

# VIPNet Endpoint Security

Решения для защиты рабочих  
станций и серверов



>> Усложнение ландшафта угроз требует комплексного подхода к обеспечению информационной безопасности IT-инфраструктуры как в целом, так и отдельных ее частей. Поэтому построение корпоративной системы информационной безопасности очень часто начинается с обеспечения защиты конечных точек. Современный рынок информационной безопасности трудно представить без средств защиты рабочих станций, которые все чаще выбираются первичными целями атак, приводящих к утечке информации, зашифровыванию критически важных данных, выводу из строя целых сегментов сети, состоящих из сотен компьютеров. Рабочие станции могут быть подвергнуты атакам как на низком программно-аппаратном уровне (UEFI BIOS), так и на уровне операционных систем, причем эти атаки могут быть осуществлены как внутренним нарушителем, так и внешним.

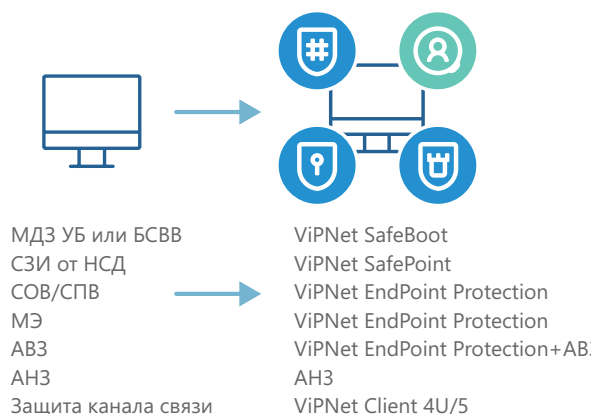
Компания «ИнфоТекС» предлагает необходимый и достаточный набор средств защиты рабочих станций, состав которого зависит от требований и решаемых заказчиками задач:

- > Построение автоматизированных систем по требованиям к ИСПДн, ГИС, АСУ ТП и КИИ
- > Построение систем по требованиям ФСБ России (СКЗИ, АК, подключение и отправка событий в ГосСОПКА)
- > Построение систем с нулевым доверием
- > Защита от продвинутых, бесфайловых и сложных атак
- > Построение защищенного канала между пользователями

### Защита рабочих станций в соответствии с организационными и техническими мерами, прописанными в приказах ФСТЭК России №№ 17, 117, 21, 31, 239

Если внимательно рассмотреть содержание приказов, то можно увидеть, что на долю средств защиты конечных устройств приходится более половины прописанных мер. Эти меры легко можно сопоставить с функциональностью продуктов разного класса:

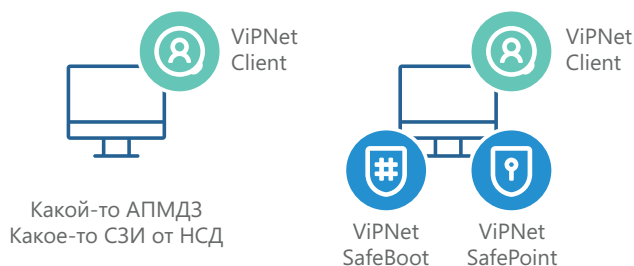
- > Средство доверенной загрузки (СДЗ)
- > Средство защиты информации от несанкционированного доступа (СЗИ от НСД)
- > Система обнаружения вторжений (СОВ)
- > Межсетевой экран (МЭ)
- > Антивирусная защита (АВЗ)
- > Анализа защищенности (АНЗ)
- > Защита канала связи



Защита рабочих станций в соответствии с мерами приказов ФСТЭК России

## Комплексная защита рабочих станций при построении систем СКЗИ

При создании информационных систем, которые используют СКЗИ высоких классов защиты, необходимо обеспечить замкнутость программной среды и доверенную загрузку. Для этого, помимо используемого для защиты информации при ее передаче по открытым каналам связи ViPNet Client, используются дополнительные средства защиты, такие как модули доверенной загрузки и работающее на уровне ОС СЗИ от НСД.



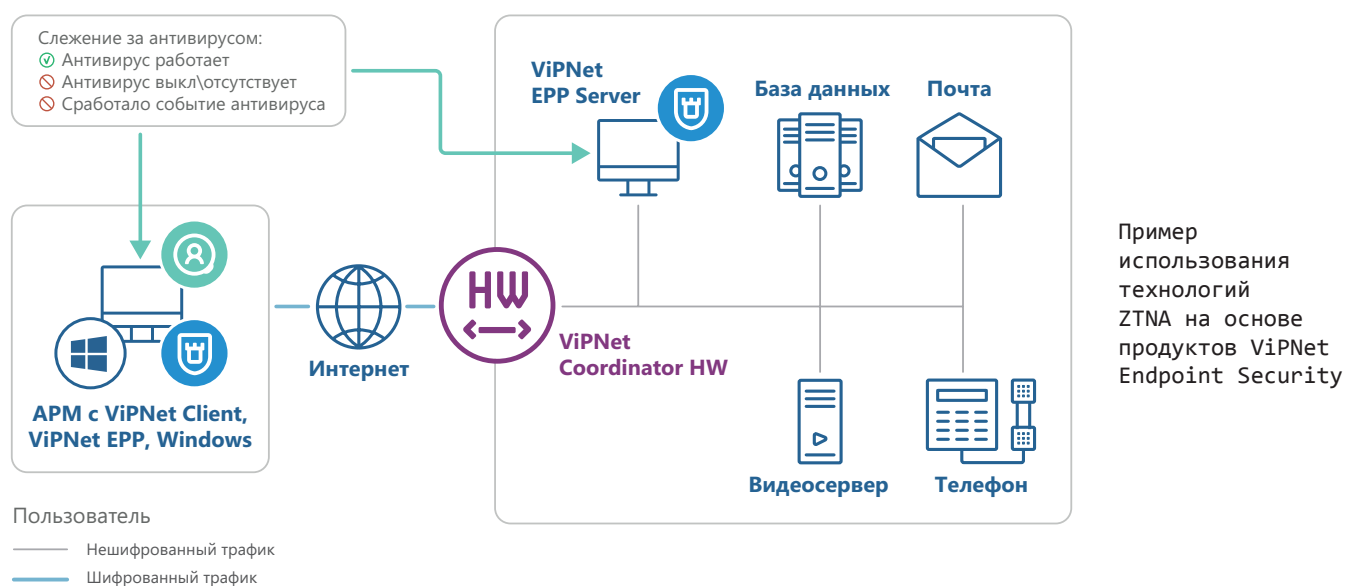
Защита рабочих станций при построении систем СКЗИ

## Построение систем с нулевым доверием (ZTNA)

С развитием информационных технологий, корпоративной мобильности и с переходом на удаленную работу многие заказчики столкнулись с задачей доверия к пользователю. Для решения этой задачи активно используется стек технологий сетевого доступа с нулевым доверием (ZTNA - Zero Trust Network Access).

Продукты линейки Endpoint Security тесно интегрированы и могут использоваться при построении ZTNA для:

- > организации идентификации и аутентификации пользователей (ViPNet SafeBoot и ViPNet SafePoint)
- > мониторинга состояния устройств, средств защиты и выполняемых политик (ViPNet SafePoint и ViPNet EndPoint Protection)
- > создания безопасных политик для пользователей (ViPNet SafePoint)
- > фильтрации трафика (ViPNet EndPoint Protection и ViPNet Client)
- > организации защищенных каналов связи (ViPNet Client)



Компания «ИнфоТекС» активно развивает направление ViPNet Endpoint Security и предлагает полный спектр средств защиты для построения систем по требованиям регуляторов.

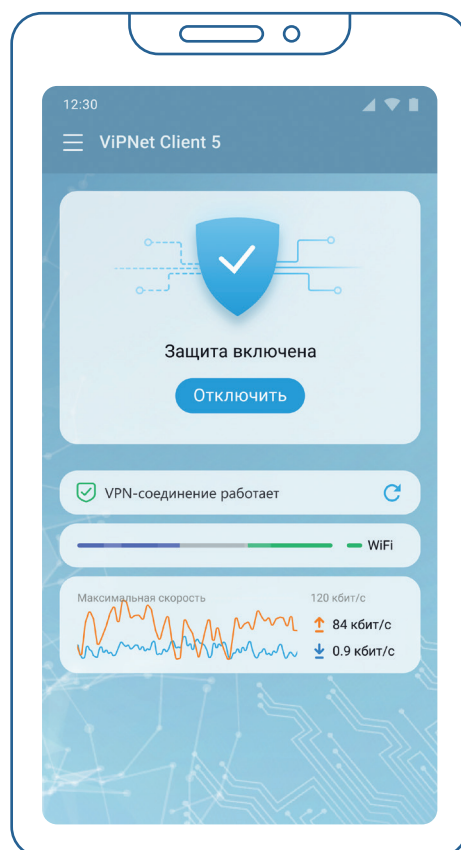


# VIPNet Client

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

## ВОЗМОЖНОСТИ

01. Продукт позволяет обеспечить унифицированный доступ к ресурсам корпоративных информационных систем из любой точки мира с использованием произвольных TCP/IP-сетей.
02. 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.
03. Архитектура продукта позволяет обеспечить одновременную работу с ресурсами различных сегментов корпоративной сети.
04. 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.



## Специальные функции

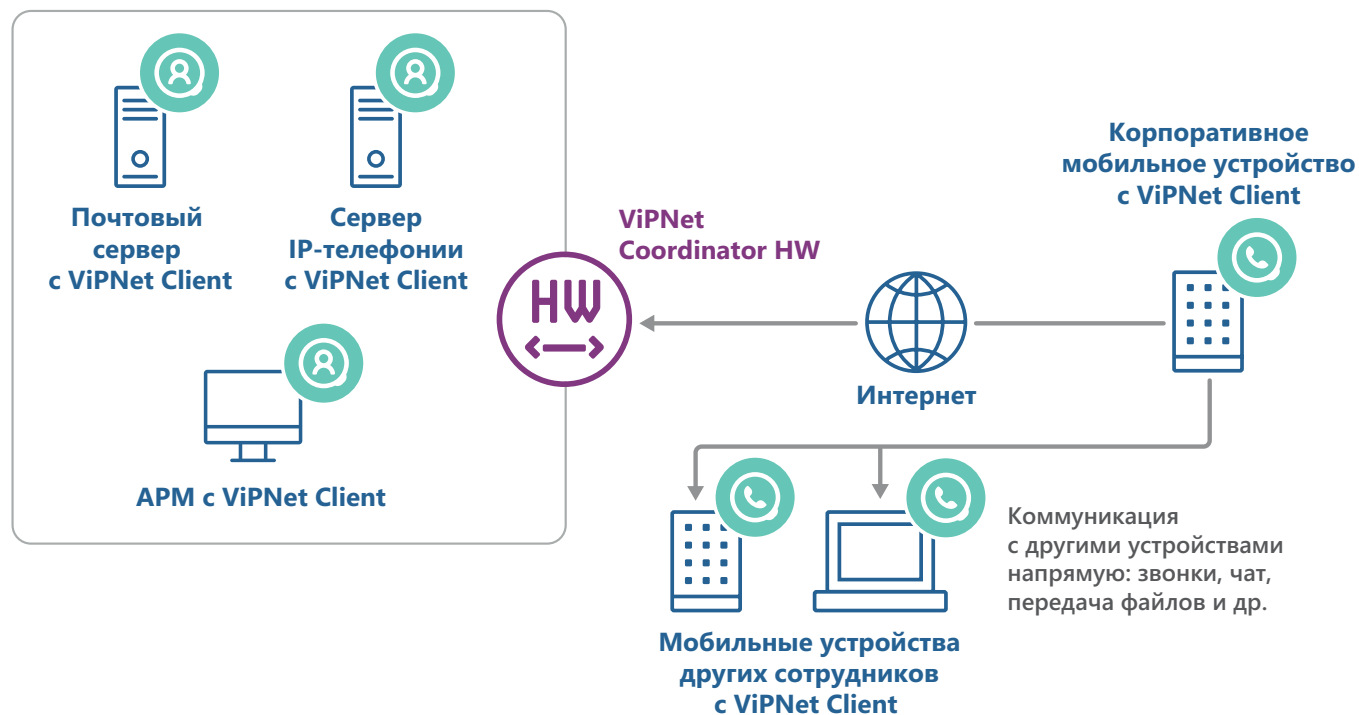
VPN-клиент – шифрование «точка-точка» и имитозащита IP-пакетов с использованием алгоритмов ГОСТ 28147-89, ГОСТ 34.12-2018 и ГОСТ 34.13-2018 на симметричных ключах 256 бит

# СЦЕНАРИИ

01. 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.
02. Дополнительно к сценариям защиты есть возможность использовать на базе существующей защищенной сети ViPNet опциональные средства защищенных коммуникаций, таких как защищенная корпоративная почта (продукт «ViPNet Деловая почта») и защищенный корпоративный мессенджер (продукт «ViPNet CSS Connect»).
03. ViPNet Client поддерживает работу на виртуальных машинах, что позволяет использовать средства защиты ViPNet в VDI-средах.
04. 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.
05. 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

Корпоративная сеть



### Модельный ряд

ViPNet Client для ОС Windows:

> Microsoft Windows 10, 11

ViPNet Client для ОС Linux:

> Любая ОС Linux, содержащая модуль TUN\TAP

ViPNet Client для ОС Android:

> Google Android  
8, 9, 10, 11, 12, 13, 14, 15, 16

ViPNet Client для ОС Аврора:

> Аврора 4, 5

### СЕРТИФИКАЦИЯ

Соответствует требованиям ФСБ России

ViPNet Client

для ОС Windows:

> СКЗИ класса

KC1, KC2 и KC3

> МЭ 4 класса

ViPNet Client

для ОС Linux:

> СКЗИ класса

KC1, KC2 и KC3

ViPNet Client

для ОС Android:

> СКЗИ класса KC1

ViPNet Client

для ОС Аврора:

> СКЗИ класса KC1



# VipNet

# SafeBoot 3

Новое поколение высокотехнологичного программного модуля доверенной загрузки (ПМДЗ), сертифицированного по требованиям ФСБ России и ФСТЭК России. Предназначен для создания точки доверия к платформе и ее компонентам, а также к загружаемой операционной системе. Ключевыми задачами продукта являются разграничение доступа к платформе, защита UEFI BIOS, контроль неизменности и защита компонентов ПК, а также организация доверенной загрузки штатной операционной системы

## ПРЕИМУЩЕСТВА

- |   |   |
|---|---|
| <p>01. Российский продукт, сертифицированный ФСБ России и ФСТЭК России</p> <p>02. Программный МДЗ с возможностью установки в UEFI BIOS различных производителей</p> | <p>03. Защита от Rootkit и Bootkit</p> <p>04. Извлекаемость, в отличие от аппаратных исполнений МДЗ</p> <p>05. Полный контроль целостности UEFI за счет проверки целостности всех его модулей</p> |
|---|---|

## КОНТРОЛЬ ЦЕЛОСТНОСТИ КОМПОНЕНТОВ

Чтобы платформе можно было доверять, нужна гарантия, что все важные модули, загружаемые при старте системы, неизменны, поэтому ViPNet SafeBoot 3 проверяет целостность:

- |  |   |
|--|---|
| <ul style="list-style-type: none"> <li>&gt; всех модулей UEFI BIOS</li> <li>&gt; загрузочных секторов жесткого диска</li> <li>&gt; таблиц ACPI, SMBIOS, карты распределения памяти</li> <li>&gt; реестра Windows</li> <li>&gt; файлов на дисках с системами FAT32, NTFS, EXT2, EXT3, EXT4 (независимо</li> </ul> | <ul style="list-style-type: none"> <li>от того, какая операционная система установлена)</li> <li>&gt; ресурсов конфигурационного пространства PCI/PCIe</li> <li>&gt; CMOS (содержимого энергонезависимой памяти)</li> <li>&gt; завершенности транзакций – NTFS, EXT3, EXT4</li> </ul> |
|--|---|

## РЕШАЕМЫЕ ЗАДАЧИ

**Выполнение требований приказов ФСТЭК России:**

- > №17, 117 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

**Выполнение требований ФСБ России при построении систем с СКЗИ:**

- > Разграничение доступа и защита от НСД
- > Организация доверенной загрузки операционной системы

**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 JaCarta, Rutoken, Guardant, ФОРОС, ESMART Token

### 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

### Возможность установки на ARM-платформы

МДЗ может быть установлен на ARM-платформы архитектуры aarch64 с различными процессорами, при наличии EDK II

### Поддержка аутентификации LDAP/AD

Возможность использовать для аутентификации корпоративную учетную запись из LDAP/AD

### Поддержка SSO

Для входа в операционную систему или ViPNet SafePoint 1.6/1.7/1.8

### Бездисковый режим работы и загрузка ОС по сети

ViPNet SafeBoot может быть установлен на zero-client (бездисковые тонкие клиенты) и осуществлять доверенную загрузку ОС по сети (поддерживаются PXE-Boot и HTTP-Boot)

### Защита от обхода и самотестирование

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

### Возможность удаленного управления из ViPNet EndPoint Protection

Доступны следующие функции: лицензирование продукта и активация, обновление, заведение/редактирование/удаление пользователей, загрузка корневых сертификатов

## КАК УСТАНОВИТЬ?

01. Скачать дистрибутив ViPNet SafeBoot 3 с документацией с сайта
02. Запустить дистрибутив в режиме диагностики для сбора логов (см. Руководство по установке)
03. Отправить в техническую поддержку собранные логи
04. Ждать вердикта:
  - > Установка возможна
  - > Установка возможна, но необходимо дополнительное расширение

## СЕРТИФИКАЦИЯ

ViPNet SafeBoot 3 соответствует следующим требованиям:

- > руководящих документов ФСТЭК России к средствам доверенной загрузки уровня базовой системы ввода-вывода 2 класса
- > ФСБ России к Средствам защиты информации реализующим механизмы доверенной загрузки 2 класса, типа сервиса Б

## ViPNet SafeBoot 3 поставляется в двух исполнениях:

Из-за особенностей сертификации продукта у разных регуляторов исполнения имеют различия в функциональности и применении.

Различия в области применения	Исполнение 1 – сертифицировано в ФСБ России и ФСТЭК России	Исполнение 2 – сертифицировано в ФСТЭК России
Может применяться для защиты ГТ	–	+
Построение АС по требованиям ФСТЭК России к ГИС, ИСПДн, АСУ ТП и КИИ	+	+
Построение систем по требованиям ФСБ России	+	–
<b>Нефункциональные различия</b>		
Возможность установки на ARM-платформы	–	+
<b>Функциональные различия</b>		
Загрузка ОС по сети, включая контроль целостности загружаемой ОС	–	+
Аутентификация на LDAP (AD)	–	+
Инициализация ПДСЧ	Первичная инициализация доступна только с предъявлением диска восстановления	Без предъявления диска восстановления доступна инициализация с использованием клавиатуры (БиоДСЧ)  При наличии диска восстановления инициализация возможна с использованием заранее подготовленной последовательности
Установка произвольного пароля	– (пароль генерируется при помощи ПДСЧ)	+
Удаленное управление из ViPNet EndPoint Protection	–	+





# VIPNet

# SafePoint

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

- |   |   |
|---|---|
| <p>01. 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:</p> <ul style="list-style-type: none"> <li>&gt; исходный идентификатор пользователя SID</li> <li>&gt; эффективный идентификатор пользователя</li> <li>&gt; «полнопутевое» имя процесса (имя исполняемого файла процесса)</li> </ul> | <p>02. Защита от внедрения в процессы (Injection)</p> <p>03. Контроль глобальных хуков</p> <p>04. Контроль обязательно запущенных процессов системы</p> <p>05. Поддержка отечественных ОС Linux с возможностью удаленной установки и обновления через РЕД АДМ сервера или ALD Pro</p> |
|---|---|

- > Возможность работы как в одноранговых сетях, так и в доменных сетях
- > Собственный сервер аудита для решения задач мониторинга событий безопасности
- > Гибкая и масштабируемая система

## РЕШАЕМЫЕ ЗАДАЧИ

- |  |  |
|--|--|
| <ul style="list-style-type: none"> <li>&gt; Защита от внедрения и выполнения вредоносных программ и кода</li> <li>&gt; Защита от атак на повышение привилегий</li> </ul> | <ul style="list-style-type: none"> <li>&gt; Защита данных от атак на уязвимости системного ПО</li> <li>&gt; Защита от инсайдеров</li> <li>&gt; Защита данных от атак на уязвимости прикладного ПО</li> </ul> |
|--|--|

# 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
- > JaCarta ГОСТ
- > Rutoken ЭЦП 3.0
- > Rutoken ЭЦП PKI
- > Rutoken ЭЦП 3.0 NFC

## Замкнутая программная среда

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

## Управление доступом к службам Windows

### 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

## Контроль доступа к печатным устройствам

### Поддержка протокола syslog

Возможность отправлять CEF-сообщения в SIEM-системы по протоколу syslog

## Разграничительная политика на основе матрицы доступа применяется к:

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

## Динамический контроль целостности

Возможность контролировать целостность приложений и используемых ими библиотек

## Шаблоны параметров безопасности

Набор настроек ViPNet SafePoint, параметры которых рекомендуется установить, чтобы информационная система соответствовала необходимому классу, категории значимости или уровню защищенности.

## 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

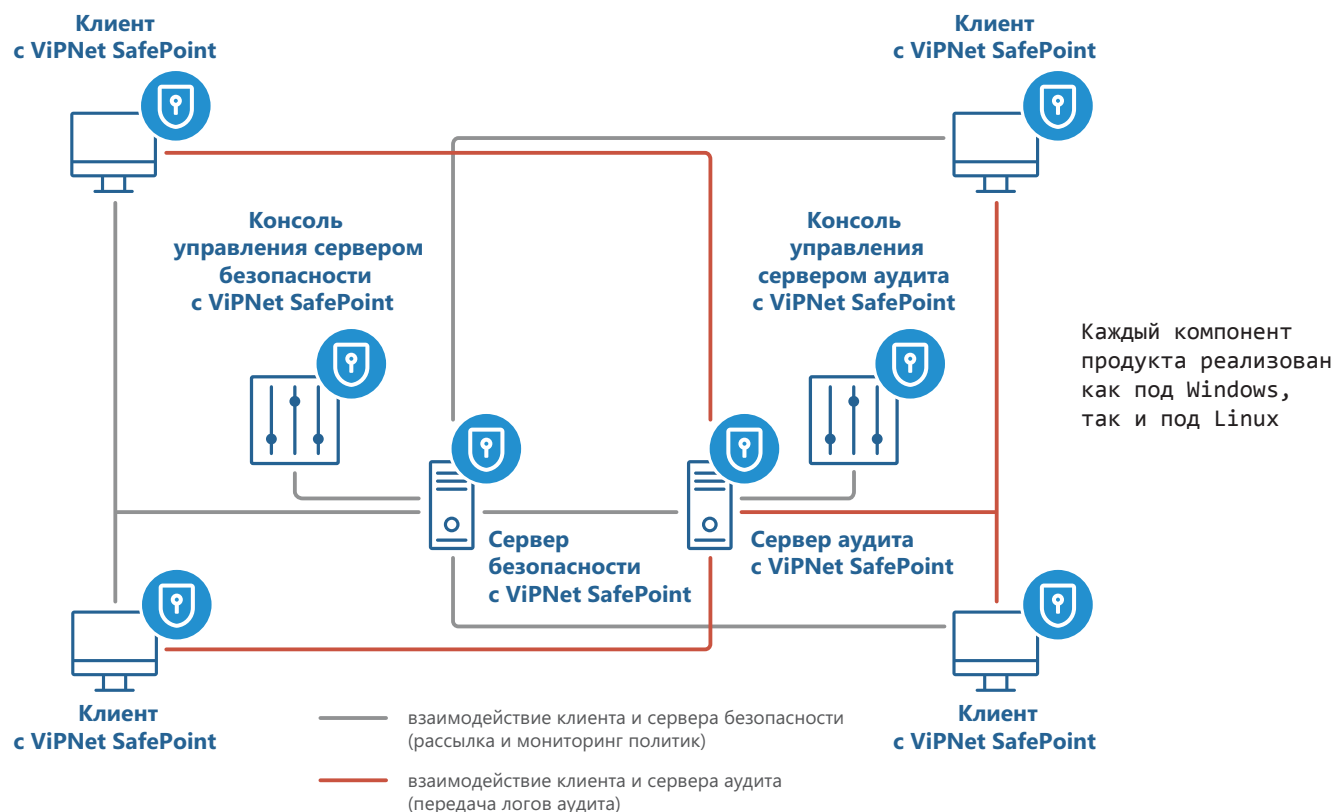
## Контроль операций с буфером обмена

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

## Гарантированное удаление и очистка памяти

Возможность исключить доступ к остаточной информации в обход разграничительной политики

## АРХИТЕКТУРА



### Поддерживаемые операционные системы

- > Microsoft Windows 11
- > Microsoft Windows 10
- > Microsoft Windows Server 2019
- > Microsoft Windows Server 2022
- > Альт Рабочая станция 10.2 и 10.4
- > РЕД ОС 7.3, 7.3.4, 8.0 МУРОМ
- > Astra Linux Special Edition 1.8 «Воронеж» и «Орел»
- > Debian 12

## СЕРТИФИКАЦИЯ

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», утвержденных приказом ФСТЭК России от 30 июля 2018 г. № 131



# VIPNet EndPoint Protection

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

Продукт  
с искусственным  
интеллектом



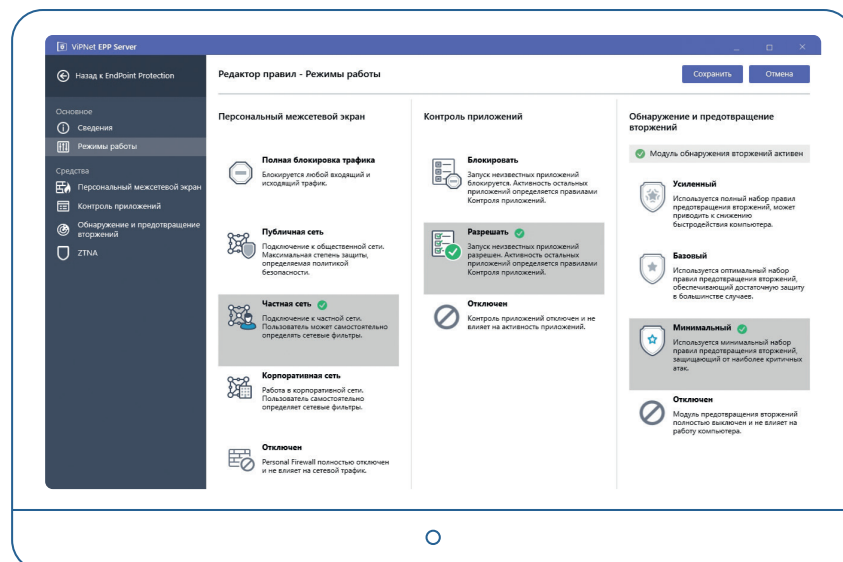
>> ViPNet  
EndPoint  
Protection –  
комплексное  
решение  
безопасности  
рабочих станций  
от внутренних  
и внешних угроз.



## Состав решения

- > проверенные в действии технологии обнаружения вторжений, дополненные настраиваемым модулем предотвращения вторжений
- > модуль межсетевое 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
- > модуль Antimalware – эвристический алгоритм, 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.)

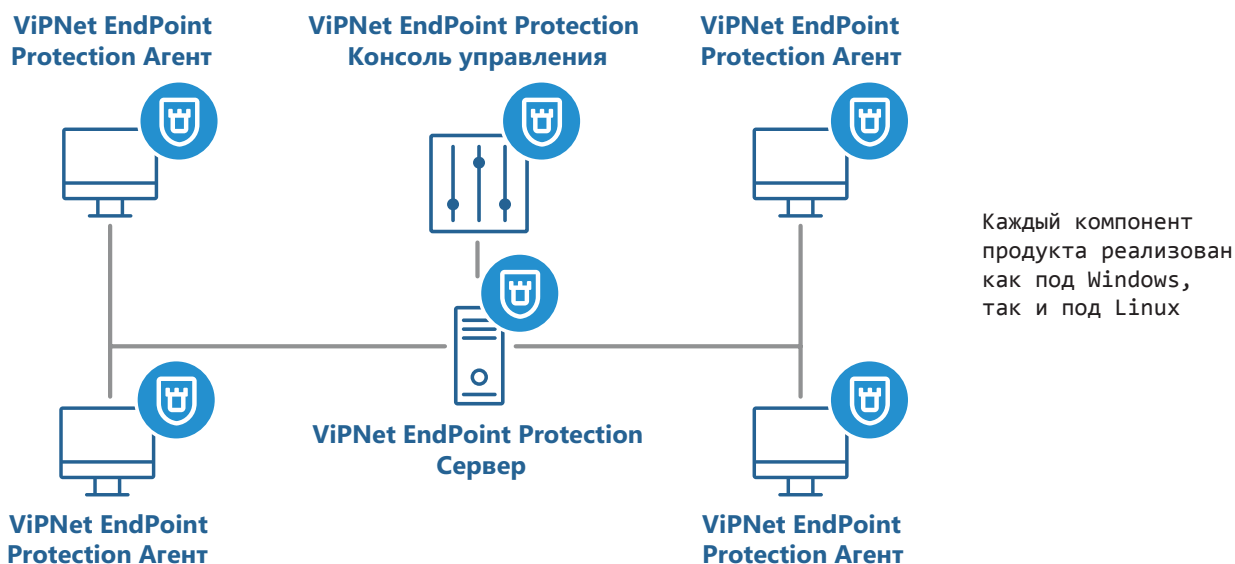
## Возможность выбора режимов работы модулей



# АРХИТЕКТУРА

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

- > 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
- > 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
- > 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, 117, 21, 31 приказов ФСТЭК России

## ВОЗМОЖНОСТИ

### Модуль обнаружения и предотвращения вторжений

Обнаружение атак происходит на основе эвристического и сигнатурного методов. 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

### 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 др.

### 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

### TLS-инспекция и Safebrowsing

Возможность расшифровывания трафика, проходящего через модули ViPNet EndPoint Protection. Осуществляется веб-фильтрация. База «bad URL» поставляется в рамках БРП. Обновляется регулярно.

### Регулярно обновляемые базы решающих правил от российского производителя

### Централизованное управление модулями ViPNet EndPoint Protection

Возможность централизованного управления, рассылки политик, обновления БРП

### Интеграция с ViPNet Client 4U/5

Возможность создания локальных фильтров открытой сети

### Стек технологий ZTNA

- > Проверка соответствия хоста на наличие необходимого/требуемого ПО, обновлений ПО, запущенных процессов, обновление антивирусных баз и т.д.
- > Блокировка входа в защищенную сеть ViPNet при несоответствии устройства политикам ZTNA, информирование пользователя об этом

### 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

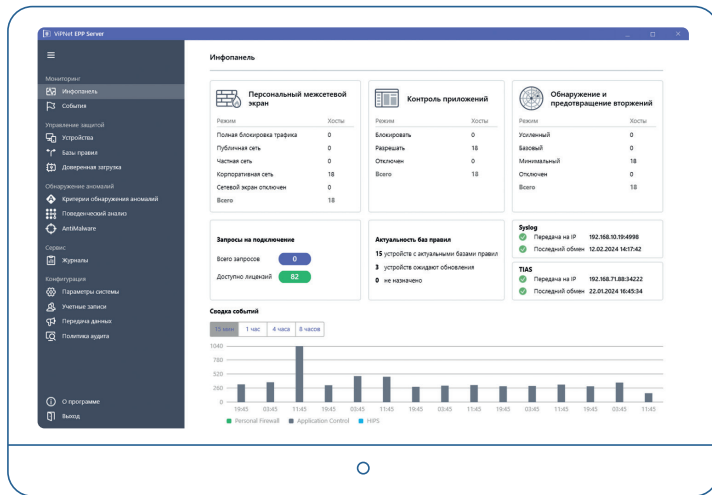
Обнаружение признаков вредоносности в исполняемых файлах с помощью сканирования AntiMalware и блокировка опасных файлов

### 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.

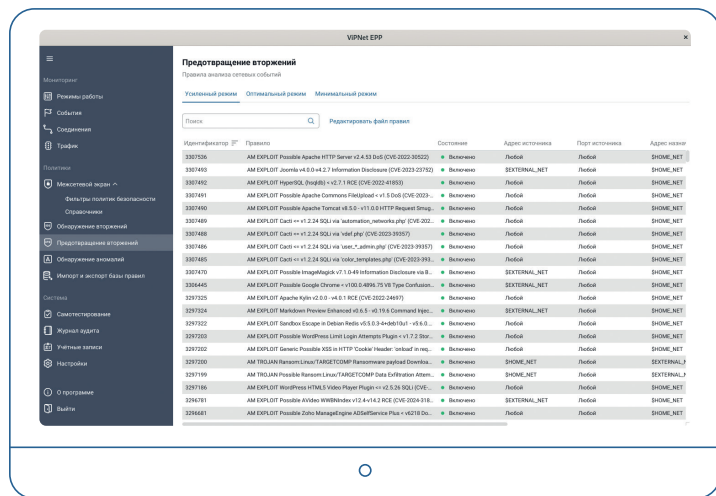


## Поддерживаемые ОС:

- > Microsoft Windows 10
- > Microsoft Windows 11
- > Microsoft Windows Server 2016
- > Microsoft Windows Server 2019
- > Windows Server 2022
- > AlterOS 9.6

## Поддерживаемые ОС:

- > Astra Linux Special Edition 1.7 и 1.8
- > Альт СП Рабочая станция релиз 10
- > Альт Рабочая станция 10.1, 10.2, 10.4
- > РЕД ОС 7.3 «Муром» Рабочая станция
- > РЕД ОС 8.0 «Муром» Рабочая станция
- > Debian 12



## СЕРТИФИКАЦИЯ

Сертифицировано во ФСТЭК России 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



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

soft@infotecs.ru  
hotline@infotecs.ru

www.infotecs.ru



Содержимое документа носит исключительно информационный характер и не является публичной офертой. Для получения подробной информации об указанных в документе продуктах и услугах вы можете обратиться в АО «ИнфоТекс». Все изображения являются лишь иллюстрациями. Все технические характеристики, внешний вид и комплектность описываемой продукции могут меняться без предварительного уведомления. Символы ™ или ® в документе не используются, однако, если не указано иного, все товарные знаки в данном документе защищены соответствующим правом, которое принадлежит их владельцам.