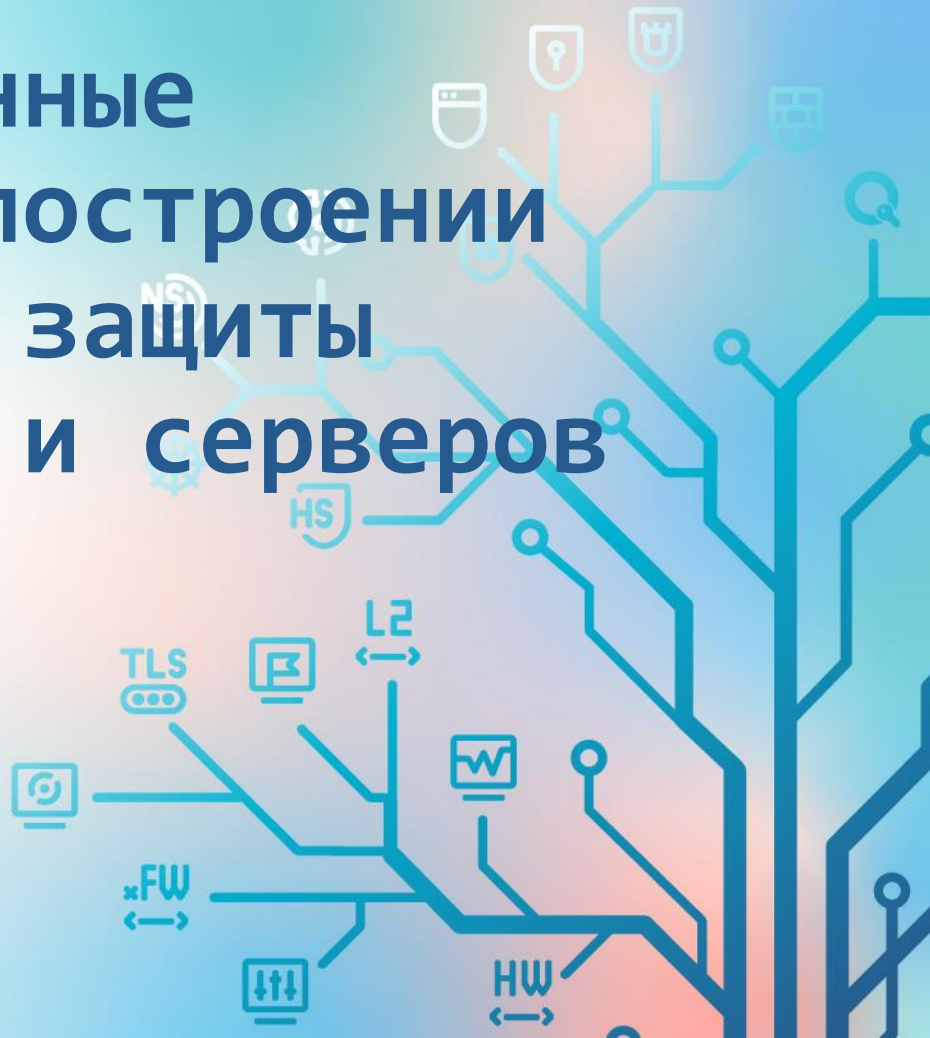
# Новые и проверенные технологии при построении эшелонированной защиты рабочих станций и серверов

**Иван Кадыков**
Руководитель направления




infotecs

# 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

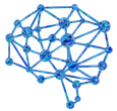
**При построении автоматизированных систем и подхода к защите рабочих станций всегда решается несколько задач:**

Построение автоматизированных систем по требованиям к ИСПДн, ГИС, АСУ ТП и КИИ

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

Защита от продвинутых, бесфайловых и сложных атак

Построение защищенного канала между пользователями



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?

*Рецепт 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

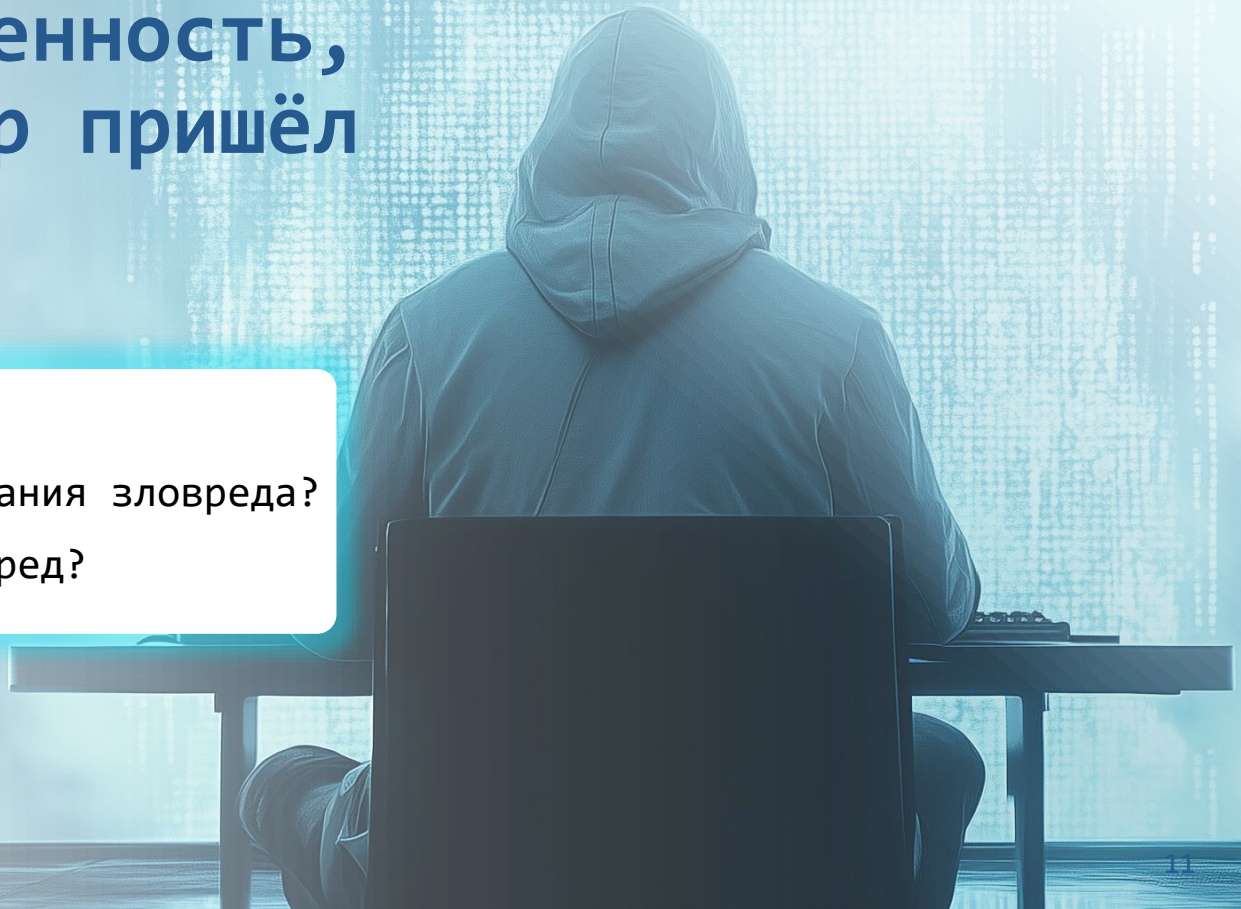
Идентификация и Аутентификация пользователей

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

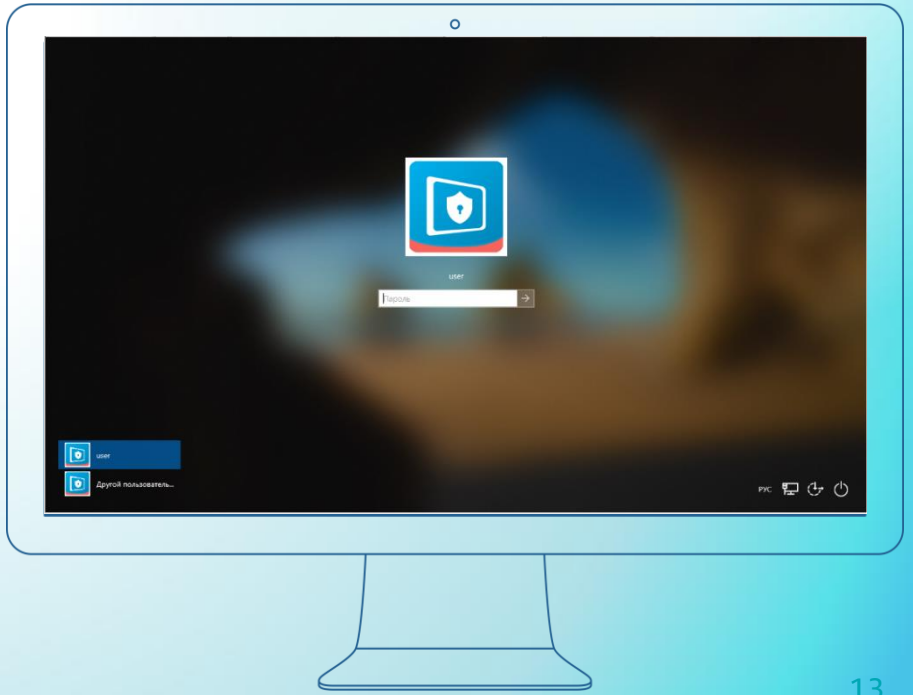
# Финальный этап доверенной загрузки

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

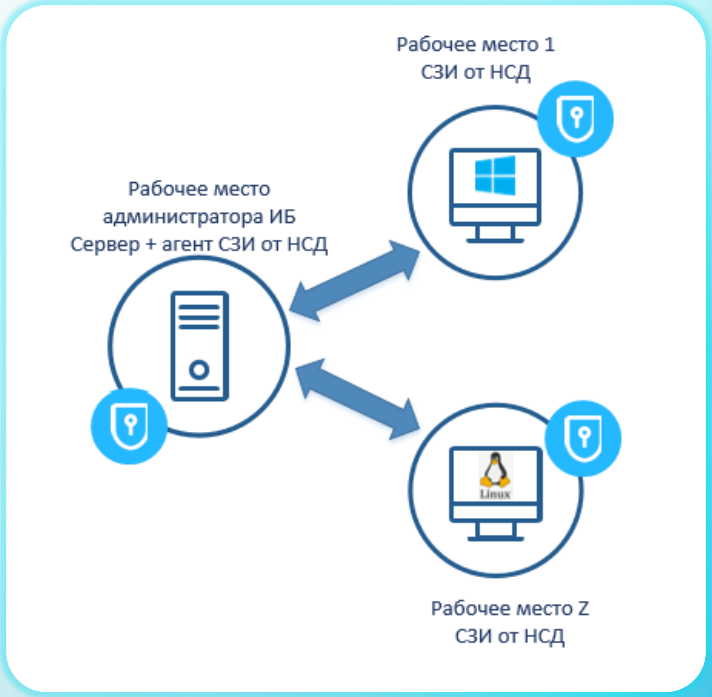
# Управление привилегированными пользователями

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

Нет

# 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:

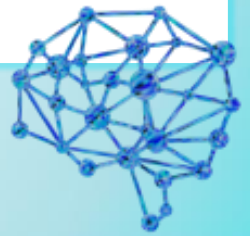
- Обнаружение аномалий с помощью критериев
- Обнаружение аномалий с помощью поведенческого анализа

# 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

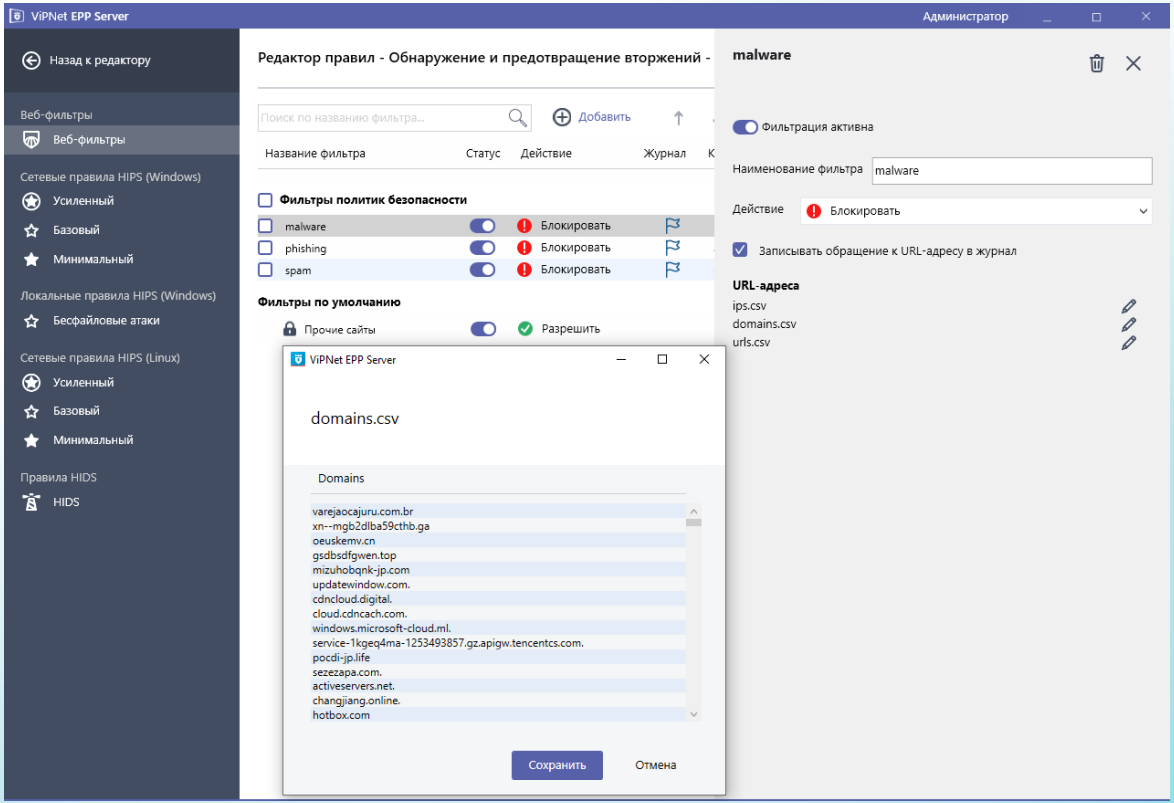
### TLS – инспекция

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

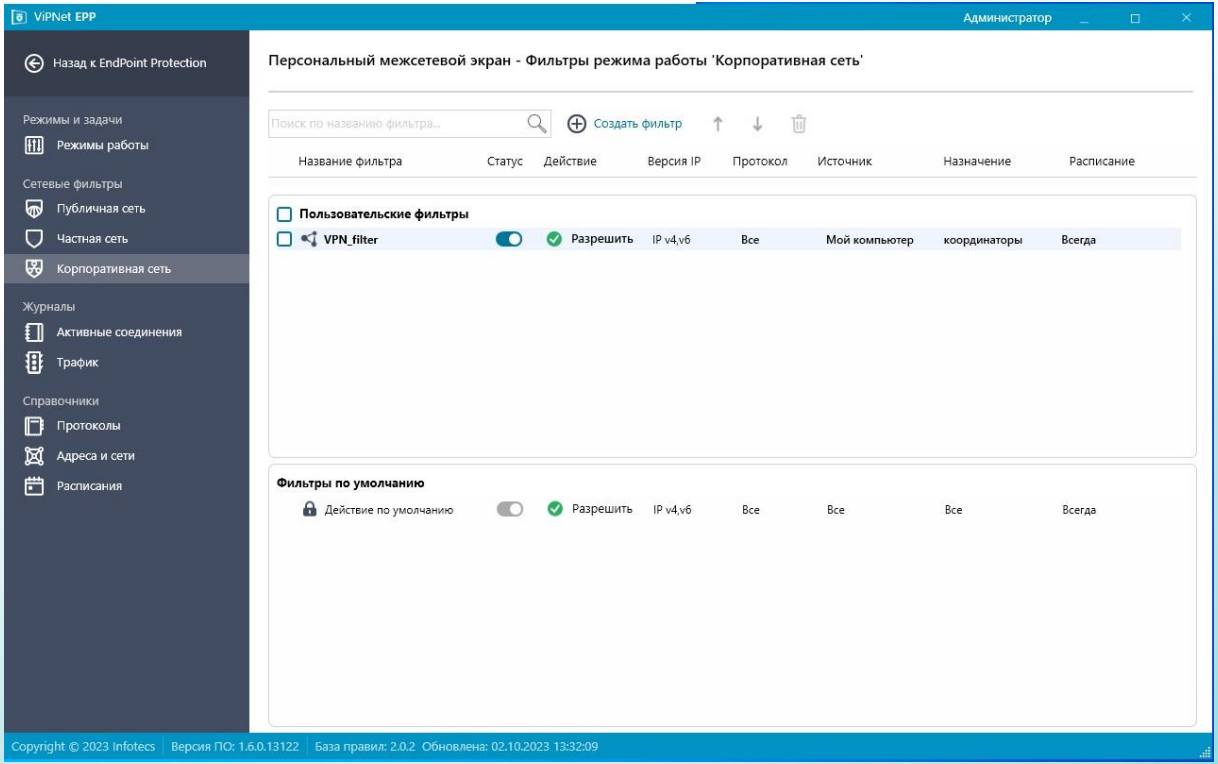


# Межсетевой экран

- 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



# Контроль приложений

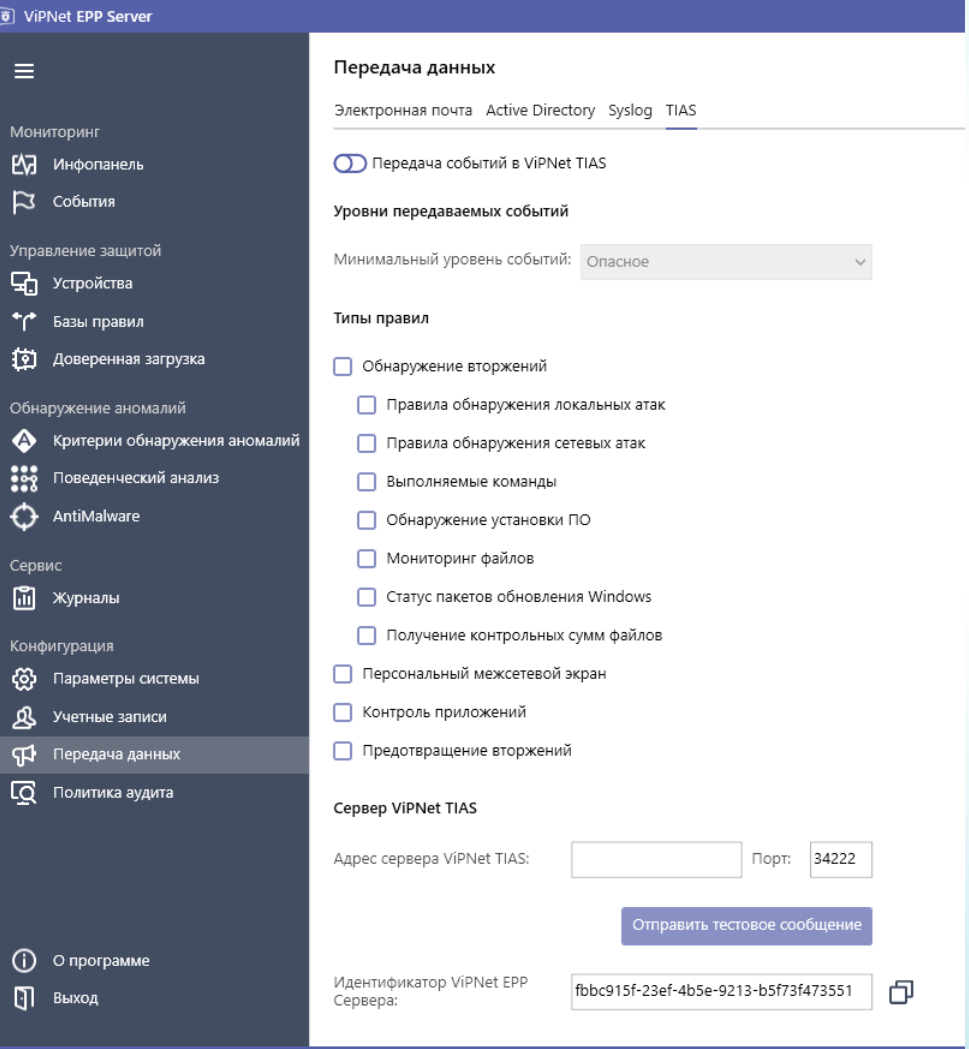
- Контроль запуска программ с использованием Черных и Белых списков программного обеспечения
- Анализ командной строки
- Защита файлов
- Защита реестра
- Контроль запуска программ, DLL-модулей, драйверов
- Контроль сетевой активности приложений

# 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




infotecs

# Передача событий

Все события могут передаваться в:

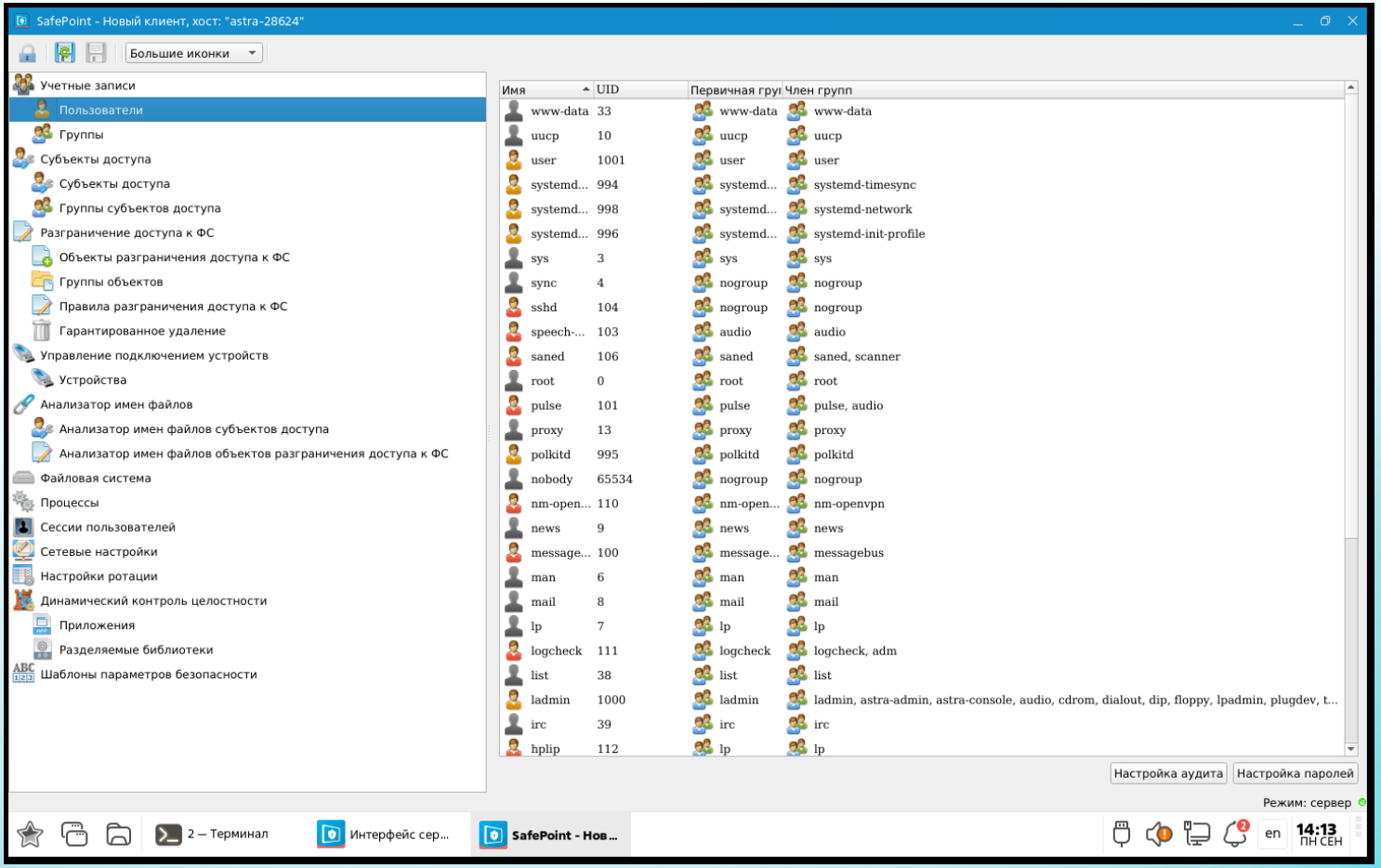
- ViPNet TIAS
- В любую SIEM

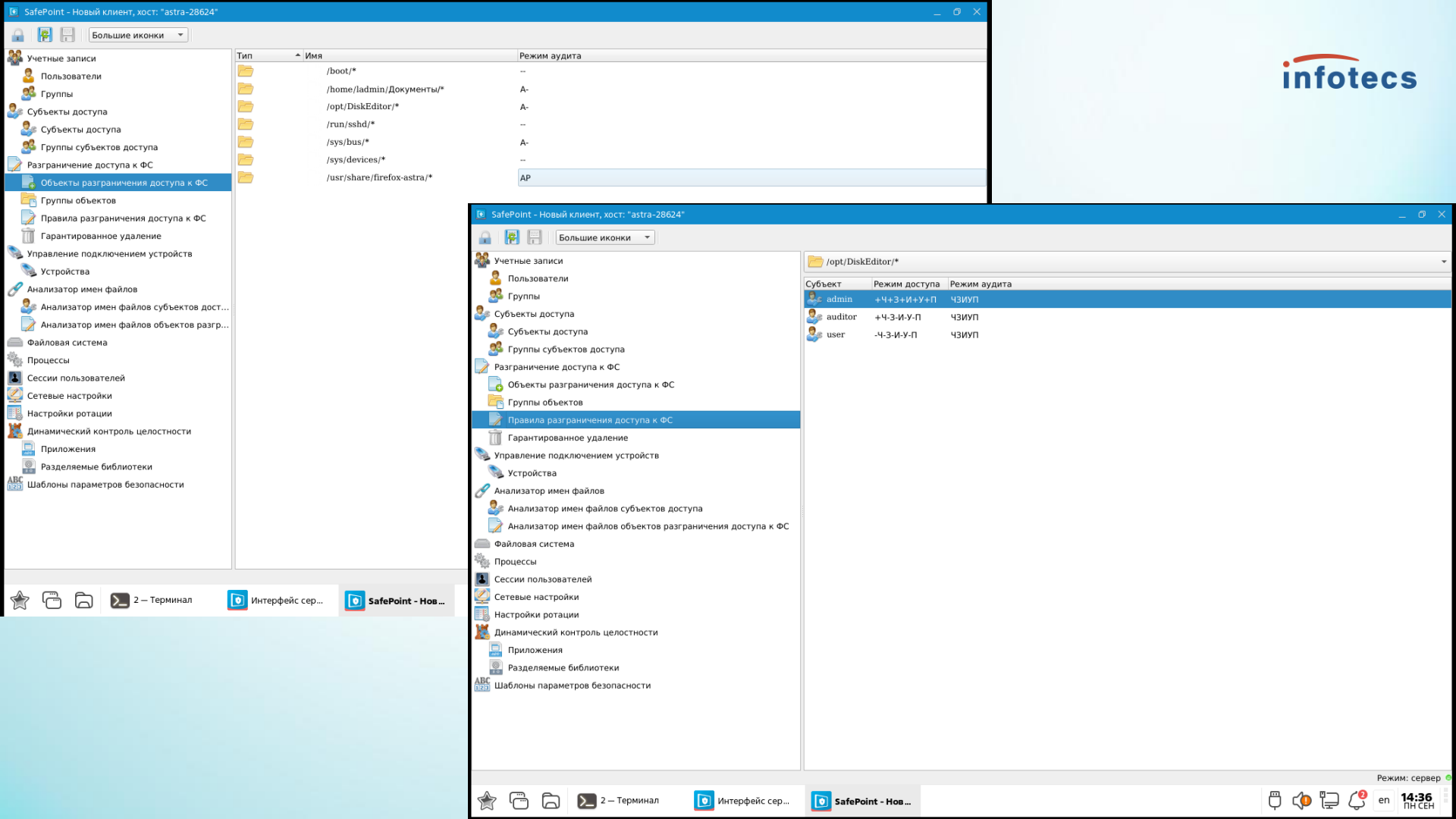
# Чего ждать до конца года?

# 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 груп
Член групп
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

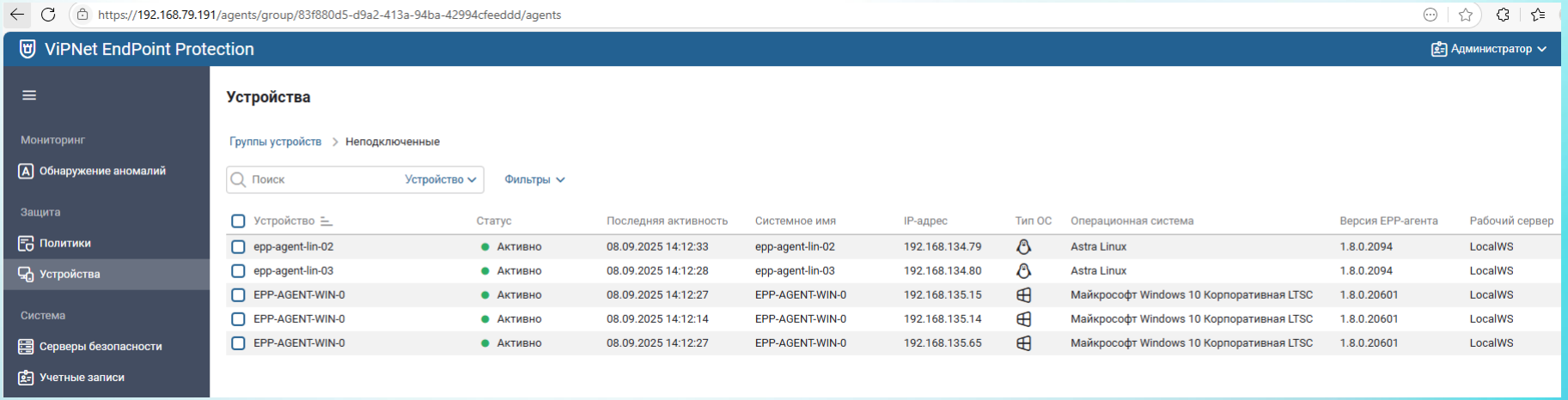

SafePoint - Новый клиент, хост: "astra-28624"
Большие иконки
Учетные записи
Пользователи
Группы
Субъекты доступа
Субъекты доступа
Группы субъектов доступа
Разграничение доступа к ФС
Объекты разграничения доступа к ФС
Группы объектов
Правила разграничения доступа к ФС
Гарантированное удаление
Управление 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
Тип
Имя
Режим аудита
/boot/* --
/home/ladmin/Документы/* A-
/opt/DiskEditor/* A-
/run/sshd/* --
/sys/bus/* A-
/sys/devices/* --
/usr/share/firefox-astra/* AP
2 — Терминал
Интерфейс сер...
SafePoint - Нов...
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
Режим: сервер
2 — Терминал
Интерфейс сер...
SafePoint - Нов...
en
14:36
ПН СЕН

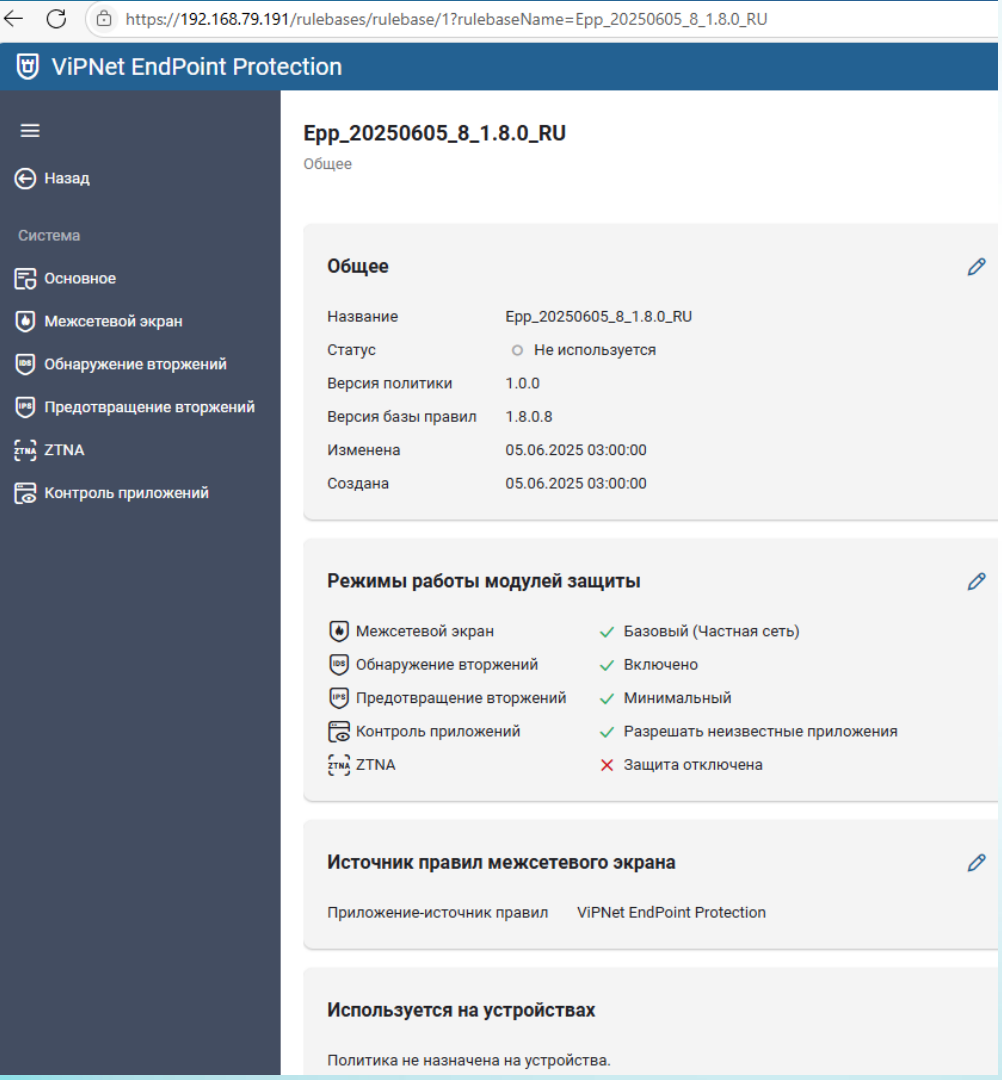
# ViPNet EndPoint Protection 1.8

Ключевые задачи релиза

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

# Работа с агентами






infotecs

# Работа с БРП

Подписывайтесь
на наши соцсети,
там много интересного

Кадыков Иван

Ivan.Kadykov@infotecs.ru