infotecs

ViPNet Endpoint Security

Решения для защиты рабочих станций и серверов

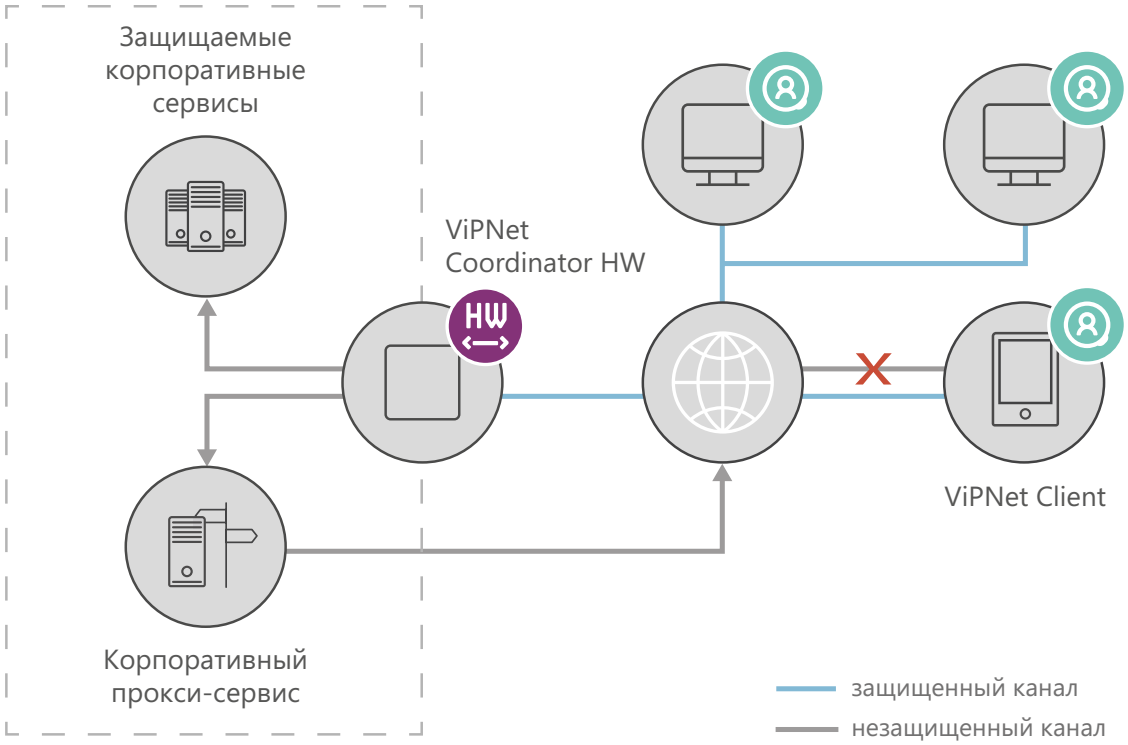
В современном мире любая организация сталкивается с проблемой защиты своих рабочих станций и серверов, а с появлением мобильных устройств – смартфонов и планшетов, которые активно вошли в инфраструктуру компаний. С каждым днем эта задача становится все более значимой.

Необходимо учитывать потребность обеспечения безопасности в части защиты от внешних нарушителей (киберпреступников), от внутреннего нарушителя (пользователя, который своими действиями может нанести вред компании), а также сохранности обрабатываемых и передаваемых с устройства на устройство данных.

С целью эффективной защиты конечных устройств компания ИнфоТеКС разработала и успешно внедряет комплекс средств обеспечения безопасности рабочих станций, серверов и мобильных устройств, которые как самостоятельно, так и совместно с другими продуктами компании способны противостоять современным угрозам информационной безопасности.

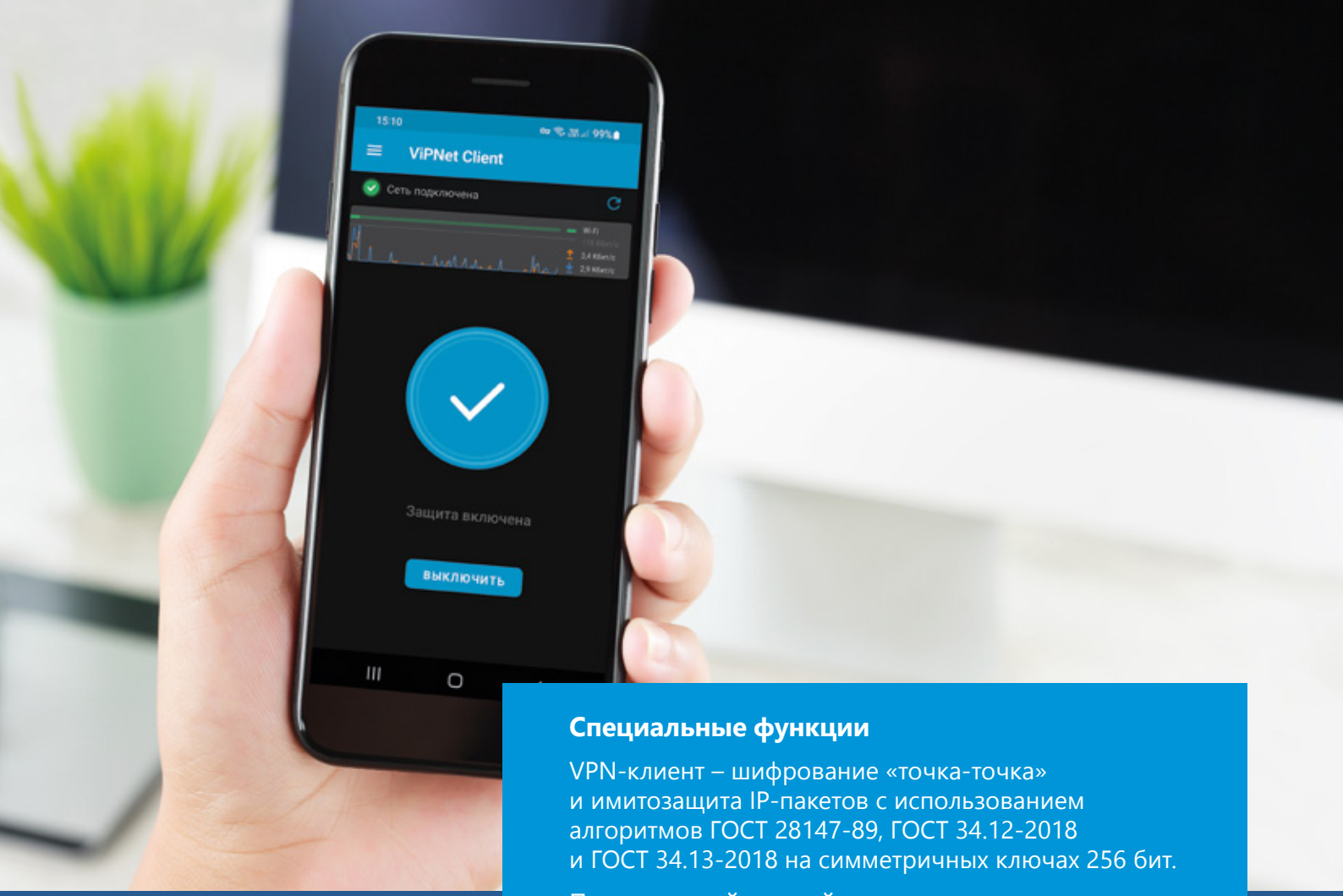
В результате многостороннего анализа уязвимостей, возникающих в корпоративной информационной системе с удаленными и мобильными пользователями, и исследования вопросов сетевой защиты компания «ИнфоТеКС» разработала ряд эффективных продуктов, созданных на основе собственной технологии ViPNet.

Сценарий защищенной и безопасной работы с ресурсами сети интернет



ViPNet Client

Программный комплекс для защиты информации
при ее передаче по открытым каналам связи
с мобильных и стационарных рабочих мест



Специальные функции

VPN-клиент – шифрование «точка-точка» и имитозащита IP-пакетов с использованием алгоритмов ГОСТ 28147-89, ГОСТ 34.12-2018 и ГОСТ 34.13-2018 на симметричных ключах 256 бит.

Персональный сетевой экран.

[ВОЗМОЖНОСТИ]

1 Продукт позволяет обеспечить унифицированный доступ к ресурсам корпоративных информационных систем из любой точки мира с использованием произвольных TCP/IP-сетей.

2 Технология ViPNet, лежащая в основе продукта, позволяет эксплуатировать территориально распределенные ИС из единого центра управления и отправлять ключи шифрования и обновления программного обеспечения по защищенному каналу.

3 Архитектура продукта позволяет обеспечить одновременную работу с ресурсами различных сегментов корпоративной сети.

4 Возможности продукта по шифрованию и фильтрации трафика позволяют в реальном времени осуществлять защиту голосового трафика, видеосвязи, IP-телефонии, почтового обмена и других служб в сетях TCP/IP.

[СЕРТИФИКАЦИЯ]

ФСБ РОССИИ

- ViPNet Client for Windows соответствует требованиям:
  - СКЗИ класса КС1, КС2 и КС3
  - МЭ 4 класса
- ViPNet Client for Linux: СКЗИ класса КС1, КС2 и КС3
- ViPNet Client for Android: СКЗИ класса КС1
- ViPNet Client for iOS: СКЗИ класса КС1
- ViPNet Client for Aurora: СКЗИ класса КС1 и КС2

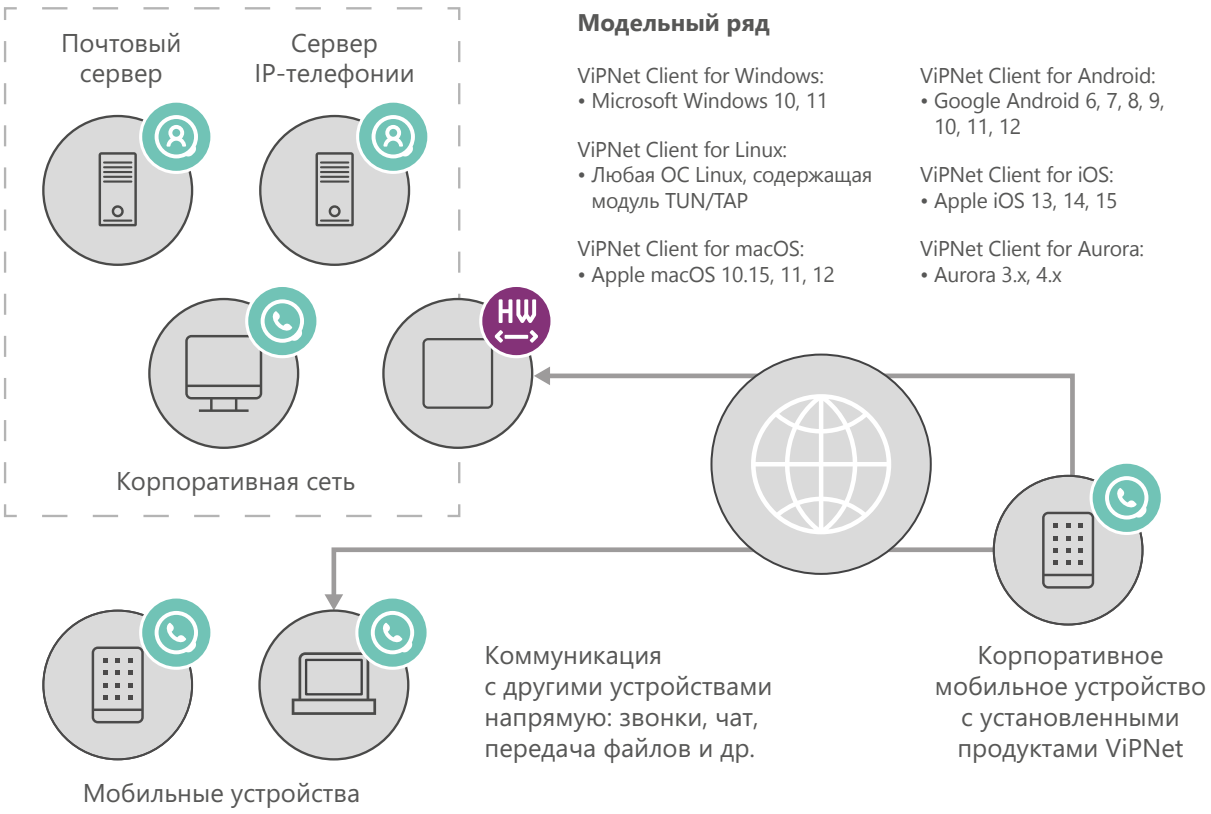
ФСТЭК РОССИИ

- ViPNet Client for Windows соответствует требованиям МЭ типа В 4 класса

[СЦЕНАРИИ]

- Безопасная работа удаленного пользователя с корпоративными ресурсами и сервисами через защищенные каналы как в парадигме Client-to-Site, так и в парадигме Client-to-Client. Работа в парадигме Client-to-Client («точка-точка») позволяет защитить информацию не только при использовании публичных каналов связи, но и при использовании ViPNet Client внутри корпоративной сети, обеспечивая защиту конфиденциальной информации от внутреннего нарушителя.
- Дополнительно к сценариям защиты есть возможность на базе существующей защищенной сети ViPNet использовать опциональные средства защищенных коммуникаций, таких как защищенная корпоративная почта (продукт «ViPNet Деловая почта») и защищенный корпоративный мессенджер (продукт «ViPNet CSS Connect»).
- ViPNet Client поддерживает работу на виртуальных машинах, что позволяет использовать средства защиты ViPNet в VDI-средах.
- ViPNet Client может быть использован и как наложенное средство информационной безопасности для защиты существующих систем почтового обмена, документооборота, IP-телефонии и видеоконференцсвязи. Использование ViPNet Client в таком сценарии не требует изменения и доработок прикладного программного обеспечения.
- В ViPNet Client можно включить конфигурацию, в которой прямой доступ устройства в интернет блокируется. В этой конфигурации устройство может обращаться в интернет только через корпоративную «зону очистки трафика» (набор средств информационной безопасности, таких как прокси-серверы, DLP-системы, средства контентной фильтрации и т.п.). Такой подход обеспечивает многоуровневую защиту устройства и позволяет применить корпоративные механизмы информационной безопасности к любым устройствам, физически покидающим защищенный периметр.

Сценарии использования и защиты мобильных и стационарных рабочих мест



Модельный ряд

ViPNet Client for Windows:
- Microsoft Windows 10, 11

ViPNet Client for Linux:
- Любая ОС Linux, содержащая модуль TUN/TAP

ViPNet Client for macOS:
- Apple macOS 10.15, 11, 12

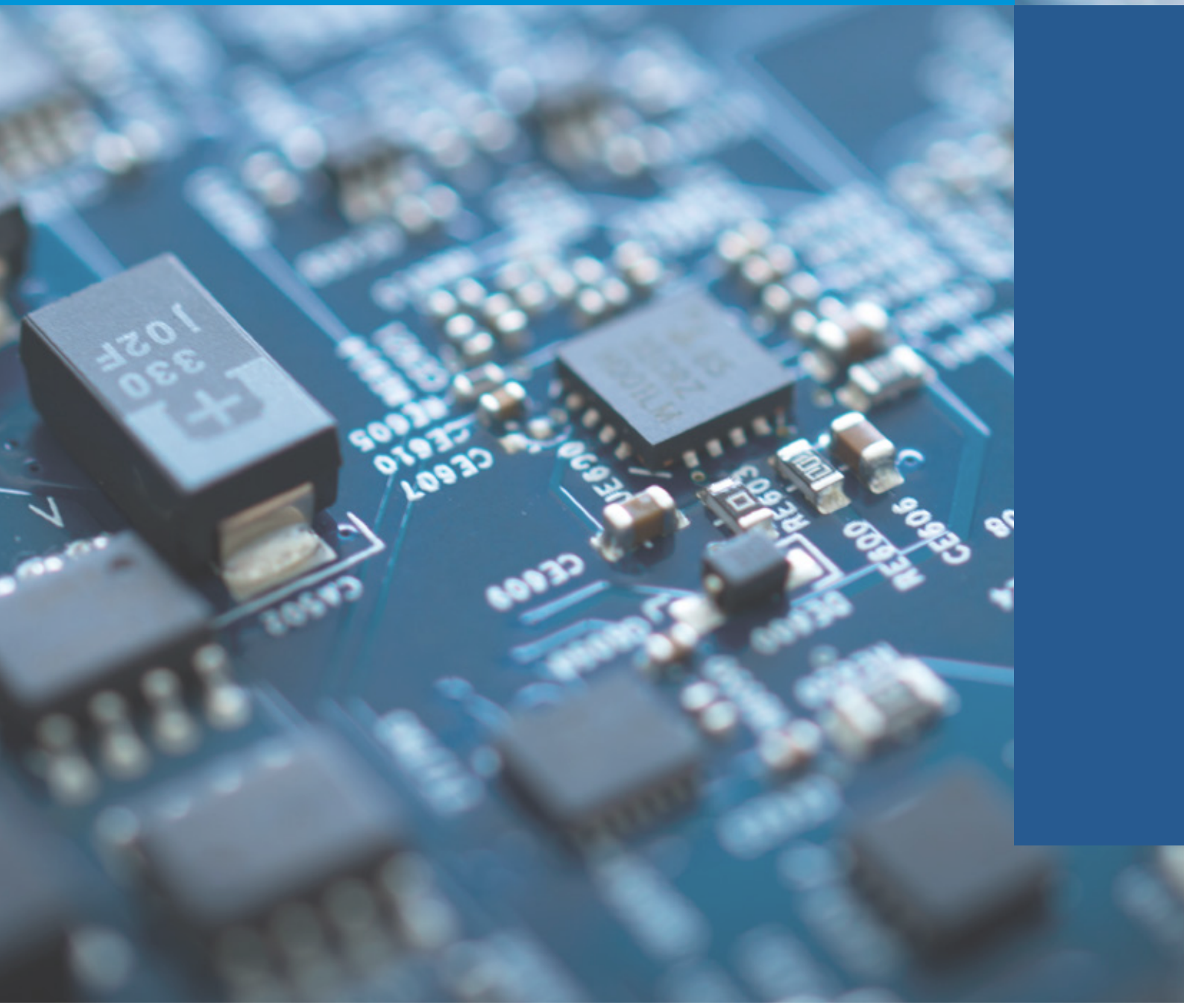
ViPNet Client for Android:
- Google Android 6, 7, 8, 9, 10, 11, 12

ViPNet Client for iOS:
- Apple iOS 13, 14, 15

ViPNet Client for Aurora:
- Aurora 3.x, 4.x

ViPNet SafeBoot

ViPNet SafeBoot – сертифицированный высокотехнологичный программный модуль доверенной загрузки (МДЗ), устанавливаемый в UEFI BIOS различных производителей. Предназначен для защиты ПК, мобильных устройств, серверов (в том числе серверов виртуализации) от различных угроз несанкционированного доступа (НСД) на этапе загрузки и от атак на BIOS.



[ПРЕИМУЩЕСТВА]

1 Программный МДЗ с возможностью установки в UEFI BIOS различных производителей

2 Упрощенные методы настройки МДЗ за счет шаблонов администрирования

3 Неизвлекаемость, в отличие от аппаратных исполнений МДЗ

4 Полный контроль целостности UEFI за счет проверки целостности всех его модулей

5 Российский продукт

[КОНТРОЛЬ ЦЕЛОСТНОСТИ КОМПОНЕНТОВ]

Чтобы платформе можно было доверять, нужна гарантия, что все важные модули, загружаемые при старте системы, неизменны. Поэтому ViPNet SafeBoot проверяет целостность:

- всех модулей UEFI BIOS
- загрузочных секторов жесткого диска
- таблиц ACPI, SMBIOS, карты распределения памяти
- реестра Windows
- файлов на дисках с системами FAT32, NTFS, EXT2, EXT3, EXT4 (независимо от того, какая операционная система установлена)
- ресурсов конфигурационного пространства PCI/PCIe
- CMOS (содержимого энергонезависимой памяти)
- завершенности транзакций – NTFS, EXT3, EXT4

[РЕШАЕМЫЕ ЗАДАЧИ]

- Выполнение требований приказов ФСТЭК России:

  №17 по защите государственных информационных систем (ГИС)

  №21 по защите информационных систем персональных данных (ИСПДн)

  №31 по защите автоматизированных систем управления технологическим процессом (АСУ ТП)

  №239 по защите КИИ

- Защита от НСД на самых ранних этапах загрузки компьютеров или устройств с UEFI

ПОЧЕМУ НУЖНА ЗАЩИТА НА УРОВНЕ BIOS?

Можно установить множество средств защиты в операционную систему, но если злоумышленник сможет внедрить вредоносную программу в BIOS или загрузить с внешнего носителя недоверенную операционную систему, то все вложения в средства защиты будут потрачены напрасно.

[ВОЗМОЖНОСТИ]

СТРОГАЯ ДВУХФАКТОРНАЯ АУТЕНТИФИКАЦИЯ

Аутентификация пользователя с помощью токена с сертификатом формата x.509 (двухфакторная), пароля или их сочетания. Поддерживаются токены: Rutoken ЭЦП, Rutoken ЭЦП 2.0, Rutoken Lite, Rutoken S, JaCarta PKI, JaCarta-2 ГОСТ, JaCarta LT, JaCarta-2 PKI/ГОСТ, Guardant ID

ЗАЩИТА ОТ MALWARE В UEFI BIOS

Невозможность развертывания вредоносного ПО из UEFI на жестких дисках при загрузке ОС

ЗАЩИТА НА УРОВНЕ SMM

Фильтрация программных SMI и ограничение их функциональности

ОБНОВЛЕНИЕ МДЗ

Возможность доверенного обновления МДЗ администратором системы

ЗАПРЕТ ЗАГРУЗКИ С ВНЕШНИХ НОСИТЕЛЕЙ

Невозможность загрузки нештатной операционной системы

ПОДДЕРЖКА АУТЕНТИФИКАЦИИ ЧЕРЕЗ LDAP/AD

Возможность использовать для аутентификации корпоративную учетную запись из LDAP/AD

ПОДДЕРЖКА SSO

Для входа в операционную систему или ViPNet SafePoint 1.2

ЖУРНАЛ СОБЫТИЙ БЕЗОПАСНОСТИ

Для удобства предусмотрены несколько режимов ведения журнала с разным уровнем детализации

ЗАЩИТА ОТ ОБХОДА И САМОТЕСТИРОВАНИЕ

МДЗ контролирует свое состояние и исключает возможность доступа к системе, если его целостность нарушена

ШАБЛОНЫ АДМИНИСТРИРОВАНИЯ

МДЗ настраивается локально на защищаемом компьютере. С помощью шаблонов настроек это можно делать в несколько раз быстрее

[КАК УСТАНОВИТЬ?]

ЗАКАЗАТЬ ПЛАТФОРМУ С ПРЕДУСТАНОВЛЕННЫМ МДЗ

Производитель МДЗ, компания ИнфоТеКС, создает совместные решения с производителями платформ. Таким образом, МДЗ может быть предустановлен на этапе производства.

САМОСТОЯТЕЛЬНО УСТАНОВИТЬ МДЗ

Вы можете установить МДЗ на определенные партии рабочих станций и серверов (необходимы наличие опытного инженера или консультации со специалистами ИнфоТеКС).

[СЕРТИФИКАЦИЯ]

ViPNet SafeBoot соответствует требованиям руководящих документов ФСТЭК России к средствам доверенной загрузки уровня базовой системы ввода-вывода 2 класса (Сертификат №3823) и может использоваться для построения:

- ИСПДн до УЗ1 включительно
- ГИС до 1 класса защищенности включительно
- АСУ ТП до 1 класса защищенности включительно
- КИИ до 1 класса защищенности

ViPNet SafePoint

Комплексная система защиты информации
от несанкционированного доступа уровня
ядра операционной системы

ViPNet SafePoint – это сертифицированная комплексная система защиты информации от несанкционированного доступа уровня ядра операционной системы (ОС). ViPNet SafePoint устанавливается на рабочие станции и серверы в целях обеспечения мандатного и дискреционного разграничения доступа пользователей к критически важной информации и подключаемым устройствам. Реализованные разграничительные (пользователя к объектам) и разделительные (между пользователями) политики доступа, основанные на автоматической разметке файлов, позволяют реализовать механизмы защиты от внешних и внутренних нарушителей.

[ПРЕИМУЩЕСТВА]

1. Реализация дискреционного метода разграничения доступа, а также управление доступом к статичным объектам файловой системы. В качестве субъекта доступа в разграничительной политике одновременно выступают три сущности:
   - исходный идентификатор пользователя SID
   - эффективный идентификатор пользователя
   - «полнопутевое» имя процесса (имя исполняемого файла процесса)
2. Защита от внедрения в процессы (Injection)
3. Контроль глобальных хуков
4. Контроль обязательно запущенных процессов системы

Возможность работы как в одноранговых сетях, так и в доменных сетях

Собственный сервер аудита для решения задач мониторинга событий безопасности

Гибкая и масштабируемая система

[ЗАДАЧИ]

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

[ВОЗМОЖНОСТИ]

ДВУХФАКТОРНАЯ АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ ПРИ ВХОДЕ В ОПЕРАЦИОННУЮ СИСТЕМУ (ОС)

В качестве идентификаторов могут использоваться:
- Rutoken Lite
- Rutoken S
- Rutoken ЭЦП 2
- JaCarta LT
- JaCarta PKI
- JaCarta PKI/ГОСТ
- JaCarta 2 PKI/ГОСТ
- JaCarta-2 ГОСТ
- JaCarta-2 SE
- JaCarta-2 PRO/ГОСТ

ЗАМКНУТАЯ ПРОГРАММНАЯ СРЕДА

Возможность контролировать неизменность разрешенных к запуску модулей, запуск Active scripts и задач позволяет усилить защиту от ранее неизвестных атак

КОНТРОЛЬ ЦЕЛОСТНОСТИ

- Файлов
- Объектов реестра ОС
- Собственных компонентов продукта

КОНТРОЛЬ ПРАВ ДОСТУПА К ОБЪЕКТАМ ФАЙЛОВОЙ СИСТЕМЫ (МАНДАТНЫЙ И ДИСКРЕЦИОННЫЙ)

Ключевая особенность контроля прав доступа к объектам ФС заключается в реализации различных принципов контроля доступа к статичным объектам (уже имеющимся в системе) и создаваемым в процессе работы

РАЗГРАНИЧИТЕЛЬНАЯ ПОЛИТИКА НА ОСНОВЕ МАТРИЦЫ ДОСТУПА ПРИМЕНЯЕТСЯ К:

- файловой системе (включая сменные)
- прямому доступу к диску
- реестру
- принтерам
- службам
- устройствам
- буферу обмена
- виртуальным машинам

КОНТРОЛЬ ПОДКЛЮЧЕНИЯ ВНЕШНИХ УСТРОЙСТВ

Контроль осуществляется на основе анализа разрешений на подключение к конкретным интерфейсам ввода (вывода) (портам USB, SATA/ATA/ATAPI, PCMCIA, COM, LPT, FIREWIRE, IEEE 1284.4) и типов подключаемых внешних программно-аппаратных устройств (адаптеров Secure Digital Memory Card (SD), Wi-Fi, Bluetooth, MTP-устройств, сетевых адаптеров, модемов, адаптеров чтения смарт-карт, ИК-адаптеров, CD/DVD/BD-приводов, любых съемных носителей и устройств Plug and Play)

КОНТРОЛЬ ОЛИЦЕТВОРЕНИЯ

Возможность контролировать доступ к сервисам олицетворения, что позволяет реализовать защиту от повышения привилегий

ГАРАНТИРОВАННОЕ УДАЛЕНИЕ И ОЧИСТКА ПАМЯТИ

Возможность исключить доступ к остаточной информации в обход разграничительной политики

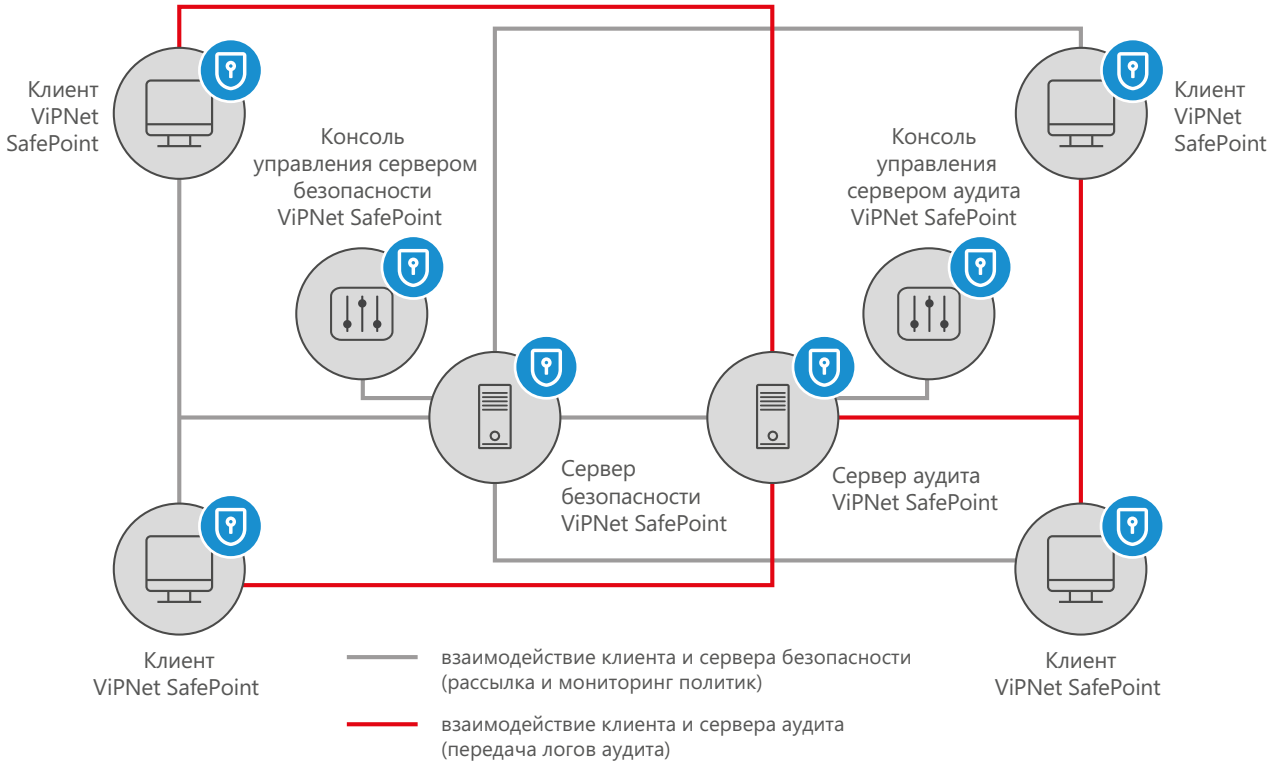
КОНТРОЛЬ ОПЕРАЦИЙ С БУФЕРОМ ОБМЕНА

Возможность управления доступом пользователей к буферу обмена, а также возможность контролировать передачу данных через OLE (Object Linking & Embedding) и Drag and Drop (перетаскивание объектов)

УПРАВЛЕНИЕ ДОСТУПОМ К СЛУЖБАМ WINDOWS

КОНТРОЛЬ ДОСТУПА К ПЕЧАТНЫМ УСТРОЙСТВАМ

[АРХИТЕКТУРА]



Сертифицировано во ФСТЭК России

По требованиям к:

- Средствам вычислительной техники. «Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации 5 класса защищенности»
- Средствам контроля съемных машинных носителей информации. «Профиль защиты средств контроля подключения съемных машинных носителей информации 4 класса защиты. ИТ.СКН.П4.ПЗ»
- 4 уровню доверия средств защиты информации – «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» утверждены приказом ФСТЭК России от 30 июля 2018 г. № 131

Поддерживаемые операционные системы

- Microsoft Windows 11
- Microsoft Windows 10
- Microsoft Windows 8.1
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019

ViPNet EndPoint Protection

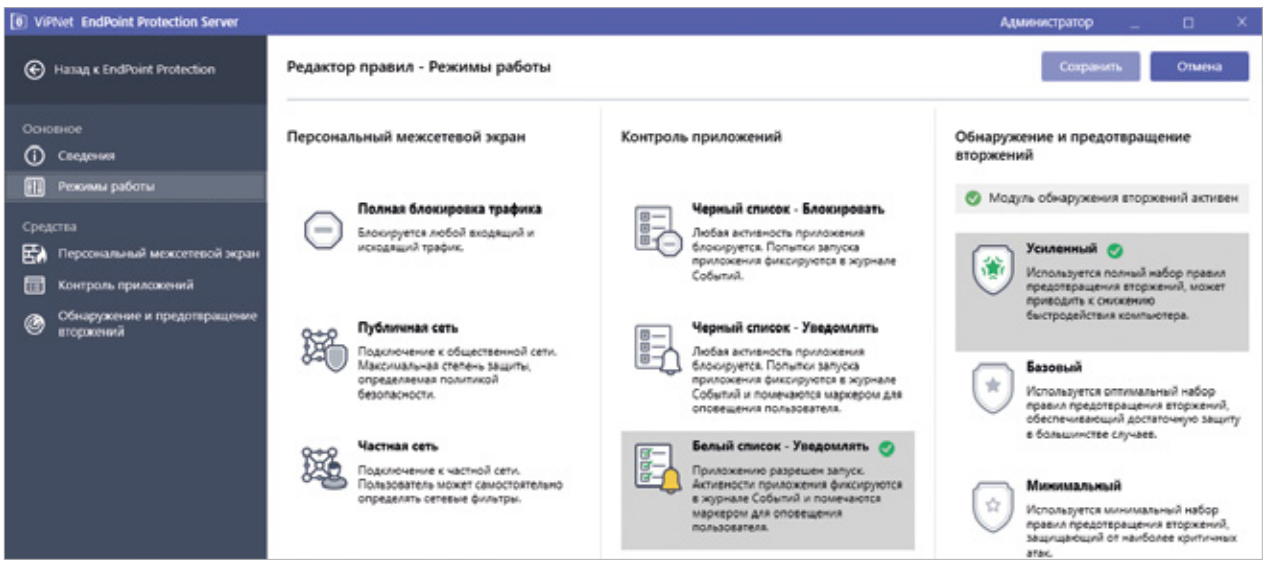
Система комплексной защиты рабочих станций и серверов, предназначенная для предотвращения «файловых» и сетевых атак, обнаружения вредоносных действий и реакции на эти действия

ViPNet EndPoint Protection – комплексное решение безопасности рабочих станций от внутренних и внешних угроз.

Состав решения

- проверенные в действии технологии обнаружения вторжений, дополненные настраиваемым модулем предотвращения вторжений
- модуль межсетевого экранирования с фильтрацией пакетов для непрерывной защиты рабочих станций от сетевых атак
- модуль контроля приложений, который работает на базе черных и белых списков программного обеспечения. Разграничивает доступ приложений к файлам, реестру ОС Windows, процессам и параметрам командной строки. Предотвращает установку и запуск вредоносного программного обеспечения
- antimalware модуль – эвристический движок, использующий собственную модель обнаружения вредоносного ПО, построенную с помощью машинного обучения
- модуль поведенческого анализа позволяет выявлять различного уровня аномалии в действиях пользователя и работе операционной системы (запуск системных утилит, задач, процессов и т.д.)

Возможность выбора режимов работы модулей



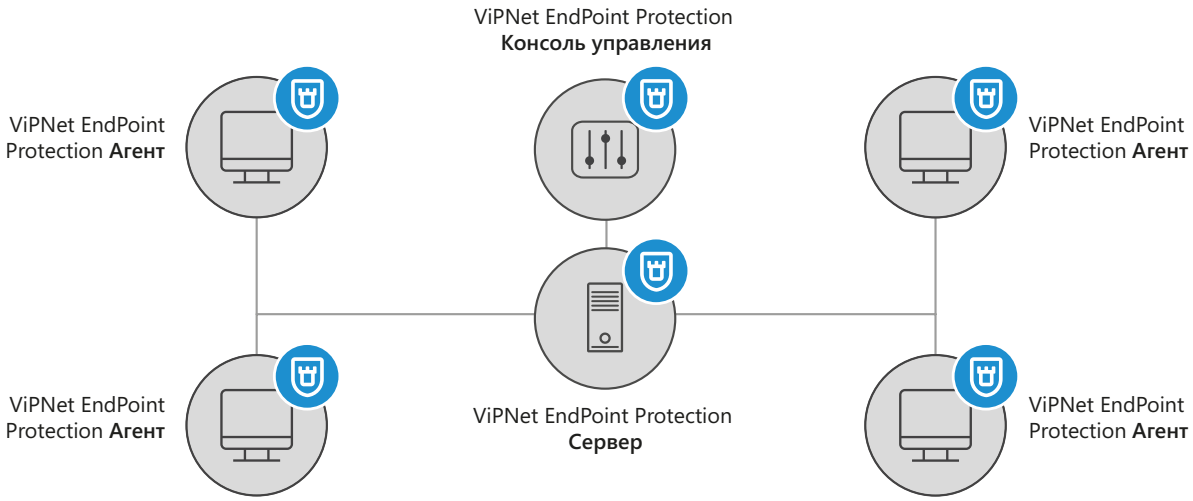
[АРХИТЕКТУРА]

ViPNet EndPoint Protection является клиент-серверным приложением и состоит из:

1 **ViPNet EndPoint Protection Агент** устанавливается на рабочие станции и серверы и осуществляет комплексную защиту хостов от внутренних и внешних угроз. В своей работе Агент использует базы решающих правил (БРП), полученные от серверного компонента

2 **ViPNet EndPoint Protection Сервер** обеспечивает централизованное управление агентами ViPNet EndPoint Protection, рассылку БРП и политик на Агенты, а также выполняет сбор и агрегацию событий информационной безопасности, поступающих с защищаемых рабочих станций и серверов

3 **ViPNet EndPoint Protection Консоль управления** предназначена для администрирования ViPNet EndPoint Protection Сервер и отображения информации о состоянии защищаемых рабочих станций и серверов



[ПРЕИМУЩЕСТВА]

- Использование технологий Endpoint Detection and Responce – мониторинг и противодействие подозрительной активности на хосте
- Эффективное решение для защиты рабочих станций и серверов от известных и неизвестных атак
- Гранулированные настройки безопасности для всех модулей продукта, применяемые как для одного, так и для группы хостов
- Выявление и удаление вредоносных исполняемых файлов, а также обнаружение и блокирование бесфайловых атак
- Использование собственных технологий behavioral analysis
- Преднастроенные режимы работы модулей ViPNet Endpoint Protection, а также регулярно обновляемые правила для модулей обнаружения и предотвращения вторжений, контроля приложений
- Интеграция ViPNet EndPoint Protection с аналитической системой ViPNet TIAS расширяет возможности обнаружения и реагирования на инциденты информационной безопасности
- Защита рабочих станций и серверов информационных систем в соответствии с требованиями 17, 21, 31 и 239 приказов ФСТЭК России*

*после получения сертификата ФСТЭК России

[ВОЗМОЖНОСТИ]

МОДУЛЬ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ

Обнаружение атак происходит на основе эвристического и сигнатурного метода. Мониторингу и анализу подвергаются следующие ключевые области:

- системные журналы ОС (Windows event log)
- журналы и логи приложений
- результаты выполнения команд
- файлы, папки, реестр ОС – создание, изменение, удаление
- трафик, проходящий через хост

На основании выявленных в результате анализа подозрительных активностей модуль блокирует атаки, руководствуясь установленными правилами блокировки с учетом критичности атаки

ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ МОДУЛЯМИ ViPNet ENDPOINT PROTECTION

Возможность централизованного управления, рассылки политик, обновления БРП

МОДУЛЬ ПОВЕДЕНЧЕСКОГО АНАЛИЗА

Используется модель нормальной активности защищаемого узла, построенная с помощью машинного обучения. Выявляются различного рода аномалии:

- аномальный вход в систему
- аномалия в создании процесса
- аномалия в создании задачи планировщику
- аномальные запуски системных утилит
- и д.р.

МОДУЛЬ КОНТРОЛЯ ПРИЛОЖЕНИЙ

Позволяет управлять установкой и запуском приложений на основе настроенных черных и белых списков, а также контролировать доступ приложений к объектам ОС Windows:

- файлам
- реестру
- процессам
- параметрам командной строки

[СЕРТИФИКАЦИЯ ВО ФСТЭК РОССИИ]

В процессе сертификации по требованиям к:

- Системам обнаружения вторжений уровня узла (СОВ У4) – «Профиль защиты систем обнаружения вторжений уровня узла четвертого класса защиты ИТ.СОВ.У4.ПЗ»
- Межсетевым экранам (МЭ 4В) – «Профиль защиты межсетевых экранов типа «В» четвертого класса защиты ИТ.МЭ.В4.ПЗ»
- 4 уровню доверия – «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» утвержденные приказом ФСТЭК России от 30 июля 2018 г. № 131

МОДУЛЬ МЕЖСЕТЕВОГО ЭКРАНИРОВАНИЯ

Осуществляет контроль и фильтрацию входящего и исходящего трафика.

Ключевые возможности:

- Фильтрация трафика IPv4 и IPv6
- Работа сетевых фильтров по расписанию
- Наличие преднастроенных фильтров
- Блокировка атакующих компьютеров
- Контроль сетевой активности программ

МОДУЛЬ ANTIMALWARE

Обнаружение признаков вредоносности в исполняемых файлах с помощью сканирования AntiMalware и блокировка опасных файлов

ОПОВЕЩЕНИЕ АДМИНИСТРАТОРА ИБ О СОБЫТИЯХ БЕЗОПАСНОСТИ

Реализован функционал оповещения администратора ИБ о критических атаках посредством передачи информации в формате CEF по протоколу syslog, а также по электронной почте. При этом все события, атаки отображаются в консоли управления продуктом

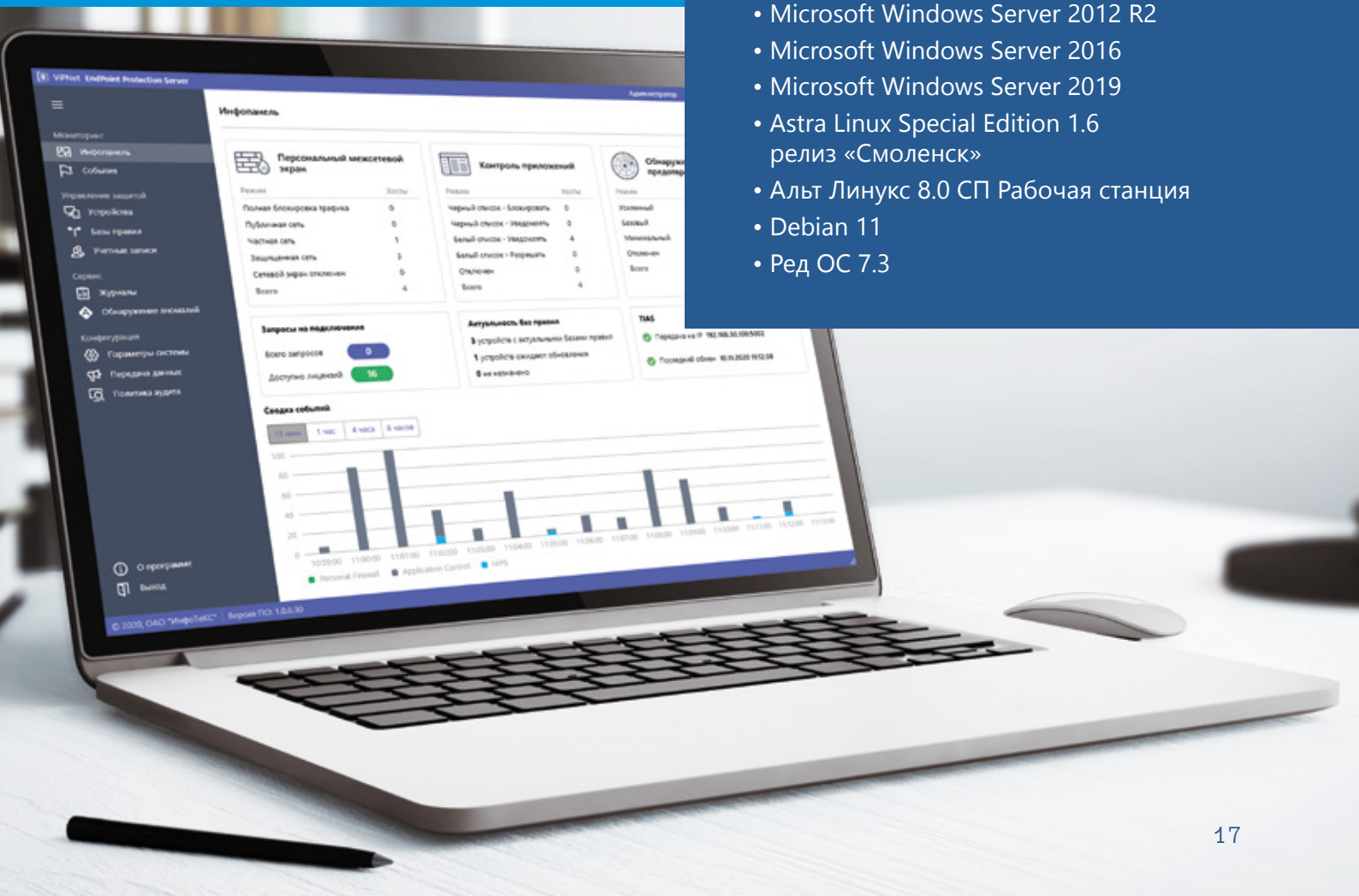
ИНТЕГРАЦИЯ С ViPNet TIAS

Передача событий информационной безопасности от ViPNet EndPoint Protection в аналитическую систему ViPNet TIAS позволяет выявлять сложные и неизвестные атаки при помощи используемых в ViPNet TIAS математической модели и метаправил. При обнаружении инцидента администратор безопасности имеет возможность оперативно отреагировать на атаку в масштабах всех защищаемых хостов сети с использованием модулей ViPNet EPP

РЕГУЛЯРНО ОБНОВЛЯЕМЫЕ БАЗЫ РЕШАЮЩИХ ПРАВИЛ ОТ РОССИЙСКОГО ПРОИЗВОДИТЕЛЯ

Поддерживаемые операционные системы:

- Microsoft Windows 10
- Microsoft Windows 8.1
- Microsoft Windows 11
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- Astra Linux Special Edition 1.6 релиз «Смоленск»
- Альт Линукс 8.0 СП Рабочая станция
- Debian 11
- Ред ОС 7.3

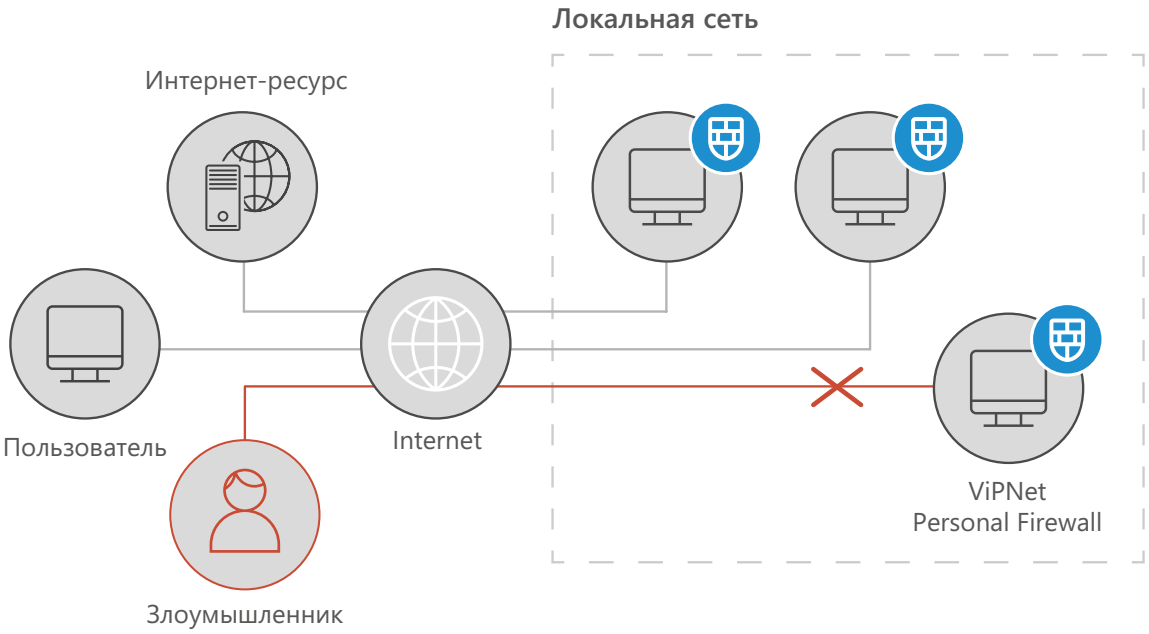


ViPNet Personal Firewall 4.5

ViPNet Personal Firewall – программный сетевой экран, предназначенный для контроля и управления трафиком рабочих мест и серверов пользователей информационных систем

Ключевая задача межсетевого экрана – это фильтрация входящего и исходящего трафика для нейтрализации следующих угроз:

- Несанкционированного доступа к информации, содержащейся на компьютере пользователя
- DoS-атаки
- Несанкционированной передачи информации
- Несанкционированного обращения приложений в сеть



[ВОЗМОЖНОСТИ]

ФИЛЬТРАЦИЯ ТРАФИКА (IPV4 И IPV6)

Для фильтрации можно использовать любую комбинацию IP-адресов или диапазонов IP-адресов (IPv4- и IPv6)

ПРЕДНАСТРОЕННЫЕ СЕТЕВЫЕ ФИЛЬТРЫ

Для удобства работы вы можете выбрать один из следующих преднастроенных фильтров:

- публичная сеть
- частная сеть
- защищенная сеть

КОНТРОЛЬ СЕТЕВОЙ АКТИВНОСТИ ПРИЛОЖЕНИЙ

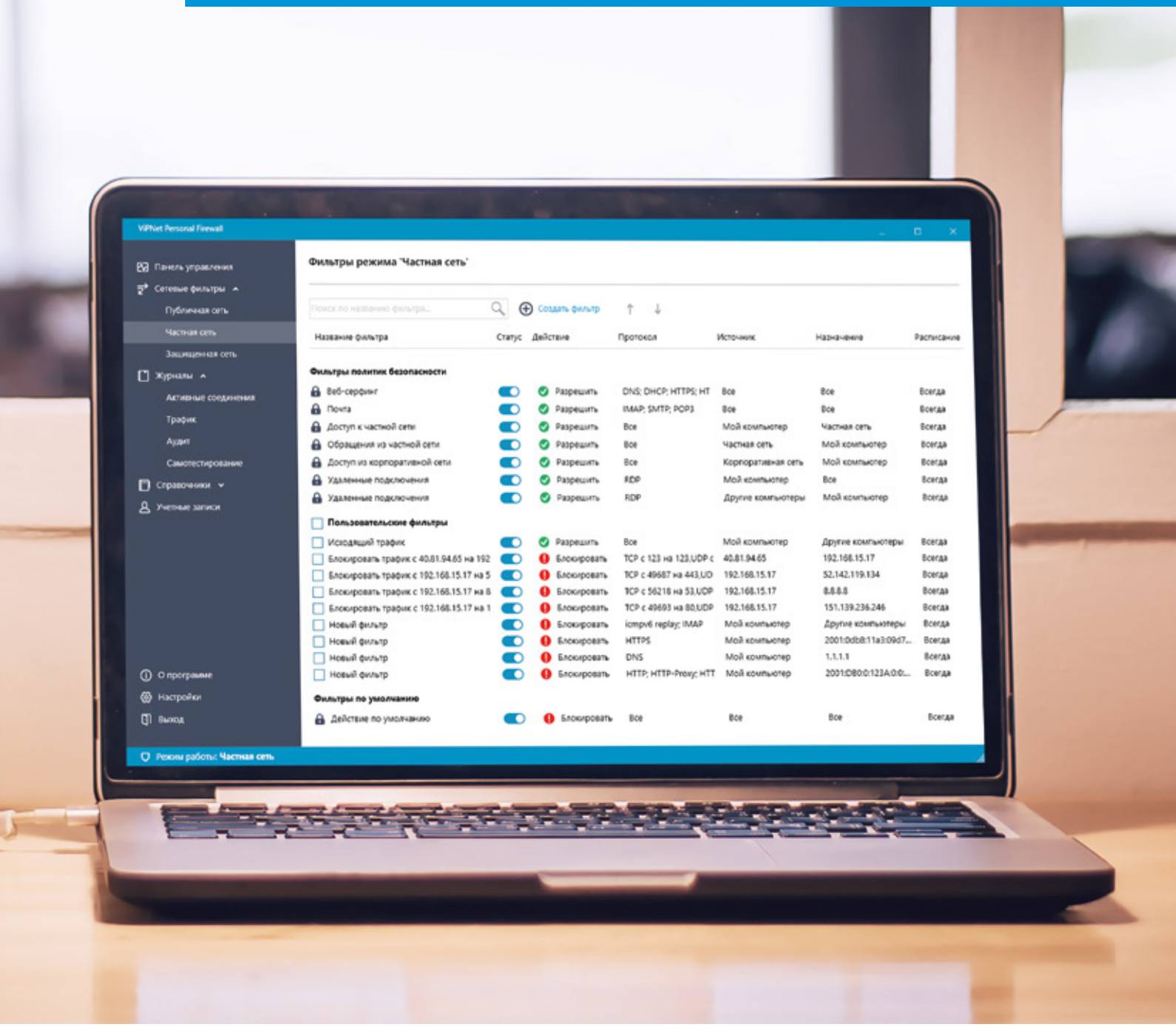
Возможность обнаруживать все активные сетевые соединения на компьютере пользователя, созданные приложениями, с возможностью блокировки как самого приложения, так и отдельно взятого соединения

РАБОТА СЕТЕВЫХ ФИЛЬТРОВ ПО РАСПИСАНИЮ

Реализована возможность применения правил фильтрации по заранее заданному расписанию, позволяющая гибко управлять и ограничивать расходы на оплату каналов связи

Поддерживаемые операционные системы:

- Astra Linux Special Edition 1.6 релиз «Смоленск»
- Альт Линукс 8.0 СП Рабочая станция
- Debian 8.7
- Ред ОС 7.2



infotecs

+7 495 737-61-92
8 800 250-0-260 (бесплатный звонок по России)

soft@infotecs.ru
hotline@infotecs.ru

www.infotecs.ru

EPP22_02RU

ViPNet Virtual Private Network