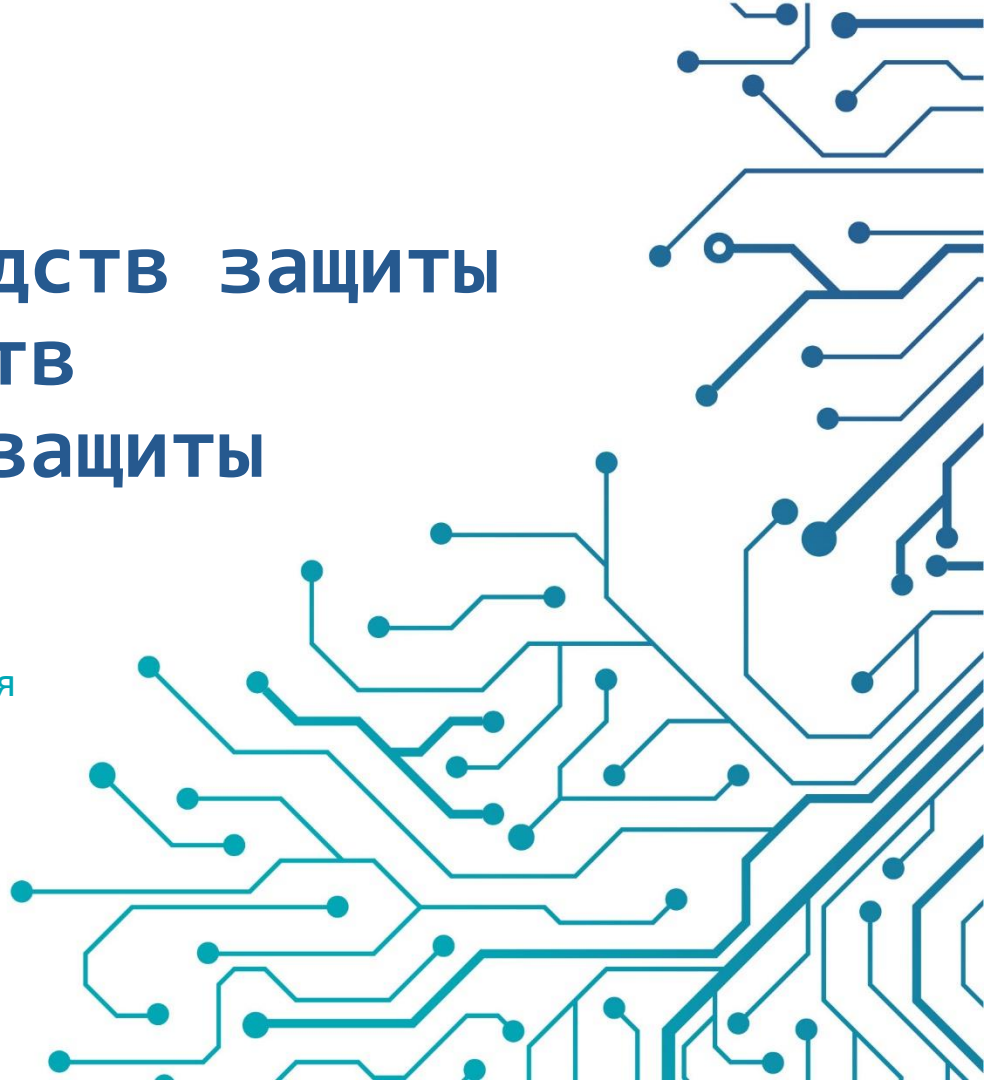
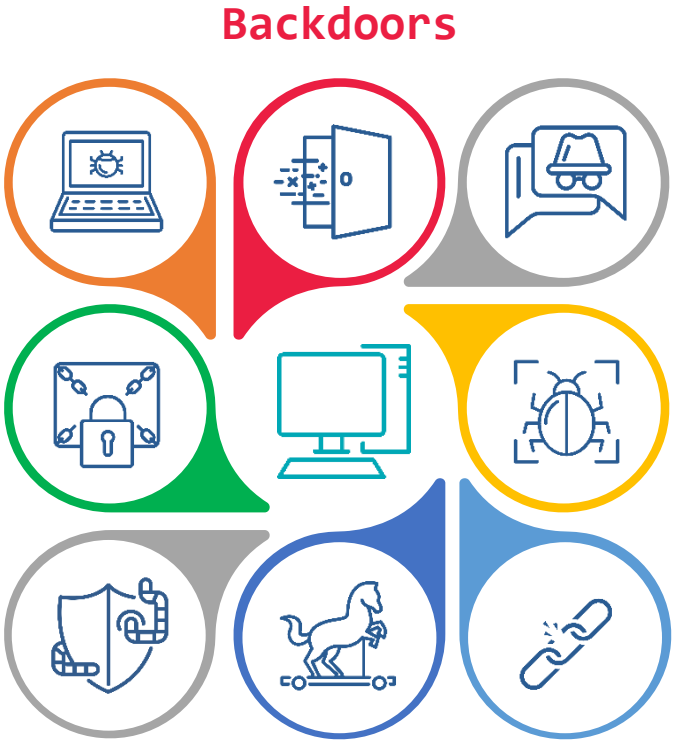
Особенности выбора и эксплуатации средств защиты информации и средств криптографической защиты информации

Григорьев Дмитрий
Руководитель обособленного подразделения



infotecs

От чего защищаемся?



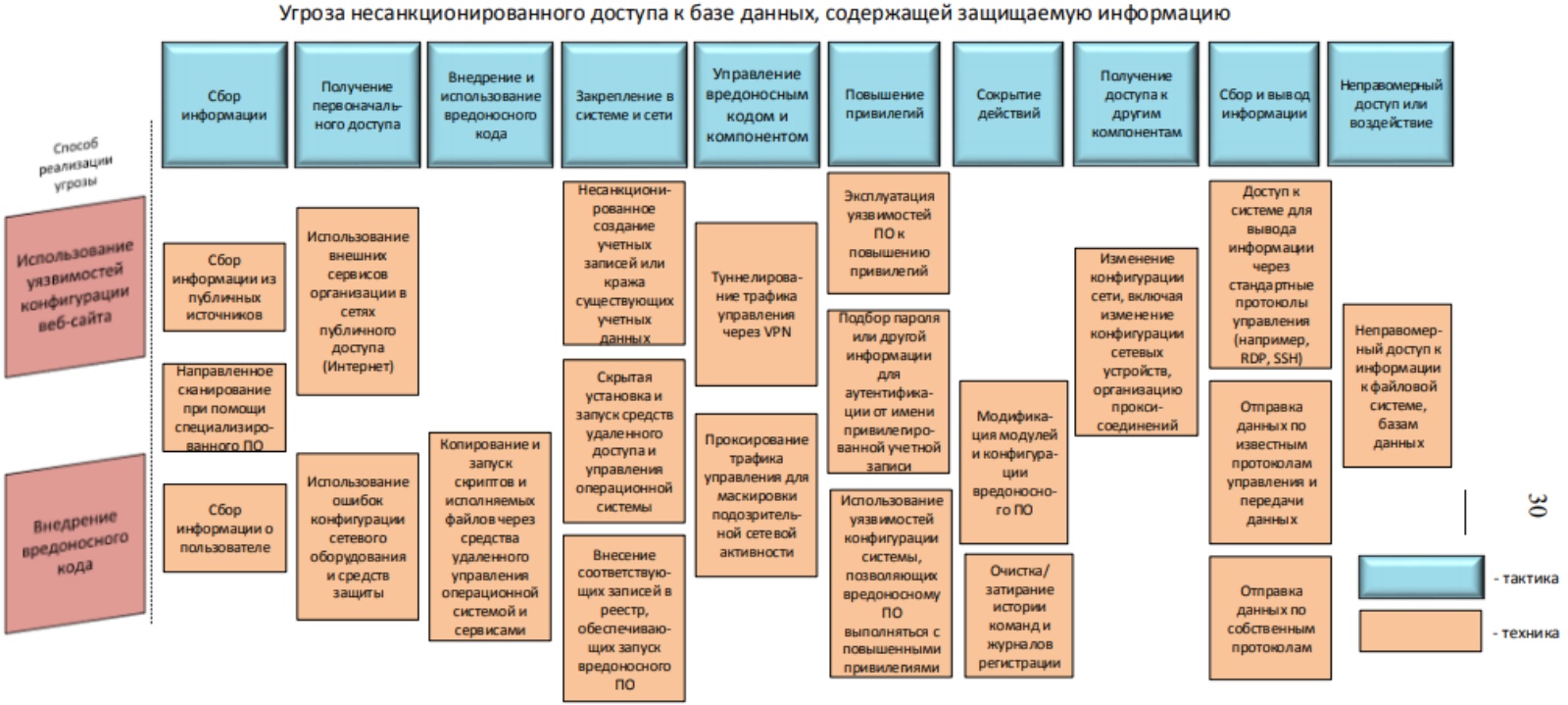
От кого защищаемся?

Инсайдеры

Иностранные вендоры, уходящие с рынка и отключающие свои продукты

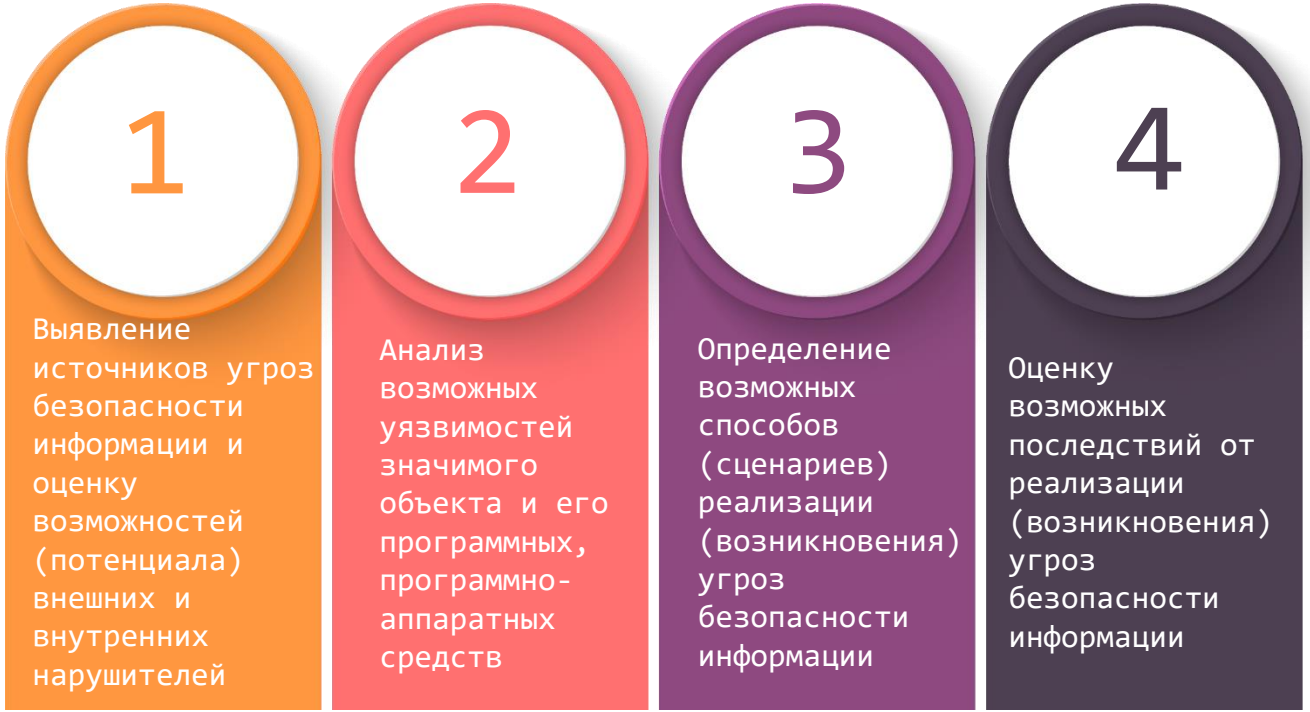
Хакеры

Методика оценки угроз безопасности информации



ВЫБОР СРЕДСТВ ЗАЩИТЫ

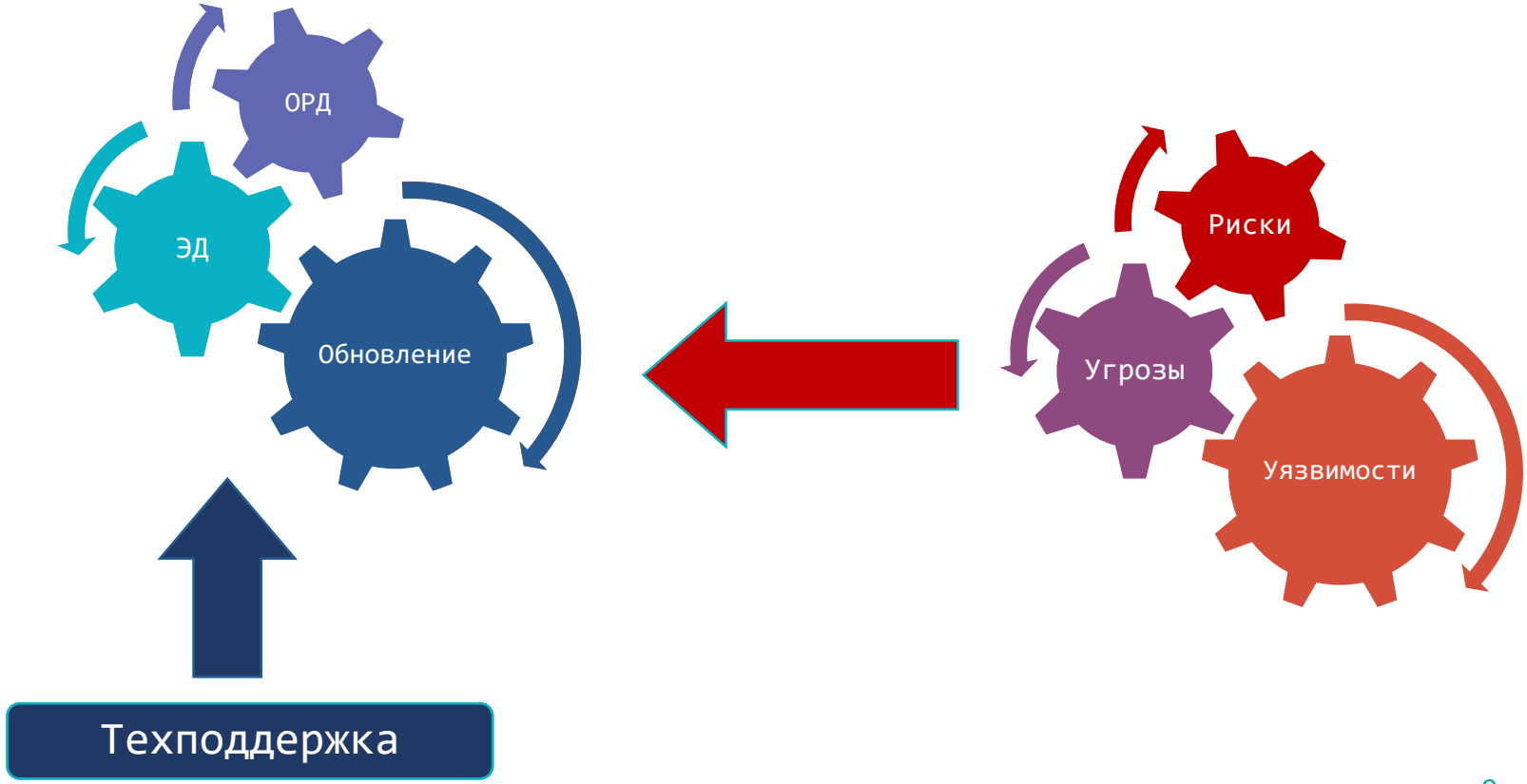
Анализ угроз безопасности информации и разработку модели угроз безопасности информации или ее уточнение:



Проектирование подсистемы безопасности значимого объекта

1. **определяются субъекты доступа** (пользователи, процессы и иные субъекты доступа) и объекты доступа;
2. **определяются политики управления доступом** (дискреционная, мандатная, ролевая, комбинированная);
3. **определяются и обосновываются организационные и технические меры**, подлежащие реализации в рамках подсистемы безопасности значимого объекта;
4. **определяются виды и типы средств защиты информации**, обеспечивающие реализацию технических мер по обеспечению безопасности значимого объекта;
5. **осуществляется выбор средств защиты информации** и (или) их разработка с учетом категории значимости значимого объекта, совместимости с программными и программно-аппаратными средствами, выполняемых функций безопасности и ограничений на эксплуатацию;
6. **разрабатывается архитектура подсистемы безопасности** значимого объекта, включающая состав, места установки, взаимосвязи средств защиты информации;
7. **определяются требования к параметрам настройки** программных и программно-аппаратных средств, включая средства защиты информации, обеспечивающие реализацию мер по обеспечению безопасности, блокирование (нейтрализацию) угроз безопасности информации и устранение уязвимостей значимого объекта;
8. **определяются меры по обеспечению безопасности** при взаимодействии значимого объекта с иными объектами критической информационной инфраструктуры, информационными системами, автоматизированными системами управления или информационно-телекоммуникационными сетями.

Эксплуатация системы ЗИ



ДАВАЙТЕ ПОПРАКТИКУЕМСЯ

Перечень угроз относящиеся к угрозам BIOS/UEFI

infotecs

Угроза

УБИ.004: Угроза аппаратного сброса пароля BIOS
УБИ.005: Угроза внедрения вредоносного кода в BIOS
УБИ.008: Угроза восстановления аутентификационной информации
УБИ.006: Угроза внедрения кода или данных
УБИ.009: Угроза восстановления предыдущей уязвимой версии BIOS
УБИ.013: Угроза деструктивного использования декларированного функционала BIOS
УБИ.018: Угроза загрузки нештатной операционной системы
УБИ.023: Угроза изменения компонентов системы
УБИ.024: Угроза изменения режимов работы аппаратных элементов компьютера
УБИ.030: Угроза использования информации идентификации/аутентификации, заданной по умолчанию
УБИ.032: Угроза использования поддельных цифровых подписей BIOS
УБИ.035: Угроза использования слабых криптографических алгоритмов BIOS
УБИ.039: Угроза исчерпания запаса ключей, необходимых для обновления BIOS
УБИ.045: Угроза нарушения изоляции среды исполнения BIOS

Перечень угроз относящиеся к угрозам BIOS/UEFI

Угроза

УБИ.053: Угроза невозможности управления правами пользователей BIOS
УБИ.072: Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS
УБИ.087: Угроза несанкционированного использования привилегированных функций BIOS
УБИ.090: Угроза несанкционированного создания учётной записи пользователя
УБИ.108: Угроза ошибки обновления гипервизора
УБИ.121: Угроза повреждения системного реестра
УБИ.123: Угроза подбора пароля BIOS
УБИ.124: Угроза подделки записей журнала регистрации событий
УБИ.129: Угроза подмены резервной копии программного обеспечения BIOS
УБИ.144: Угроза программного сброса пароля BIOS
УБИ.145: Угроза пропуска проверки целостности программного обеспечения
УБИ.150: Угроза сбоя процесса обновления BIOS
УБИ.152: Угроза удаления аутентификационной информации
УБИ.154: Угроза установки уязвимых версий обновления программного обеспечения BIOS
УБИ.179: Угроза несанкционированной модификации защищаемой информации

ViPNet SafeBoot

Программный модуль доверенной загрузки, устанавливаемый в UEFI BIOS различных производителей.

Предназначен для защиты компьютеров и серверов от угроз НСД и атак на сам BIOS.

Обеспечивает:

- Доверенную загрузку ОС
- Контроль целостности ПО и данных
- Авторизацию на уровне BIOS
- Защиту на уровне SMM - фильтрация программных SMI

(system management interrupt и ограничение их функциональности)

ИАФ | УПД | ОЦЛ | АУД

Сертификаты: ФСТЭК России – СДЗ - 2 класса защиты, ТДБ – 2 уровень

Расширяя границы доверенной загрузки

Доверие и защита платформы

- Защита UEFI BIOS
  - Защиту BIOS от перезаписи, чтения и от изменений EFI-переменных
  - 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 системных таблиц
  - Защита дисков от записи
  - Блокировка UEFI Option Rom
- Эмуляция NVRAM

Угрозы доверия к операционной системе и пользователю

УБИ.029: Угроза использования вычислительных ресурсов суперкомпьютера «паразитными» процессами

УБИ.067: Угроза неправомерного ознакомления с защищаемой информацией

УБИ.091: Угроза несанкционированного удаления защищаемой информации

УБИ.143: Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации

УБИ.161: Угроза чрезмерного использования вычислительных ресурсов суперкомпьютера в ходе интенсивного обмена межпроцессорными сообщениями

УБИ.170: Угроза неправомерного шифрования информации

ViPNet SafePoint

Средство защиты информации от несанкционированного доступа

Обеспечивает:

- Идентификацию и аутентификацию пользователей
- Контроль (разграничение) прав доступа пользователей
- Контроль целостности
- Контроль устройств
- Контроль запуска приложений и замкнутость программной среды

ИАФ | УПД | ЗНИ

АУД | ОЦЛ | ОПС

Сертификаты: ФСТЭК России – СВТ - 5 класс, СКН – 4 класса, ТДБ – 4 уровень

ViPNet SafePoint

- Контроль входа пользователей в систему
- Реализация замкнутой программной среды, разграничивает доступ к файлам
- Защита от олицетворения прав пользователя, тем самым не позволяет получать доступ к ПО и файлам от лица других пользователей системы
- Контроль и разграничение права на отключение и подключение к системе различных устройств
- Контроль целостности заданных файлов и объектов реестра ОС с возможностью автоматического восстановления их эталонного состояния в случае модификации

Дополнительные защитные механизмы

- Защита от внедрения и выполнения вредоносных программ и кода
- Защита от атак на повышение привилегий
- Защита данных от атак на уязвимости системного ПО
- Защита от инсайдеров
- Защита данных от атак на уязвимости прикладного ПО

Угрозы для рабочей станции при подключении Internet

УБИ.062: Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера

УБИ.098: Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб

УБИ.167: Угроза заражения компьютера при посещении неблагонадёжных сайтов

УБИ.175: Угроза «фишинга»

УБИ.178: Угроза несанкционированного использования системных и сетевых утилит

УБИ.170: Угроза неправомерного шифрования информации

ViPNet EndPoint Protection

Средство защиты АРМ и серверов, предназначенное для предотвращения «файловых» и сетевых атак, обнаружения вредоносных действий и реакции на эти действия.

Обеспечивает:

- Мониторинг и противодействие подозрительной активности на хосте
- Защиту от сетевых атак
- Защиту от внедрения и выполнения вредоносных программ и кода
- Контроль запуска приложений
- Поддержка Windows, Linux

СОВ ИНЦ АУД

Сертификаты (в процессе сертификации):
ФСТЭК России – МЭ типа «В» 4 класса, СОВ – уровня узла 4 класса, ТДБ – 4 уровень

ViPNet EndPoint Protection

infotecs

ViPNet EndPoint Protection

infotecs

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

ViPNet EndPoint Protection

infotecs

Обнаружение и предотвращение бесфайловых атак

- Расширение возможностей модуля обнаружения и предотвращения вторжений
- Отслеживаем техники Keylogging и Process injection

Эвристический Antimalware движок

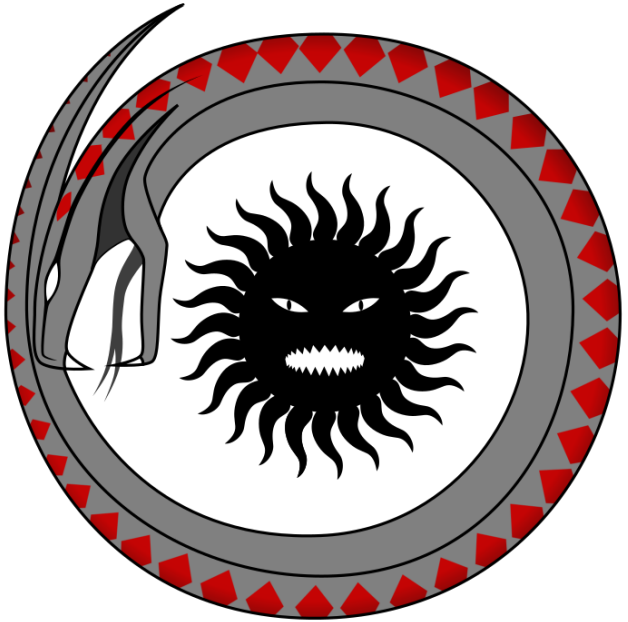
- Возможность сканирования исполняемых файлов и библиотек с целью выявления зловреда
- Эвристический Antimalware использует собственную модель построенную с помощью машинного обучения
- Модель постоянно обновляется в рамках подписки на БРП

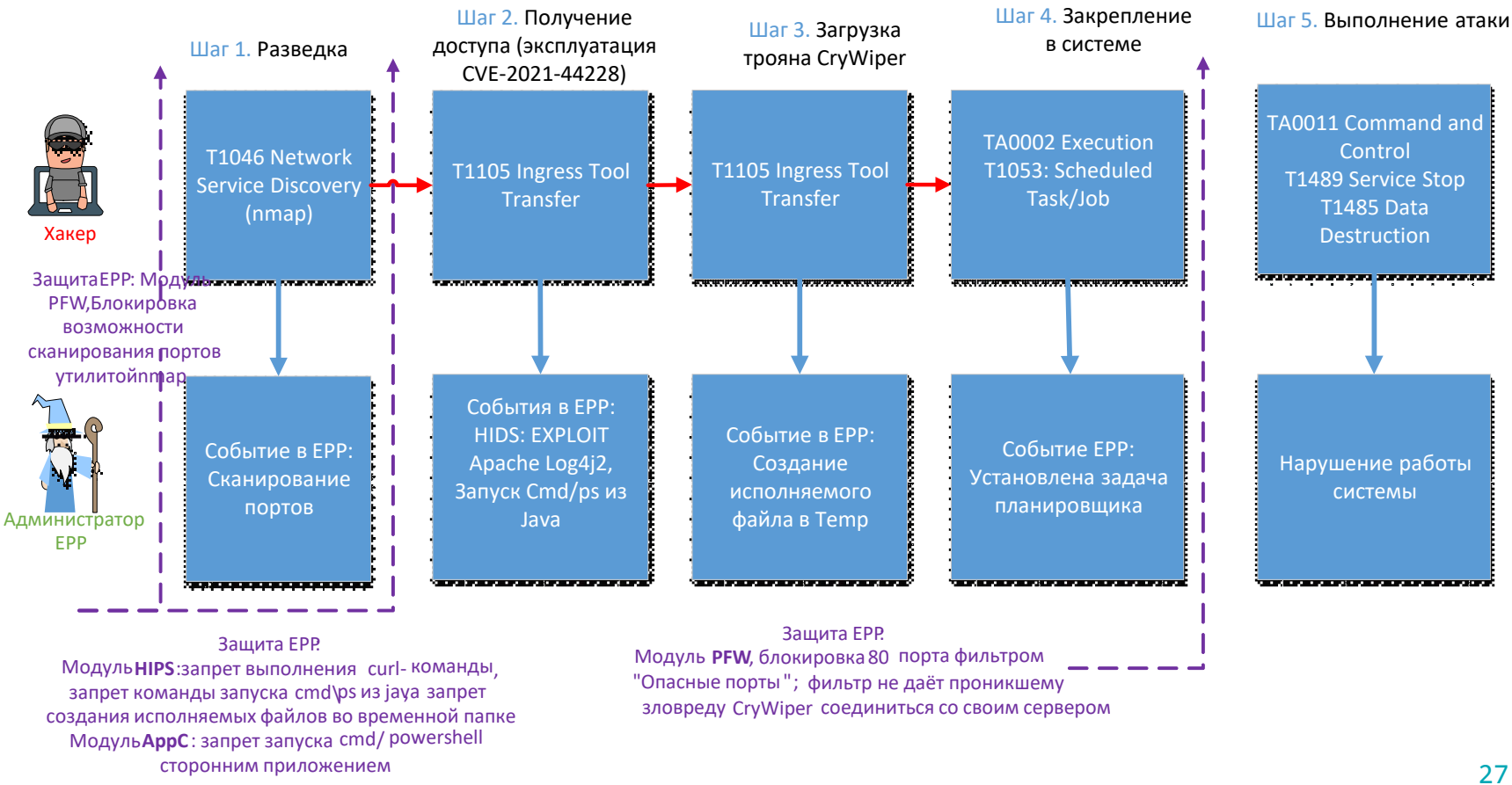
Дополнительные защитные механизмы

- Добавление набора функций из стека технологий ZTNA и интеграция с ViPNet Client 4U / 5:
  - Проверка соответствия хоста на наличие требуемого ПО, обновлений ПО, запущенных процессов, обновление антивирусных баз и т.д.
  - Блокировка защищенной сети на устройстве при несоответствии устройства политикам ZTNA, информирование пользователя об этом.

Пример: шифровальщик CryWiper

- Троян-шифровальщик CryWiper – «клиент-серверное приложение»
- Обнаружен – Лабораторией Касперского
- «Шифрует» данные навсегда, но требует выкуп
- Уничтожает данные при помощи случайной последовательности данных
- Запрещает доступ по RDP, чтобы быстро не решить проблему у удалённых сотрудников
- Активно атаковал системы госрганов




Шаг 1. Разведка
Шаг 2. Получение доступа (эксплуатация CVE-2021-44228)
Шаг 3. Загрузка трояна CryWiper
Шаг 4. Закрепление в системе
Шаг 5. Выполнение атаки
Хакер
T1046 Network Service Discovery (nmap)
T1105 Ingress Tool Transfer
T1105 Ingress Tool Transfer
TA0002 Execution T1053: Scheduled Task/Job
TA0011 Command and Control T1489 Service Stop T1485 Data Destruction
Защита EPP: Модуль PFW,Блокировка возможности сканирования портов утилитойnmap
Событие в EPP: Сканирование портов
События в EPP: HIDS: EXPLOIT Apache Log4j2, Запуск Cmd/ps из Java
Событие в EPP: Создание исполняемого файла в Temp
Событие EPP: Установлена задача планировщика
Нарушение работы системы
Администратор EPP
Защита EPP.
Модуль HIPS:запрет выполнения curl- команды, запрет команды запуска cmd\ps из jaya запрет создания исполняемых файлов во временной папке
Модуль AppC : запрет запуска cmd/ powershell сторонним приложением
Защита EPP.
Модуль PFW, блокировка 80 порта фильтром "Опасные порты"; фильтр не даёт проникшему зловреду CryWiper соединиться со своим сервером

Перечень угроз относящиеся к угрозам для рабочей станции

- **УБИ.003: Угроза использования слабостей криптографических алгоритмов и уязвимостей в программном обеспечении их реализации;**
- УБИ.036: Угроза использования слабостей протоколов сетевого/локального обмена данным;
- **УБИ.055: Угроза незащищённого администрирования облачных услуг;**
- УБИ.067: Угроза неправомерного ознакомления с защищаемой информацией;
- УБИ.069: Угроза неправомерных действий в каналах связи;
- УБИ.076: Угроза несанкционированного доступа к виртуальным каналам передачи

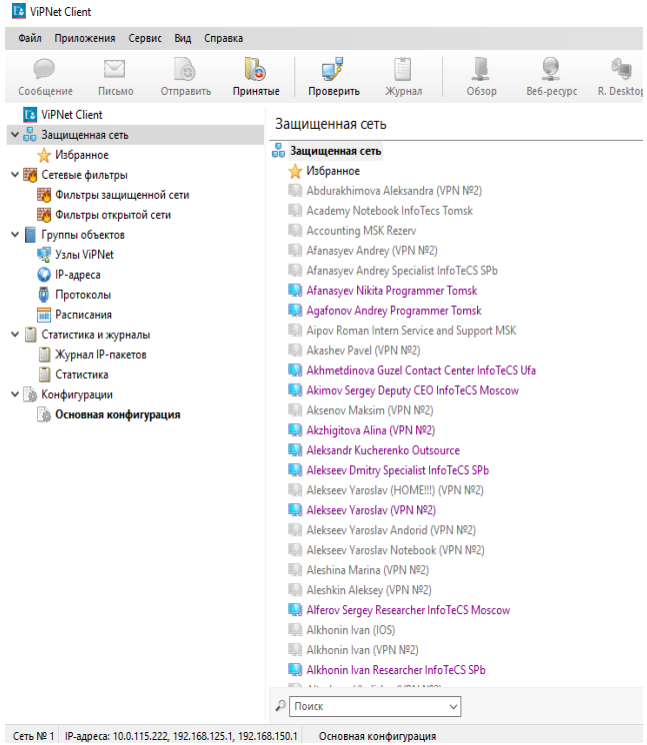
Что такое ViPNet Client

- VPN-клиент для работы в защищенных сетях ViPNet
- Прозрачен для приложений пользователя и сервисов ОС
- Независим от физических каналов связи
- Подключается к неограниченному количеству сегментов сети
- Соответствует требованиям **ФСБ России** к **СКЗИ** классов **КС1, КС2 и КС3**, в зависимости от варианта исполнения
- Соответствует требованиям **ФСТЭК** к **МЭ** класса **4** типа **В**
- Поддерживает ОС **Windows, Linux, macOS, Android, iOS, Aurora, Kaspersky OS***

ViPNet Client for **Windows** | ViPNet Client for **Linux** | ViPNet Client for **macOS** | ViPNet Client for **Android** | ViPNet Client for **iOS** | ViPNet Client for **Aurora**

* В разработке

ViPNet Client 4

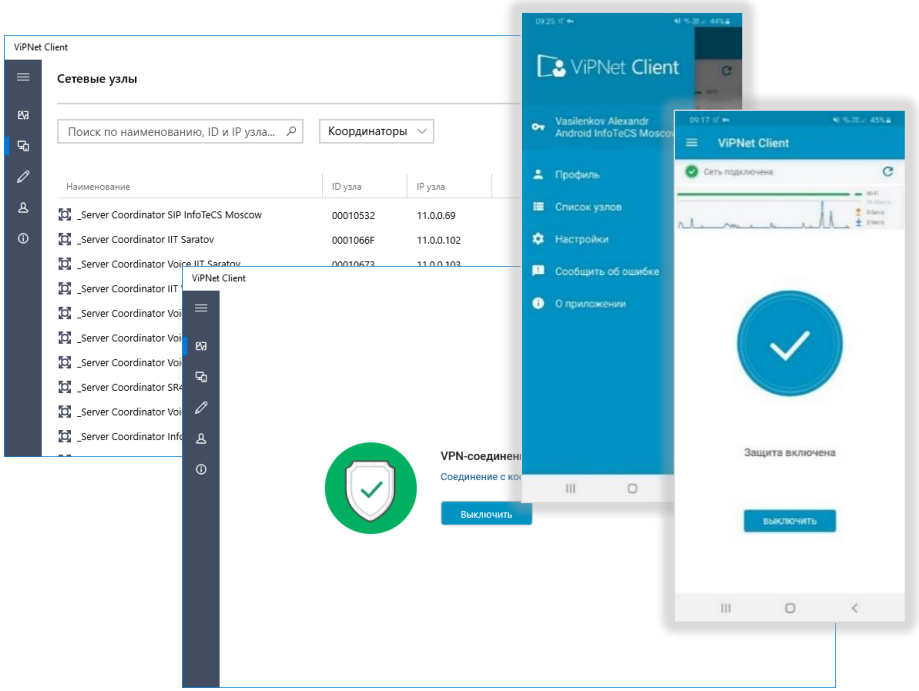


- VPN-соединение с использованием технологии ViPNet по IP адресу/DNS имени или внутреннему идентификатору узла сети ViPNet
- Двухфакторная аутентификация
- Прозрачен для приложений пользователя и сервисов ОС
- Совместим с ПО ViPNet «Деловая почта»
- Поддержку Windows, Linux, MacOS, Android, iOS, Aurora (Sailfish)

Сертификаты: ФСБ России - СКЗИ класса – КС1, КС2, КС3

ViPNet Client 4U

Поколение продукта ViPNet Client на базе единого универсального исходного кода



- Установка из магазинов приложений или из инсталлятора
- Двухфакторная авторизация
- Поддержка максимального количества ОС и архитектур
- SDK для сторонних приложений
- Совместим с ViPNet BM, CSS Connect, EPP
- Разрабатывается в соответствии с требованиями к СКЗИ классов КС1, КС2 и КС3

ViPNet Client 4U

ИАФ АУД ЗИС

Особенности поколения 4U продуктов:

- Централизованное управление тонкими настройками продукта через ViPNet Administrator/ViPNet Prime
- Интеграция с ViPNet EPP
- Сертифицируемые версии могут быть легитимно размещены в магазинах приложений
- Возможность блокировки открытого трафика при включенном VPN и фильтрация защищенного трафика (прием политик Policy Manager)

Сертификаты:

- ФСБ России - СКЗИ класса КС1-3 (for Linux)
- ФСБ России - СКЗИ класса КС1-3 (for Windows)
- ФСБ России - СКЗИ класса КС1 (for mobile)

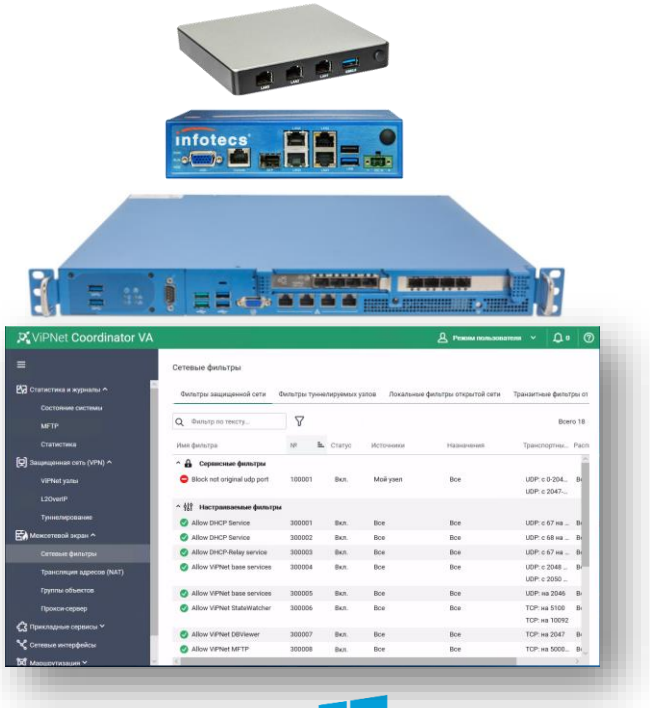
Перечень угроз относящиеся к угрозам для информационной системы

- УБИ.003: Угроза использования слабостей криптографических алгоритмов и уязвимостей в программном обеспечении их реализации;
- УБИ.034: Угроза использования слабостей кодирования входных данных;
- УБИ.073: Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети;
- УБИ.069: Угроза неправомерных действий в каналах связи;
- УБИ.16: Угроза перехвата данных, передаваемых по вычислительной сети;

ViPNet Coordinator HW

- Криптографическая защита каналов связи
- Межсетевое экранирование до 4 уровня модели OSI
- Сегментирование сети
- Сетевые и сервисные функции
- Доверенная платформа

ИАФ | УПД | АУД | ЗИС



Сертификаты:

ФСБ России - СКЗИ класса – КС1,КС3, МЭ – 4 класса
ФСТЭК России – МЭ типа «А», «Б» - 4 класса,
ТДБ - 4 уровень

ViPNet Coordinator HW

Криптографическая защита

- Защита каналов передачи данных с использованием алгоритмов ГОСТ
- Защита каналов связи при подключении к сетям общего пользования, в том числе беспроводных каналов связи
- Защищенный доступ удаленных и мобильных пользователей
- Соответствие требованиям ФСБ России

ViPNet Coordinator HW

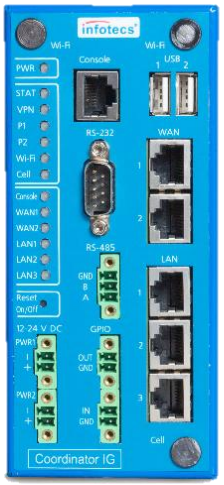
Межсетевое экранирование

- Фильтрация сетевых соединений и поддержка политик безопасности
- Защита периметра
- Сегментация сети, организация DMZ
- Сокрытие адресов и информации о структуре сети
- Создание безопасных соединений при выходе в Интернет
- Соответствие требованиям ФСТЭК России и ФСБ России

ИАФ | УПД | АУД | ЗИС | ОДТ

ViPNet Coordinator IG

- Криптографическая защита каналов связи
- Межсетевое экранирование
- Глубокая фильтрация промышленных протоколов
- Преобразование Modbus RTU/TCP
- Расширенный температурный диапазон работы



ИАФ | УПД | АУД | ЗИС | ОДТ

Сертификаты:

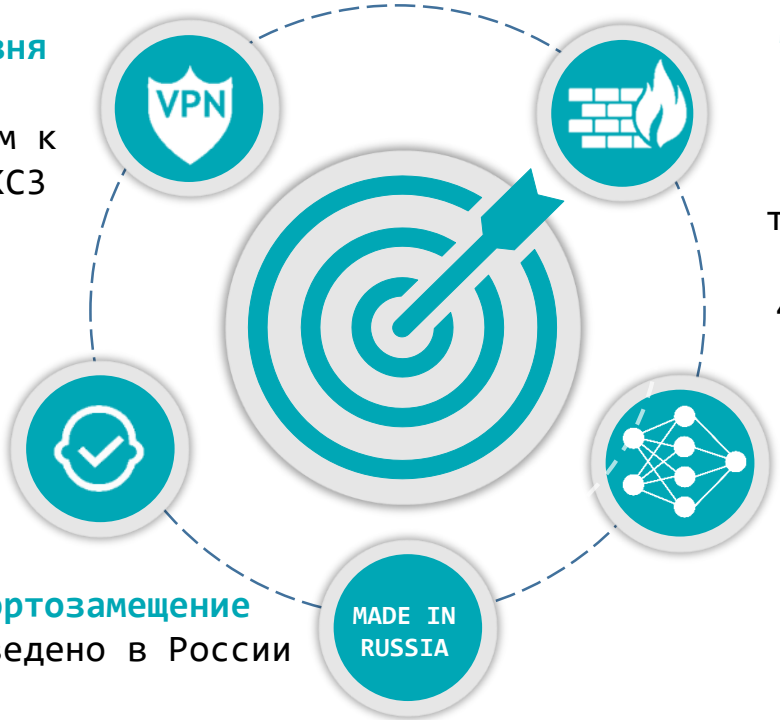
- ФСБ России - СКЗИ класса - КС3, МЭ – 4 класса
- ФСТЭК России – МЭ типа «А» и «Д» - 4 класса, ТДБ - 4 уровень

ViPNet Coordinator IG

VPN-шлюз уровня L3, L2
По требованиям к СКЗИ класса КС3

4 уровень доверия
по требованиям ФСТЭК России

Импортозамещение
Произведено в России



Межсетевой экран
Типа «А» 4 класса,
Типа «Б» 4 класса
Типа «Д» 4 класса по требованиям ФСТЭК России

4 класс защищенности по требованиям ФСБ России

Маршрутизатор, беспроводной роутер
Проводные,
4G/3G, Wi-Fi

ViPNet Coordinator IG100 I5

- Производительность L3 VPN – 60 Мбит/с
- Производительность МЭ – 60 Мбит/с
- Максимальное количество одновременных сессий – 15000
- Питание: 24В DC, PoE
- Ethernet: 2 x LAN 10/100BASE-T для подключения к локальной сети с возможностью питать PoE- устройства по стандартам IEEE 802.3af и IEEE 802.3at (PoE PSE)
- 1 x WAN 10/100BASE-T для подключения к внешней сети с возможностью получать питание по стандартам IEEE 802.3af и IEEE 802.3at (PoE PD)
- GSM-модуль (опционально) - LTE
- Wi-Fi 802.11 b/g/n 2,4 ГГц (опционально)
- Порты ввода-вывода: USB 2.0x2, RS-232/485
- Рабочая температура - -20⁰С* …+50⁰С
- ЭМС - ГОСТ Р51318-22 (СИСПР 22), ГОСТ CISPR 24 2013 (СИСПР 24)

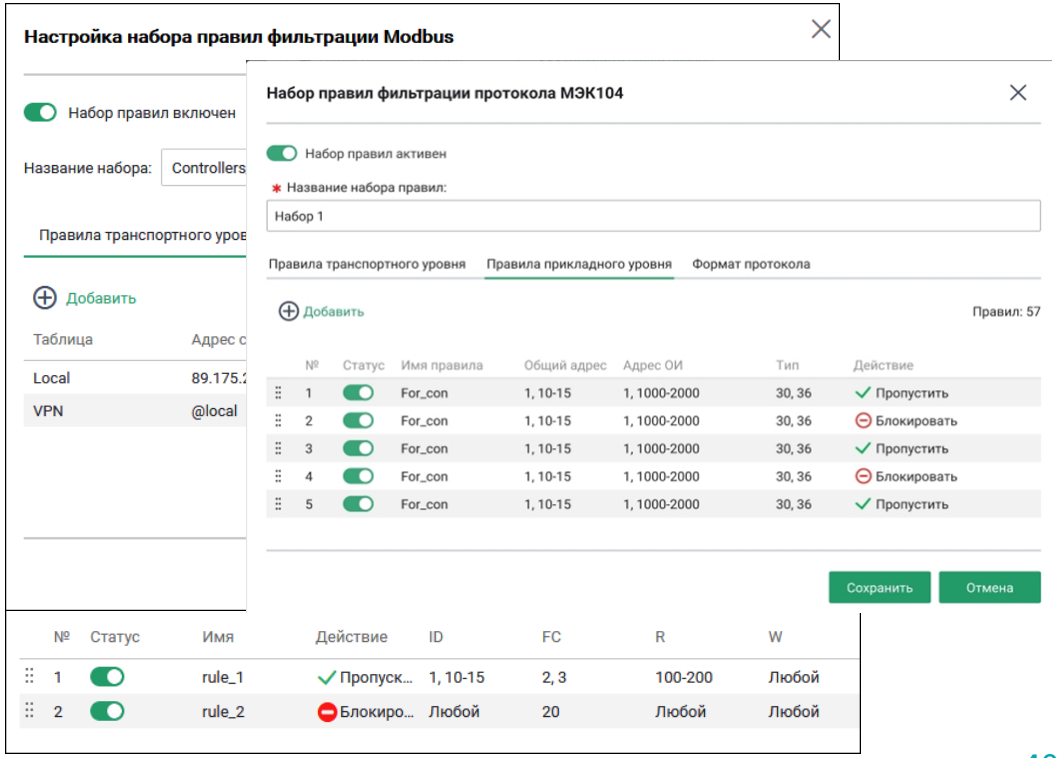
Фильтрация протоколов

Modbus

- Номер порта
- Адреса устройств
- Коды функций
- Регистры чтения и записи

МЭК 60870-5-104

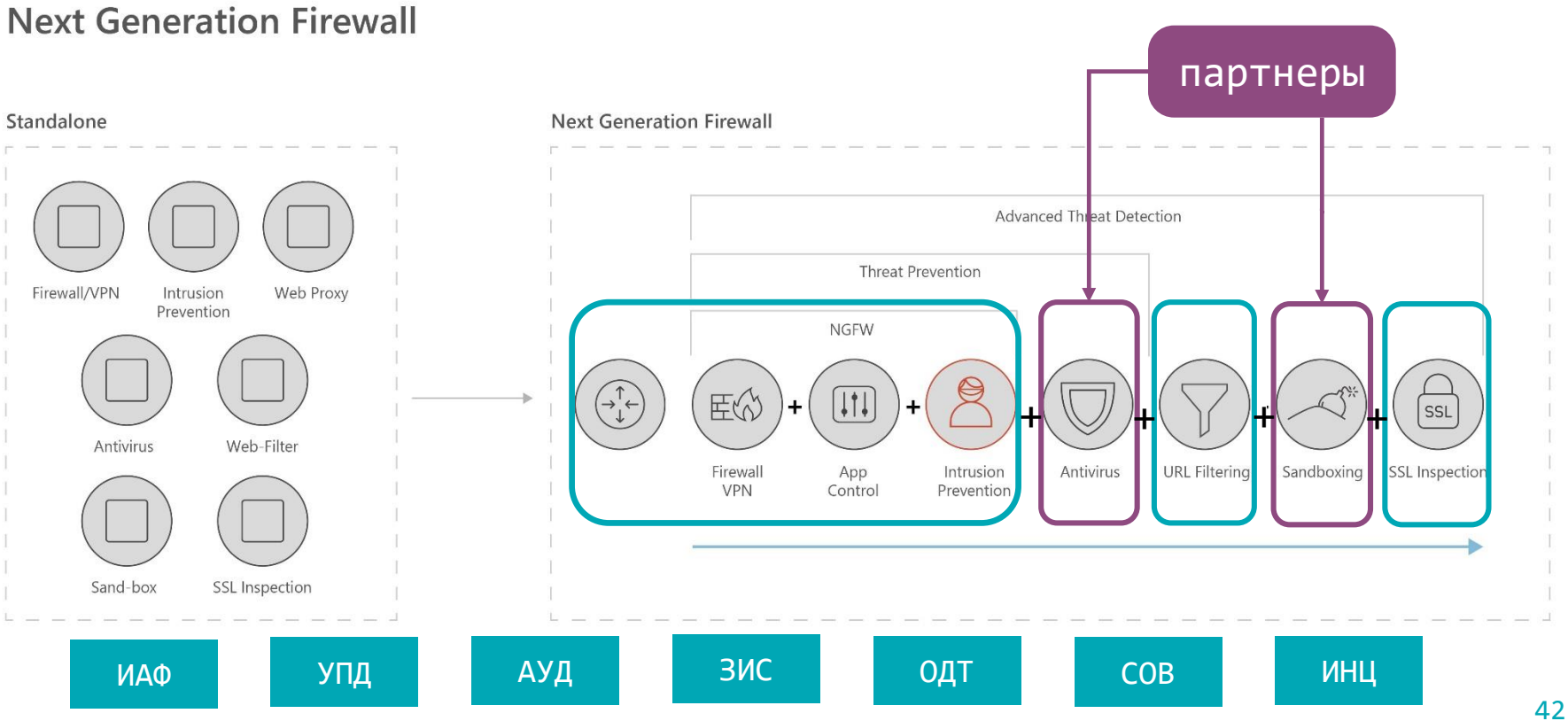
- Номер порта
- Идентификатор типа (Type Identifier)
- Адрес ASDU (ASDU Address)
- Адрес объекта информации (Information Object Address)



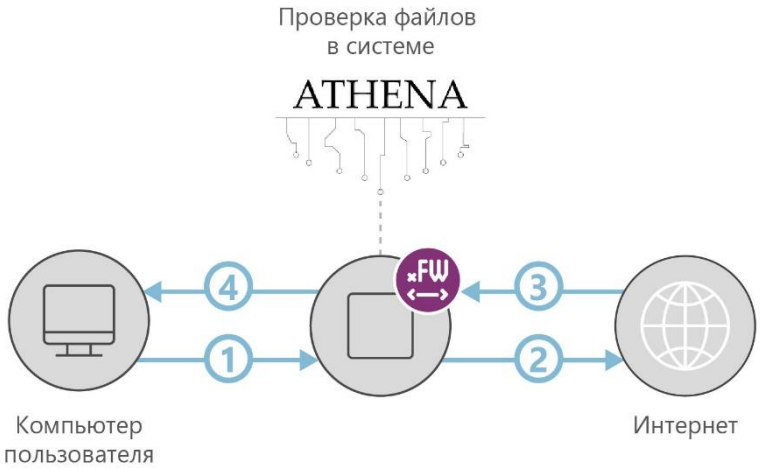
Перечень угроз относящиеся к угрозам для информационной системы

- **УБИ.012: Угроза деструктивного изменения конфигурации/среды окружения программ;**
- **УБИ.063: Угроза некорректного использования функционала программного и аппаратного обеспечения;**
- УБИ.068: Угроза неправомерного/ некорректного использования интерфейса взаимодействия с приложением;
- **УБИ.073: Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети;**
- УБИ.077: Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение;
- **УБИ.170: Угроза неправомерного шифрования информации**

ViPNet xFirewall



Поддержка песочниц



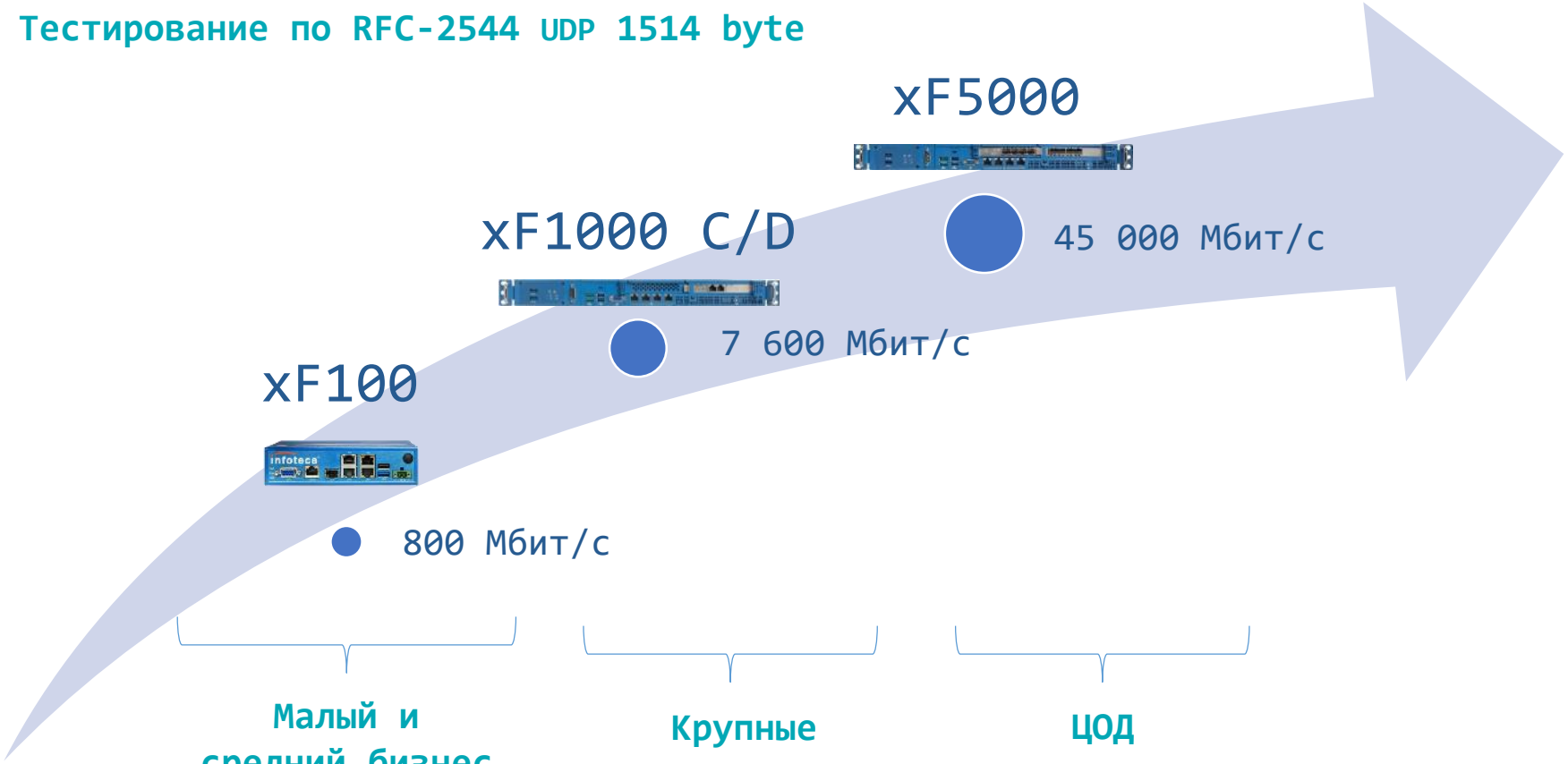
Тестировался сценарий проверки на содержание вредоносного контента файлов, загружаемых из сети Интернет в «песочницу» ATHENA через службу прокси-сервера xFirewall по протоколу ICAP

Межсетевой экран ViPNet xFirewall служит шлюзом между приложениями, функционирующими на узлах локальной сети, и внешними сетевыми ресурсами, к которым эти приложения обращаются (выполняет функции прокси-сервера)

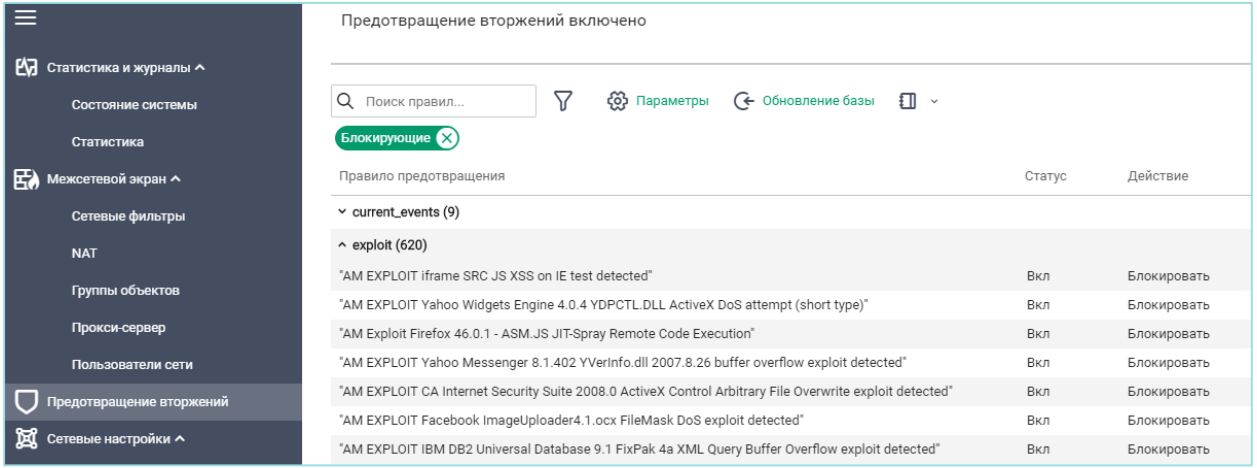
Система AVSOFT ATHENA работает на основе комбинации технологий мультисканера и «песочницы» для исследования файлов на подозрительное содержимое и поведение существенно повышает точность результата проверки

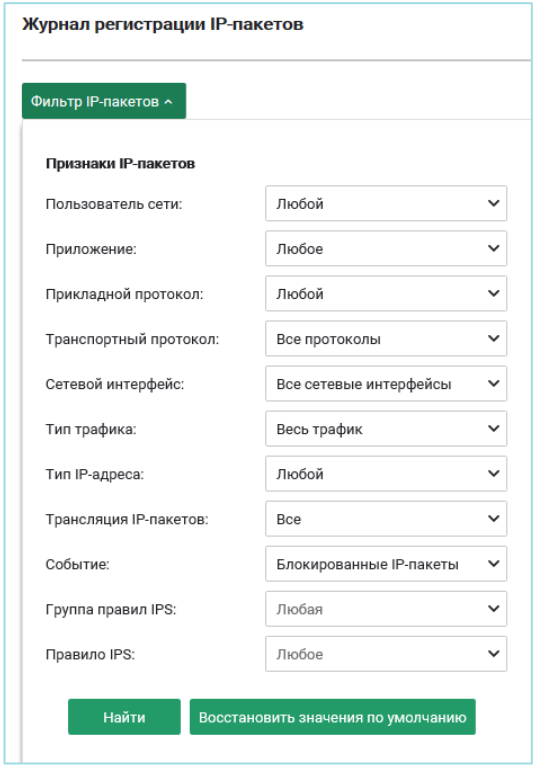
Модельный ряд xFirewall

Тестирование по RFC-2544 UDP 1514 byte



Система предотвращения вторжений

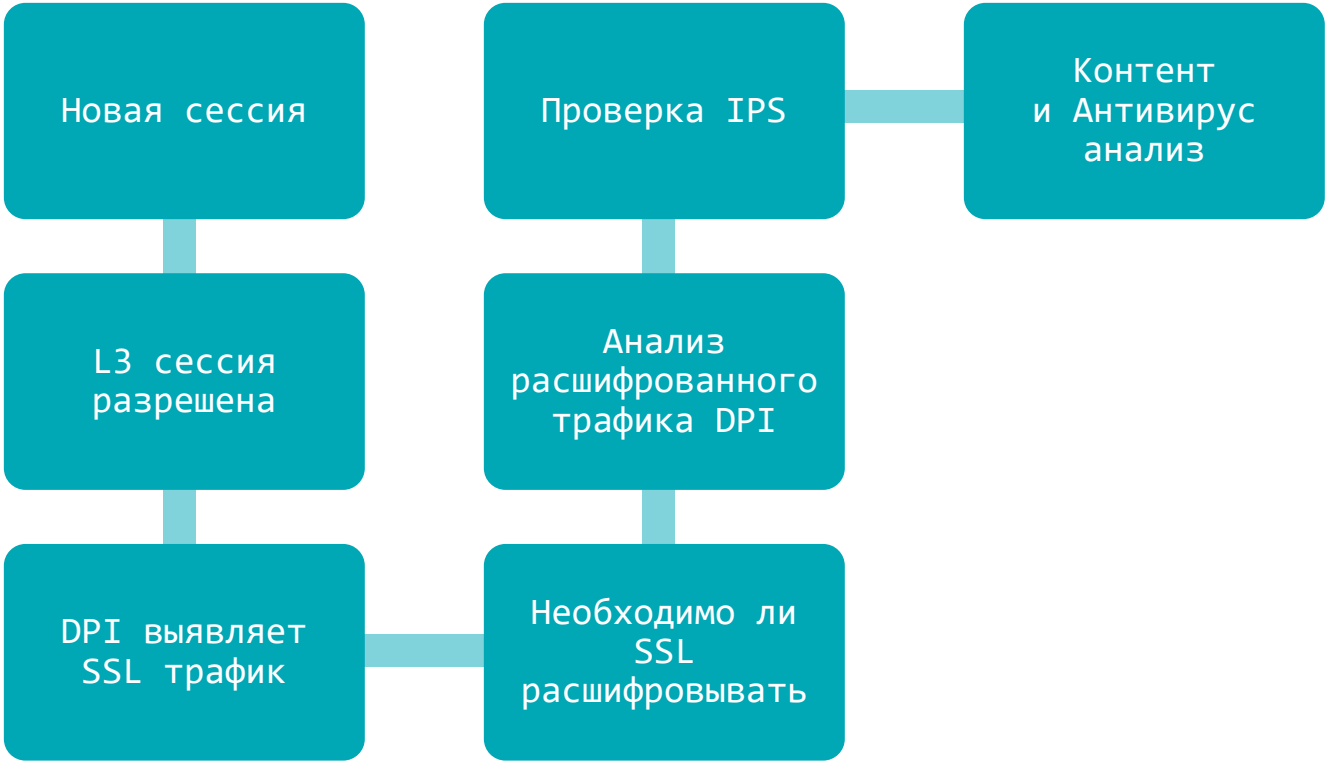




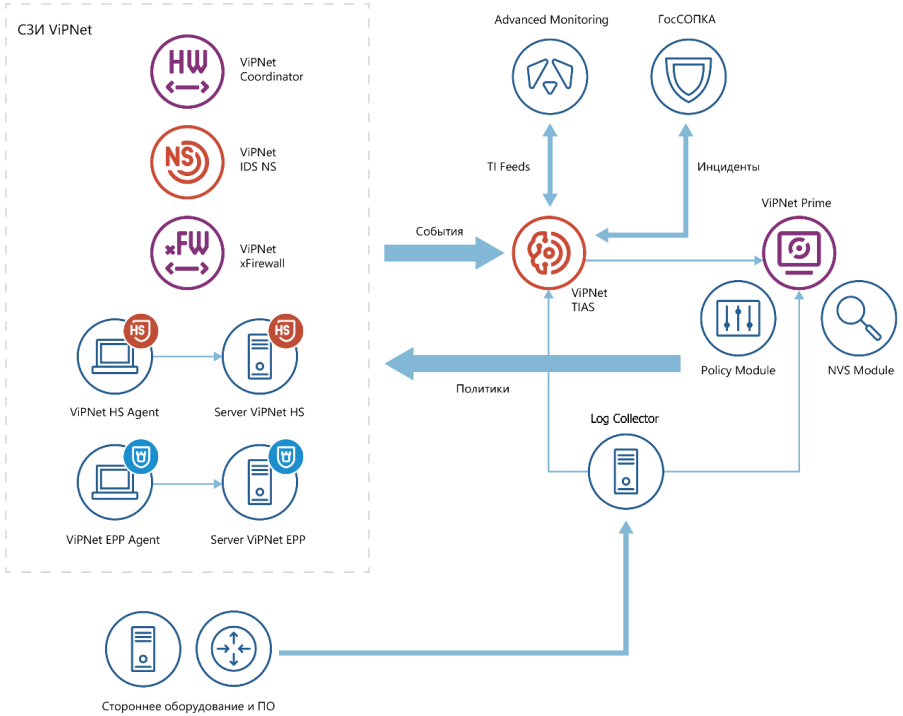
Классификация SSL

- Разрешить тот SSL-трафик, который известен:
  - Yandex, Google, Facebook и тд
- Блокировать известный SSL запрещенных политикой приложений: социальные сети, мессенджеры и тд
- Запретить любой неизвестный SSL-трафик

Схема проверки трафика

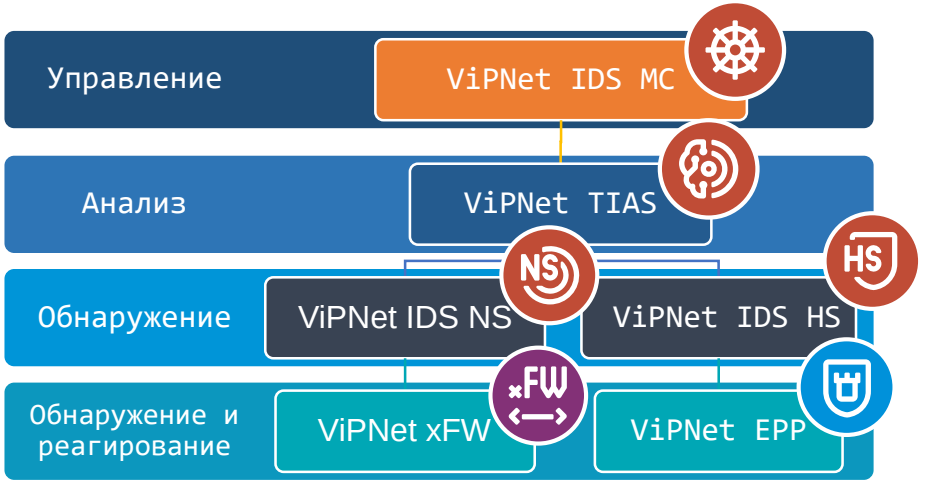


Обнаружение вторжений и угроз



- Выпущены официальные версии продуктов:
  - ViPNet IDS NS 3.8
  - ViPNet IDS MC 1.8
  - ViPNet TIAS 3.7.1
  - ViPNet IDS HS 1.5.2
  - Сертификация Q3 2022
- Поддержка новых вариантов исполнения:
  - ПАК ViPNet IDS NS 10000
  - ПАК ViPNet TIAS 10000
  - ViPNet IDS NS VA 100/500/1000/2000
- Новые возможности:
- ViPNet IDS NS:
  - DPDK
  - Возможность записи сетевой сессии
- ViPNet TIAS:
  - ViPNet EPP и ViPNet xFW в TIAS
  - Обогащение анализа в TIAS за счет использования данных от сканеров уязвимостей и IoC

Решение ViPNet TDR



ViPNet TIAS 3.8

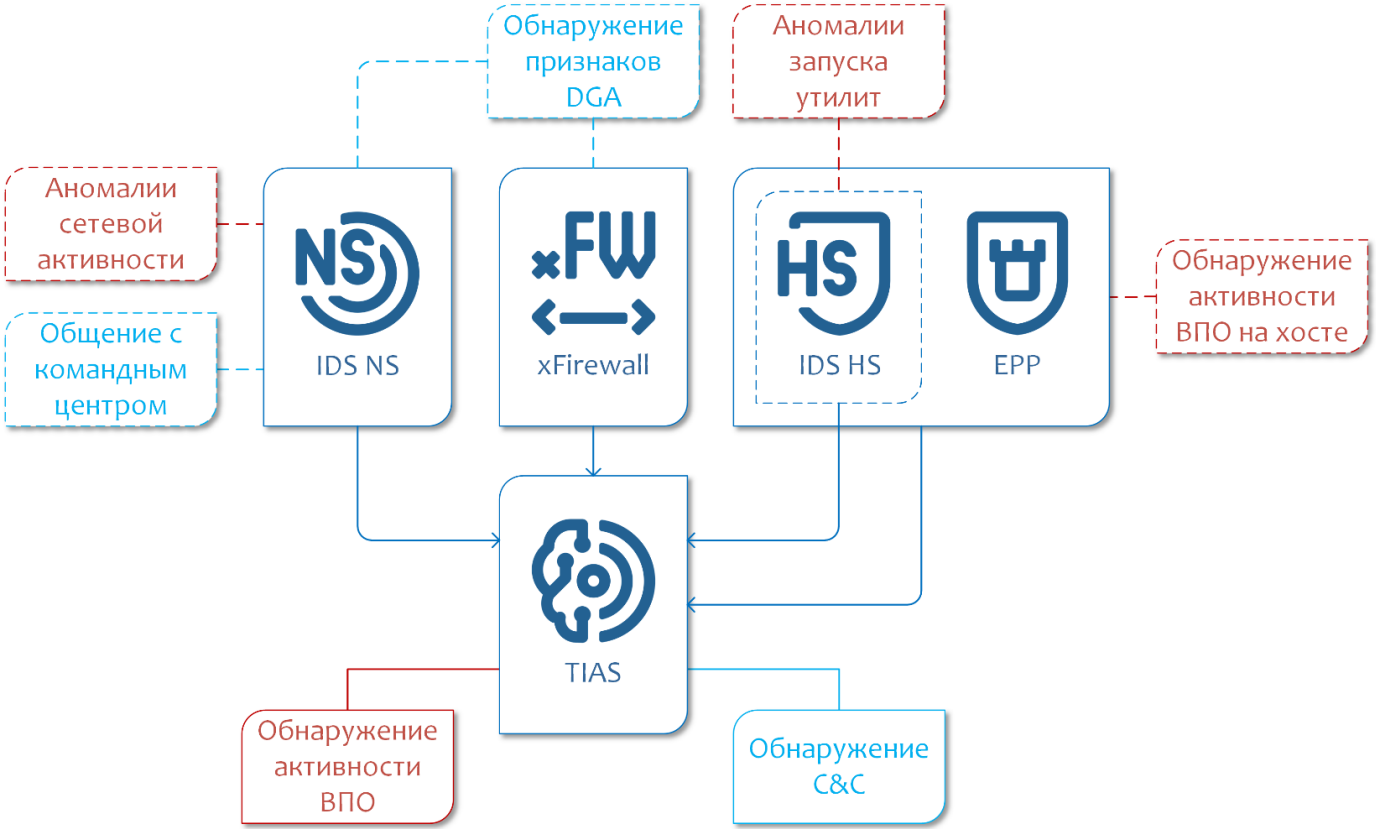
Основные улучшения и новые возможности

Пользовательские метаправила
возможность написания собственных правил анализа событий и выявления инцидентов

Дообучение модели
возможность дообучения модели машинного обучения как на новых экспертных данных, так и на размеченных данных пользователей

Новый источник событий
Прием и обработка событий ИБ, от шлюза безопасности ViPNet Coordinator HW 5

Модели машинного обучения



Спасибо за внимание!

Григорьев Дмитрий
gdw@infotecs.ru

Селифанов Валентин
Valentin.Selifanov@infotecs.ru

Иван Хабаров
Ivan.Khabarov@infotecs.ru

Подписывайтесь на наши соцсети

vk.com/infotecs_news

https://t.me/infotecs_official

rutube.ru/channel/24686363