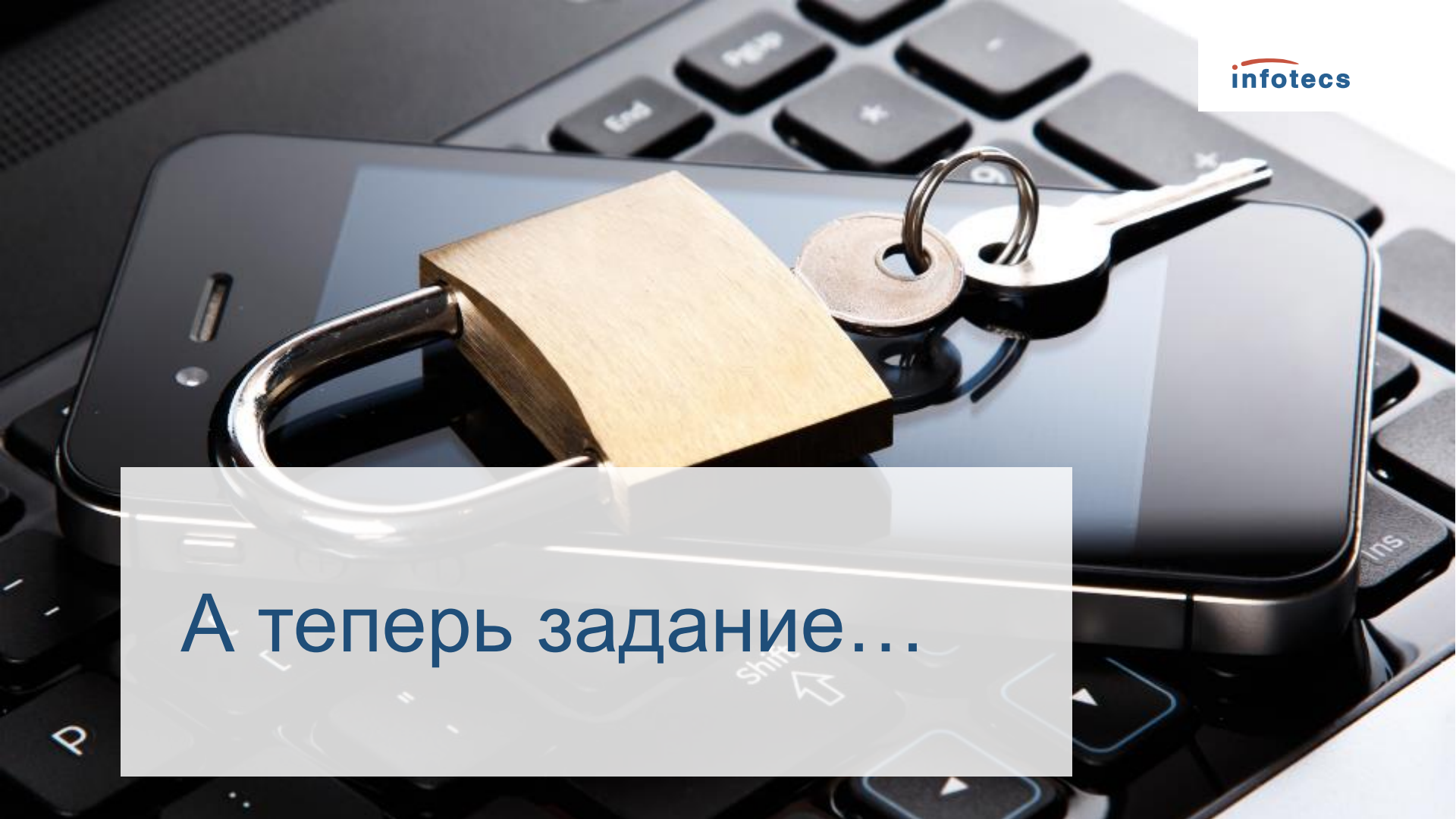
# Преимущества VPN



**Технологии VPN** на основе симметричной криптографии:

- позволяют быстро построить VPN-сеть любой масштабности, не обращая внимания на адресную структуру,
- позволяют размещать VPN-модули, как на компьютерах внутри локальных сетей, защищенных NAT-устройствами, так и на VPN-шлюзах на границе локальных сетей для защиты локальной сети в целом или ее фрагментов.

Предоставляется возможность обеспечить безопасность информации при наличии внутренних и внешних нарушителей.




# А теперь задание…

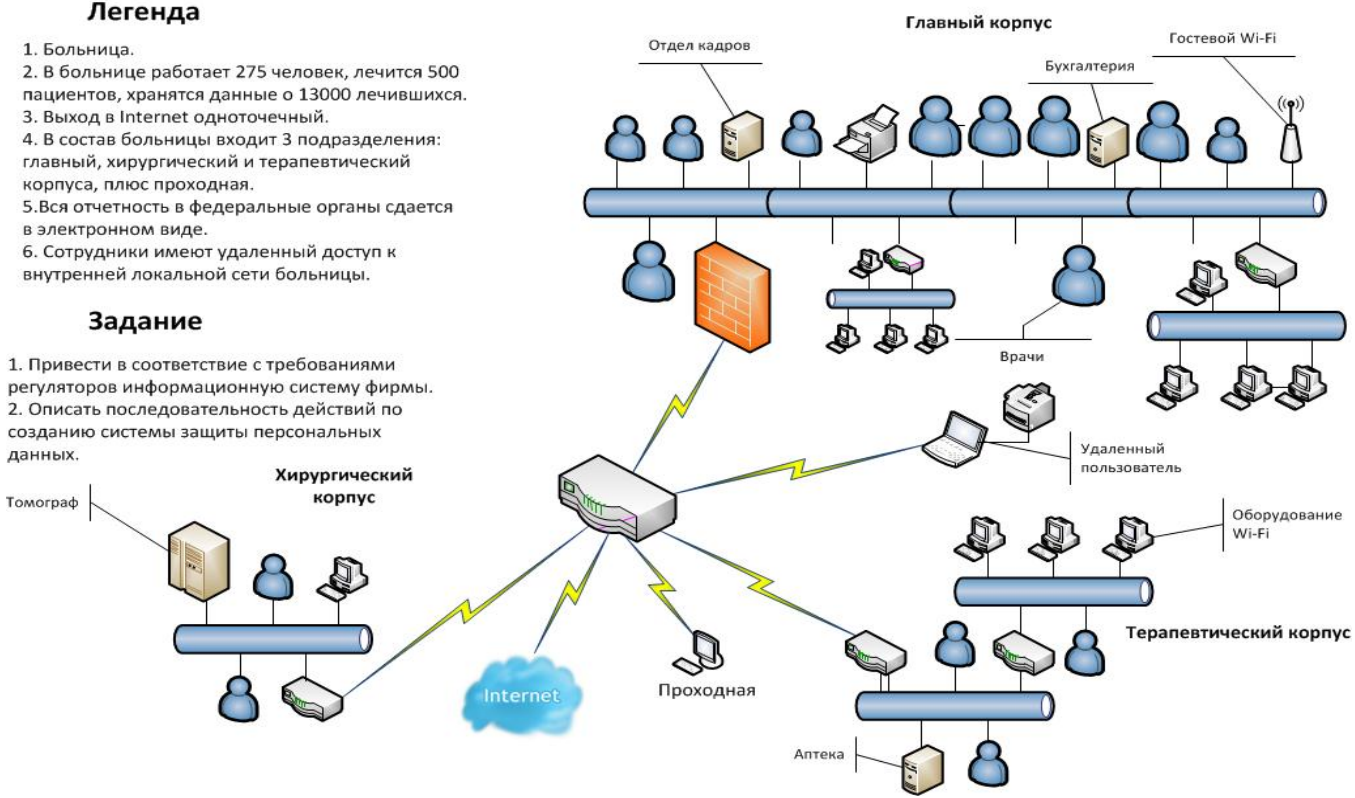
# Больница

## Легенда

1. Больница.
2. В больнице работает 275 человек, лечится 500 пациентов, хранятся данные о 13000 лечившихся.
3. Выход в Internet одноточечный.
4. В состав больницы входит 3 подразделения: главный, хирургический и терапевтический корпуса, плюс проходная.
5. Вся отчетность в федеральные органы сдается в электронном виде.
6. Сотрудники имеют удаленный доступ к внутренней локальной сети больницы.

## Задание

1. Привести в соответствие с требованиями регуляторов информационную систему фирмы.
2. Описать последовательность действий по созданию системы защиты персональных данных.




infotecs
Спасибо за внимание!