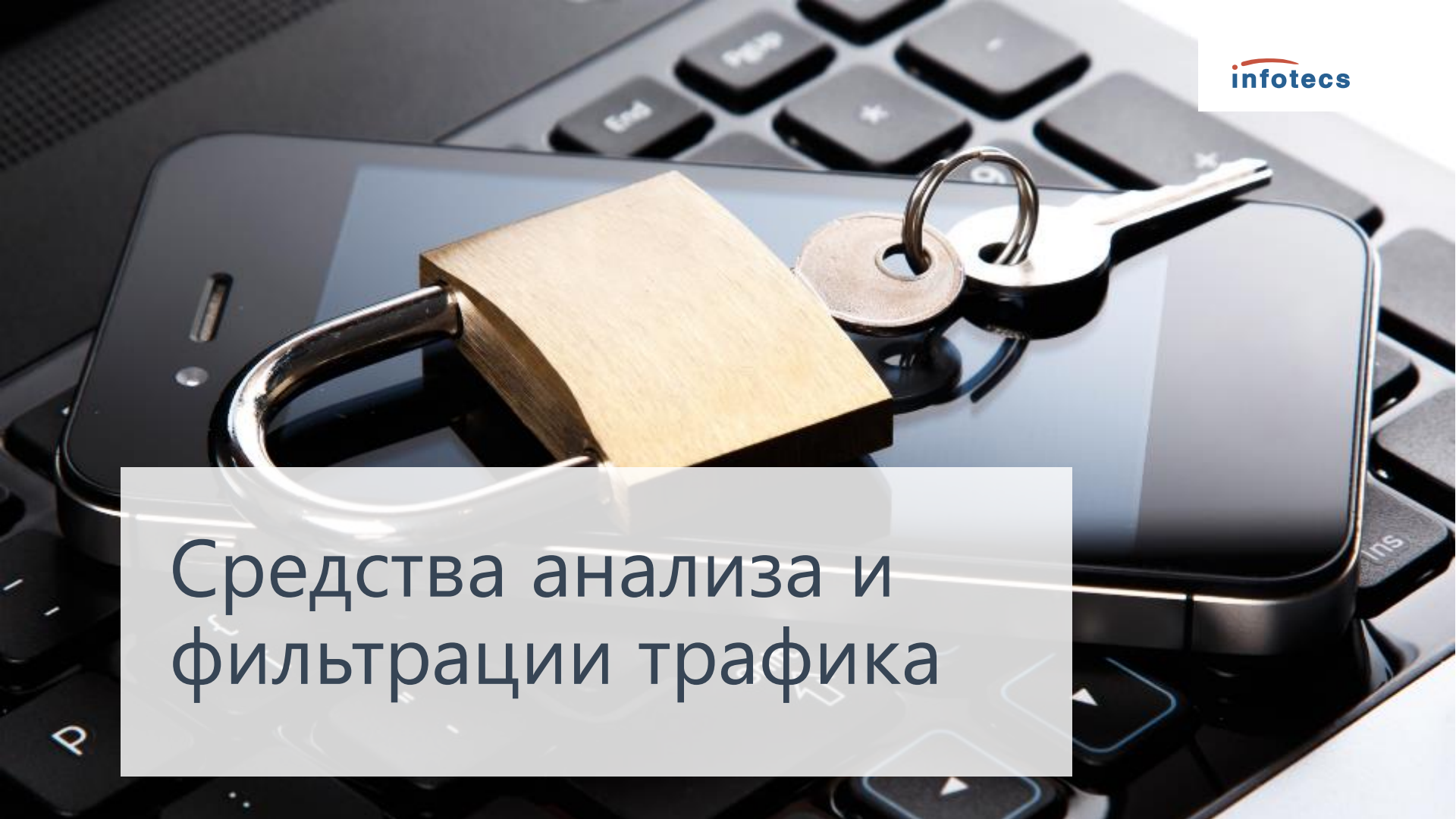


Средства защиты информации

Средства защиты



©2018, ОАО «ИнфоТеКС».



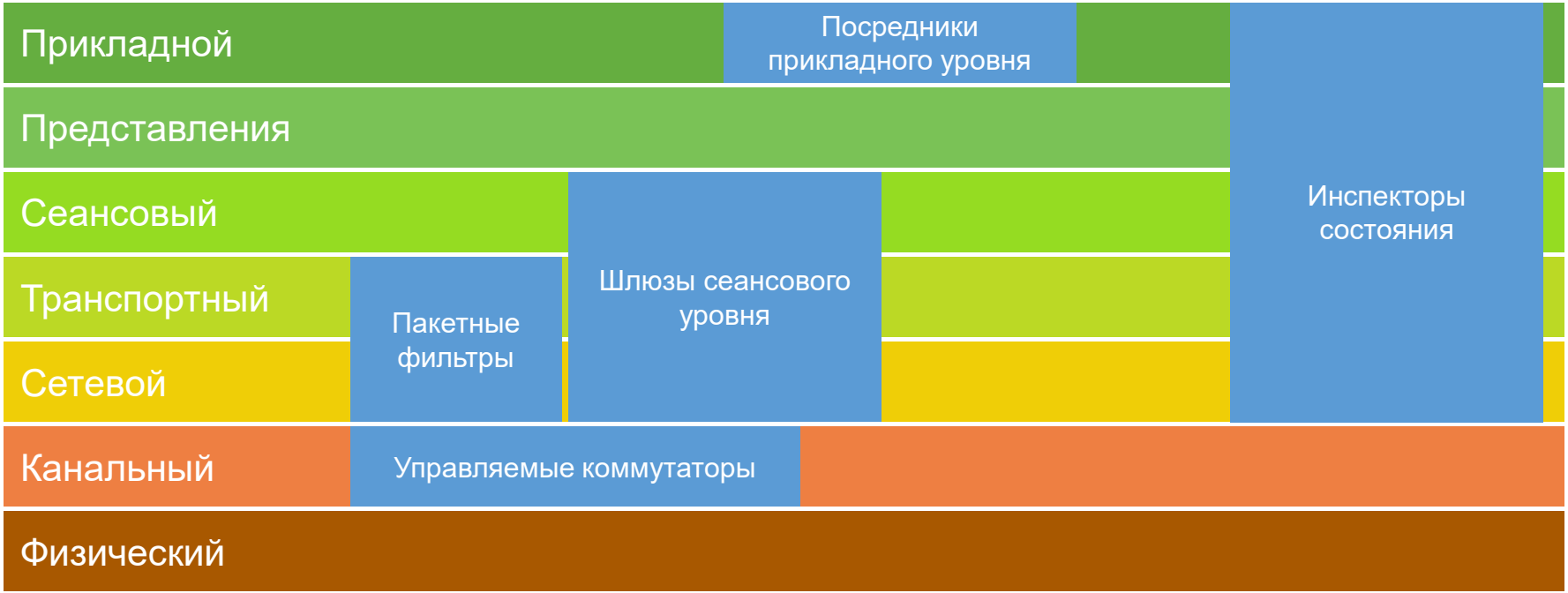
Средства анализа и фильтрации трафика

Виды межсетевых экранов

- коммутаторы, функционирующие на канальном уровне;
- сетевые или пакетные фильтры, которые, как видно из названия, функционируют на сетевом уровне;
- шлюзы сеансового уровня (circuit-level proxy);
- посредники прикладного уровня (application proxy или application gateway);
- инспекторы состояния (stateful inspection).

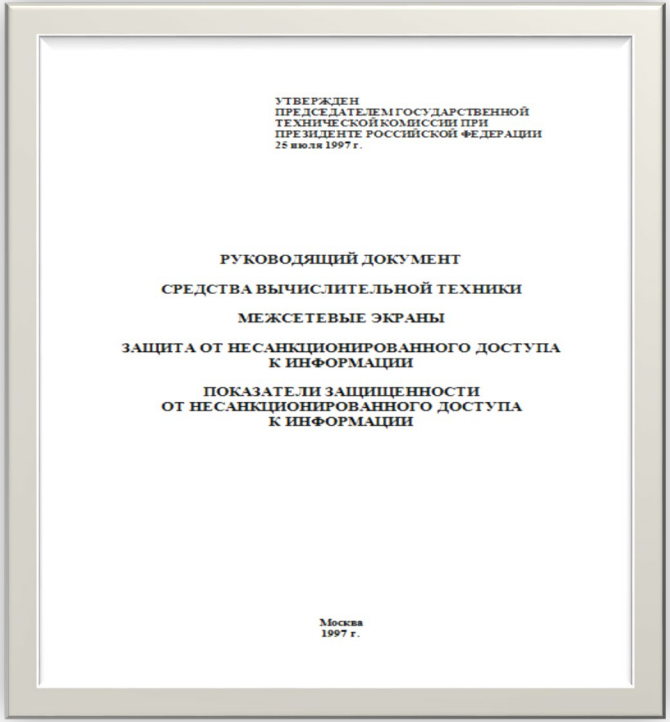
©2018, ОАО «ИнфоТеКС».

Классификация межсетевых экранов



©2018, ОАО «ИнфоТеКС».

Требования к межсетевым экранам



УТВЕРЖДЕН
ПРЕДСЕДАТЕЛЕМ ГОСУДАРСТВЕННОЙ
ТЕХНИЧЕСКОЙ КОМИССИИ ПРИ
ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ
25 июля 1997 г.

РУКОВОДЯЩИЙ ДОКУМЕНТ

СРЕДСТВА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

МЕЖСЕТЕВЫЕ ЭКРАНЫ

ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА
К ИНФОРМАЦИИ

ПОКАЗАТЕЛИ ЗАЩИЩЕННОСТИ
ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА
К ИНФОРМАЦИИ

Москва
1997 г.

- устанавливал классификацию межсетевых экранов (5 классов) по уровню защищенности от несанкционированного доступа к информации на базе перечня показателей защищенности (12 показателей: 9 по функциям и 3 по свидетельствам) и совокупности описывающих их требований;
- предназначался для заказчиков и разработчиков межсетевых экранов, а также вычислительных сетей, распределенных автоматизированных систем с целью использования при формулировании и реализации требований по их защите от несанкционированного доступа к информации;
- устанавливал соответствие классов межсетевых экранов классам автоматизированных систем.

©2018, ОАО «ИнфоТеКС».

Современные угрозы безопасности информации

Опыт разработчиков межсетевых экранов

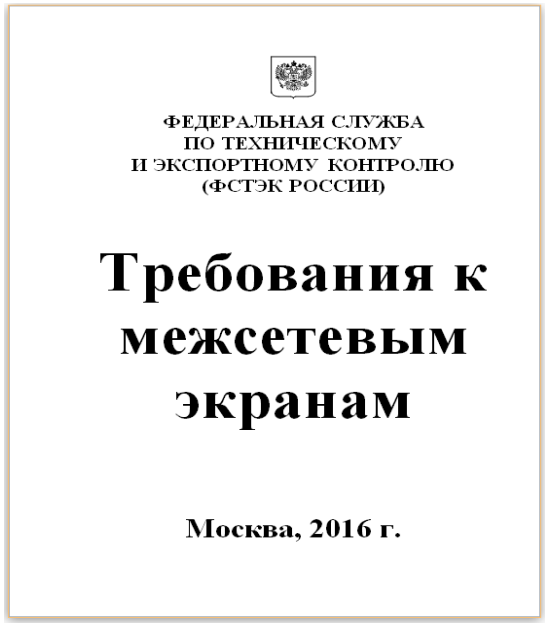
Современные технологии межсетевого экранирования

Требования к СОВ

ГОСТ Р ИСО/МЭК 15408

Опыт организаций по защите информации

Зарубежные требования к межсетевым экранам

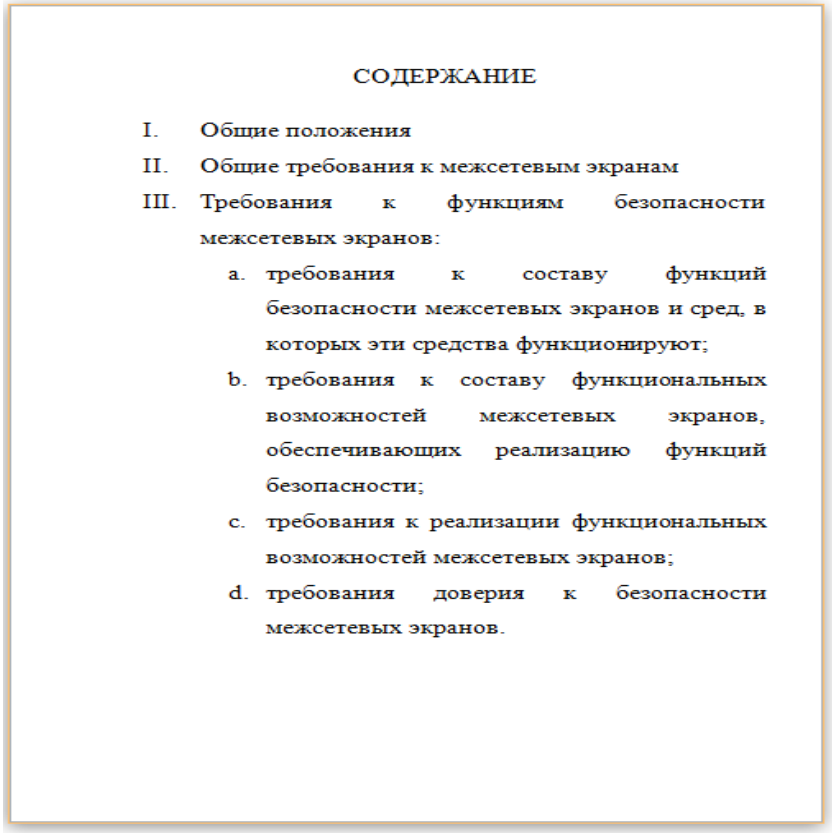

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК РОССИИ)

Требования к межсетевым экранам

Москва, 2016 г.

©2018, ОАО «ИнфоТеКС».

Требования к межсетевым экранам



СОДЕРЖАНИЕ

I. Общие положения
II. Общие требования к межсетевым экранам
III. Требования к функциям безопасности межсетевых экранов:
  a. требования к составу функций безопасности межсетевых экранов и сред, в которых эти средства функционируют;
  b. требования к составу функциональных возможностей межсетевых экранов, обеспечивающих реализацию функций безопасности;
  c. требования к реализации функциональных возможностей межсетевых экранов;
  d. требования доверия к безопасности межсетевых экранов.

Требования предназначены для:

- разработчиков межсетевых экранов;
- производителей межсетевых экранов;
- заявителей на сертификацию межсетевых экранов;
- испытательных лабораторий средств защиты информации;
- органов по сертификации средств защиты информации.

©2018, ОАО «ИнфоТеКС».

Функция безопасности	Руководящий документ, 1997 г.	Требования к межсетевым экранам, 2016 г.
Контроль и фильтрация	Имеется	Усилено
Идентификация и аутентификация	С 3 класса	С 6 класса, усилено
Регистрация событий безопасности (аудит)	Имеется	Усилено
Оповещение о критичных видах событий безопасности	**Отсутствует**	Имеется
Сохранение и восстановление штатного режима функционирования при сбоях и ошибках	В части восстановления	Имеется, усилено
Тестирование межсетевого экрана	Имеется	Усилено
Проверка целостности программного обеспечения и конфигурации (параметров) межсетевого экрана	Имеется	Усилено
Преобразование сетевых адресов	**Со 2 класса**	С 4 класса, усилено
Маскирование наличия межсетевого экрана	**Отсутствует**	Имеется
Приоритезация информационных потоков	**Отсутствует**	Имеется
Администрирование	Имеется	Усилено
Взаимодействие с другими СЗИ	**Отсутствует**	Имеется

©2018, ОАО «ИнфоТеКС».

Требование доверия	Руководящий документ, 1997 г.	Требования к межсетевым экранам, 2016 г.
Описание архитектуры безопасности	**Отсутствует**	Имеется
Функциональная спецификация с полной аннотацией	**Отсутствует**	Имеется
Архитектурный проект	Частично	Имеется
Руководства пользователя и администратора, формуляр	Частично	Имеется
Подготовительные процедуры	Частично	Имеется
Средства управления авторизацией	Частично	Имеется
Охват управления конфигурацией представления реализации	**Отсутствует**	Имеется
Процедуры поставки	**Отсутствует**	Имеется
Идентификация мер безопасности	**Отсутствует**	Имеется
Определенная разработчиком модель жизненного цикла	**Отсутствует**	Имеется
Задание по безопасности	**Отсутствует**	Имеется
Анализ покрытия	**Отсутствует**	Имеется
Тестирование: базовый проект	Имеется	Имеется
Правила по безопасной настройке	Имеется	Имеется

©2018, ОАО «ИнфоТеКС».

Требование доверия	Руководящий документ, 1997 г.	Требования к межсетевым экранам, 2016 г.
Полное независимое тестирование	Имеется	Имеется
Анализ уязвимостей	**Отсутствует**	Имеется
Полная функциональная спецификация	**Отсутствует**	Имеется
Полное отображение представления реализации функциональных возможностей безопасности	**Отсутствует**	Имеется
Базовый модульный проект	**Отсутствует**	Имеется
Поддержка генерации, процедуры приемки и автоматизация	**Отсутствует**	Имеется
Базовое устранение недостатков	**Отсутствует**	Имеется
Полностью определенные инструментальные средства разработки	**Отсутствует**	Имеется
Усиленный методический анализ (уязвимостей)	**Отсутствует**	Имеется
Процедуры обновления программного обеспечения	**Отсутствует**	Имеется
Анализ влияния обновлений на безопасность	**Отсутствует**	Имеется
Контроль отсутствия НДВ	**Отсутствует**	Имеется

©2018, ОАО «ИнфоТеКС».

Общие угрозы

Внешние

- Несанкционированный доступ к информации, содержащейся в информационной системе
- Отказ в обслуживании информационной системы
- Вызов нарушения функционирования межсетевого экрана
- Несанкционированное получение сведений о сети и её узлах

Внутренние

- Несанкционированная передача информации из информационной системы
- Отказ в обслуживании информационной системы
- Вызов нарушения функционирования межсетевого экрана

Тип межсетевого экрана

А	уровня сети
Б	уровня логических границ сети
В	уровня узла
Г	уровня приложения
Д	уровня промышленной сети

©2018, ОАО «ИнфоТеКС».

Классификация межсетевых экранов

Классы защиты межсетевого экрана	Классы защищенности ГИС	Уровни защищенности ИСПД	Классы защищенности АСУ ТП
6	3, 4	3, 4	3
5	2	2	2
4	1	1	1
3	**Применяются в информационных системах, обрабатывающих информацию, содержащую сведения, составляющие государственную тайну**		
2			
1			

©2018, ОАО «ИнфоТеКС».

IDS

ОБНАРУЖЕНИЕ ВТОРЖЕНИЙ (Intrusion detection, ID) – это процесс мониторинга и определения несанкционированных попыток доступа и управления системами.

IDS – это системы, служащие для скорейшего обнаружения опасного содержимого.

Обнаружив потенциальную угрозу, называемую событием, система IDS записывает в журнал данные о рассматриваемой транзакции, а также отправляет оповещение (различными способами), перенаправляет атаку или нейтрализует вредоносное действие.

©2018, ОАО «ИнфоТеКС».

IDS

IDS используются для обнаружения потенциально опасных событий, таких как:

- попытка подмены личности (атака на протоколы аутентификации);
- взлом пароля;
- атаки на протоколы;
- переполнение буфера;
- установка набора утилит, скрывающих присутствие в системе;
- несанкционированные команды;
- факты использования программных уязвимостей;
- вредоносный код, вирусы, черви, «троянские кони»;
- нелегальное управление данными;
- несанкционированный доступ к файлам;
- атаки на отказ в обслуживании.

©2018, ОАО «ИнфоТеКС».

IDS

Типы IDS и модели обнаружения

В зависимости от ресурсов и имущества, IDS может использоваться для защиты **узла** или **всей сети**.

Все системы IDS соответствуют одной или двум моделям обнаружения вторжений:

- **обнаружение аномалий;**
- **обнаружение признаков.**

©2018, ОАО «ИнфоТеКС».

IDS

Узловые IDS (HIDS) устанавливаются на узле (сервер, рабочая станция, принтер, маршрутизатор, шлюз), который они будут отслеживать.
HIDS проверяет каждую команду, ищет признаки вредоносного воздействия или просто отслеживает несанкционированное изменение файлов.

HIDS, предназначенные для контроля целостности файлов (используют **моментальные "снимки" файлов** и контрольные суммы), создают хэш важных файлов в известном "чистом" состоянии, а затем через определенное время, проверяют эти файлы посредством сравнения.

Системы HIDS, отслеживающие выполняемые в системах действия, осуществляют **мониторинг в режиме реального времени** и перехват потенциально вредоносных действий.

©2018, ОАО «ИнфоТеКС».

IDS

Сетевые IDS (NIDS) более популярны в области обнаружения вторжений.

Их функционирование заключается в перехвате и анализе сетевых пакетов, проходящих по каналам связи.

В отличие от HIDS, NIDS предназначены для защиты более чем одного узла.

©2018, ОАО «ИнфоТеКС».

IDS

Чтобы мониторинг был эффективным, необходимо наличие, по крайней мере, одного проверяющего NIDS-устройства в каждом сетевом сегменте. Это устройство может представлять собой полнофункциональный компьютер IDS или просто повторитель трафика, иначе называемый датчиком или заглушкой.

Датчики и заглушки – это небольшие сетевые устройства, специально предназначенные для NIDS и имеющие два или более сетевых порта.

Заглушки и датчики, как правило, невидимы для злоумышленников.

©2018, ОАО «ИнфоТеКС».

IDS

Модель обнаружения аномалий (AD)

Работа модели заключается в установке определенных базовых шаблонов и выявлении отклонений от них.

Если IDS отслеживает на предмет расхождений лишь заголовки сетевых пакетов, то AD выполняет обнаружение аномалий в протоколах.

Цель AD - обеспечить возможность обнаружения широкого спектра вредоносных вторжений, включая те, для которых не существует предустановленных признаков.

©2018, ОАО «ИнфоТеКС».

IDS

Основные события, отслеживаемые и пресекаемые системой AD

- необычная активность учетной записи пользователя;
- слишком активный доступ к файлам и объектам;
- высокая степень использования процессора;
- некорректное использование протокола;
- необычная частота процедур входа в систему;
- высокое число фактов единовременного входа в систему;
- высокое число сеансов;
- любые операции над программным кодом;
- неожиданные попытки использования привилегий;
- необычное содержимое.

©2018, ОАО «ИнфоТеКС».

IDS

Компоненты и архитектура системы обнаружения атак

Модуль слежения (сенсор , монитор, зонд) обеспечивает сбор данных из контролируемого пространства (журнала регистрации или сетевого трафика).

Подсистема обнаружения атак осуществляет анализ информации, получаемой от модуля слежения. По результатам этого анализа данная подсистема может идентифицировать атаки, принимать решения относительно вариантов реагирования, сохранять сведения об атаке в хранилище данных и т.д.

База знаний - в зависимости от методов, используемых в системе обнаружения атак, база знаний может содержать профили пользователей и вычислительной системы, сигнатуры атак или подозрительные строки, характеризующие несанкционированную деятельность.

©2018, ОАО «ИнфоТеКС».

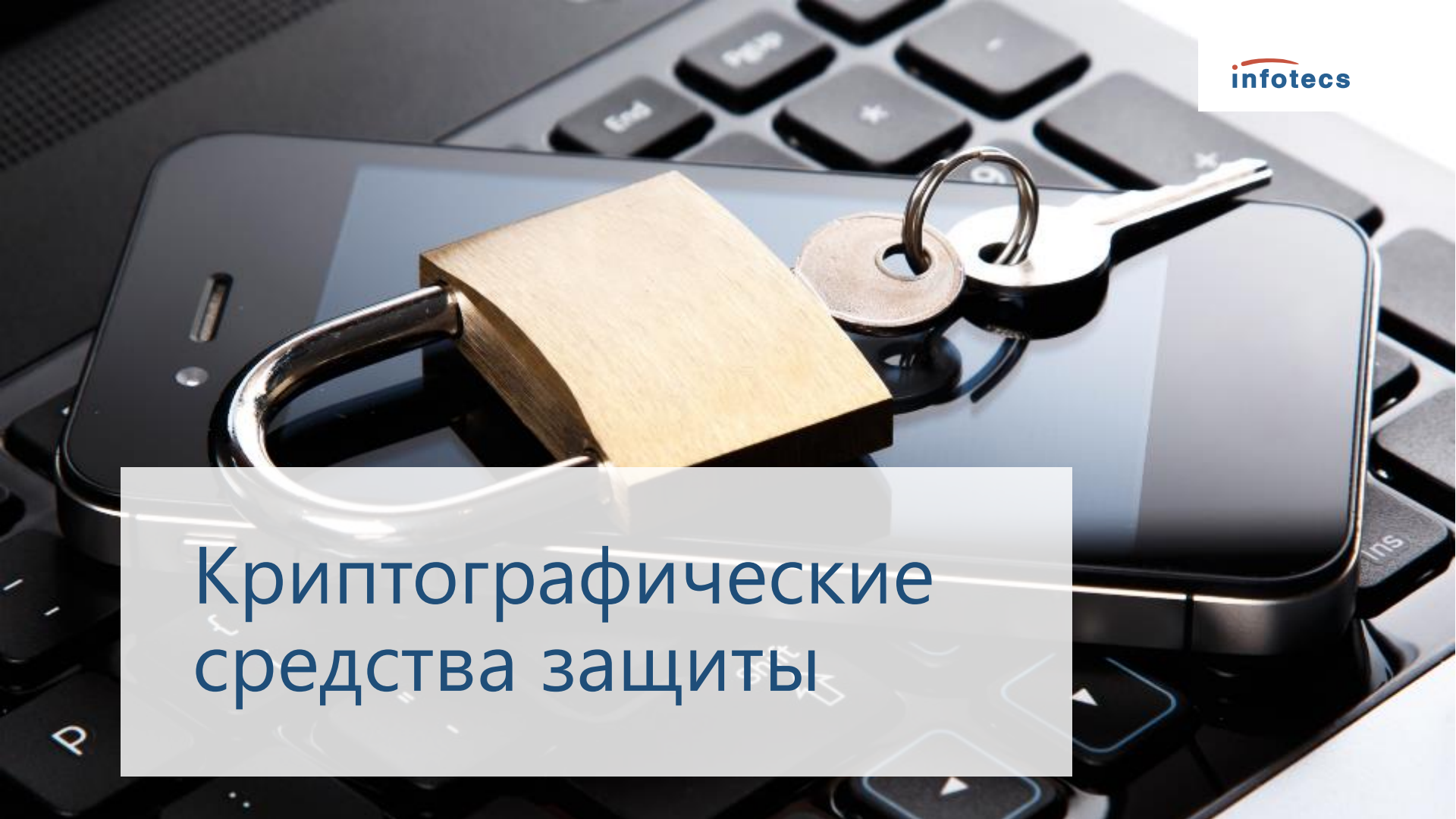
IDS

Хранилище данных обеспечивает хранение данных, собранных в процессе функционирования системы обнаружения атак.

Подсистема реагирования осуществляет реагирование на обнаруженные атаки и иные контролируемые события.

Подсистема управления предназначена для управления различными компонентами системы обнаружения атак (изменения политики безопасности для различных компонентов системы обнаружения атак, например, модулей слежения, получение информации от этих компонент. Управление может осуществляться при помощи как внутренних протоколов и интерфейсов, так и уже разработанных стандартов.

©2018, ОАО «ИнфоТеКС».

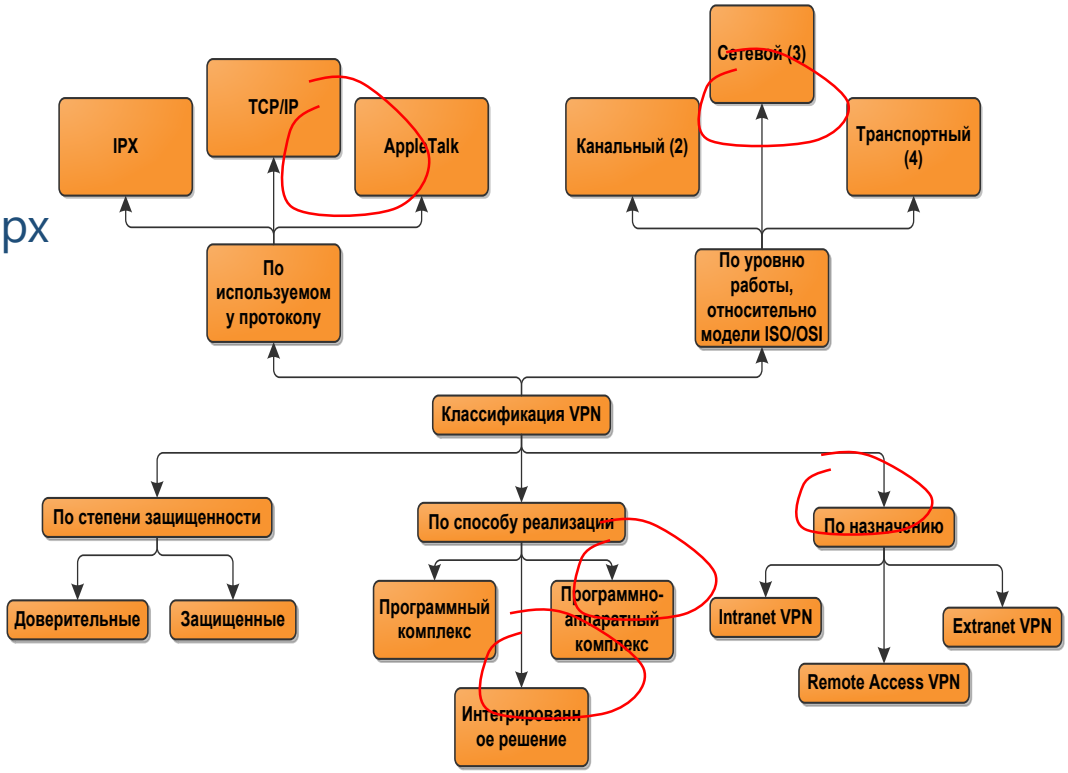


Криптографические средства защиты

Классификация VPN

VPN (*Virtual Private Network* — виртуальная частная сеть) —

логическая сеть, создаваемая поверх другой сети, например Интернет.

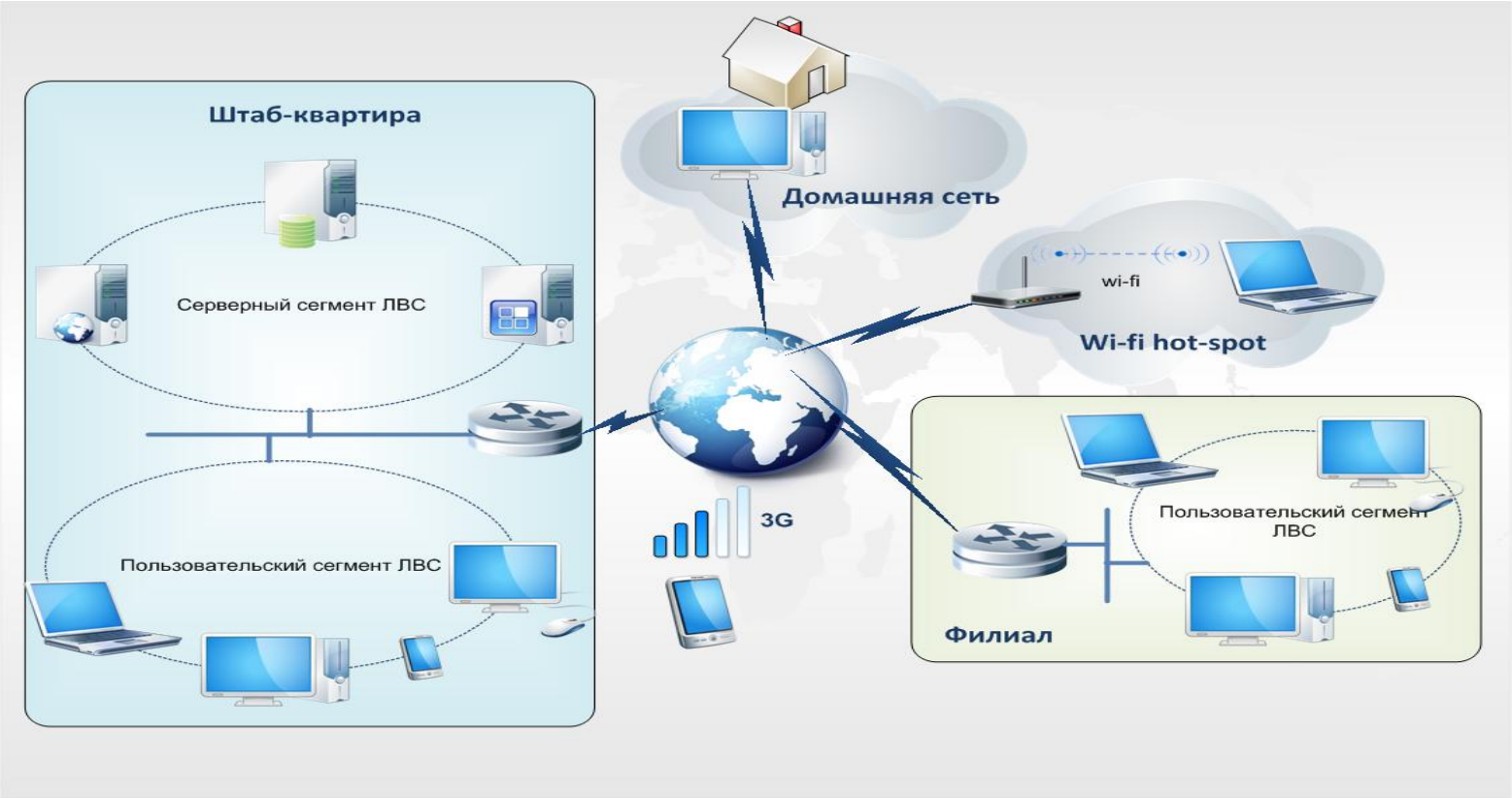


Примеры технологий VPN

- L2TP/IPSec
- PPTP
- OpenVPN
- **ViPNet**
- **…**

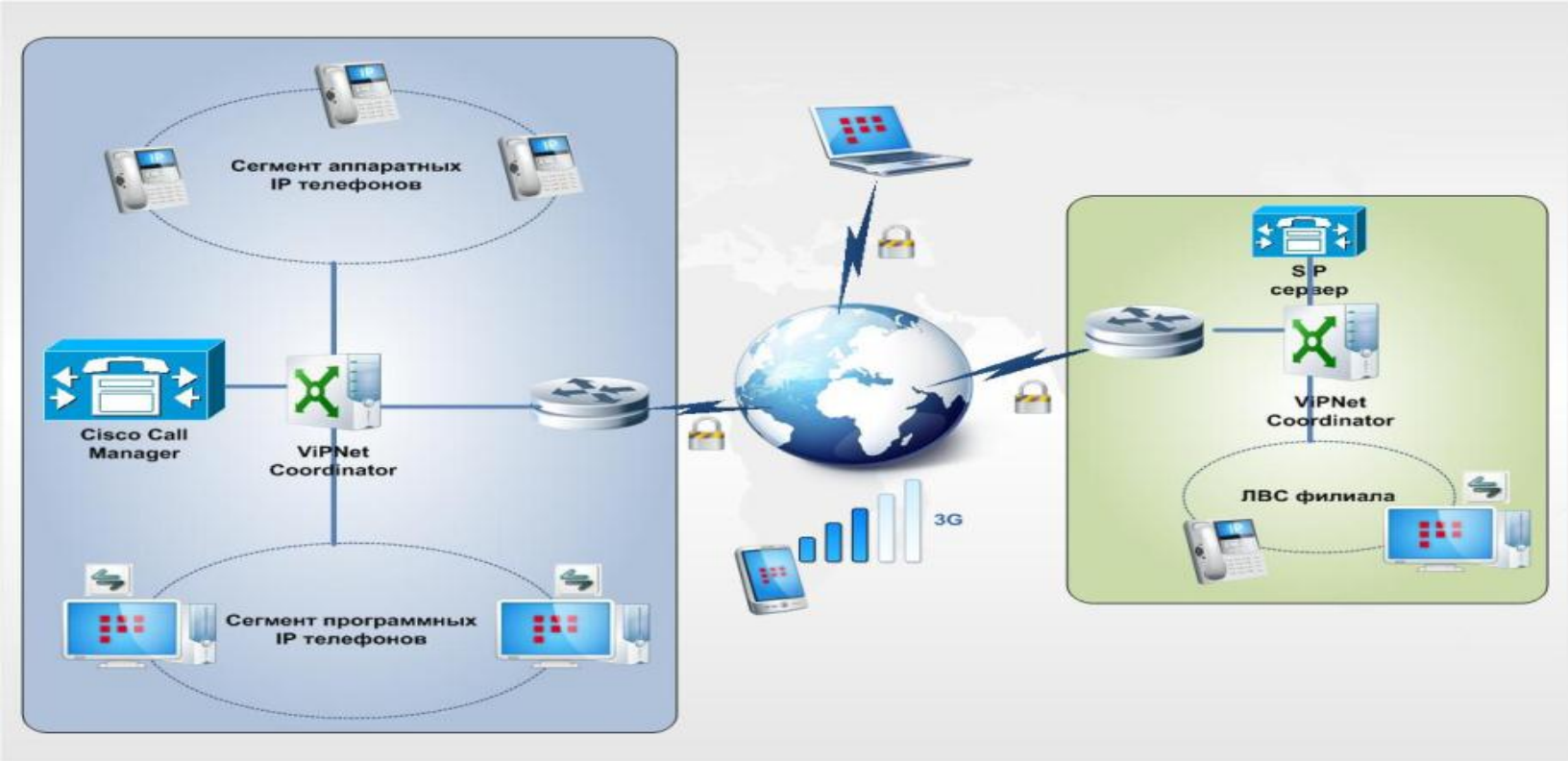
Примеры

Пример 1



©2018, ОАО «ИнфоТеКС».

Пример 2

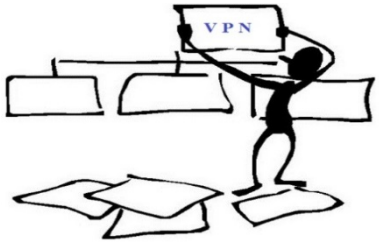


©2018, ОАО «ИнфоТеКС».

Структура VPN

VPN состоит из двух частей:

- «внутренняя» (подконтрольная) сеть, которых может быть несколько,
- и «внешняя» сеть, по которой проходит инкапсулированное соединение (обычно используется Интернет).



©2018, ОАО «ИнфоТеКС».

Классификация VPN

По степени защищенности используемой среды:

- **Защищённые -** с его помощью возможно создать надежную и защищенную сеть на основе ненадёжной сети, как правило, Интернета. Примером защищённых VPN являются: IPSec, OpenVPN и PPTP.
- **Доверительные -** используются в случаях, когда передающую среду можно считать надёжной и необходимо решить лишь задачу создания виртуальной подсети в рамках большей сети.

Примеры: Multi-protocol label switching (MPLS) и L2TP (Layer 2 Tunnelling Protocol) (например L2TP, как правило, используется в паре с IPSec).

©2018, ОАО «ИнфоТеКС».

Классификация VPN

По способу реализации:

- **Программно-аппаратные**

Реализация VPN сети осуществляется при помощи специального комплекса программно-аппаратных средств. Такая реализация обеспечивает высокую производительность и, как правило, высокую степень защищённости.

- **Программные**

Используют персональный компьютер со специальным программным обеспечением, обеспечивающим функциональность VPN.

- **Интегрированные**

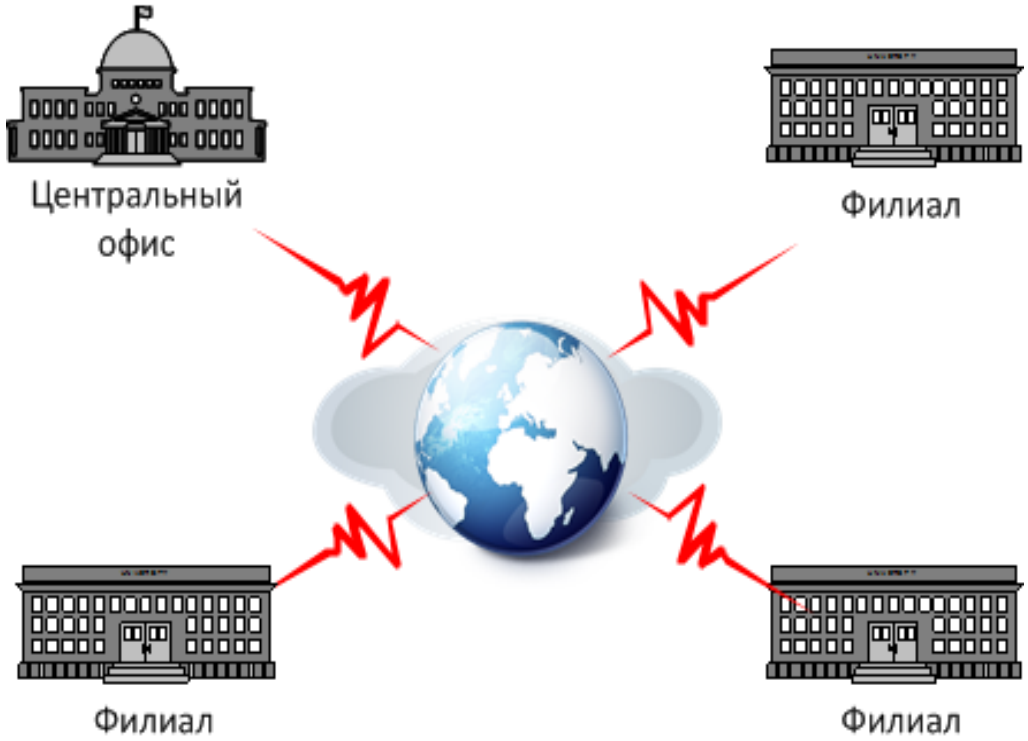
Функциональность VPN обеспечивает комплекс, решающий также задачи фильтрации сетевого трафика, организации сетевого экрана и обеспечения качества обслуживания.

©2018, ОАО «ИнфоТеКС».

Классификация VPN

Интранет VPN

внутрикорпоративная виртуальная сеть - объединяет в единую защищенную сеть несколько филиалов одной организации, взаимодействующих по открытым каналам связи.



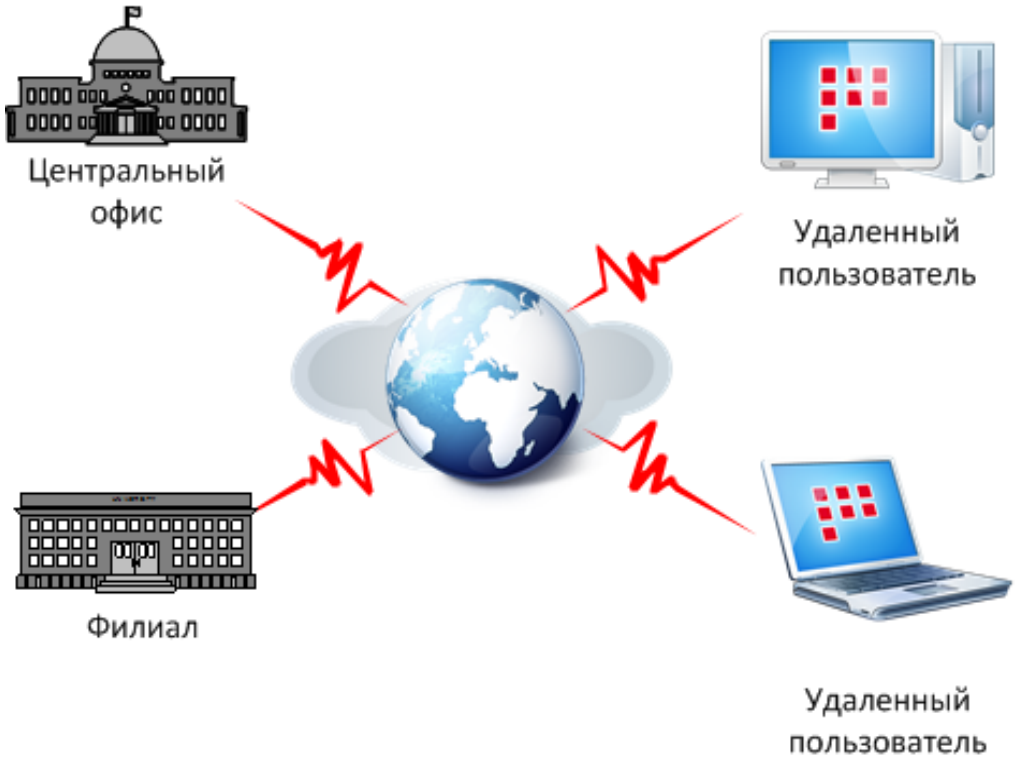
©2018, ОАО «ИнфоТеКС».

Классификация VPN

Remote Access VPN

(VPN с удаленным подключением)

виртуальная сеть с удаленным доступом. Реализует защищенное взаимодействие между сегментом корпоративной сети и одиночным пользователем

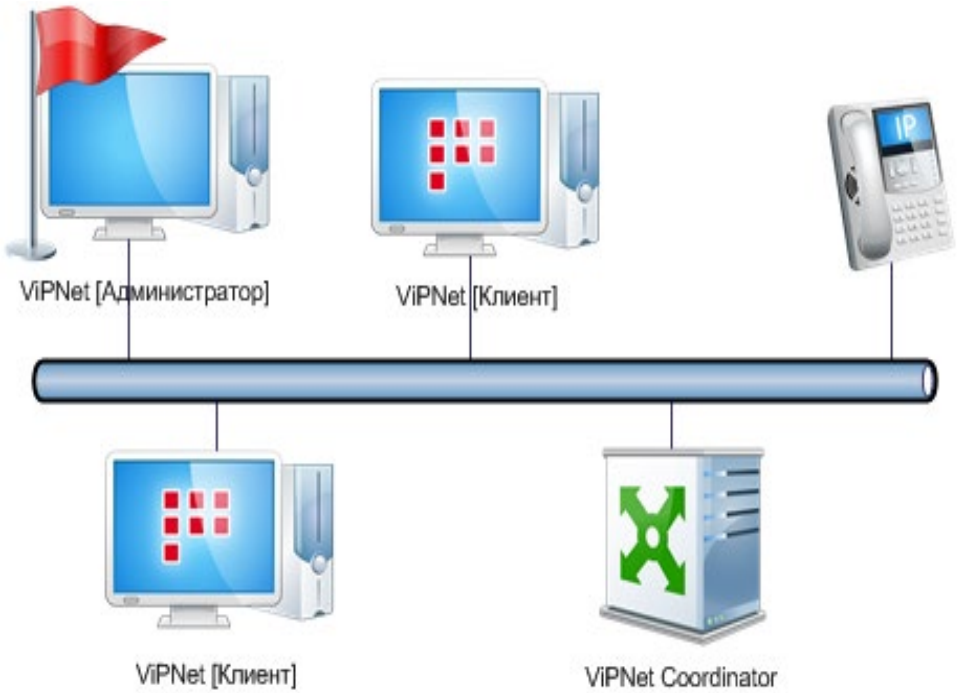


©2018, ОАО «ИнфоТеКС».

Классификация VPN

Клиент-Сервер и Клиент-Клиент VPN

обеспечивает защиту передаваемых данных между двумя узлами в корпоративной сети

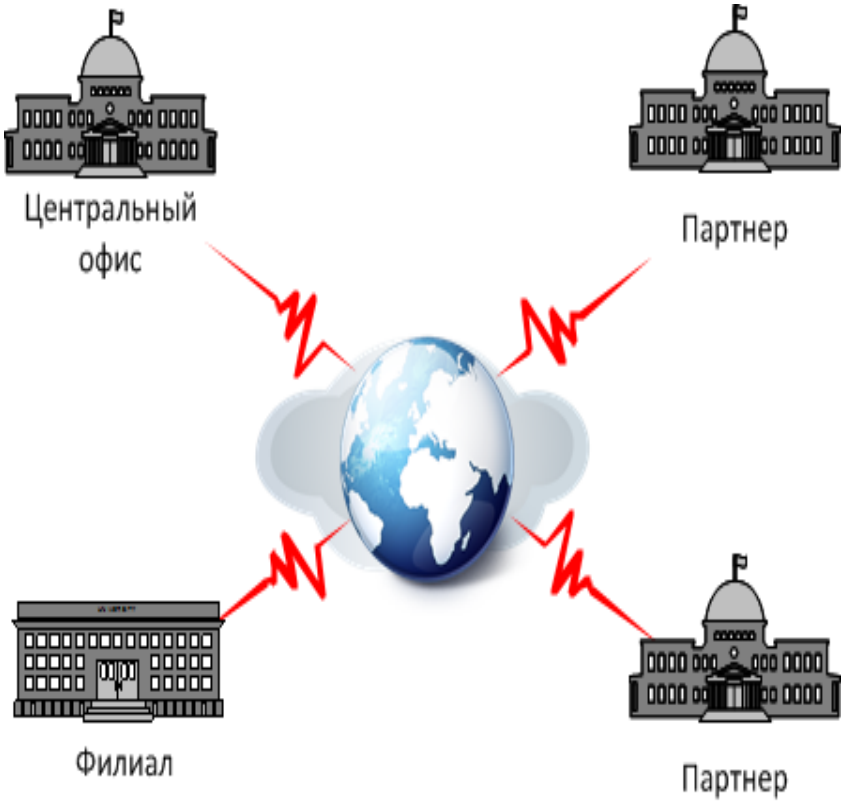


©2018, ОАО «ИнфоТеКС».

Классификация VPN

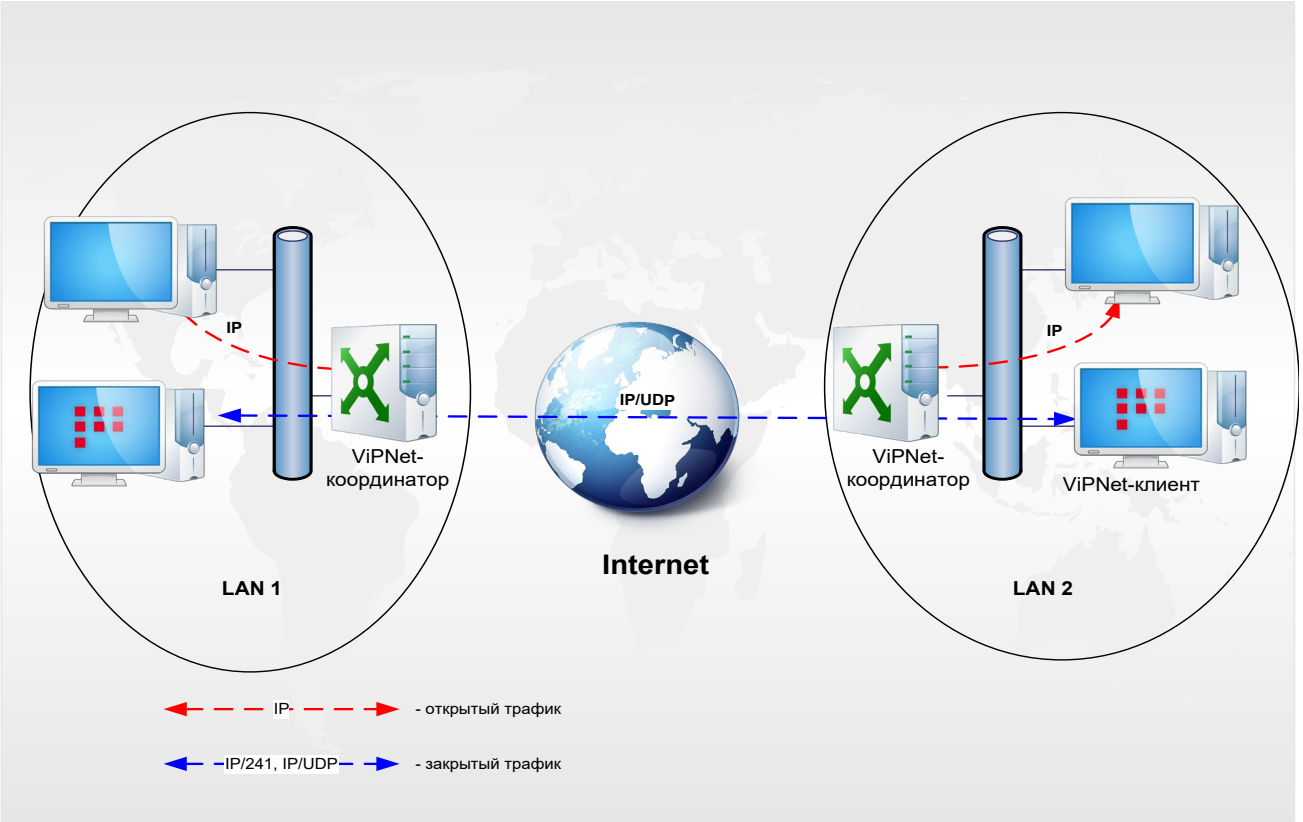
Экстранет VPN

межкорпоративная виртуальная сеть реализует защищенное соединение компании с ее деловыми партнерами и клиентами



©2018, ОАО «ИнфоТеКС».

Защита канала связи LAN-LAN



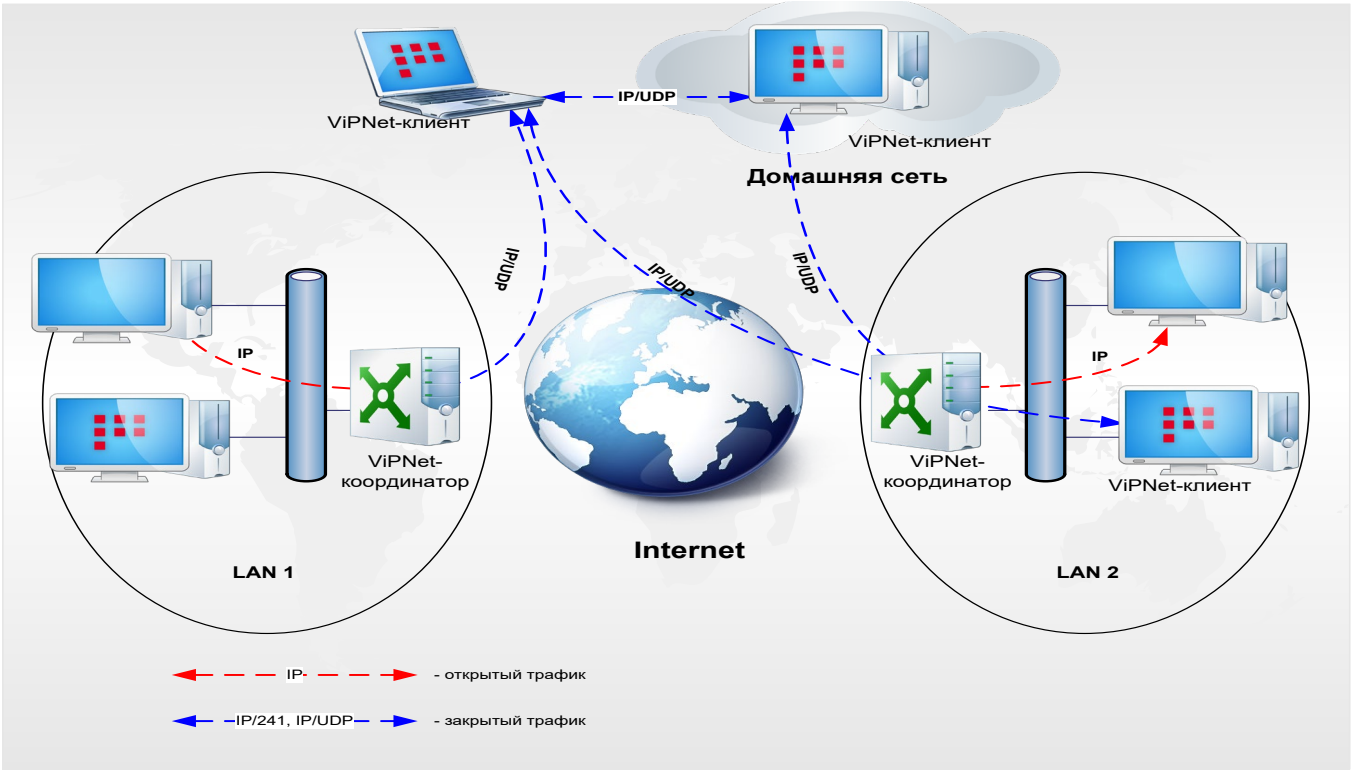
©2018, ОАО «ИнфоТеКС».

Терминальный доступ



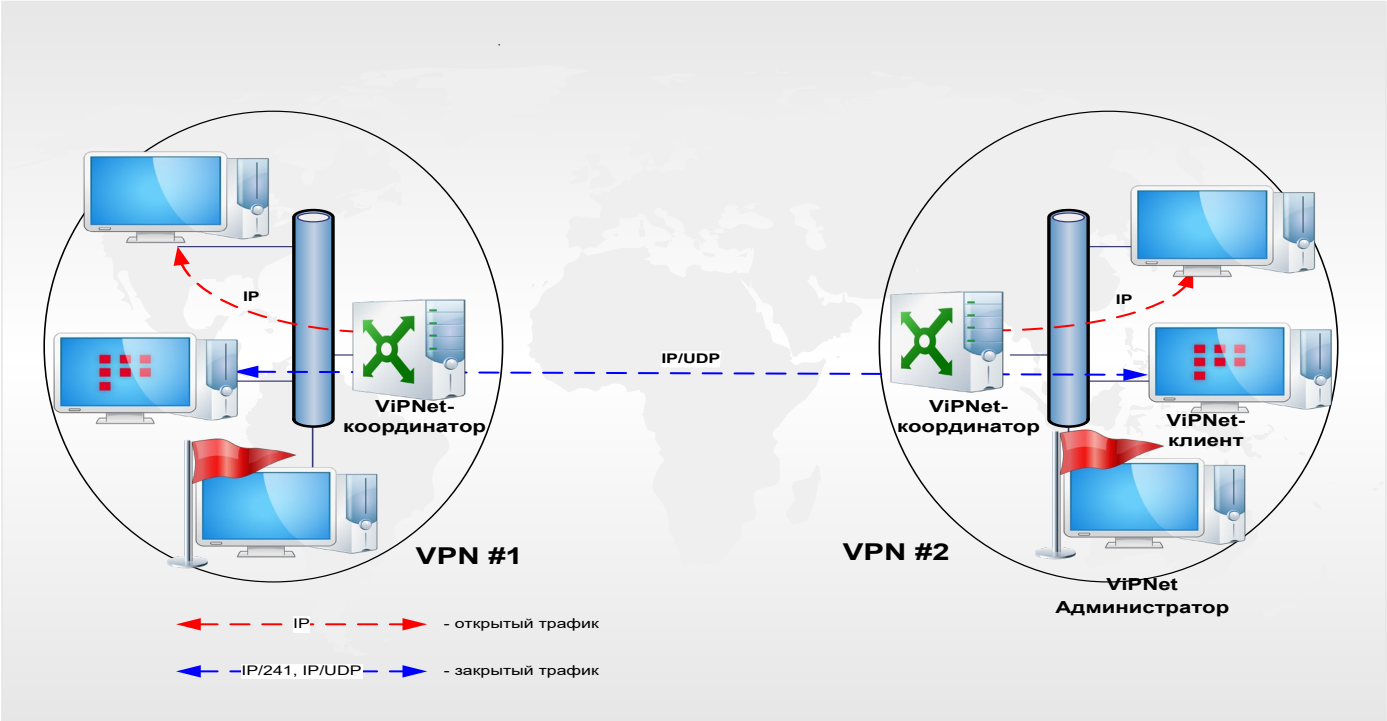
©2018, ОАО «ИнфоТеКС».

Защищенный удаленный доступ



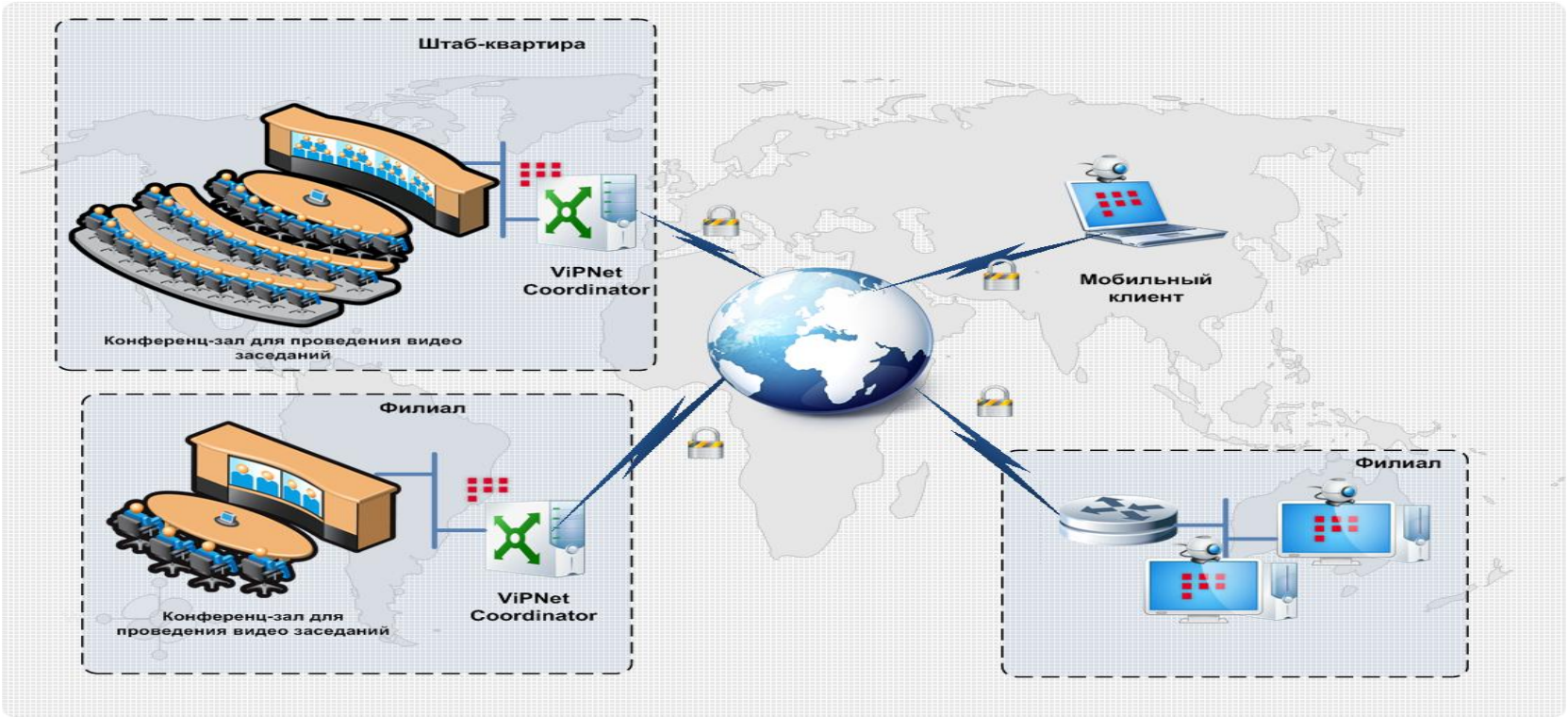
©2018, ОАО «ИнфоТеКС».

Межсетевое взаимодействие



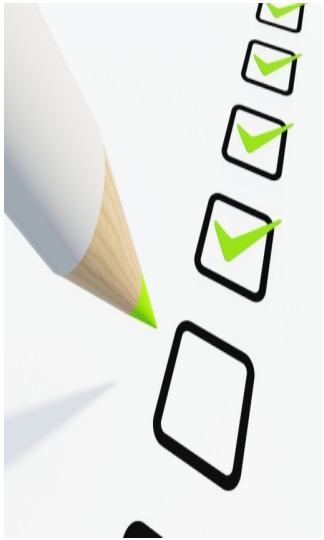
©2018, ОАО «ИнфоТеКС».

Защита видеоконференцсвязи



©2018, ОАО «ИнфоТеКС».

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.

©2018, ОАО «ИнфоТеКС».

Технология ViPNet

Network Security

Защита корпоративного уровня ViPNet VPN	Обнаружение и пресечение вторжений и атак Intrusion & Threats Detection and Prevention	Защита портальных и WEB based систем Web Secured Gateways

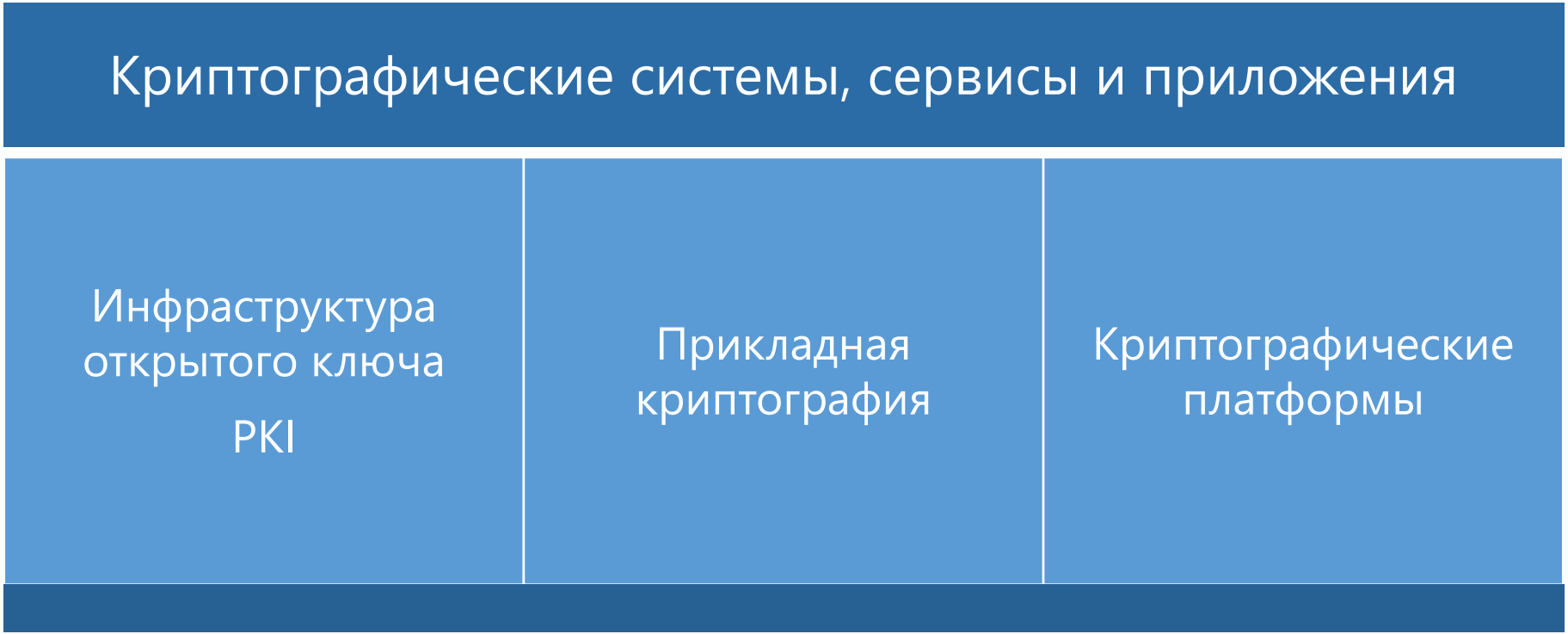
©2018, ОАО «ИнфоТеКС».

Технология ViPNet



©2018, ОАО «ИнфоТеКС».

Технология ViPNet



©2018, ОАО «ИнфоТеКС».


infotecs
Спасибо за внимание!