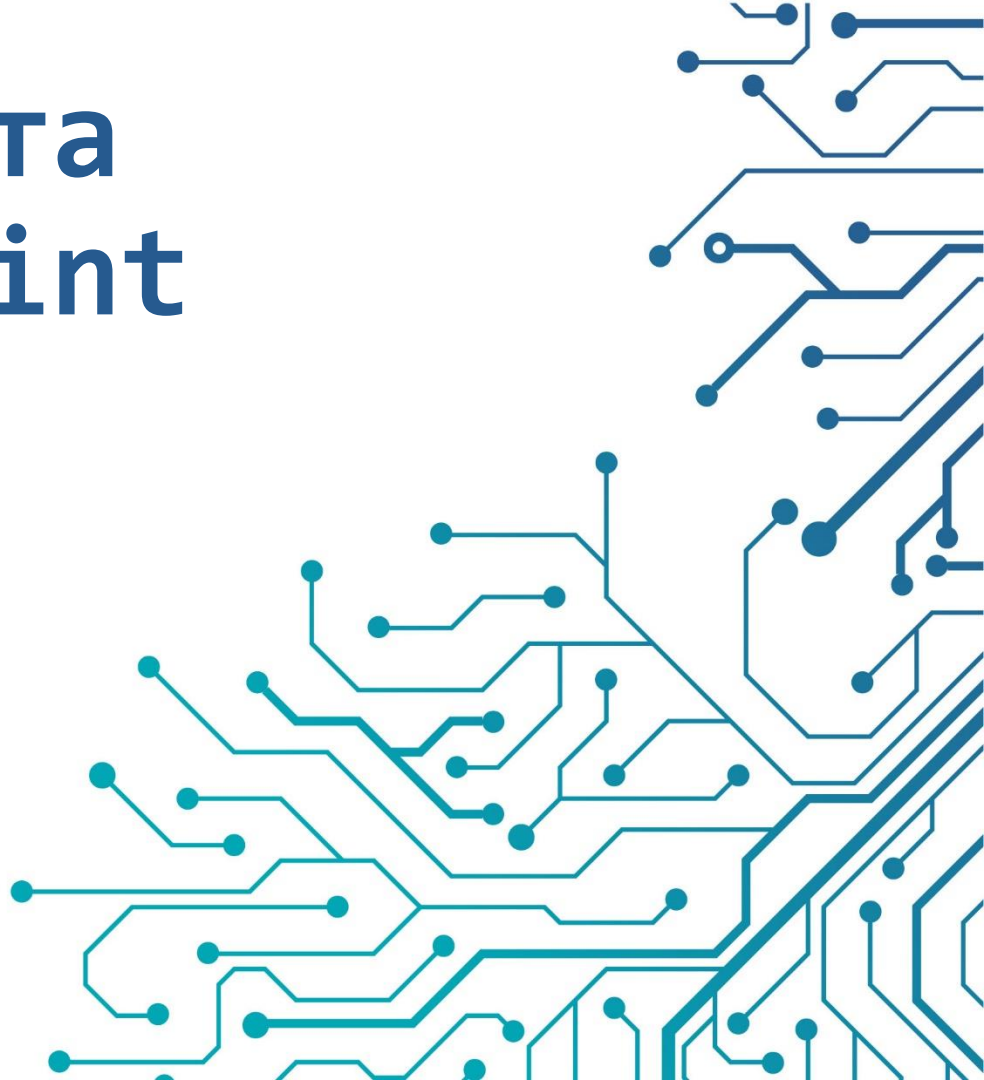
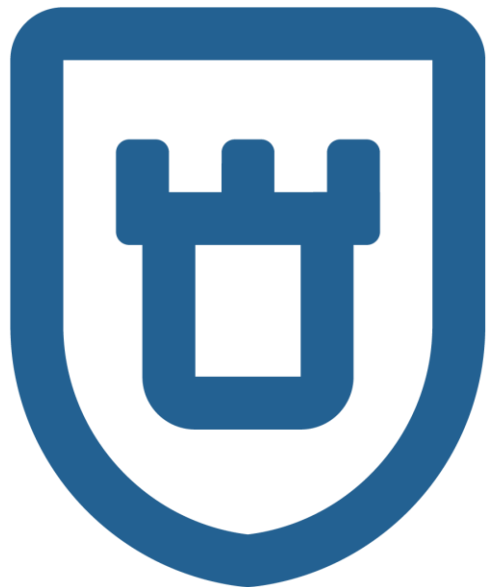


Обзор продукта ViPNet EndPoint Protection версия 1.6

Кадыков Иван

The logo for infotecs, featuring a stylized orange and red arc above the word "infotecs" in a bold, blue, sans-serif font.





VIPNet EndPoint Protection

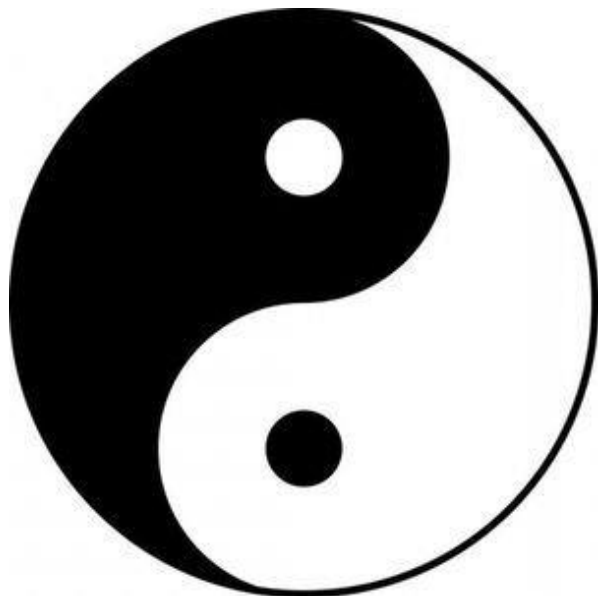
Система комплексной защиты рабочих станций и серверов, предназначенная для предотвращения «файловых», «бесфайловых» и сетевых атак, обнаружения вредоносных действий и реакции на эти действия.

Защитные механизмы

Контроль приложений



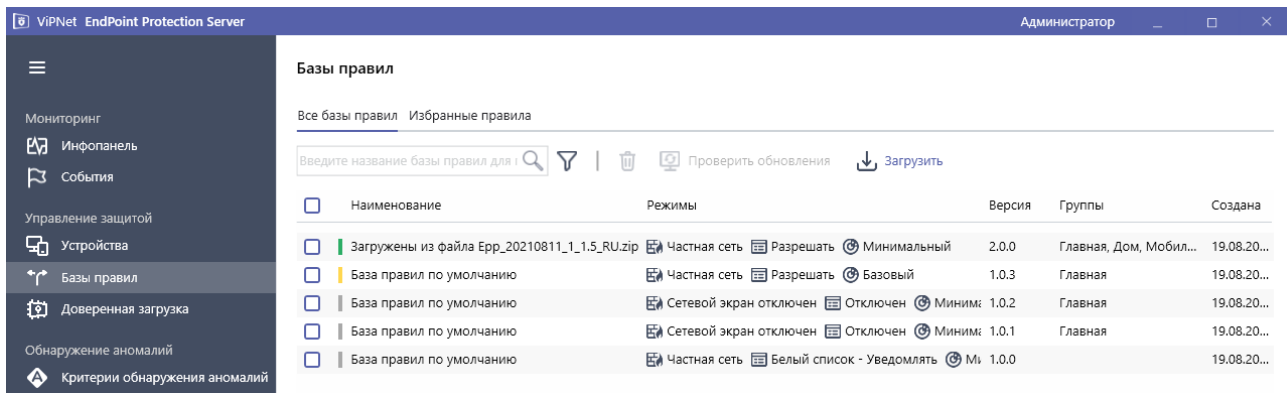
ViPNet EndPoint Protection – комбинирование методов защиты



- 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

Работаем по правилам и моделям!

EndPoint Protection работает по БРП



Состоит из:

- Правил системы обнаружения и предотвращения вторжений
- Фильтров Межсетевое экрана
- Списков ПО для Черного и Белого списка
- Эвристический движок Anti-malware
- Модель обнаружения аномального поведения системных утилит

VPNNet EndPoint Protection admin

Журнал событий

Введите идентификатор события > 🔍 | 🗑️ | 🔄 Обновить | 🗑️

<input type="checkbox"/>	Дата, время	Идентификатор	Описание	Модуль	Попытки
<input type="checkbox"/>	18.09.2023 16:06:11	6000001	Обнаружено блокируемое событие HIDS SIG=3195048.	HIPS	3
<input type="checkbox"/>	18.09.2023 16:06:11	3195048	AM EXPLOIT Apache Log4j2 JNDI RCE via LDAP (CVE-2021-44228)	HIDS	1
<input type="checkbox"/>	18.09.2023 16:06:11	3195047	AM EXPLOIT Possible Apache Log4j2 JNDI RCE (CVE-2021-44228)	HIDS	1
<input type="checkbox"/>	18.09.2023 16:06:11	3193909	AM EXPLOIT Apache Log4j2 <= 2.14.1 JNDI RCE via HTTP Header var 1 (CVE-2021-...	HIDS	1
<input type="checkbox"/>	18.09.2023 16:06:11	5030009	Запуск дочернего процесса запрещён	AppC	1
<input type="checkbox"/>	18.09.2023 16:06:11	300001	Создание пр Запуск дочернего процесса запрещён	HIDS	1
<input type="checkbox"/>	18.09.2023 16:06:11	300748	Возможный вредоносный артефакт: запуск "cmd/powershell" через "Java"	HIDS	1
<input type="checkbox"/>	18.09.2023 16:06:11	304000	Правило для модуля поведенческого анализа	HIDS	1
<input type="checkbox"/>	18.09.2023 16:05:31	100016	Изменение типа запуска службы (реестр)	HIDS	1
<input type="checkbox"/>	18.09.2023 16:04:58	300054	Создание процесса (consent)	HIDS	1
<input type="checkbox"/>	18.09.2023 16:04:58	400050	Регистрация доверенного процесса входа	HIDS	2
<input type="checkbox"/>	18.09.2023 16:04:58	300001	Создание процесса	HIDS	3
<input type="checkbox"/>	18.09.2023 16:04:58	304000	Правило для модуля поведенческого анализа	HIDS	3
<input type="checkbox"/>	18.09.2023 16:04:17	400069	Обновление задачи планировщика	HIDS	1
<input type="checkbox"/>	18.09.2023 16:03:57	300001	Создание процесса	HIDS	6
<input type="checkbox"/>	18.09.2023 16:03:57	304000	Правило для модуля поведенческого анализа	HIDS	6
<input type="checkbox"/>	18.09.2023 16:03:57	400069	Обновление задачи планировщика	HIDS	1

Мы всё видим

Все события с хостов собираются на сервере и выводятся на экран для администратора ИБ



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

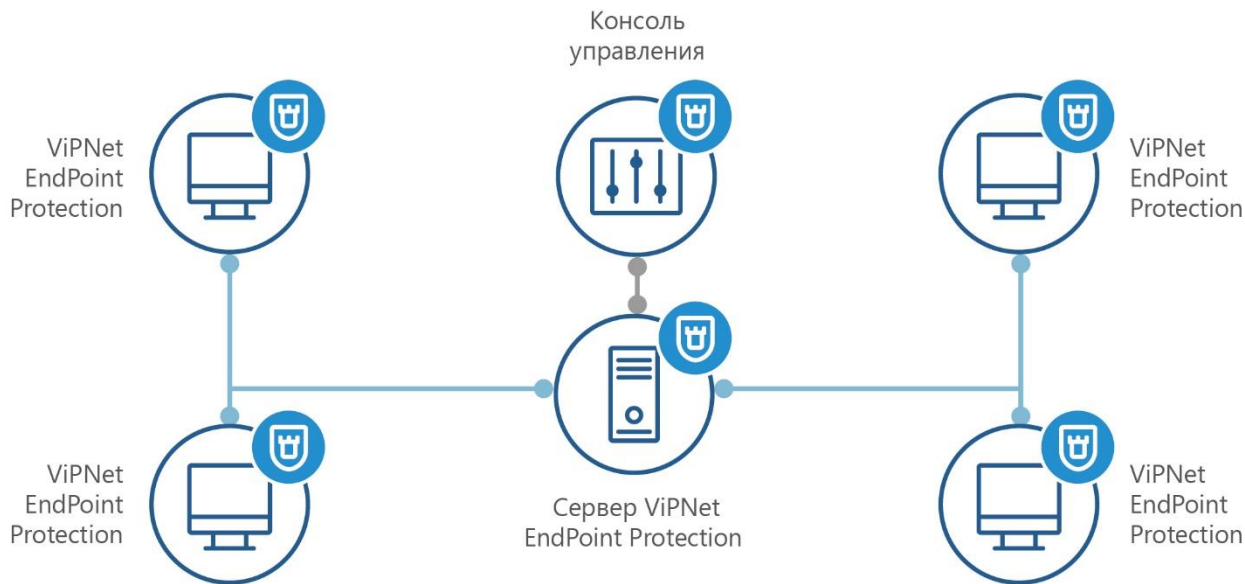
Адрес сервера VIPNet TIAS: Порт: Идентификатор VIPNet EPP Сервера: 

Передача событий

Все события могут передаваться в:

- VIPNet TIAS
- В любую SIEM

Архитектура ViPNet EndPoint Protection



- Клиент
- Сервер
- Консоль управления

СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ № 4666

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
22 марта 2023 г.

Выдан: 22 марта 2023 г.
Действителен до: 22 марта 2028 г.

Настоящий сертификат удостоверяет, что изделие **VIPNet EndPoint Protection**, разработанное и производимое АО «ИнфоТеКС», является программным средством защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну, реализующим функции межсетевой экрана и системы обнаружения вторжений, соответствует требованиям по безопасности информации, установленным в документах «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) - по 4 уровню доверия, «Требования к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа В четвертого класса защиты. ИТ.МЭ.В4.ПЗ» (ФСТЭК России, 2016), «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011), «Профиль защиты систем обнаружения вторжений уровня узла четвертого класса защиты. ИТ.СОВ.У4.ПЗ» (ФСТЭК России, 2012) и задании по безопасности ФРКЕ.00238-01 98 01 при выполнении указаний по эксплуатации, приведенных в формуляре ФРКЕ.00238-01 30 01.

Сертификат выдан на основании технического заключения от 21.02.2023, оформленного по результатам сертификационных испытаний испытательной лабораторией АНО «Институт инженерной физики» (аттестат аккредитации от 18.11.2016 № СЗИ RU.0001.01БИ00.Б012), и экспертного заключения от 03.03.2023, оформленного органом по сертификации ООО «ЦБИ» (аттестат аккредитации от 11.04.2016 № СЗИ RU.0001.01БИ00.А001).

Заявитель: АО «ИнфоТеКС»
Адрес: 127083, г. Москва, ул. Мишина, д. 56, стр. 2, эт. 2, помещение IX,
комната 29
Телефон: (495) 737-6192

Сертифицировано!

- Межсетевой экран тип В класс 4
- Система обнаружения вторжений У4
- 4 класс ТДБ

Таблица 1 – Реализация ViPNet EPP мер по защите информации

№ п/п	Содержание меры по обеспечению безопасности в [1], [2] и ее условное обозначение	Содержание меры по обеспечению безопасности в [3], [7] и ее условное обозначение
1.	ИАФ.1* Идентификация и аутентификация пользователей, являющихся работниками оператора	ИАФ.1* Идентификация и аутентификация пользователей и иницилируемых ими процессов
2.	ИАФ.3* Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	ИАФ.3* Управление идентификаторами
3.	ИАФ.4* Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	ИАФ.4* Управление средствами аутентификации
4.	ИАФ.5* Защита обратной связи при вводе аутентификационной информации	В [3], [7] отсутствует соответствующая мера
5.	УПД.1* Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	УПД.1* Управление учетными записями пользователей
6.	УПД.2 Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	УПД.2 Реализация модели управления доступом
7.	УПД.3 Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между	ЗИС.6 Управление сетевыми потоками

Меры прописаны в правилах пользования

На картинке представлена
лишь часть мер прописанных в
документе

Версия 1.6

Что нового?

Сервер под Linux!



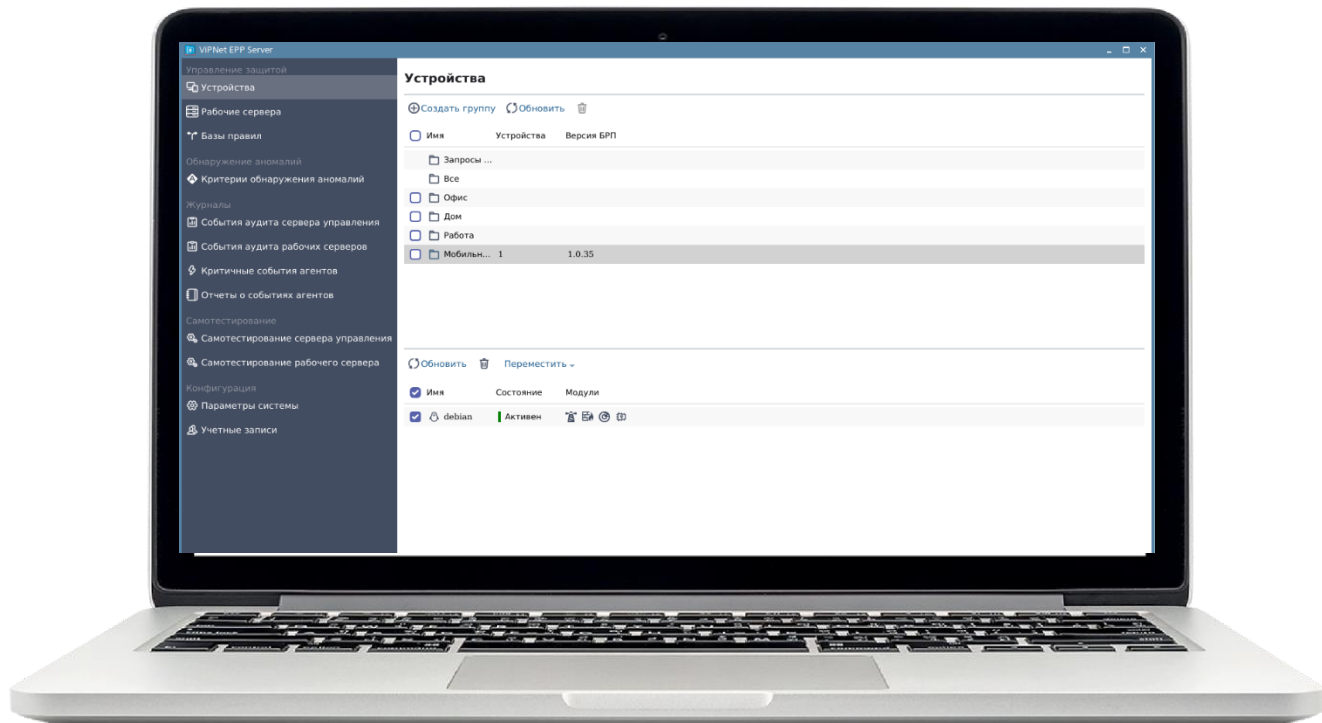
Разработан компонент ViPNet EndPoint Protection Server под Astra Linux Special Edition 1.7.4

Пока реализована возможность управление следующими модулями:

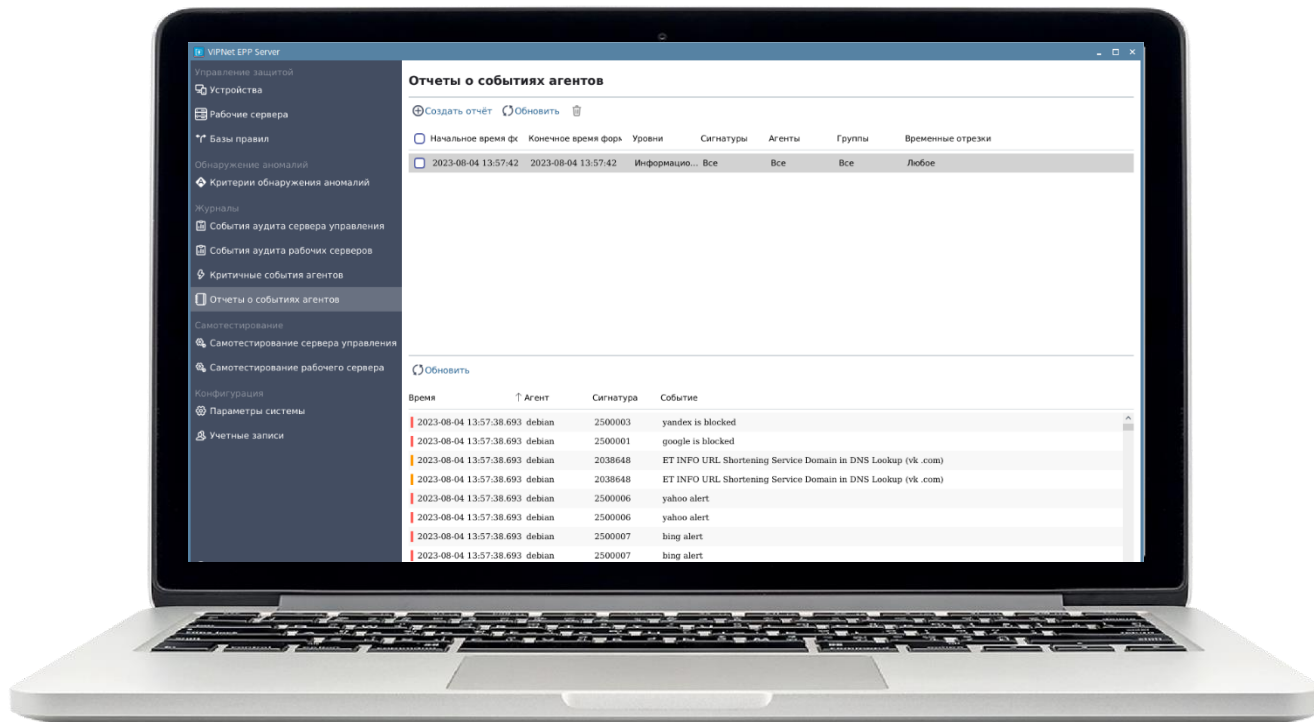
- Персональный межсетевой экран
- Модуль обнаружения и предотвращения вторжений
- Модуль обнаружения аномалий в части обнаружения с помощью критериев

Так же реализована возможность отслеживания работы антивирусов.

Управление устройствами



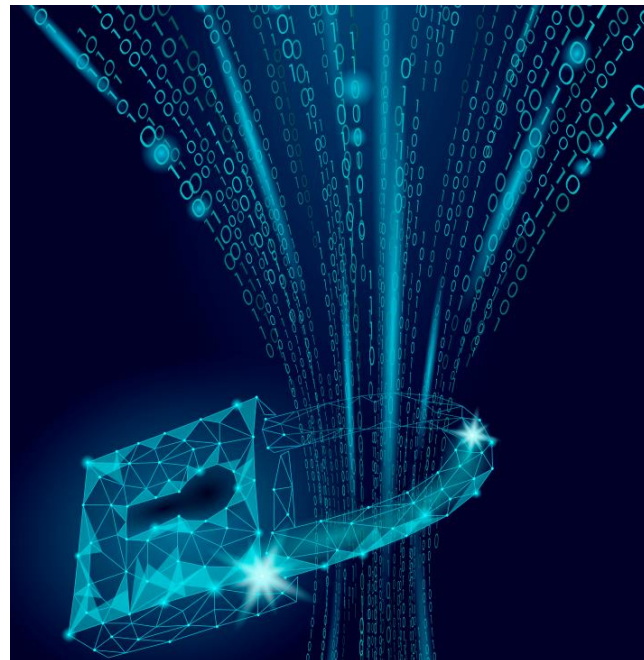
События от агентов



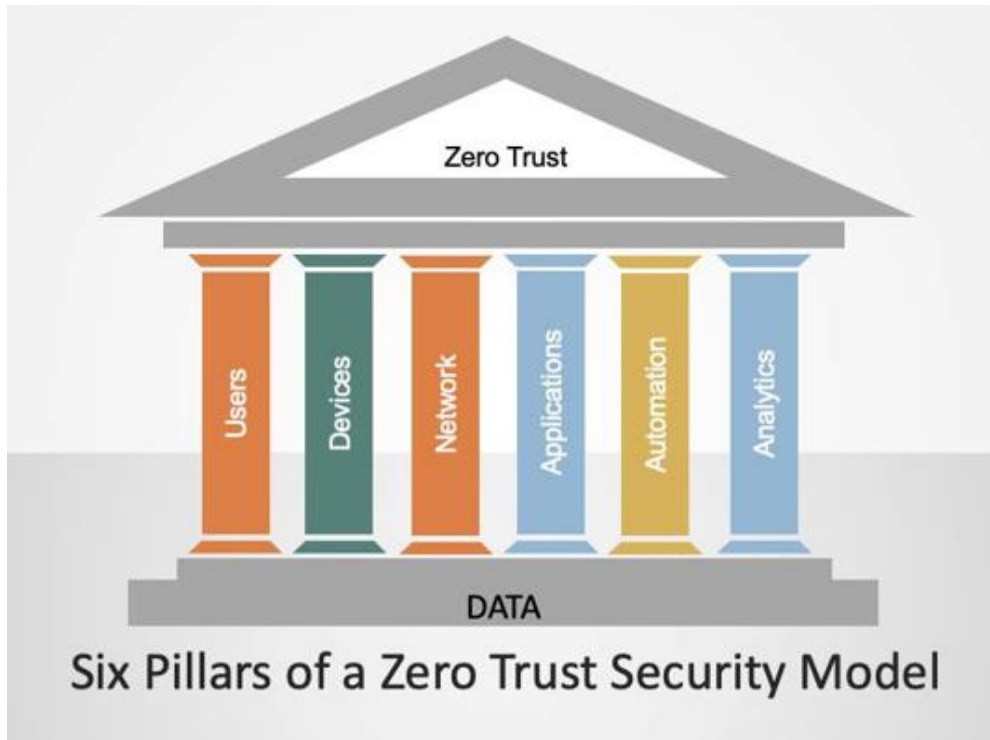
Изменения в модуле межсетевого экрана

Добавились новые возможности:

- **Стек технологий ZTNA**
- Интеграция с Client 4U
- Добавление\Редактирование\Удаление фильтров защищённой сети из локальной консоли ViPNet EndPoint Protection (агент)



Что такое Zero Trust?

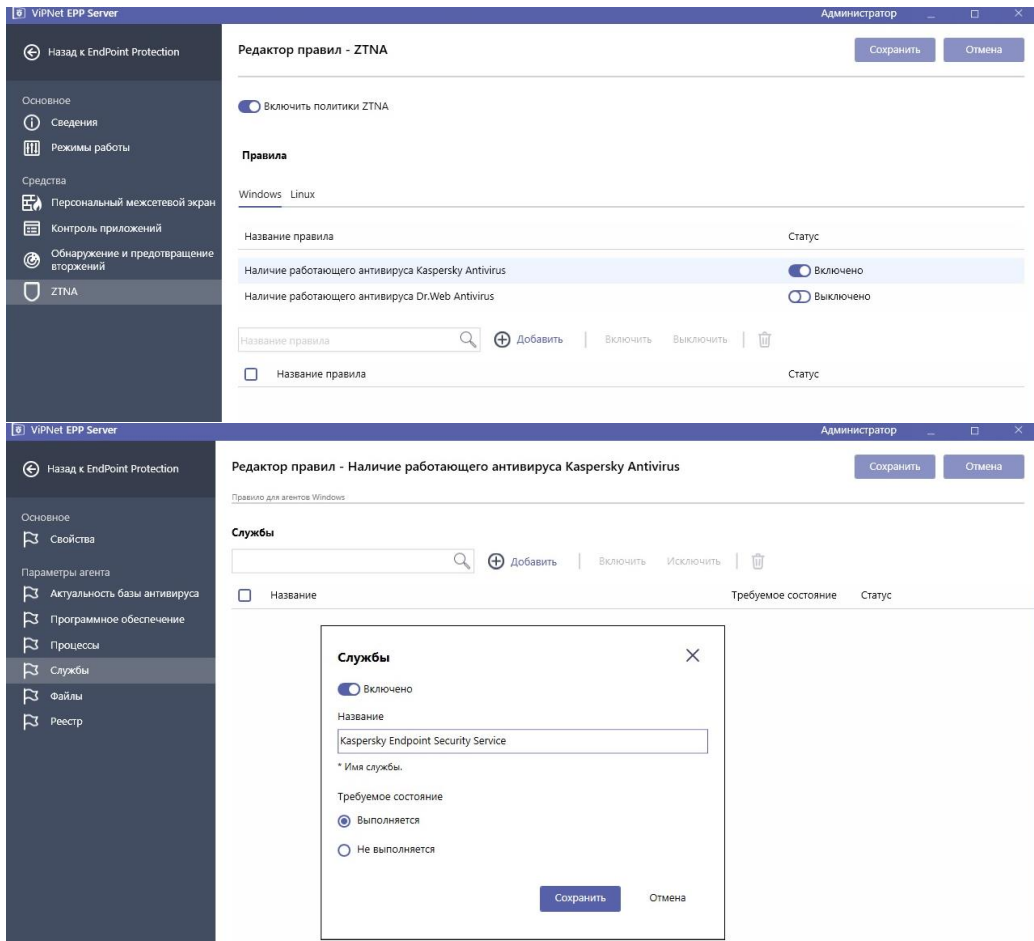


Zero Trust (ZT) или «нулевое доверие» – набор постоянно развивающихся концепций и идей, направленных на принятие точных решений о доступе субъекта к объекту с минимальными привилегиями для каждого запроса доступа.

Что уже реализовано

- Проверка соответствия хоста на наличие необходимого/требуемого ПО, обновлений ПО, запущенных процессов, обновление антивирусных баз и т.д.
- Блокировка входа в защищенную сеть ViPNet при несоответствии устройства политикам ZTNA, информирование пользователя об этом.





Значения политики ZTNA

Включить политики ZTNA

Правила

Windows Linux

Название правила	Статус
Наличие работающего антивируса Kaspersky Antivirus	<input checked="" type="checkbox"/> Включено
Наличие работающего антивируса Dr.Web Antivirus	<input type="checkbox"/> Выключено

Название правила |

Название правила Статус

Редактор правил - Наличие работающего антивируса Kaspersky Antivirus

Правило для агентов Windows

Службы

|

Название	Требуемое состояние	Статус
<input type="checkbox"/> Название <input type="text"/>	<input type="text"/>	<input type="text"/>

Службы

Включено

Название

* Имя службы.

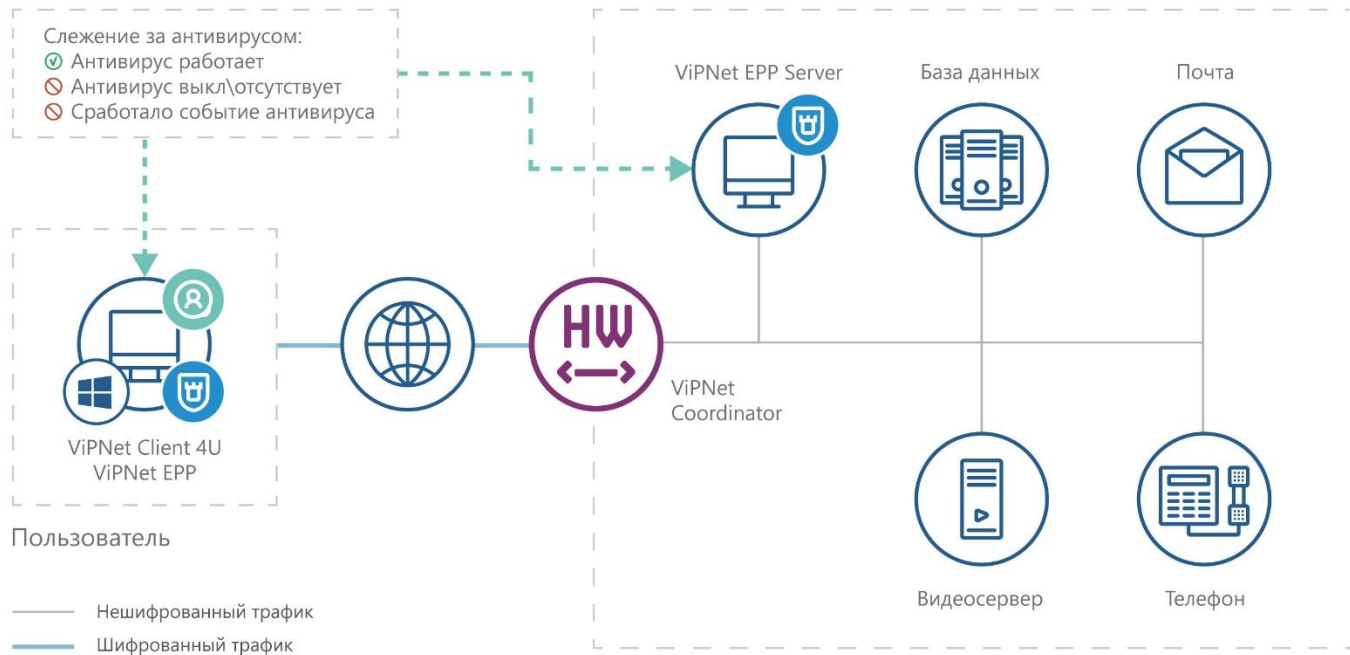
Требуемое состояние

Выполняется

Не выполняется

Редактирование правил ZTNA

ZTNA «В картинках»



Создание фильтров защищённой сети

Скриншот административного интерфейса VIPNet EPP. В заголовке окна указано 'VIPNet EPP' и 'Администратор'. В центре экрана отображается панель управления фильтрами для режима работы 'Корпоративная сеть'. Вверху панели есть поле для поиска по названию фильтра, кнопка 'Создать фильтр' и иконки для сортировки и удаления. Ниже расположен список фильтров с заголовками: Название фильтра, Статус, Действие, Версия IP, Протокол, Источник, Назначение, Расписание.

Название фильтра	Статус	Действие	Версия IP	Протокол	Источник	Назначение	Расписание
Пользовательские фильтры							
<input type="checkbox"/> VPN_filter	<input checked="" type="checkbox"/>	Разрешить	IP v4,v6	Все	Мой компьютер	координаторы	Всегда
Фильтры по умолчанию							
<input checked="" type="checkbox"/> Действие по умолчанию	<input type="checkbox"/>	Разрешить	IP v4,v6	Все	Все	Все	Всегда

В левом меню навигации доступны следующие пункты: 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. В нижнем левом углу экрана отображены метаданные: Copyright © 2023 Infotecs, Версия ПО: 1.6.0.13122, База правил: 2.0.2, Обновлено: 02.10.2023 13:32:09.

Используя UI ViPNet EndPoint Protection agent можно создавать пользовательские фильтры защищённой сети для ViPNet Client 4U

Изменения в модуле системы обнаружения и предотвращения вторжений

- TLS – инспекция – возможность расшифровывания трафика проходящего через модули VipNet EndPoint Protection. База «bad URL» поставляется в рамках БПП, обновляется регулярно
- SafeBrowsing – безопасный сёрфинг в интернете (веб-фильтрация)



Видео-скриншот интерфейса администратора VIPNet EPP Server. В центре экрана открыт редактор правил для обнаружения и предотвращения вторжений. В правой панели настроен фильтр 'malware' с активированной фильтрацией и действием 'Блокировать'. В нижней части экрана открыто диалоговое окно для редактирования файла 'domains.csv', в котором перечислены различные доменные адреса.

Редактор правил - Обнаружение и предотвращение вторжений

Поиск по названию фильтра...

Название фильтра	Статус	Действие	Журнал
Фильтры политик безопасности			
<input type="checkbox"/> malware	<input checked="" type="checkbox"/>	❗ Блокировать	📄
<input type="checkbox"/> phishing	<input checked="" type="checkbox"/>	❗ Блокировать	📄
<input type="checkbox"/> spam	<input checked="" type="checkbox"/>	❗ Блокировать	📄
Фильтры по умолчанию			
<input checked="" type="checkbox"/> Прочие сайты	<input checked="" type="checkbox"/>	✅ Разрешить	

malware

Фильтрация активна

Наименование фильтра: malware

Действие: ❗ Блокировать

Записывать обращение к URL-адресу в журнал

URL-адреса

- ips.csv
- domains.csv
- urls.csv

domains.csv

Domains

- varejaocajuru.com.br
- xn--mgb2d1ba59cthb.ga
- oeuskemv.cn
- gsdbsdfgwen.top
- mizuhobqnk-jp.com
- updatewindow.com
- cdncloud.digital
- cloud.cdncach.com
- windows.microsoft-cloud.ml
- service-1kgeq4ma-1253493857.gz.apigw.tencentcs.com
- podci-jp.life
- sezezapa.com
- activeservers.net
- changjiang.online
- hotbox.com

Сохранить Отмена

Как это выглядит



Fileless attacks

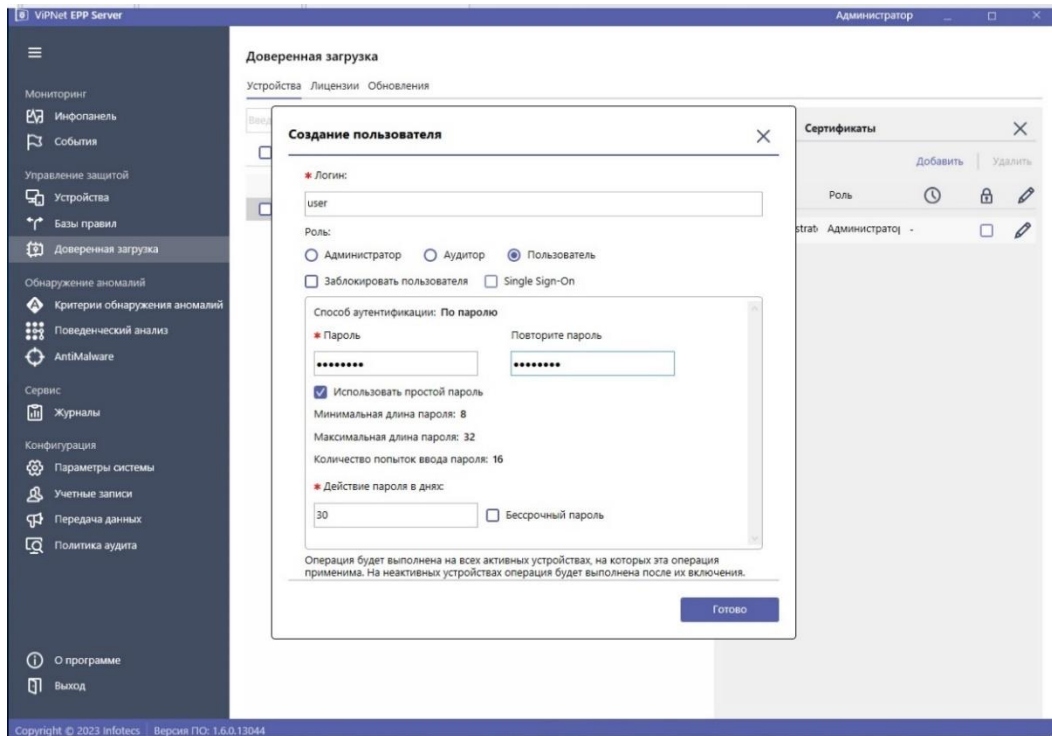
Внедрение новых техник предотвращения бесфайловых атак:

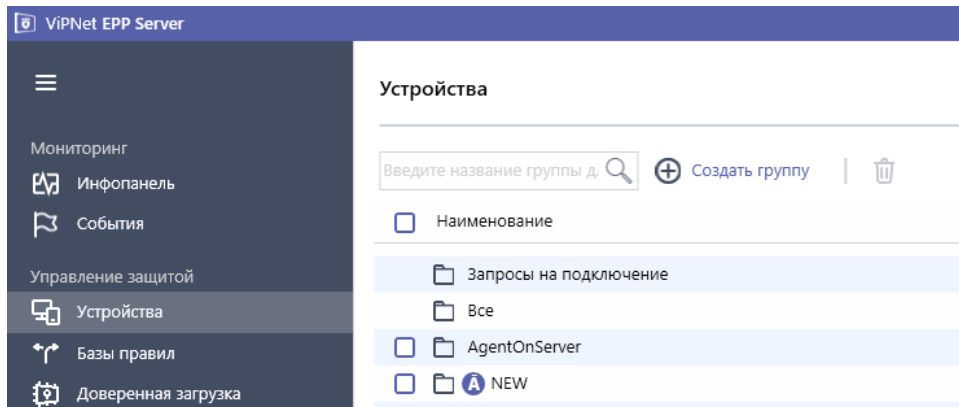
- Hollowed / replaced
- Doppelganger

Управление ViPNet SafeBoot

Дополнительные механизмы удалённого управления ViPNet SafeBoot:

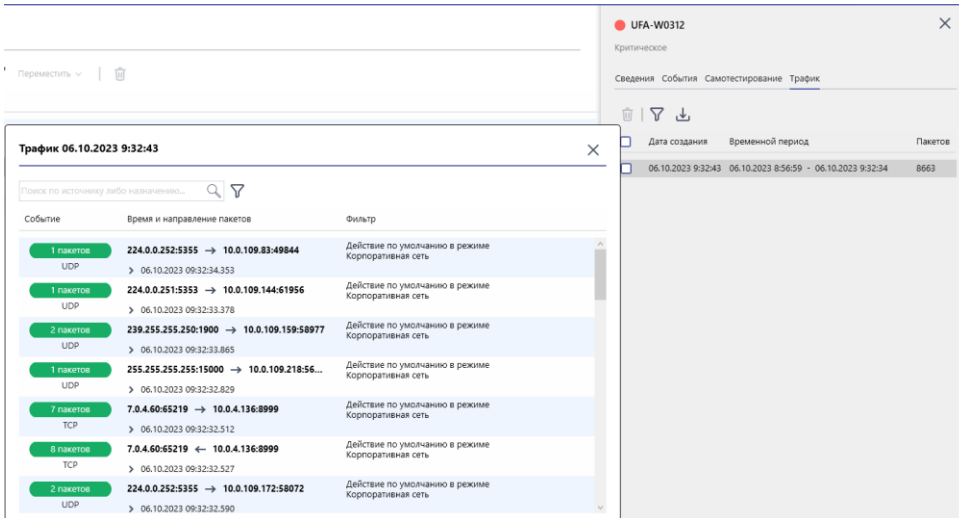
- Обновление МДЗ
- Управление пользователями
- Установка корневых сертификатов



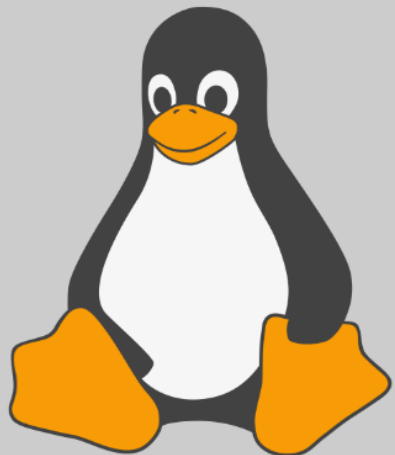


И ещё добавили...

- Автоматическое подключение защищаемых узлов к ViPNet EPP Сервер
- Запрос журнала регистрации трафика с ViPNet EPP



Поддержка новых ОС Linux



L I N U X

Astra Linux Special Edition 1.7.4

Альт СП Рабочая станция релиз 10

Альт Рабочая станция 10.1

РЕД ОС 7.3.2 «Муром» Рабочая станция

РЕД ОС 7.3.3 «Муром» Рабочая станция



Спасибо за внимание!

Подписывайтесь на наши соцсети



vk.com/infotecs_news



https://t.me/infotecs_official



rutube.ru/channel/24686363