Комплекс продуктов ViPNet для защиты конечных устройств и выполнения мер приказа ФСТЭК России №117

инфотекс

Защита рабочих станций это комплекс мер и задач

При построении автоматизированных систем и подхода к защите рабочих станций всегда решается несколько задач

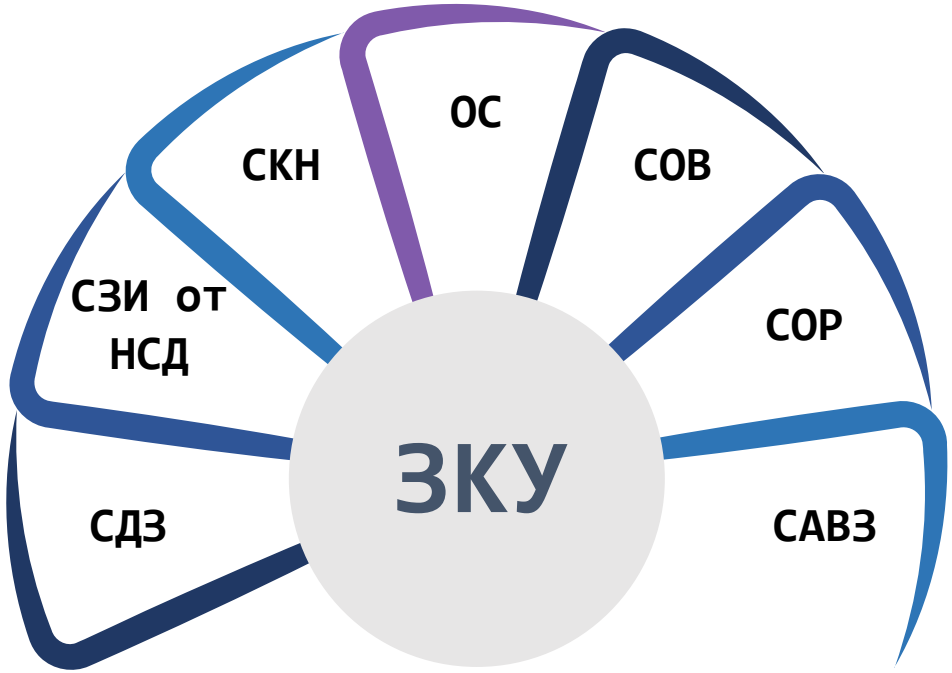
- Построение автоматизированных систем по требованиям к ИСПДн, ГИС, АСУ ТП и КИИ
- Построение систем по требованиям ФСБ России (СКЗИ, АК, подключение и отправка событий в ГосСОПКА)
- Построение систем с нулевым доверием (ZTNA)
- Защита от продвинутых, бесфайловых и сложных атак
- Построение защищенного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

Набор мер 117 приказа

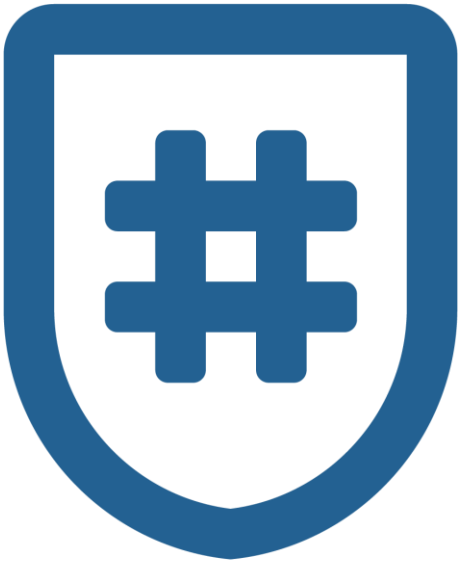
Идентификация и аутентификация	Управление доступом	Защита конечных устройств	Регистрация событий безопасности	Защита каналов связи и сетевого взаимодействия
Обнаружение и предотвращение вторжений на сетевом уровне	Сегментация и межсетевое экранирование	Защита мобильных устройств	Антивирусная защита	Защита виртуализации и облачных технологий
Защита от атак направленных на отказ в обслуживании	Защита технологий контейнерных сред	Защита сервисов электронной почты	Защита веб-технологий	Защита программных интерфейсов взаимодействия приложений (API)
	Защита устройств «интернета вещей»	Защита систем искусственного интеллекта	Защита точек беспроводного доступа	

Защита конечных устройств (ЗКУ)

- ЗКУ.1 - Контроль доступа
- ЗКУ.2 - Контроль целостности
- ЗКУ.3 - Антивирусная защита и обнаружение и предотвращение вторжений на конечных устройствах
- ЗКУ.4 - Мониторинг процессов и состояния устройства
- ЗКУ.5 - Контроль и фильтрация трафика на устройстве
- ЗКУ.6 - Регистрация, анализ и реагирование на события безопасности



ViPNet SafeBoot 3



Новое поколение высокотехнологичного программного модуля доверенной загрузки (ПМДЗ). Предназначен для создания точки доверия к платформе и её 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.

Идентификация и аутентификация

- Варианты идентификации и аутентификации:
  - Логин + пароль
  - Логин + сертификат на токене
  - Логин + сертификат на токене + пароль
  - Логин + PIN на токене
- Возможность идентификации и аутентификации на LDAP/AD
- Реализация SSO с ViPNet SafePoint и операционными системами

Идентификация и аутентификация | Управление доступом | Защита конечных устройств

Контроль целостности программных и аппаратных компонентов

- файлов на диске (на разделах с ФС FAT*, NTFS, ext2/3/4)
- реестра Windows (на уровне ключей/значений)
- CMOS (на уровне регистров)
- конфигурационных пространств PCI
- таблиц ACPI
- структур SMBIOS (DMI)
- карты распределения памяти
- модулей UEFI BIOS
- загрузочных секторов диска (загрузочного)
- переменных NVRAM
- системных таблиц UEFI

Защита конечных устройств

(ЗКУ.2)

Дополнительные функции безопасности

- Защита UEFI BIOS
  - Защиту BIOS от записи и чтения
  - Защита после S3 - защита при выходе из спящего режима
  - Блокировка обновлений UEFI BIOS
  - Фильтрация и контроль программных SMI
- Защита от malware
  - Блокировка ACPI WPBT
  - Защита дисков от записи
  - Блокировка UEFI Option Rom
- Эмуляция NVRAM (защита от записи и чтения EFI-переменных)

ViPNet SafePoint

ViPNet SafePoint –

сертифицированный программный комплекс защиты информации от несанкционированного доступа уровня ядра операционной системы (ОС)

ViPNet SafePoint –

устанавливается на рабочие станции и сервера в целях обеспечения мандатного и дискреционного разграничения доступа пользователей к критически важной информации и подключаемым устройствам

Ключевой набор функциональности для СЗИ от НСД

- Идентификация и аутентификация пользователей
- Дискреционная модель доступа (контроль доступа к файлам, реестру, процессам, службам)
- Замкнутая программная среда
- Контроль целостности
- Контроль времени работы
- Контроль подключения съемныхносителей
- Мандатный контроль доступа

Идентификация и аутентификация

Управление доступом

Защита конечных устройств

Регистрация событий безопасности

Всё под контролем

- Контроль целостности и восстановление
  - Файлов
  - Объектов реестра ОС
- Контроль запуска разрешенных/запрещенных процессов
- Контроль активности обязательных процессов
- Контроль доступа к альтернативным потокам
- Контроль доступа к атрибутам файлов

Защита конечных устройств (ЗКУ.2)

Контроль подключения съемных носителей

Возможность использования только определённых (зарегистрированных) съемных устройств

Контроль копирования информации на съёмные носители (фиксация событий в журнале аудита)

Защита от запуска программ и скриптов с внешних накопителей

Идентификация и аутентификация

Регистрация событий безопасности

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

Обнаружение и предотвращение вторжений

Непрерывная работа на уровне:

- Операционной системы
- Сети

Дополнительные механизмы:

- Обнаружение аномалий с помощью критериев
- Обнаружение аномалий с помощью поведенческого анализа

Защита конечных устройств (ЗКУ.3)

Регистрация событий безопасности

Дополнительное в модуле системы обнаружения и предотвращения вторжений

TLS – инспекция

возможность расшифровывания трафика проходящего через модули ViPNet EndPoint Protection. База «bad URL» поставляется в рамках БРП, обновляется регулярно

SafeBrowsing

безопасный сёрфинг в интернете (веб-фильтрация)

Межсетевой экран

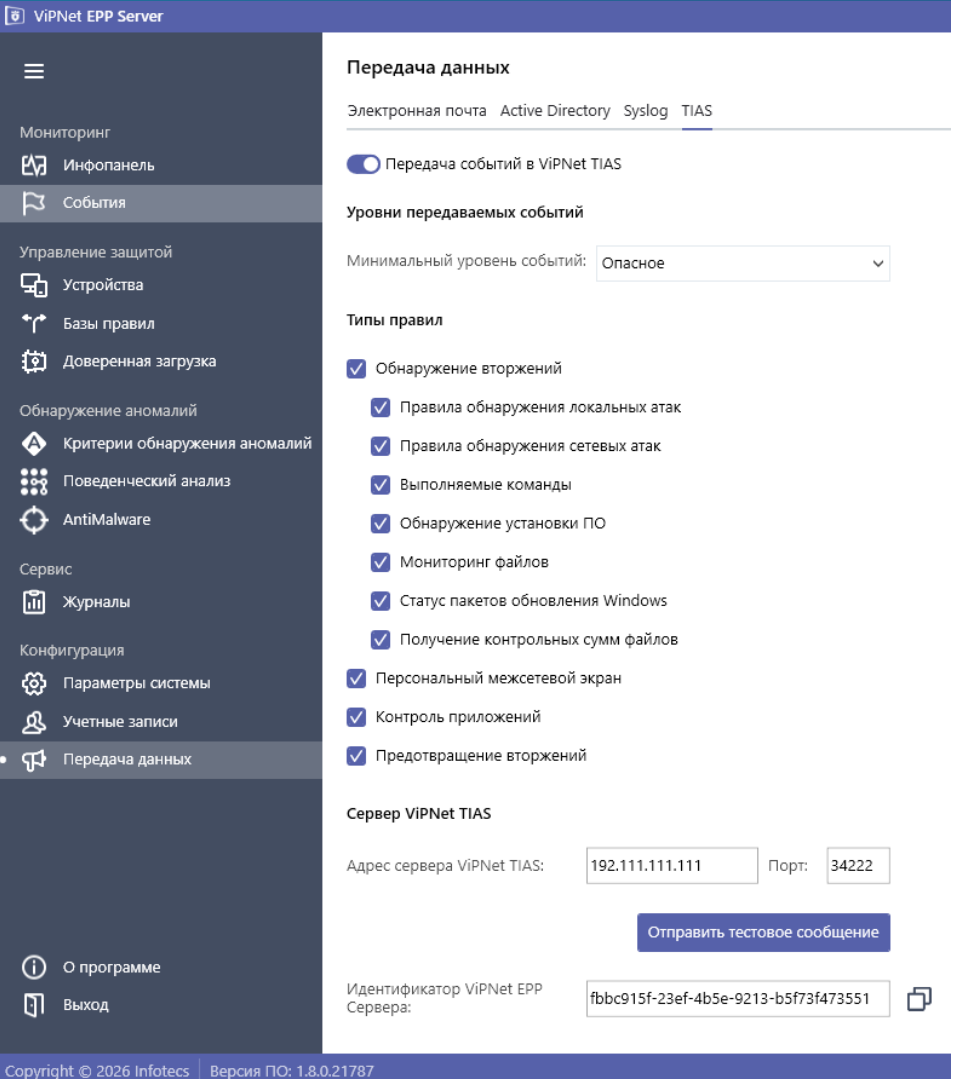
- Фильтрация трафика Ipv4 и Ipv6
- Интеграция с ViPNet Client 4U/5

Добавление\Редактирование\Удаление фильтров защищённой сети из локальной консоли ViPNet EndPoint Protection (агент)

Защита конечных устройств (ЗКУ.5)

Контроль приложений

- Контроль запуска программ с использованием Черных и Белых списков программного обеспечения
- Анализ командной строки
- Защита файлов
- Защита реестра
- Контроль запуска программ, DLL-модулей, драйверов
- Контроль сетевой активности приложений



Передача событий

Все события могут передаваться в:

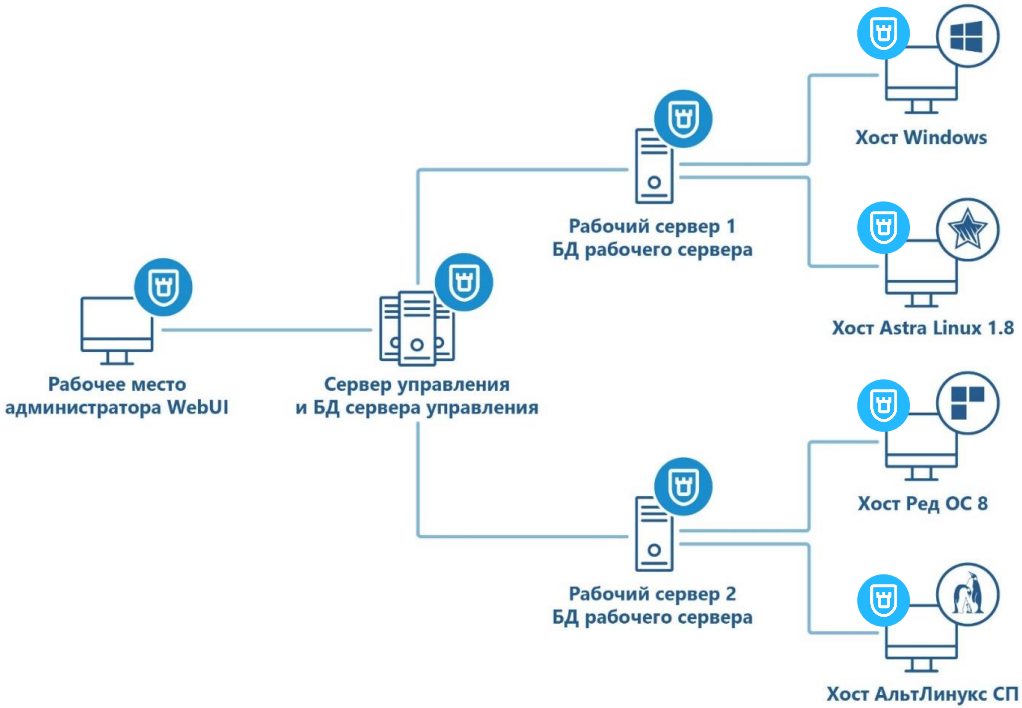
- ViPNet TIAS
- В любую SIEM

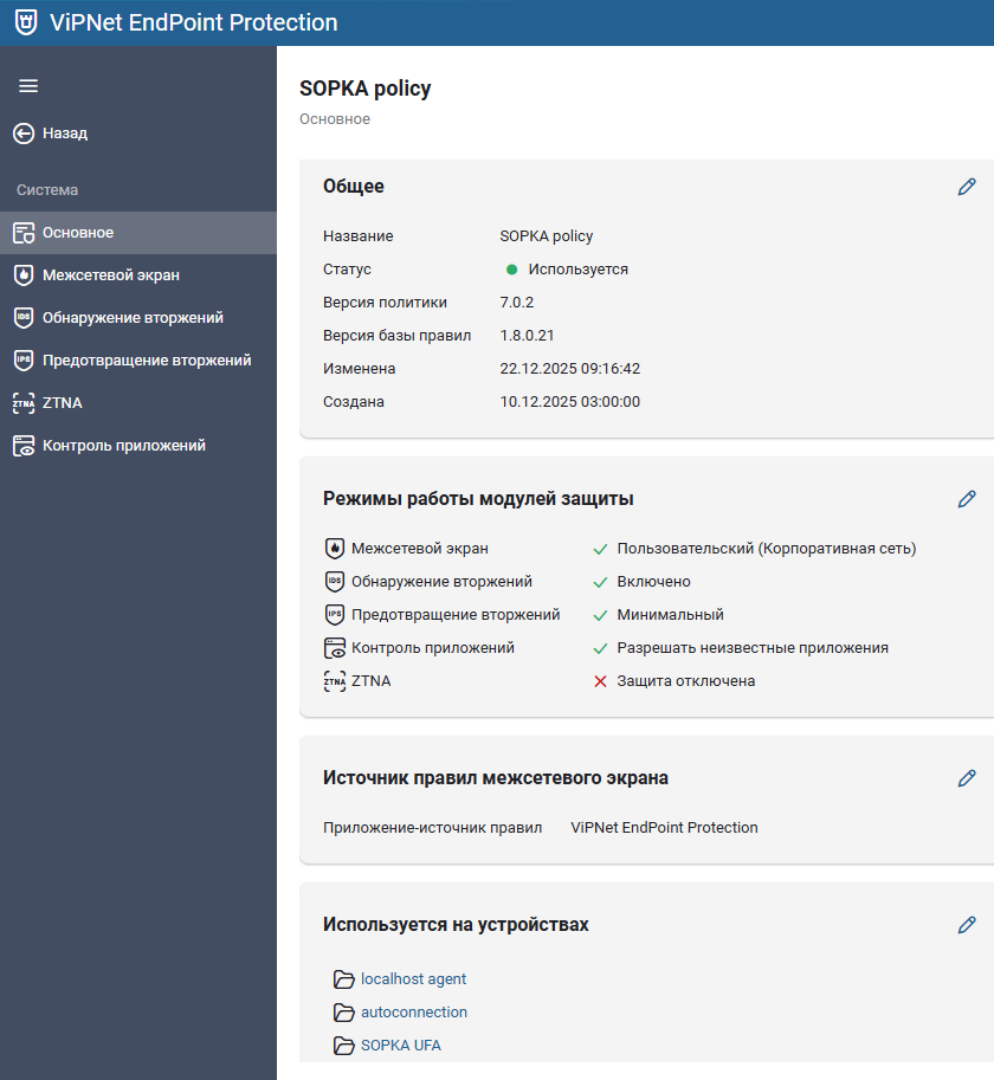
Регистрация событий безопасности

Новое в EPP версии 1.8

- Доработка сервера ViPNet EPP под *NIX:
  - Возможность работы с БРП
  - Переход на управление через WebUI
  - Изменение архитектуры для возможности масштабирования продукта в крупных сетях
  - Управление и win-агентами и lin-агентами

Архитектура Linux-сервера EPP





Работа с БРП через WebUI

Подписывайтесь
на наши соцсети,
там много интересного

инфотекс