

С чего начинается...



Построение корпоративной системы информационной безопасности чаще всего начинается с обеспечения защиты рабочих станций



Рабочие станции – первичные и основные цели атак

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



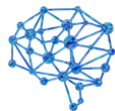
Защита от продвинутых, бесфайловых и сложных атак



Построение защищенного канала между пользователями



Построение систем по требованиям ФСБ России (СКЗИ, АК, подключение и отправка событий в ГосСОПКА)



Построение систем с нулевым доверием (ZTNA)

Потенциальный внутренний нарушитель



«Классические» внутренние нарушители (инсайдеры)

сотрудники, которые злоупотребляют своим законным доступом к конфиденциальным данным в корыстных целях



Подкупленный сотрудник

нанятый внешними компаниями для кражи, изменения или удаления конфиденциальных данных



Недовольные бывшие сотрудники

которые хотят навредить своим работодателям



Безрассудные сотрудники

тип инсайдеров, которые пренебрегают ИБ-политиками

Потенциальный внешний нарушитель



Конкуренты / промышленный шпионаж

«лица», желающие получить дополнительную информацию или навредить конкурирующему бизнесу



Недобросовестные поставщики / партнёры

лица осуществляющие злонамеренные действия в процессе поставки IT-продуктов/средств (атака на цепочку поставок)



Хакер «бизнесмен»

лицо или группа лиц, осуществляющие атаки с целью обогащения – получение денег от внешних заказчиков или напрямую от жертв



Службы (официальные и теневые) недружественных государств

тип злоумышленников, наносящих вред критически важным объектам(компаниям) для дестабилизации

От чего защищаемся?



Что и как использовать для защиты рабочих станций и серверов?

Рецензент от ИнфоТеКС



Наш рецепт безопасности хостов



ViPNet SafeBoot 3

Решаемые задачи - Доверие к платформе
и организация доверенной загрузки



Сертификаты ФСТЭК России
и ФСБ России



ViPNet SafePoint

Решаемые задачи - Доверие к пользователю
и организация замкнутой программной среды



Сертификат
ФСТЭК России



ViPNet EndPoint Protection

Решаемые задачи - Защита от внешних нарушителей
и обнаружение зловредной активности на хостах



Сертификат
ФСТЭК России



Доверенная загрузка – первый и ключевой шаг к защите рабочих станций и серверов

Все средства защиты установленные
в ОС бессильны если:

- Любой пользователь может включить компьютер
- Получить доступ к UEFI BIOS
- Загрузить любую ОС с внешнего носителя

«Классика» доверенной загрузки



**Идентификация
и Аутентификация
пользователей**



**Контроль
целостности
программной и
аппаратной среды**



**Передача
управления
доверенному
загрузчику ОС**

Вопрос: есть ли уверенность, что компьютер пришёл «ЧИСТЫМ»?

- Как обнаружить?
- Как не допустить попадания зловреда?
- А что может такой зловред?

ViPNet SafeBoot 3

Обнаружит и нейтрализует



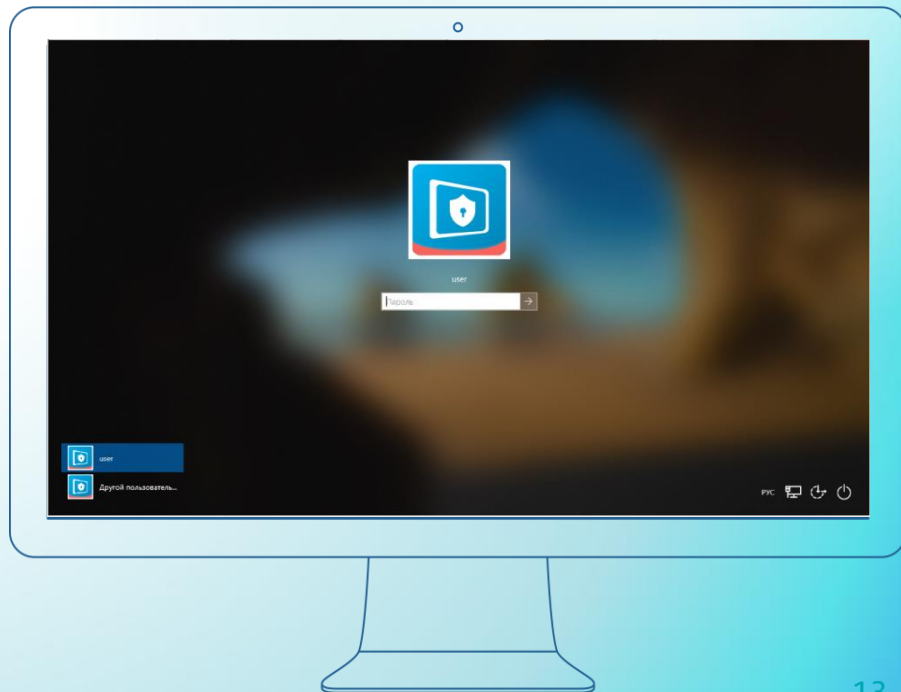
Финальный этап доверенной загрузки

ViPNet SafeBoot 3 передаёт управление загрузчику операционной системы (не используя SecureBoot)

Операционная система должна быть:

- Сертифицированной
- Несертифицированной, с наложенными СЗИ от НСД

Для удобства использования есть механизм SSO – передача аутентификационных данных в ОС или ViPNet SafePoint





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 съемных носителей
- Мандатный контроль доступа



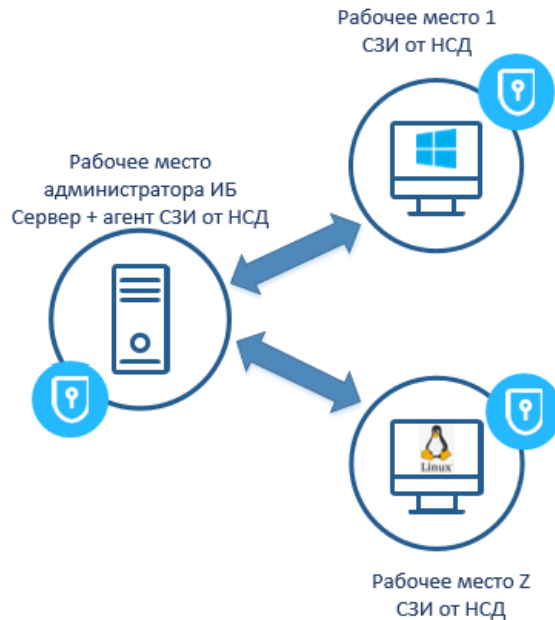
Управление привилегированными пользователями

В СЗИ от НСД – реализована защита и контроль непосредственно на хостах.

Субъекта доступа формируется из трёх сущностей

- исходный идентификатор пользователя SID
- эффективный идентификатор пользователя (контекст безопасности (маркер-token) процесса при доступе)
- «полнопутевое» имя процесса (имя исполняемого файла процесса)

**PIM/PAM/PUM – контролируют подключение привилегированными пользователями к целевым системам и их работу только в соответствующих сессиях*



Защита от появления и исполнения зловредных программ

За счёт функции «Контроль доступа к файлам» можно создать политику:

- Файлы с расширением *.exe, *.bat, *.js и т.д. может создавать только администратор

За счёт функции «Контроль доступа к объектам реестра» можно создать политику:

- Доступ к настройке служб в реестре ОС разрешен только администратору
(HKLM\SYSTEM*ControlSet*\services*)

ViPNet SafePoint предотвращает такие попытки для пользователя с фиксацией информации в журнале аудита



Защита от действий «неопытного» пользователя

Запрет запуск приложений, скриптов из писем (защита от фишинговых атак по почте). Переход по нежелательным ссылкам

Как реализовать:

- запрет запуска, приложений из почтового клиента Outlook (кроме, например, Word, Excel, Acrobat Reader). Дополнительно политика на запрет запуска приложений, скриптов из Word, Excel, Reader.
- Запуск файла из почты порождает процесс, этому процессу запрещено обращаться к ранее созданным размеченным файлам.



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



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

СЗИ от НСД «прародитель» EDR?

Да

HeT



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.

ViPNet EndPoint Protection – комбинирование методов защиты



- Сигнатурные методы защиты:
 - правила белого/чёрного списка
 - правила для HIDS/HIPS
 - фильтры межсетевого экрана
- Эвристические методы защиты:
 - Поведенческий анализ
 - Эвристический антивирус (NGAV - бессигнатурный)
 - Математические модели построенные при помощи искусственного интеллекта
- Средства мониторинга и передача событий для последующего анализа

Обнаружение и предотвращение вторжений

Непрерывная работа на уровне:

- Операционной системы
- Сети

Дополнительные механизмы:

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



Модуль поведенческого анализа

Используем модель нормальной активности защищаемого узла, построенной с помощью машинного обучения.

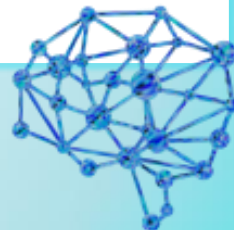
Выявляем различного рода аномалии, например:

Аномальный вход в систему

Аномалия в создании процесса

Аномальные запуски системных утилит, таких как powershell, rundll32, regsrv32 и т.д.

Аномалия в создании задачи планировщику



Дополнительное в модуле системы обнаружения и предотвращения вторжений

TLS – инспекция

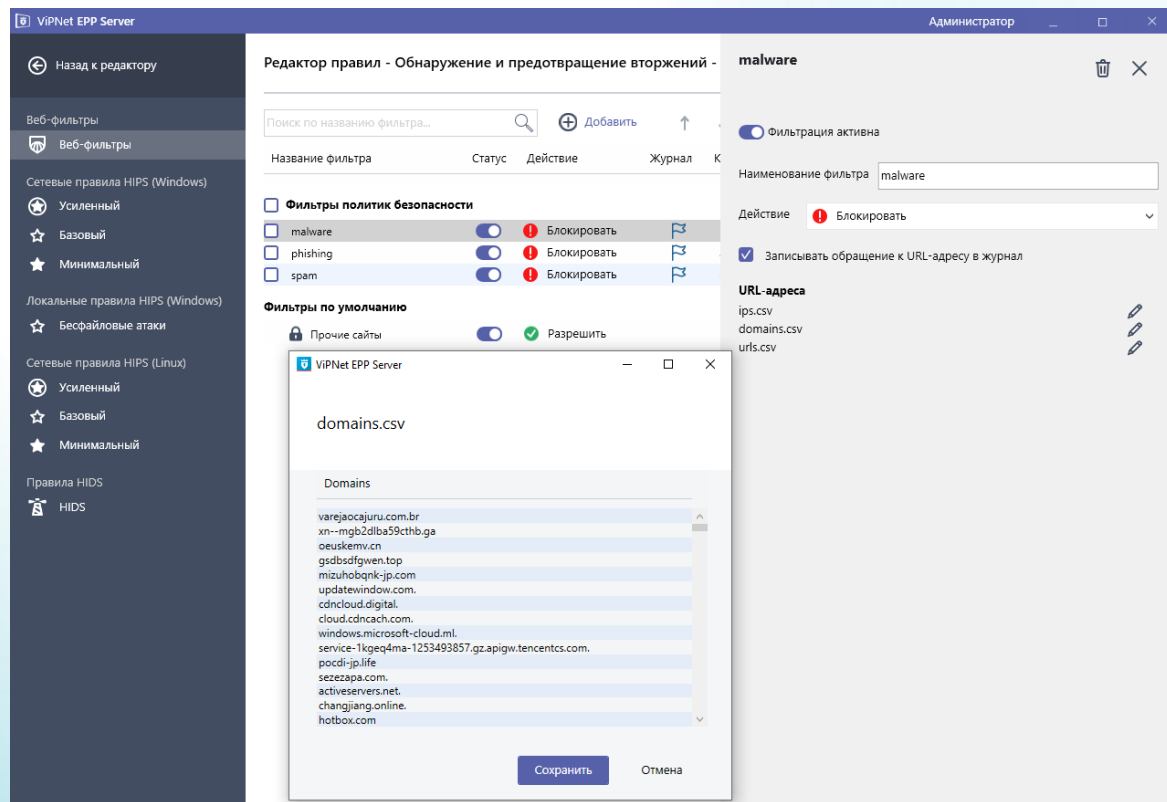
возможность расшифровывания трафика проходящего через модули ViPNet EndPoint Protection. База «bad URL» поставляется в рамках БРП, обновляется регулярно

SafeBrowsing

безопасный сёрфинг в интернете (веб-фильтрация)



Как это выглядит



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)



Создание фильтров защищённой сети

ViPNet EPP Администратор

Назад к EndPoint Protection

Режимы и задачи

- Режимы работы
- Сетевые фильтры
 - Публичная сеть
 - Частная сеть
 - Корпоративная сеть
- Журналы
 - Активные соединения
 - Трафик
- Справочники
 - Протоколы
 - Адреса и сети
 - Расписания

Персональный межсетевой экран - Фильтры режима работы 'Корпоративная сеть'

Поиск по названию фильтра...

Создать фильтр

Название фильтра	Статус	Действие	Версия IP	Протокол	Источник	Назначение	Расписание
Пользовательские фильтры							
☒ VPN_filter	☒	Разрешить	IP v4,v6	Все	Мой компьютер	координаторы	Всегда
Фильтры по умолчанию							
☒ Действие по умолчанию	☒	Разрешить	IP v4,v6	Все	Все	Все	Всегда

Copyright © 2023 Infotecs | Версия ПО: 1.6.0.13122 | База правил: 2.0.2 | Обновлено: 02.10.2023 13:32:09

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



Эвристический Antimalware движок

Возможность сканирования
исполняемых файлов и библиотек
с целью выявления зловреда

Эвристический Antimalware
использует собственную модель
построенную с помощью машинного
обучения

Модель постоянно обновляется
в рамках подписки на БРП





Мониторинг

Инфопанель

События

Управление защитой

Устройства

Базы правил

Доверенная загрузка

Обнаружение аномалий

Критерии обнаружения аномалий

Поведенческий анализ

AntiMalware

Сервис

Журналы

Конфигурация

Параметры системы

Учетные записи

Передача данных

Политика аудита

О программе

Выход

Передача данных

Электронная почта Active Directory Syslog TIAS

☒ Передача событий в ViPNet TIAS

Уровни передаваемых событий

Минимальный уровень событий: Опасное

Типы правил

- ☐ Обнаружение вторжений
 - ☐ Правила обнаружения локальных атак
 - ☐ Правила обнаружения сетевых атак
 - ☐ Выполняемые команды
 - ☐ Обнаружение установки ПО
 - ☐ Мониторинг файлов
 - ☐ Статус пакетов обновления Windows
 - ☐ Получение контрольных сумм файлов
- ☐ Персональный межсетевой экран
- ☐ Контроль приложений
- ☐ Предотвращение вторжений

Сервер ViPNet TIAS

Адрес сервера ViPNet TIAS:

Порт:

Отправить тестовое сообщение

Идентификатор ViPNet EPP
Сервера:

fbbc915f-23ef-4b5e-9213-b5f73f473551



Передача событий

Все события могут передаваться в:

- ViPNet TIAS
- В любую SIEM

Чего ждать до конца года?

VIPNet SafePoint 1.8

Ключевая задача релиза:

- Выпуск linux-сервера
- Передача релиза на продление сертификата



SafePoint - Новый клиент, хост: "astra-28624"

Большие иконки

Учетные записи

- Пользователи
- Группы
- Субъекты доступа
- Субъекты доступа
- Группы субъектов доступа
- Разграничение доступа к ФС
- Объекты разграничения доступа к ФС
- Группы объектов
- Правила разграничения доступа к ФС
- Гарантированное удаление
- Управление подключением устройств
- Устройства
- Анализатор имен файлов
- Анализатор имен файлов субъектов доступа
- Анализатор имен файлов объектов разграничения доступа к ФС
- Файловая система
- Процессы
- Сессии пользователей
- Сетевые настройки
- Настройки ротации
- Динамический контроль целостности
- Приложения
- Разделяемые библиотеки
- Шаблоны параметров безопасности

Имя	UID	Первичная группа	Член группы
www-data	33	www-data	www-data
uucp	10	uucp	uucp
user	1001	user	user
systemd...	994	systemd...	systemd-timesync
systemd...	998	systemd...	systemd-network
systemd...	996	systemd...	systemd-init-profile
sys	3	sys	sys
sync	4	nogroup	nogroup
sshd	104	nogroup	nogroup
speech-...	103	audio	audio
saned	106	saned	saned, scanner
root	0	root	root
pulse	101	pulse	pulse, audio
proxy	13	proxy	proxy
polkitd	995	polkitd	polkitd
nobody	65534	nogroup	nogroup
nm-open...	110	nm-open...	nm-openvpn
news	9	news	news
message...	100	message...	messagebus
man	6	man	man
mail	8	mail	mail
lp	7	lp	lp
logcheck	111	logcheck	logcheck, adm
list	38	list	list
ladmin	1000	ladmin	ladmin, astra-admin, astra-console, audio, cdrom, dialout, dip, floppy, lpadmin, plugdev, t...
irc	39	irc	irc
hplip	112	lp	lp

Настройка аудита Настройка паролей

Режим: сервер

2 — Терминал

Интерфейс сер...

SafePoint - Нов...

en 14:13 ПН СЕН

SafePoint - Новый клиент, хост: "astra-28624"

Большие иконки

Тип	Имя	Режим аудита
Папка	/boot/*	--
Папка	/home/ladmin/Документы/*	A-
Папка	/opt/DiskEditor/*	A-
Папка	/run/ssh/*	--
Папка	/sys/bus/*	A-
Папка	/sys/devices/*	--
Папка	/usr/share/firefox-astra/*	AP

Учетные записи

- Пользователи
- Группы
- Субъекты доступа
- Субъекты доступа
- Группы субъектов доступа
- Разграничение доступа к ФС
- Объекты разграничения доступа к ФС
- Группы объектов
- Правила разграничения доступа к ФС
- Гарантированное удаление
- Управление подключением устройств
- Устройства
- Анализатор имен файлов
- Анализатор имен файлов субъектов дост...
- Анализатор имен файлов объектов разгр...
- Файловая система
- Процессы
- Сессии пользователей
- Сетевые настройки
- Настройки ротации
- Динамический контроль целостности
- Приложения
- Разделяемые библиотеки
- Шаблоны параметров безопасности



SafePoint - Новый клиент, хост: "astra-28624"

Большие иконки

/opt/DiskEditor/*

Субъект	Режим доступа	Режим аудита
admin	+Ч+З+И+У+П	ЧЗИУП
auditor	+Ч-З-И-У-П	ЧЗИУП
user	-Ч-З-И-У-П	ЧЗИУП

Учетные записи

- Пользователи
- Группы
- Субъекты доступа
- Субъекты доступа
- Группы субъектов доступа
- Разграничение доступа к ФС
- Объекты разграничения доступа к ФС
- Группы объектов
- Правила разграничения доступа к ФС
- Гарантированное удаление
- Управление подключением устройств
- Устройства
- Анализатор имен файлов
- Анализатор имен файлов субъектов доступа
- Анализатор имен файлов объектов разграничения доступа к ФС
- Файловая система
- Процессы
- Сессии пользователей
- Сетевые настройки
- Настройки ротации
- Динамический контроль целостности
- Приложения
- Разделяемые библиотеки
- Шаблоны параметров безопасности

Режим: сервер

14:36 ПН СЕН

ViPNet EndPoint Protection 1.8

Ключевые задачи релиза

- Доработанный linux-сервер
- Переход на Web-UI
- Переход на схему работы с «рабочими серверами» - решение вопроса масштабируемости



Работа с агентами

← ↻ <https://192.168.79.191/agents/group/83f880d5-d9a2-413a-94ba-42994cfeecdd/agents> ⋮ ☆ ⚙ ⌵

ViPNet EndPoint Protection Администратор ▾

☰

Мониторинг

Обнаружение аномалий

Защита

Политики

Устройства

Система

Серверы безопасности

Учетные записи

Устройства

Группы устройств > Неподключенные

🔍 Поиск Устройство ▾ Фильтры ▾

☐ Устройство	Статус	Последняя активность	Системное имя	IP-адрес	Тип ОС	Операционная система	Версия EPP-агента	Рабочий сервер
☐ epp-agent-lin-02	● Активно	08.09.2025 14:12:33	epp-agent-lin-02	192.168.134.79	🐧	Astra Linux	1.8.0.2094	LocalWS
☐ epp-agent-lin-03	● Активно	08.09.2025 14:12:28	epp-agent-lin-03	192.168.134.80	🐧	Astra Linux	1.8.0.2094	LocalWS
☐ EPP-AGENT-WIN-0	● Активно	08.09.2025 14:12:27	EPP-AGENT-WIN-0	192.168.135.15	🪟	Майкрософт Windows 10 Корпоративная LTSC	1.8.0.20601	LocalWS
☐ EPP-AGENT-WIN-0	● Активно	08.09.2025 14:12:14	EPP-AGENT-WIN-0	192.168.135.14	🪟	Майкрософт Windows 10 Корпоративная LTSC	1.8.0.20601	LocalWS
☐ EPP-AGENT-WIN-0	● Активно	08.09.2025 14:12:27	EPP-AGENT-WIN-0	192.168.135.65	🪟	Майкрософт Windows 10 Корпоративная LTSC	1.8.0.20601	LocalWS



Назад

Система

Основное

Межсетевой экран

Обнаружение вторжений

Предотвращение вторжений

ZTNA

Контроль приложений

Epp_20250605_8_1.8.0_RU

Общее

Общее

Название	Epp_20250605_8_1.8.0_RU
Статус	☐ Не используется
Версия политики	1.0.0
Версия базы правил	1.8.0.8
Изменена	05.06.2025 03:00:00
Создана	05.06.2025 03:00:00

Режимы работы модулей защиты

☒ Межсетевой экран	✓ Базовый (Частная сеть)
☒ Обнаружение вторжений	✓ Включено
☒ Предотвращение вторжений	✓ Минимальный
☒ Контроль приложений	✓ Разрешать неизвестные приложения
☒ ZTNA	✗ Защита отключена

Источник правил межетевого экрана

Приложение-источник правил ViPNet EndPoint Protection

Используется на устройствах

Политика не назначена на устройства.

Работа с БРП

Подписывайтесь
на наши соцсети,
там много интересного



infotecs

Кадыков Иван

Ivan.Kadykov@infotecs.ru