infotecs

Защита конечных устройств

Эволюция EndPoint

infotecs

1985 первый IBM PC

10.1991 – portable computer PowerBook от Apple

Начало 2000х первые PDA

2005-2015 Мобильные устройства BYOD

2015-по н.в.– Smart Devices, IoT, Inustrial

©2018, ОАО «ИнфоТеКС».

А вот что происходило «вокруг»

infotecs

1985 первый IBM PC

Компьютер – это вещь!

10.1991 – portable computer PowerBook от Apple

Какие-то вирусы начинают мешать жить

Начало 2000х первые PDA

Границы размываются… вирусы…

2005-2015 Мобильные устройства BYOD

Периметра нет! Защищаем каналы! Атаки! Что с узлами?

2015-по н.в.– Smart Devices, IoT, Inustrial

Что вообще происходит!!!

©2018, ОАО «ИнфоТеКС».

А вот что происходит....

...и не все понимают что....

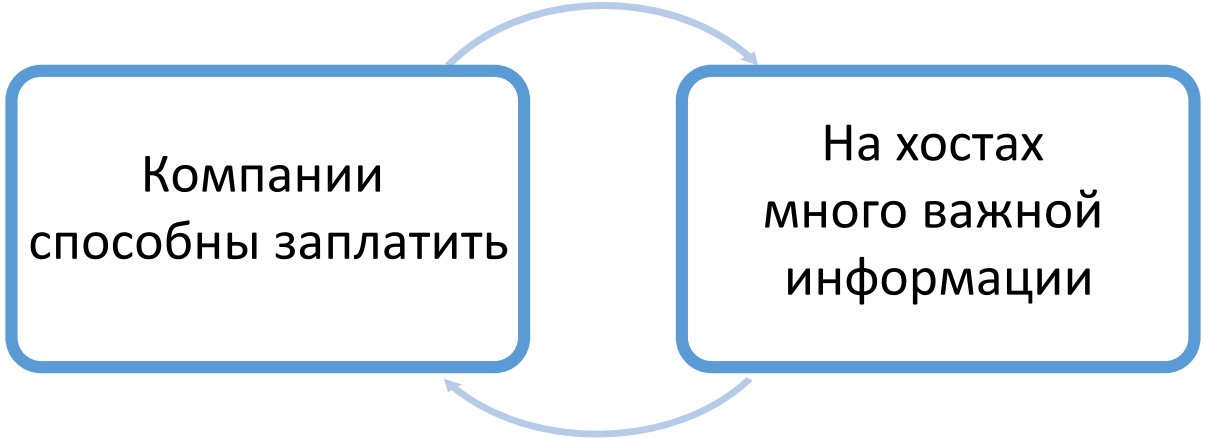
©2018, ОАО «ИнфоТеКС».

«Что в тренде?»

- Программы вымогатели (Locky, Globeimposter, WannaCry)
- Вредоносное ПО
  - Программы крипто-майнеры (Coinhive с сентября 2017)
  - Вредоносное ПО для банков (Zeus – троян под Windows – кейлогер, захват информации из заполняемых форм)
- Вредоносная реклама (RoughTed – реклама которая переадресует пользователей на сайты где происходит загрузка эксплоит-китов, ransomeware, вымогателей и т.д.)
- Уязвимости в системах АСУ ТП

©2018, ОАО «ИнфоТеКС».

Конечные устройства - главная цель



©2018, ОАО «ИнфоТеКС».

Как можно заразить хост?

infotecs

- Атаки на сеть
- Непосредственная атака на рабочие станции
- Внутренний нарушитель

©2018, ОАО «ИнфоТеКС».

Меняются атаки, меняются и методы

infotecs

EndPoint Protection

Сигнатуры – защищаем от того что знаем

EndPoint Detection and Response

Эвристика и аномалии – ищем то чего не знаем

©2018, ОАО «ИнфоТеКС».

Что предлагают на рынке?

©2018, ОАО «ИнфоТеКС».

infotecs

Что предлагаем мы для защиты Endpoint

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.

©2018, ОАО «ИнфоТеКС».

Решаемые задачи ViPNet SafeBoot

infotecs

Организация доверенной загрузки

Контроль целостности

- UEFI BIOS
- MBR
- Таблицы ACPI, SMBIOS, карты распределения памяти
- Файлов
- CMOS

Разграничение доступа

- Двухфакторная аутентификация
- Журнал Аудита

©2018, ОАО «ИнфоТеКС».

Сертифицировано

- Сертифицирован по требованиям руководящих документов к средствам доверенной загрузки уровня базовой системы ввода-вывода **второго** класса и возможность использования в ИСПДн до УЗ1 включительно и в ГИС до 1-го класса защищенности включительно.

- Набор мер прописан в формуляре

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 3823

Выдан 14 ноября 2017 г.
Действителен до 14 ноября 2020 г.

Настоящий сертификат удостоверяет, что **программный комплекс «Программный модуль доверенной загрузки VIPNet SafeBoot»**, разработанный и производимый ОАО «ИнфоТеКС» в соответствии с техническими условиями ФРКЕ.00180-01 97 01 ТУ, является программным средством доверенной загрузки уровня базовой системы ввода-вывода соответствует требованиям документов «Требования к средствам доверенной загрузки» (ФСТЭК России, 2013) и «Профиль защиты средств доверенной загрузки уровня базовой системы ввода-вывода второго класса защиты. ИТ.СДЗ.УБ2.ПЗ» (ФСТЭК России, 2013) при выполнении указаний по эксплуатации, приведенных в формуляре ФРКЕ.00180-01 30 01 ФО.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ООО «ЦБИ» (аттестат аккредитации от 11.04.2016 № СЗИ RU.0001.01БИ00.Б004) - техническое заключение от 28.07.2017, экспертного заключения от 12.10.2017 органа по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002).

Заявитель: ОАО «ИнфоТеКС» (ИНН 7710013769)
Адрес: 127287, г. Москва, Старый Петровско-Разумовский проезд, д. 1/23, стр. 1
Телефон: (495) 737-6192

Контроль маркирования знаками соответствия сертифицированной продукции и инспекционный контроль её соответствия требованиям документов, указанных в настоящем сертификате, осуществляется испытательной лабораторией ООО «ЦБИ».

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В. Лютиков

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации
14 ноября 2017 г.

©2018, ОАО «ИнфоТеКС».

ViPNet Client

infotecs

VPN-клиент для работы в защищенных сетях ViPNet

Персональный сетевой экран

Прозрачность для приложений пользователя и сервисов операционных систем

Независимость от физических каналов связи

Поддержка ОС Windows, Linux, Android, iOS, MacOS, Sailfish

Наличие сертификатов ФСБ на СКЗИ по классам от КС1 до КС3

ViPNet Client for Windows → ViPNet Client for Linux → ViPNet Client for iOS → ViPNet Client for Android → ViPNet Client for MacOS → ViPNet Client for Sailfish

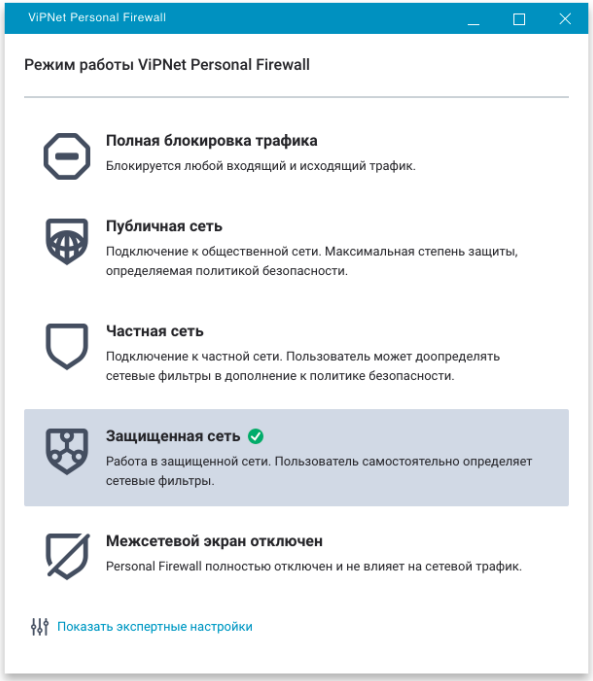
©2018, ОАО «ИнфоТеКС».

ViPNet Personal Firewall 4.5

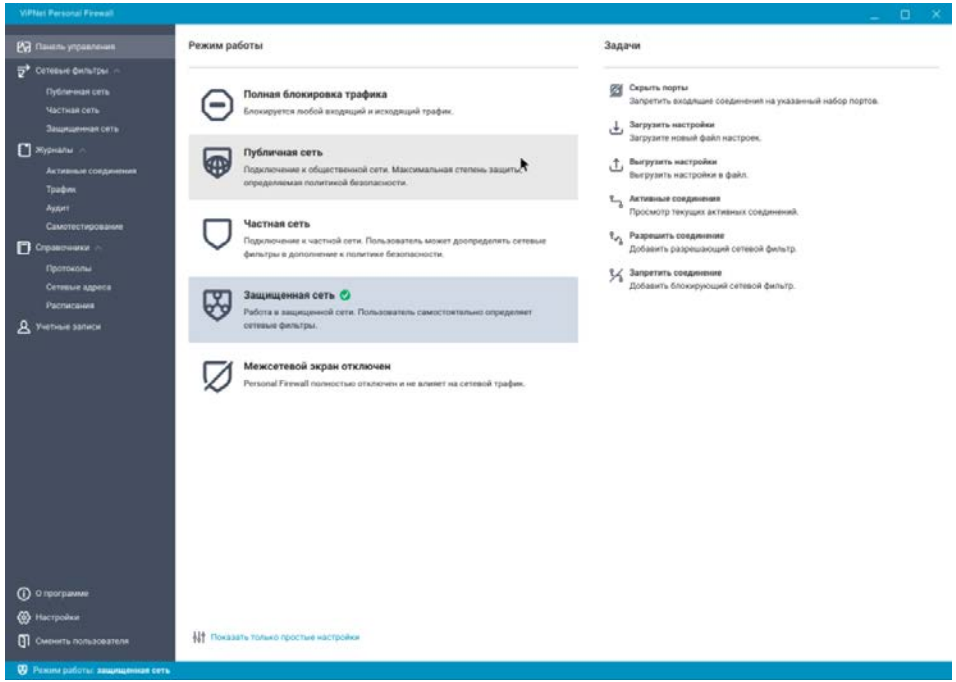
- ViPNet Personal Firewall 4.5 — новый, полностью обновлённый программный межсетевой экран, предназначенный для контроля и управления трафиком рабочих мест и серверов пользователей информационных систем.

©2018, ОАО «ИнфоТеКС».

Внешний вид



Режим пользователя



Режим администратора

©2018, ОАО «ИнфоТеКС».

ViPNet IDS HS

ViPNet IDS HS - система обнаружения вторжений, осуществляющее мониторинг и обработку событий внутри хоста, с применением сигнатурного и эвристического метода анализа атак, используя отечественные правила и сигнатуры .

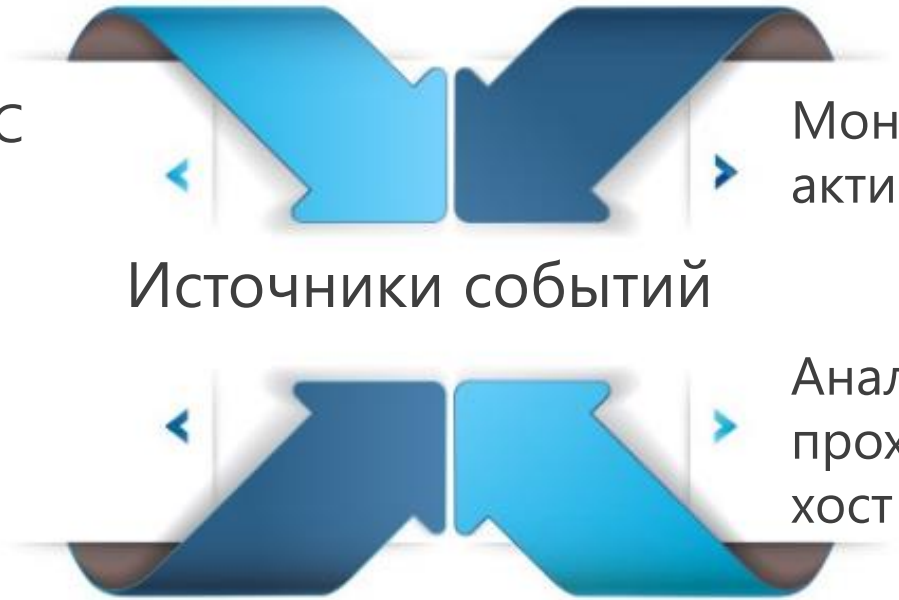
©2018, ОАО «ИнфоТеКС».

Ключевая функциональность

infotecs

Анализ системных журналов и логов ОС и приложений

Мониторинг файловой активности и реестра



Результаты выполнения команд или изменений результатов команд

Анализ трафика проходящего через хост

©2018, ОАО «ИнфоТеКС».

Сертификация

- Сертификат ФСТЭК России по требованиям к системам обнаружения вторжения уровня узла 4 класса.
- Список мер из приказов №21 и №17:
  - ИАФ.1, ИАФ.5
  - УПД.4
  - РСБ.1, РСБ.3, РСБ.4, РСБ.5, РСБ.6, РСБ.7
  - **СОВ.1, СОВ.2**
  - АНЗ.3
  - ОЦЛ.1, ОЦЛ.3
  - ИНЦ.2, ИНЦ.3, ИНЦ.4.

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 3802

Выдан 12 октября 2017 г.
Действителен до 12 октября 2020 г.

Настоящий сертификат удостоверяет, что **система обнаружения вторжений ViPNet IDS HS,** разработанная и производимая ОАО «ИнфоТеКС» в соответствии с техническими условиями ФРКЕ.00177-01 97 01, является системой обнаружения вторжений уровня узла, соответствует требованиям документов «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011) и «Профиль защиты систем обнаружения вторжений уровня узла четвертого класса защиты. ИТ.СОВ.У4.ПЗ» (ФСТЭК России, 2012).

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ООО «ЦБИ» (аттестат аккредитации от 11.04.2016 № СЗИ RU.0001.01БИ00.Б004) - техническое заключение от 23.05.2017, экспертного заключения от 29.08.2017 органа по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002).

Заявитель: ОАО «ИнфоТеКС» (ИНН 7710013769)
Адрес: 127287, г. Москва, Старый Петровско-Разумовский проезд, д. 1/23, стр. 1
Телефон: (495) 737-6192

Контроль маркирования знаками соответствия сертифицированной продукции и инспекционный контроль её соответствия требованиям документов, указанных в настоящем сертификате, осуществляется испытательной лабораторией ООО «ЦБИ».

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В. Лютиков

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации
12 октября 2017 г.

infotecs

Спасибо!