Защита рабочих мест удаленно работающих сотрудников с использованием ViPNet SafePoint

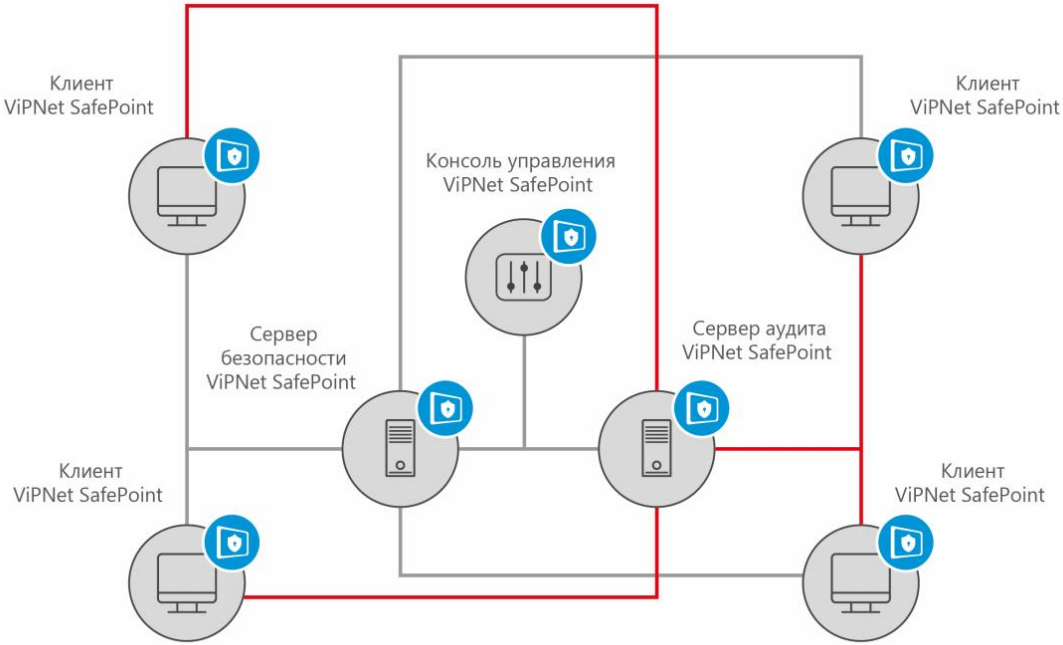
ViPNet SafePoint – краткий обзор продукта

ViPNet SafePoint

Средство защиты информации от несанкционированного доступа, устанавливаемое на рабочие станции и сервера, предназначенное для мандатного и дискреционного разграничения доступа к критически важной информации. Реализована разграничительная (пользователя к объектам) и разделительная (между пользователями) политика доступа, основанная на автоматической разметке создаваемых файлов.

Архитектура

- Клиент – ПО, устанавливаемое на рабочие станции и сервера, обеспечивает все заявленные защитные механизмы (содержит локальную консоль управления)
- Сервер безопасности – необходим для управления клиентской частью, рассылки политик защиты
- Сервер аудит – необходим для просмотра записей событий аудита в реальном времени
- Консоль управления сервером безопасности – интерфейс для работы с сервером



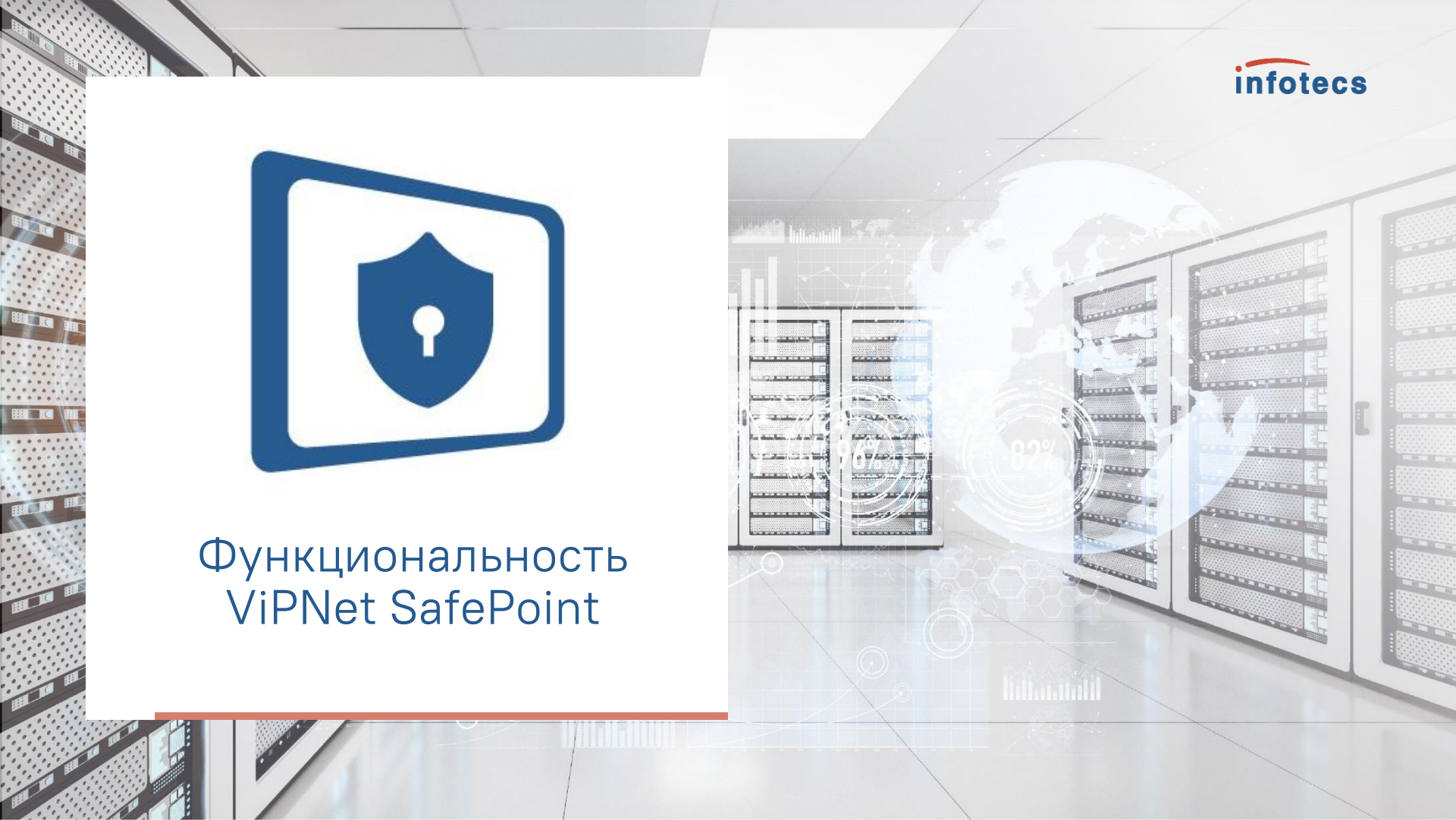
Поддерживаемые ОС

- Microsoft Windows 10 (64-разрядная)
- Microsoft Windows 8.1 (64-разрядная)
- Microsoft Windows Server 2012 R2 (Standard или Datacenter)
- Microsoft Windows Server 2016 (Standard или Datacenter)

Ожидание по сертификации

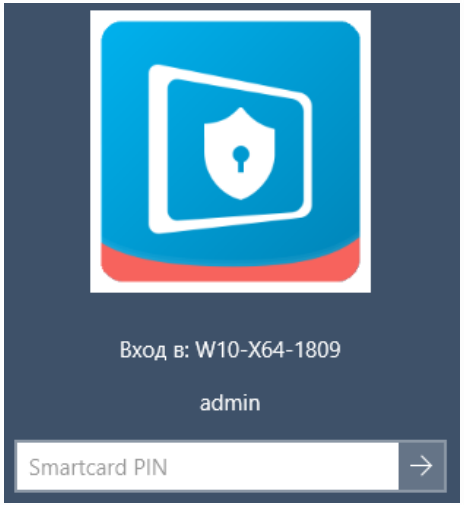
Продукт будет передан на сертификацию
по линии ФСТЭК России по требованиям к:

- 5 классу защищенности СВТ
- 4 классу защиты СКН (ИТ.СКН.П4.ПЗ)
- 4 классу ТДБ



Функциональность ViPNet SafePoint

Идентификация и аутентификация пользователей при входе в систему



- Двухфакторная аутентификация пользователей
- Поддержка USB-токенов и смарт-карт:
  - JaCarta ГОСТ
  - JaCarta PKI
  - JaCarta LT
  - Rutoken S
  - Rutoken Lite
  - Rutoken ЭЦП

Разграничение доступа

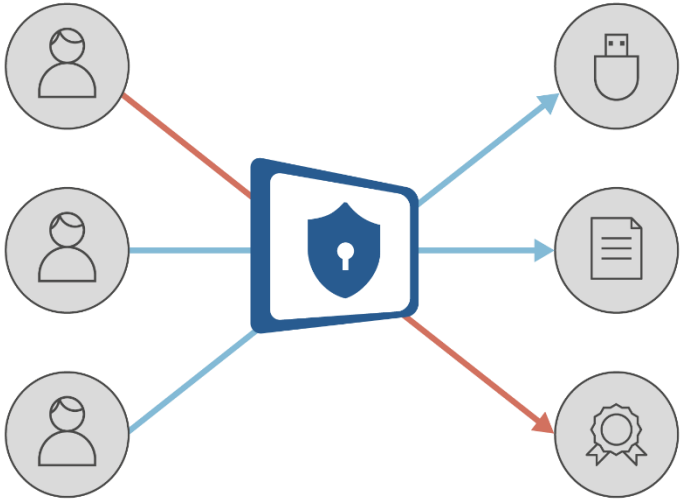
После прохождения идентификации и аутентификации, в соответствии с требованиями, необходимо организовать разграничения доступа для данного пользователя, чтобы он:

- Работал только с тем ПО, которое разрешено
- Мог работать только с теми файлами/документами, для которых хватает прав(полномочий)
- В системе запускались только разрешенные процессы
- Не модифицировал(-ись) важные модули

Дискреционный контроль доступа

Разграничительная политика на основе матрицы доступа

- ФС (вкл. сменные)
- прямой доступ к диску
- реестр
- принтеры
- службы
- устройства
- буфер обмена
- виртуальные машины



Особенности реализации дискреционного доступа

В качестве субъекта доступа в разграничительной политике одновременно выступают три сущности:

- исходный идентификатор пользователя SID
- эффективный идентификатор пользователя (контекст безопасности (маркер-token) процесса при доступе)
- «полнопутевое» имя процесса (имя исполняемого файла процесса)

Такой подход позволяет задавать: каким пользователем и процессом, к какому ресурсу разрешен доступ (в рамках реализации той или иной роли)

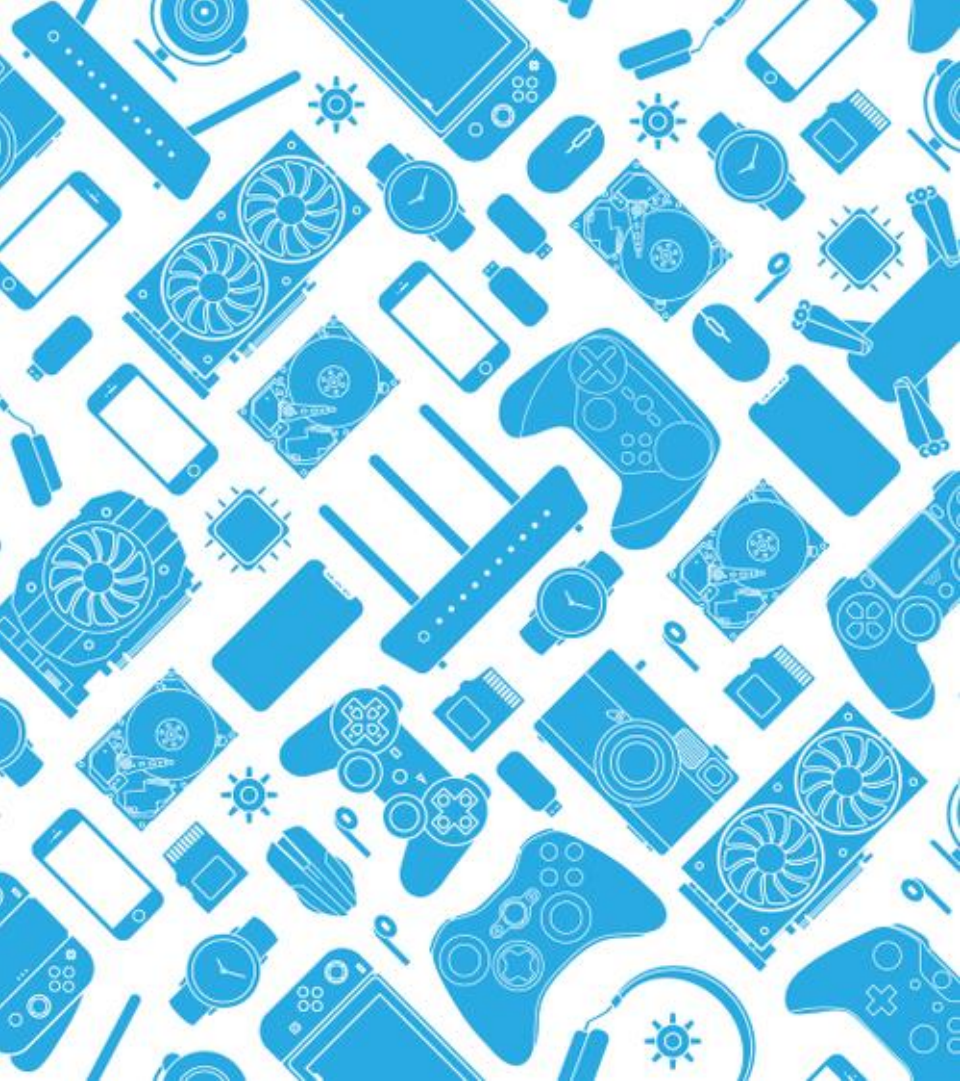
Мандатный контроль доступа пользователей и процессов

Разграничительная политика
на основе меток безопасности

Замкнутая программная среда и контроль времени работы

Замкнутая программная среда

- Защита от модификации запускаемых модулей
- Контроль запуска скриптов Active Scripts
- Контроль запуска задач



infotecs

Контроль устройств

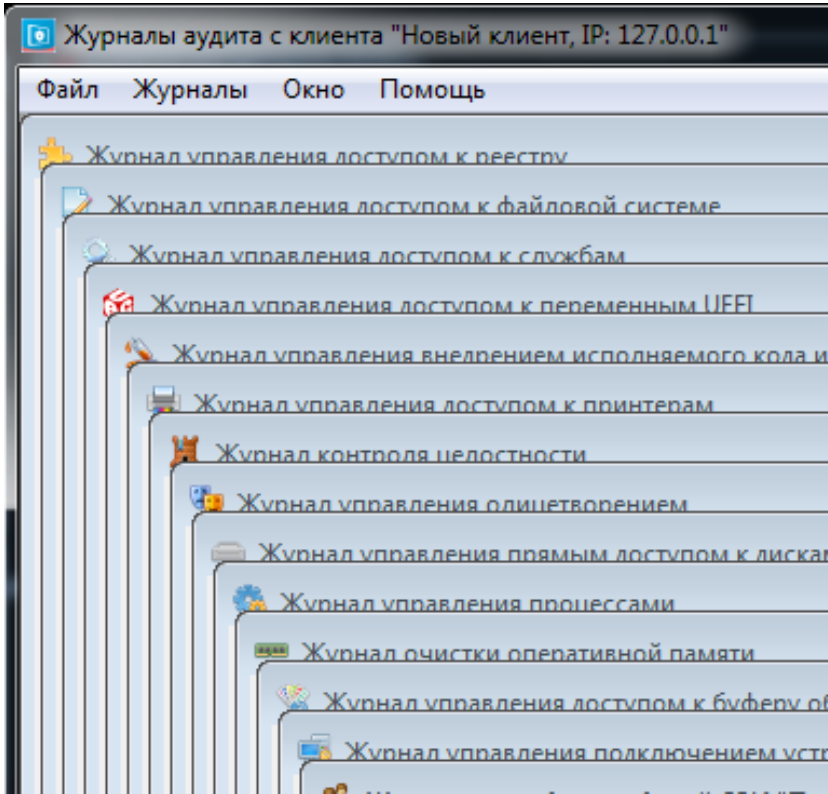
- Контроль и разграничение доступа к подключаемым внешним устройствам
- Разграничение доступа к принтерам

Контроль устройств

- Контроль монтирования (подключения) и отключения
- При наличии файловой системы поддерживаются: Чтение, Запись, Исполнение, Удаление, Переименование
- Аудит этих событий

Аудит событий безопасности

Сервер аудита осуществляет регистрацию событий в реальном времени



infotecs

А если отбросить сертификат?

Реальное применение есть?

Решаемые задачи (дополнительные возможности)

- Защита от внедрения и выполнения вредоносных программ и кода
- Защита от атак на повышение привилегий
- Защита данных от атак на уязвимости системного ПО
- Защита от инсайдеров
- Защита данных от атак на уязвимости прикладного ПО

Пример – защита почты

Можно запретить:

- Запуск приложений, скриптов из писем (защита от фишинговых атак по почте)
- Переход по нежелательным ссылкам

Как реализовать:

- Запрет запуска приложений из почтового клиента Outlook (кроме, например, Word, Excel, Acrobat Reader). Дополнительно: политика на запрет запуска приложений, скриптов из Word, Excel, Reader
- Запуск файла из почты порождает процесс. Этому процессу запрещено обращаться к ранее созданным размеченным файлам

Пример – Browser Security

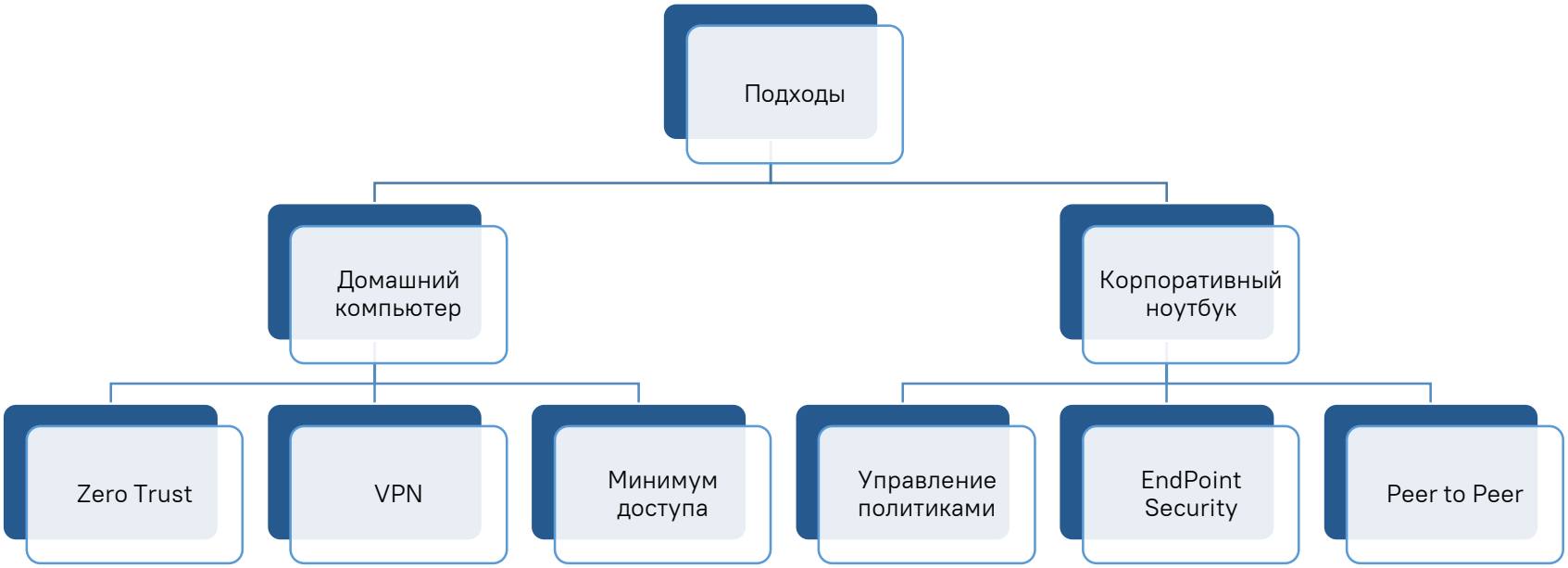
Защита от скриптов и зловредов, которые могут попасть после посещения зараженного сайта

Как сделать:

- Запрет на запуск новых приложений
- Разрешен запуск только доверенных приложений папок %SYSTEMROOT% и %ProgramFiles%
- Системным процессам и службам запрещается создание и модификация исполнимых файлов, которые были разрешены к выполнению
- Запрет на обращение к реестру

ViPNet SafePoint и защита рабочих мест удаленных пользователей

Подходы


Подходы
Домашний компьютер
Корпоративный ноутбук
Zero Trust
VPN
Минимум доступа
Управление политиками
EndPoint Security
Peer to Peer

Корпоративный ноутбук – плюсы и минусы

infotecs

ПЛЮСЫ

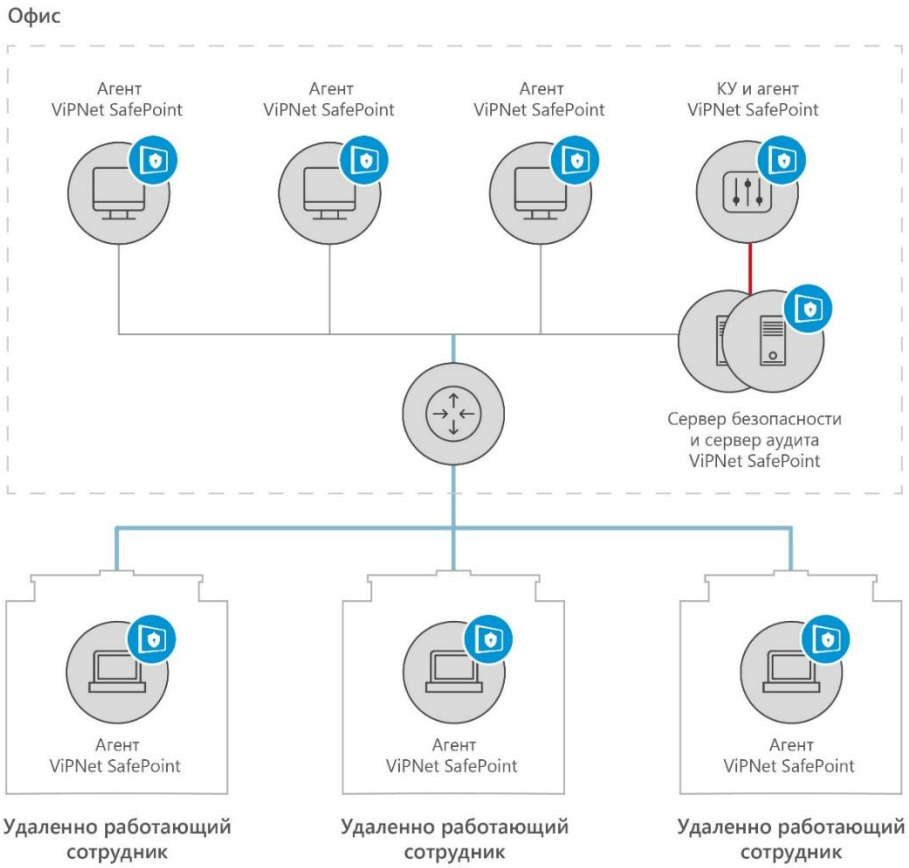
- Сами выбираем подходы к защите – не надо уговаривать сотрудника ставить что-то на домашний компьютер
- Выбираем необходимый набор ПО
- Можем вводить в домен, устанавливать необходимые политики
- Сотрудник с выданным ноутбуком, хоть и далеко, но является частью организации, а зачастую и входит в «границы периметра»

МИНУСЫ

- Надо быть уверенным, что сотрудник работает со всеми включенными средствами защиты
- Надо быть уверенным, что сотрудник работает с определенным набором ПО и не может устанавливать дополнительное без одобрения ИБ- и ИТ службы
- Необходим дополнительный контроль за миграцией документов с удаленного ноутбука
- Сотрудник с выданным ноутбуком, хоть и далеко, но является частью организации, а зачастую входит и в «границы периметра»

Типовой набор средств для удаленного пользователя

- ViPNet SafeBoot – обеспечение доверенной загрузки, контроль программной и аппаратной составляющей – доверие к платформе
- ViPNet SafePoint – защита от внутреннего нарушителя и обеспечение замкнутой программной среды
- ViPNet EndPoint Protection – средство защиты от внешних нарушителей
- ViPNet Client – обеспечение доверенного защищенного канала и доверенные коммуникации
- Антивирус

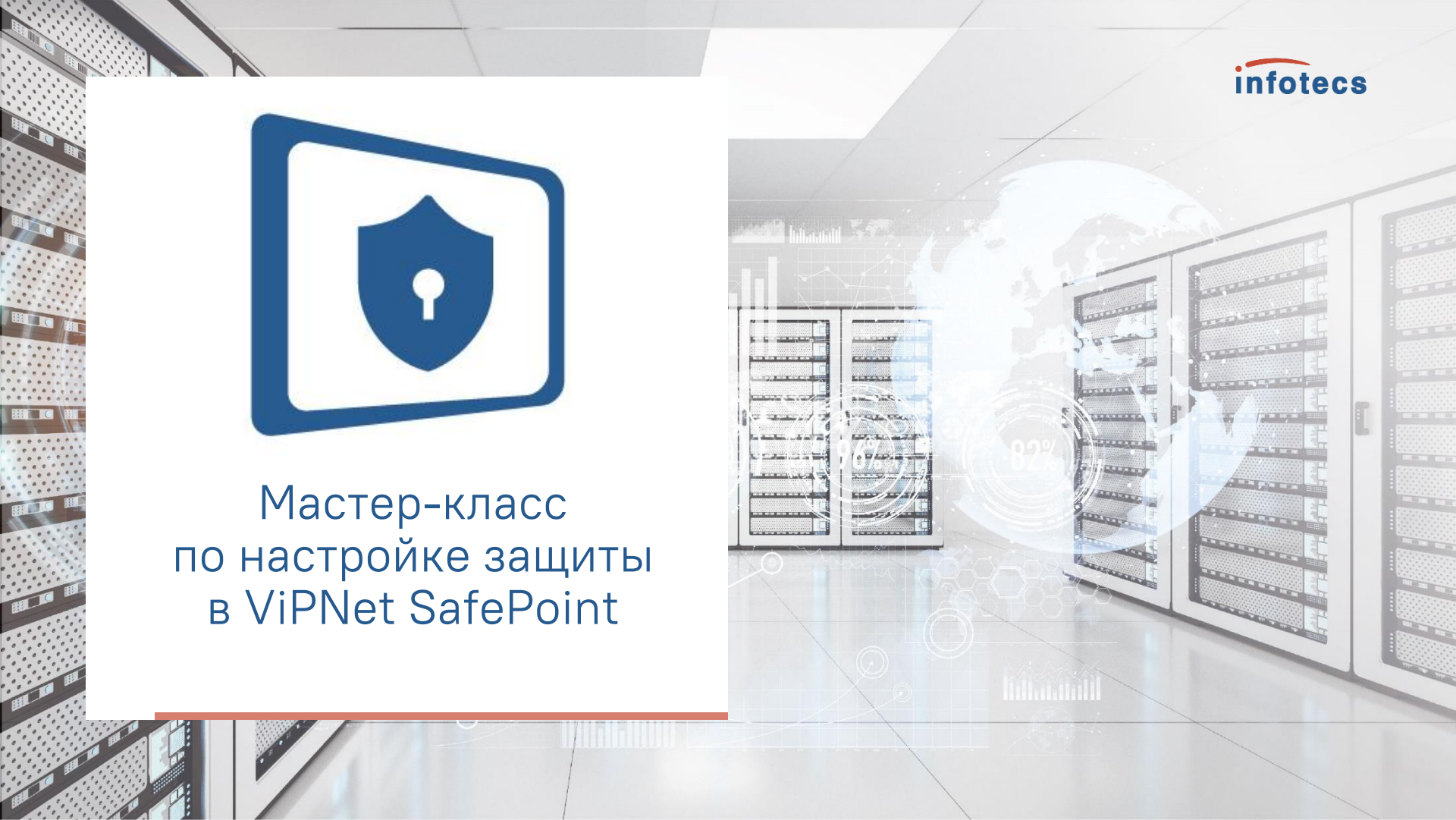


Вариант развертывания ViPNet SafePoint при удаленной работе

SafePoint и защита удаленного хоста

infotecs

Минимальный режим	• Важно, чтобы пользователь не имел возможность отключить средства защиты • Ставим на аудит события, связанные с появлением нового ПО
Базовый режим	• Важно, чтобы пользователь не имел возможность отключить средства защиты • Пользователь работает с набором ПО, расположенным в %Program Files%, %System Root% и %WinDir% - данное ПО нельзя модифицировать, удалять. Есть возможность установки нового ПО (но следить за данными событиями) • Ставим на аудит события, связанные с подключением внешних носителей и копированием объектов на них
Максимальный режим	• Все средства защиты включены, нет возможности отключить • Пользователь работает с строго установленным набором ПО - данное ПО нельзя модифицировать, удалять. Новое ПО может установить только admin • Офисным приложениям и браузерам запрещено запускать скрипты, cmd • Пользователь работает с выбранным набором внешних устройств • По всем событиям ведется аудит, все события направляются в SIEM



Мастер-класс по настройке защиты в ViPNet SafePoint

Пара слов о стенде и сценарии

- Имеем 3 виртуальных машины:
  - ВМ1 – Сервер безопасности, Сервер аудита и агент
  - ВМ2 – Агент
  - ВМ3 – без ViPNet SafePoint (для демонстрации последствий некоторых атак)
- Часть правил в ViPNet SafePoint уже будет настроена
- Краткий сценарий:
  - Подготавливаем и настраиваем защитные механизмы – передаем на агенты
  - Проверяем защитные механизмы в действии
  - Делаем пост-разбор на сервере аудита


START

И вот сотрудник работает из дома

Вопросы?

Иван Кадыков,
руководитель направления
Ivan.Kadykov@infotecs.ru

infotecs

Спасибо за внимание!

Подписывайтесь на наши соцсети

@infotecs.ru

@vpninfotecs

@InfoTeCS_Moscow