

VIPNet Endpoint Security.

Свежий взгляд на классические
подходы к защите рабочих станций.

Иван Кадыков
Руководитель направления

**Меняется мир
Меняются атаки**

Растущее количество атак и не доверенных аппаратных компонент

Доверие к платформе и обеспечение доверенной загрузки ОС

Разграничение доступа и защита данных

Пользователь - внутренний нарушитель, низкий уровень осведомленности

Удаленная работа, проведение частных разговоров

Обеспечение защищенных коммуникаций

Защита от внешних атак и угроз

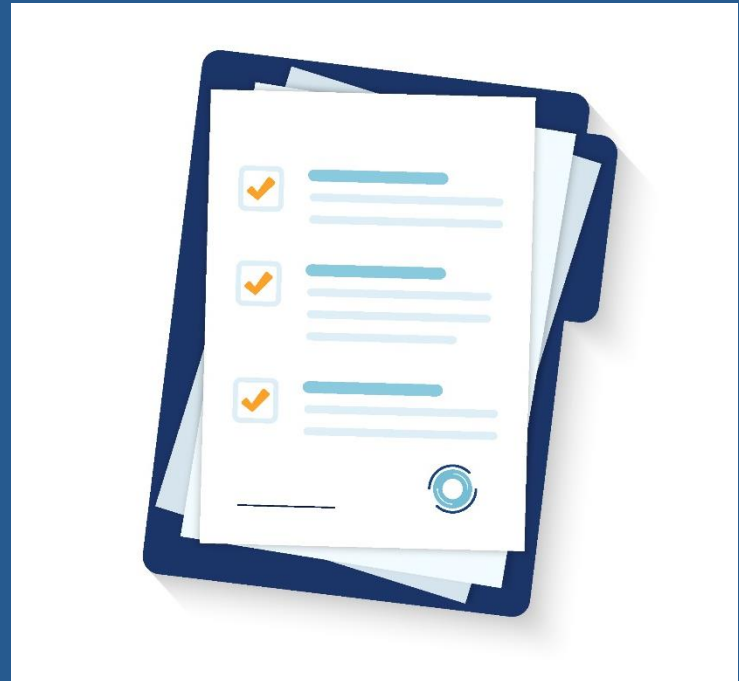
Malware, Ransomware, Fileless & Never-seen-before attacks

Подход к защите рабочих станций от ИнфоТеКС

Первый эшелон защиты

Доверие к платформе и загружаемой операционной системе

- Уверенность в платформе:
 - Неизменность BIOS
 - Аппаратных составляющих
 - Невозможность работы низкоуровневого зловредного обеспечения
- Доступ к платформе должен получить только легитимный пользователь
- Должна загружаться только доверенная операционная система с установленными СЗИ



VIPNet SafeBoot



Высокотехнологичный программный модуль доверенной загрузки, устанавливаемый в UEFI BIOS различных производителей. Предназначен для защиты компьютеров и серверов (в т.ч. и серверов виртуализации) от современных угроз НСД, связанных с загрузкой ОС и атак на сам BIOS.

Организация доверенной загрузки

Контроль целостности

Разграничение доступа

UEFI BIOS

MBR

Таблицы ACPI,
SMBIOS, карты
распределения
памяти

Файлов

CMOS

Двухфакторная
аутентификация

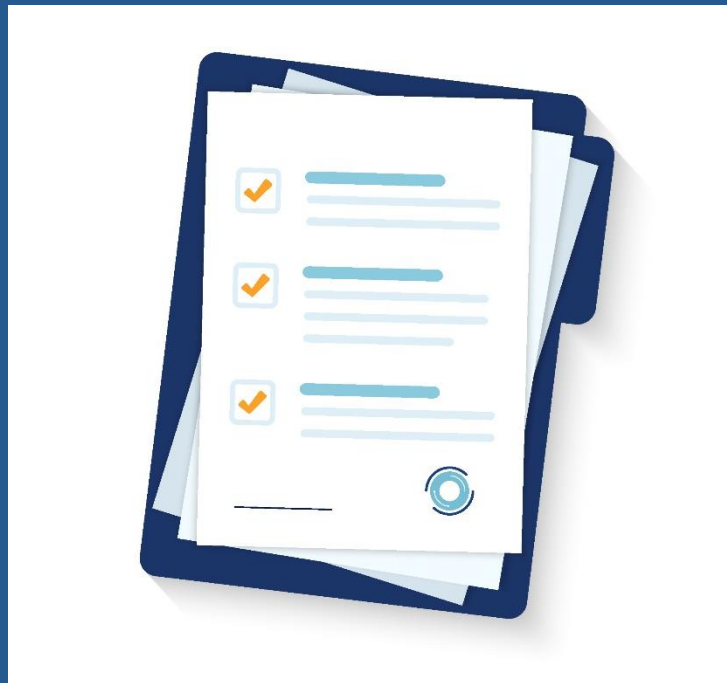
Авторизация
в AD/LDAP

Подход к защите рабочих станций от ИнфоТеКС

Второй эшелон защиты

Доверие к операционной системе и пользователю

- Каждый пользователь должен работать только в созданном информационном пространстве, в соответствии со своей матрицей доступа
- Исключение злонаправленных действий пользователей (хищение данных, с целью передачи третьим лицам)
- Контроль подключения внешних устройств
- Регулярный контроль целостности критически важных объектов ОС





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.

Ключевые решаемые задачи

Идентификация
и аутентификация
пользователей



Дискреционный
контроль доступа
пользователей



Замкнутая
программная
среда



Контроль
подключаемых
устройств



Контроль
целостности
программной среды

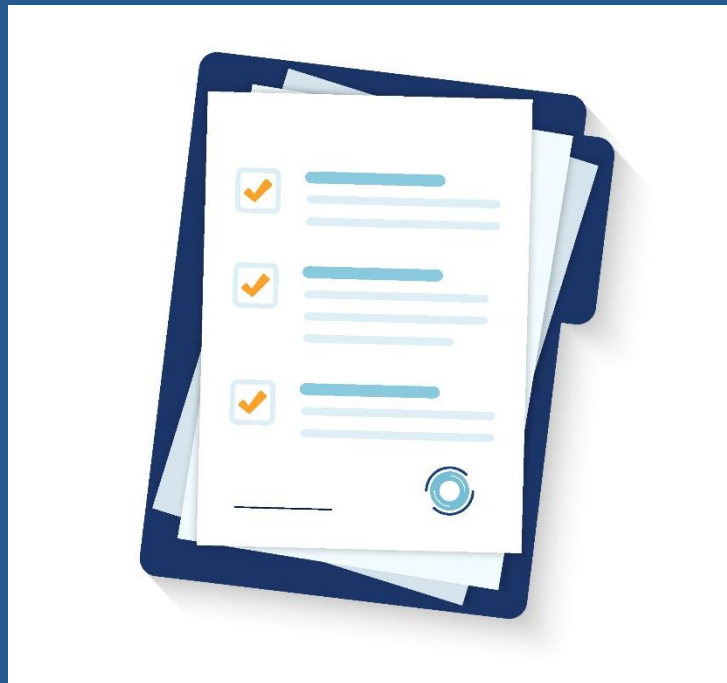


Подход к защите рабочих станций от ИнфоТеКС

Третий эшелон защиты

Защита от внешних нарушителей и угроз

- Мониторинг и противодействие подозрительной активности на хосте
- Защита и предотвращение сетевых атак
- Защита от внедрения и выполнения вредоносных программ и кода
- Защита легитимных процессов

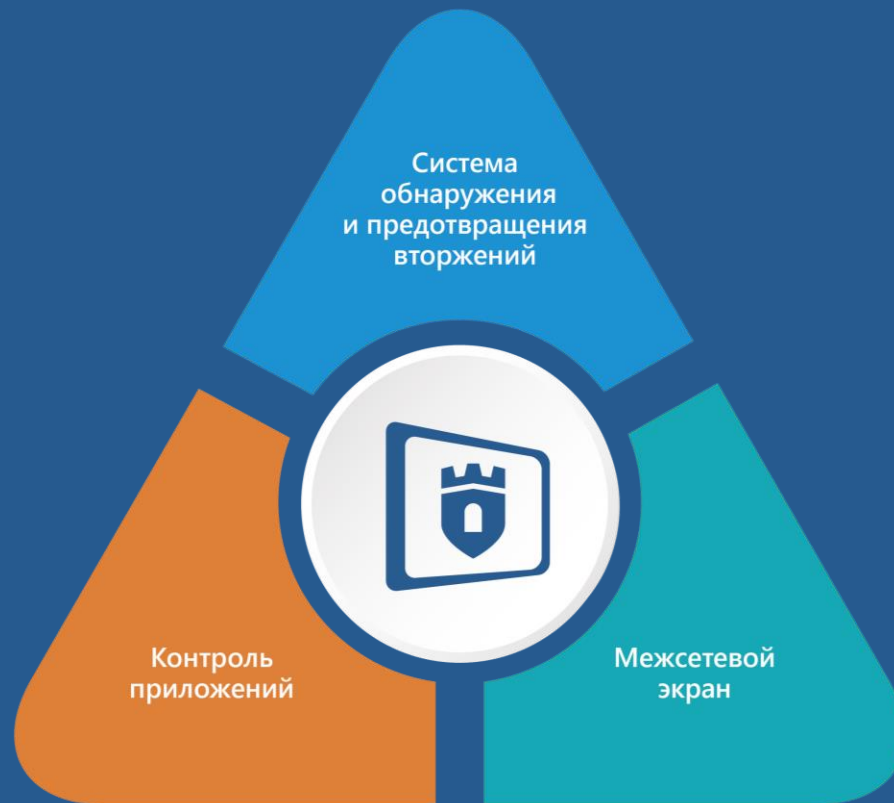


ViPNet EndPoint Protection



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

Модули продукта



Подход к защите рабочих станций от ИнфоТеКС

Четвертый эшелон защиты



Главная

Сетевые узлы

Безопасность



VPN-соединение на устройстве включено

VPN-соединение работает 

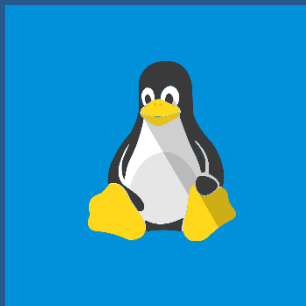
Выключить

VIPNet Client 4U

Новый продукт, выполняющий функции клиента сети VIPNet, созданный с чистого листа, за основу которого взят единый универсальный исходный код

ViPNet Client – защита каналов связи рабочих станций и конечных устройств

КОМПЬЮТЕРЫ
НОУТБУКИ



Встраиваемая
версия
ViPNet Client



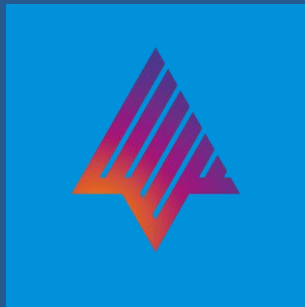
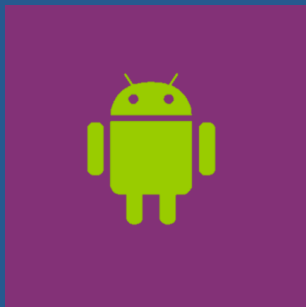
LINUX BASED



MIPS



ТЕЛЕФОНЫ
ПЛАШЕТЫ



КОНТРОЛЛЕРЫ И КОНЕЧНЫЕ
УСТРОЙСТВА АВТОМАТИЗАЦИИ

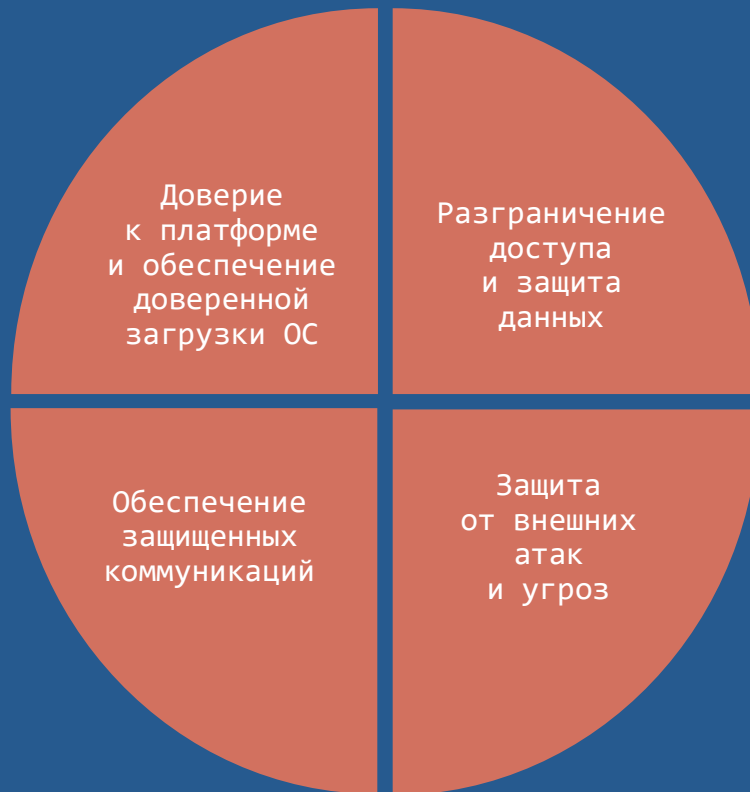
Комплексная защита



ViPNet SafeBoot



ViPNet Client 4U



ViPNet SafePoint



ViPNet EndPoint Protection



Вопросы

Иван Кадыков

e-mail: ivan.kadykov@infotecs.ru

Подписывайтесь на наши соцсети



[@infotecs.ru](https://www.instagram.com/infotecs.ru)



[@vpninfotecs](https://www.facebook.com/vpninfotecs)



[@InfoTeCS_Moscow](https://twitter.com/InfoTeCS_Moscow)



Спасибо за внимание!

Иван Кадыков

e-mail: ivan.kadykov@infotecs.ru

Подписывайтесь на наши соцсети



[@infotecs.ru](https://www.instagram.com/infotecs.ru)



[@vpningotecs](https://www.facebook.com/vpningotecs)



[@InfoTeCS_Moscow](https://twitter.com/InfoTeCS_Moscow)