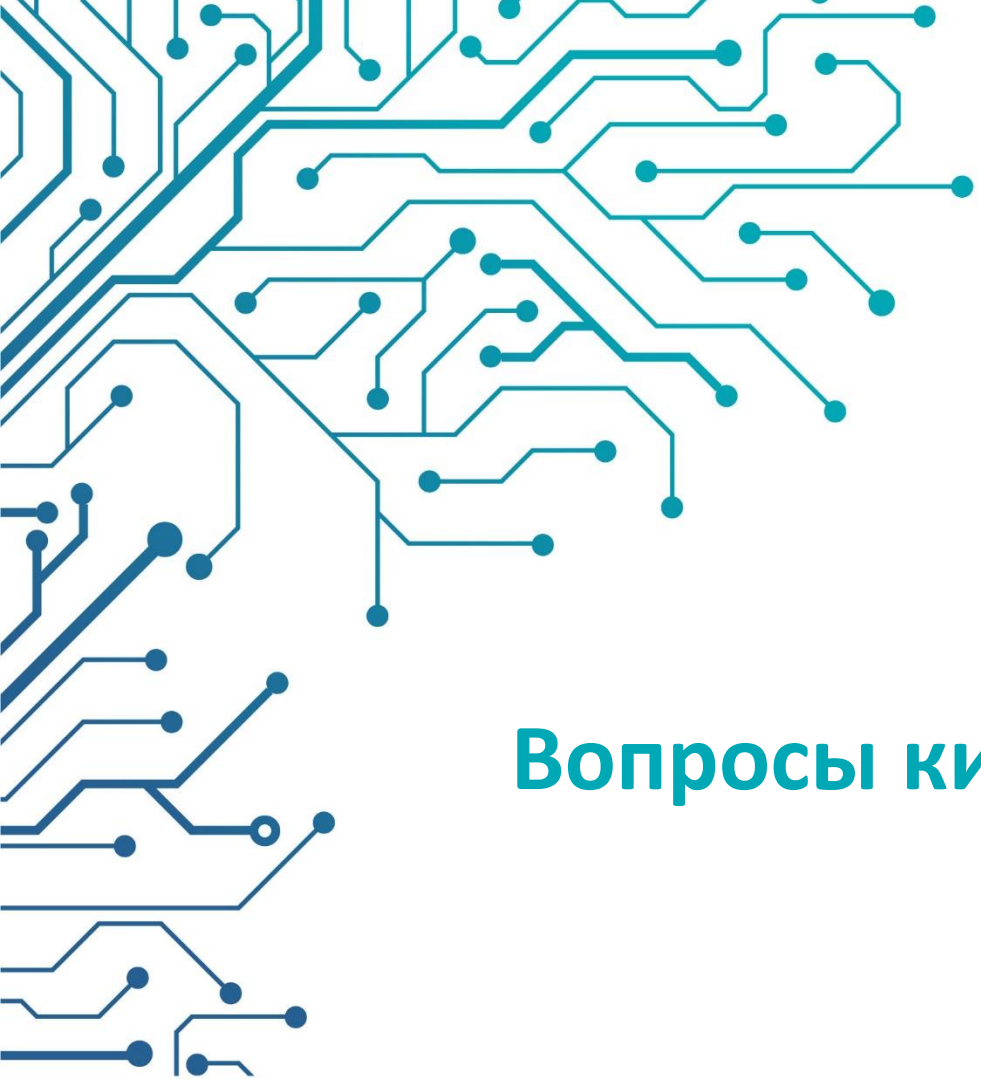


infotecs

Вопросы кибербезопасности в новых реалиях

Николай Смирнов

Программа мероприятия

- Текущие реалии
  - Немного по ситуации («Кто виноват»)
- Подходы и меры
  - Немного о реагировании («Что делать»)
- Детали и Подробности
  - Собственно, что можно сделать

Программа мероприятия

- Текущие реалии
  - Немного по ситуации («Кто виноват»)
- По
- Детали и Подробности
  - Собственно, что можно сделать

Докладчики:
Смирнов Николай
Виталий Беличко
Иван Кадыков
Светлана Старовойт

Программа мероприятия

- Текущие реалии
  - Немного по ситуации («Кто виноват»)
- По
- Детали и Подробности
  - Собственно, что можно сделать

На вопросы отвечают:
Алексей Данилов
Александр Василенков
Иван Дорошенко

Текущие реалии

Политика VS Экономика

- Маркс, Риски и Госрегулирование
- Госкапитализм – это оксюморон для широкого рынка
- Когда влияние гос. регулирования распространяется на все секторы, это не капитализм, это диктатура

Текущие реалии

Ситуация в РФ

- Отказ в обслуживании
- Нарушение цепочек поставок
- Целевые атаки и апдейт моделей нарушителя (внешняя мотивация)

Текущие реалии

Ситуация в РФ

- Отказ в обслуживании
- Немного вакуума вкупе с интенсификацией кибератак
- мотивация)

Подходы и меры

- **Оперативные**

  Обеспечение неразрывности бизнес-процессов

- **Стратегические**

  Прагматичный подход к выбору партнеров, поставщиков и импортозамещению

Подходы и меры

- Оперативные
  - Обеспечение неразрывности бизнес-процессов
- Стр
  - Пра
  - партнеров, поставщиков и импортозамещению

Чтобы не быть Капитаном Очевидность, предложение:


Защищенные коммуникации
Промышленная безопасность
Мобильная безопасность
Квантовое распределение ключей
Криптографические системы и сервисы
Защита рабочих станций и серверов
Защищенный документооборот
Защита каналов связи
Структура Продуктов
Крипто-графия
Фильтрация
Анализ
ViPNet VPN
L2
ML
Обнаружение вторжений и угроз

Подходы и меры

Оперативные

Защита каналов связи	Системы управления и мониторинга	Защита рабочих станций и серверов	Обнаружение и предотвращение компьютерных атак
• ViPNet Coordinator VA • ViPNet xFirewall VA • ViPNet TLS Gateway VA • ViPNet PKI Client • ViPNet Client	• ViPNet Administrator • ViPNet Policy Manager	• ViPNet SafeBoot • ViPNet SafePoint • ViPNet IDS HS*	• ViPNet TIAS VA • ViPNet IDS MC VA • ViPNet IDS NS VA • ViPNet IDS HS*

Подходы и меры

Оперативные

Защита каналов связи	Системы управления и мониторинга	Защита рабочих станций и серверов	Обнаружение и предотвращение компьютерных атак
• ViPNet Coordinator VA • ViPNet xFirewall • ViPNet TLS Gateway VA • ViPNet PKI Client • ViPNet Client	• ViPNet Administrator	• ViPNet	• ViPNet TIAS VA • ViPNet IDS MC • ViPNet IDS NS VA • ViPNet IDS HS*

Лицензии на перечисленные продукты предоставляются безвозмездной основе на 6 месяцев

Подходы и меры

Оперативные

Защита каналов связи	Системы управления и мониторинга	Защита рабочих станций и серверов	Обнаружение и предотвращение компьютерных атак
• ViPNet Coordinator VA • ViPNet xFirewall V • ViPNet TLS Gateway VA • ViPNet PKI Client • ViPNet Client	• ViPNet Administrator	• ViPNet	• ViPNet TIAS VA • ViPNet IDS MC VA • ViPNet IDS NS VA • ViPNet IDS HS*

sos@infotecs.ru

Подходы и меры

Оперативные

Защита каналов связи	Системы управления и мониторинга	Защита рабочих станций и серверов	Обнаружение и предотвращение компьютерных атак
• ViPNet Coordinator VA • ViPNet xFirewall V • ViPNet TLS Gateway VA • ViPNet PKI Client • ViPNet Client	• ViPNet Administrator	• ViPNet	• ViPNet TIAS VA • ViPNet IDS MC VA • ViPNet IDS NS VA • ViPNet IDS HS*

infotecs

infotecs

Переходим к деталям по продуктам

Спасибо за внимание

ViPNet Coordinator VA

Виртуализированный шлюз безопасности

Беличко Виталий

ViPNet Coordinator HW-VA

Поддерживаемые платформы виртуализации:

- VMware ESXi 6.7
- VMware Workstation 12.x
- Microsoft Hyper-V 10.0
- Oracle VM VirtualBox 5.x

Ограничения:

- Для шифрования трафика можно использовать не более 2-х CPU
- Число туннелей задается в ЦУС (лицензируется)
- Не сертифицировано

ViPNet Coordinator VA

- Защита данных внутри виртуальной и облачной инфраструктуры
- Функциональность, соответствующая аппаратным шлюзам
- Удобство управления и скорость развертывания
- Отсутствие дополнительных затрат на размещение и обслуживание оборудования
- Поддержка распространённых систем виртуализации
- Гибкое лицензирование и быстрое масштабирование

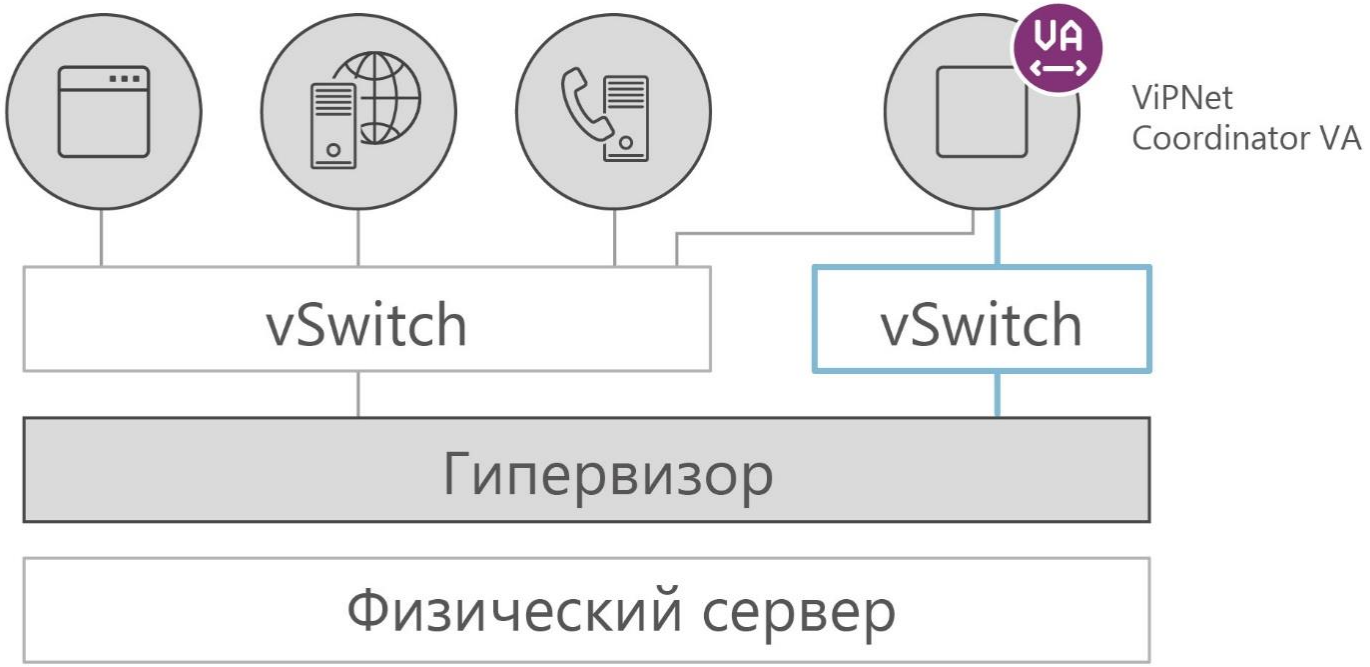
Сертификация

- **ViPNet Coordinator VA** - исполнение ViPNet Coordinator HW 4
- **ФСБ России** – действующий сертификат до 01.06.2024 г.
  - СКЗИ класса КС1
- **ФСТЭК России** – подготовка отчетных материалов в ИЛ*
  - Межсетевой экран тип «Б» 4 класса
  - 4-й уровень доверия средств защиты информации
- **Минцифры России** – в Реестре российского ПО

* Статус сертификации на 28.03.2022

Сценарии использования

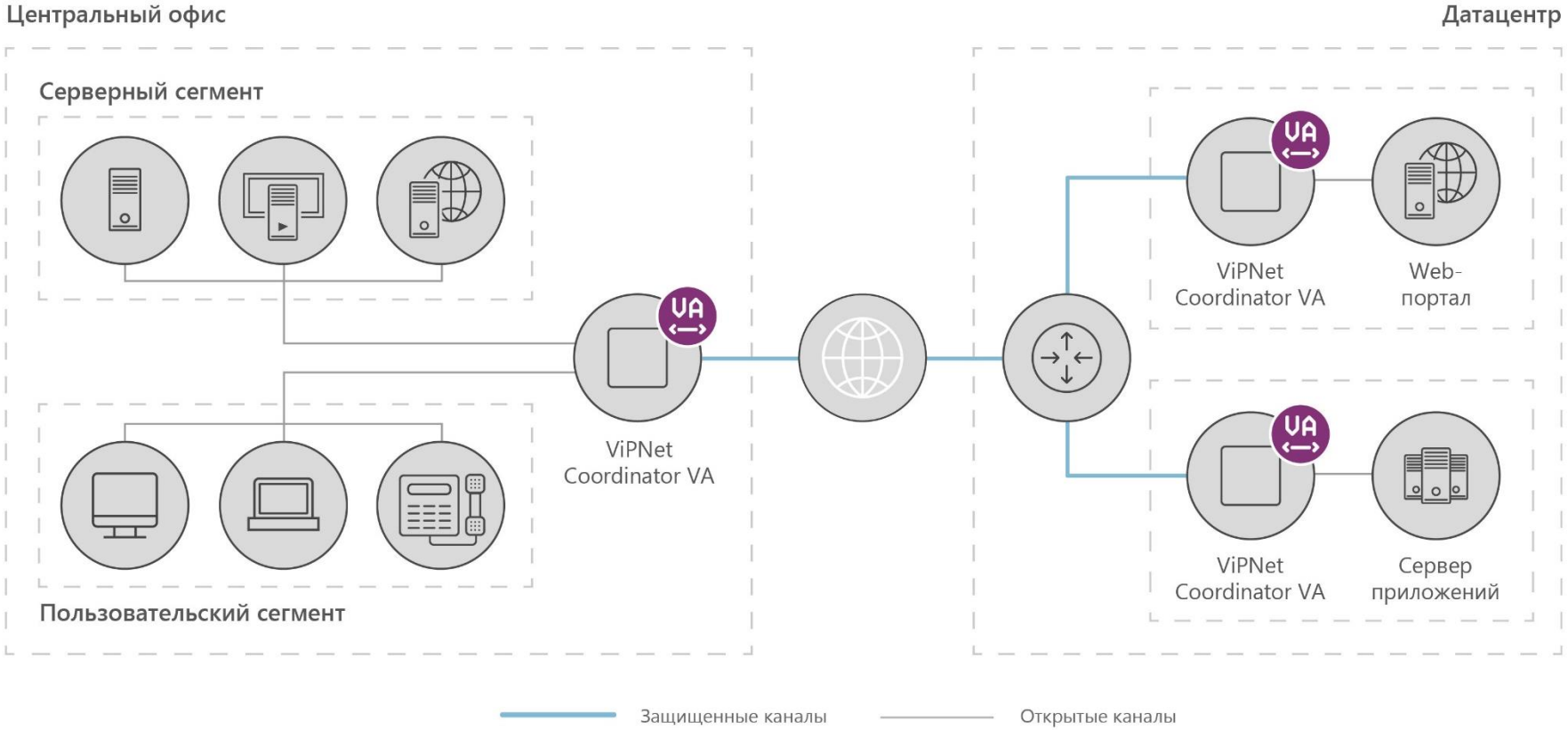
Сетевая безопасность внутри виртуальной инфраструктуры



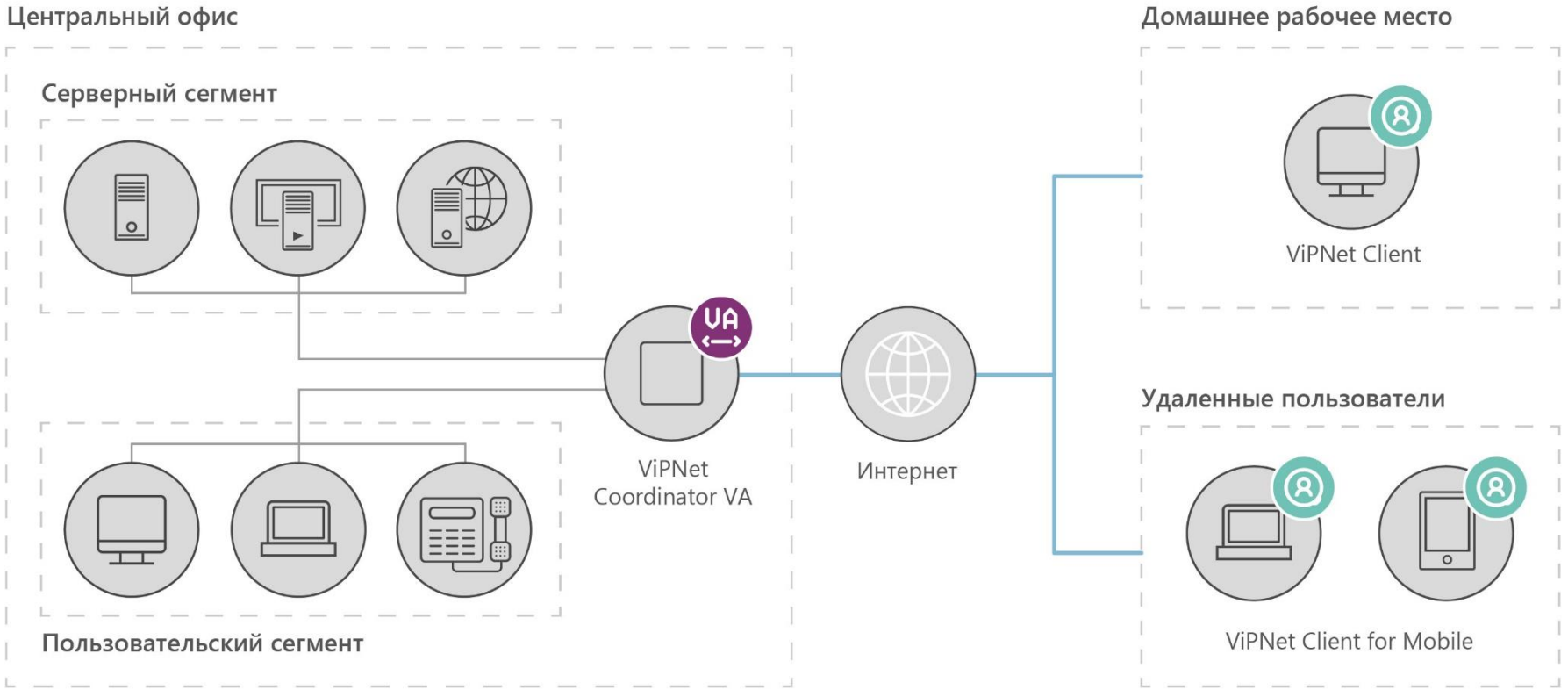
Защищенные каналы

Открытые каналы

Сегментация сетей и безопасность частного облака



Безопасное удаленное подключение



ViPNet Client

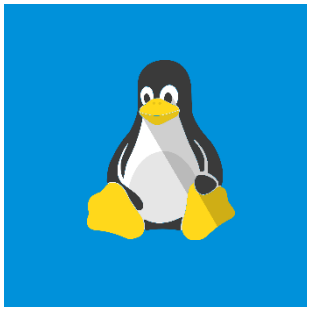
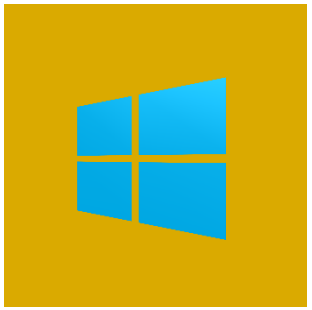
- VPN-клиент для работы в защищенных сетях ViPNet
- Прозрачен для приложений пользователя и сервисов ОС
- Независим от физических каналов связи
- Подключается к неограниченному количеству сегментов сети
- Имеет сертификаты ФСБ России на СКЗИ по классам от КС1 до КС3
- Поддерживает ОС Windows, Linux, MacOS, Android, iOS, Aurora

ViPNet Client for Windows | ViPNet Client for Linux | ViPNet Client for Android | ViPNet Client for iOS | ViPNet Client for MacOS | ViPNet Client for Aurora

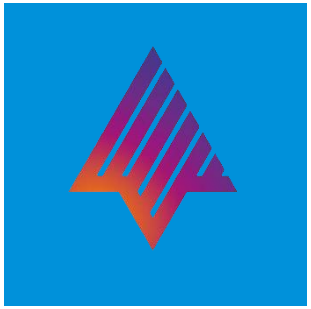
ViPNet Client и многообразие ОС

КОМПЬЮТЕРЫ
НОУТБУКИ

ТЕЛЕФОНЫ
ПЛАНШЕТЫ





Встраиваемая
версия
ViPNet Client

LINUX BASED

MIPS

МЦСТ
ЭЛЬБРУС

КОНТРОЛЛЕРЫ И КОНЕЧНЫЕ
УСТРОЙСТВА АВТОМАТИЗАЦИИ

Функциональные возможности

Функциональные возможности

VPN

- VPN-шлюз сетевого уровня (L3 VPN)
- VPN-шлюз канального уровня (L2OverIP VPN)
- Сервер IP-адресов
- Маскирование структуры трафика в UDP, TCP

МЕЖСЕТЕВОЙ ЭКРАН

- Межсетевой экран с контролем состояния сессий
- Раздельная фильтрация открытого и шифруемого IP-трафика
- NAT/PAT
- Прокси-сервер с ICAP

СЕТЕВЫЕ ФУНКЦИИ

- MultiWAN: Резервирование и балансировка
- Динамическая маршрутизация
- Политики маршрутизации (PBR)
- Поддержка VLAN
- Агрегирование сетевых интерфейсов
- Классификация и приоритизация трафика

СЕРВИСНЫЕ ФУНКЦИИ

- DNS-, DHCP-, NTP-сервер и DHCP-Relay
- Мониторинг по протоколу SNMP
- Экспорт событий по протоколу CEF
- Кластер горячего резервирования

Поддерживаемые гипервизоры

- KVM, QEMU-KVM и Libvirt
- VMware ESXi 6.5, 6.7, 7.0
- VMware Workstation 14.x, 15.x, 16.x
- Microsoft Hyper-V Server 2019
- Oracle VM Server 3.4
- Oracle VM VirtualBox 6.x

Лицензирование

Роль узла	Роль кластера	Макс. CPU	Кол-во туннелей
Coordinator VA100	Failover100	2	unlim
Coordinator VA500	Failover500	2	unlim
Coordinator VA1000	Failover1000	4	unlim
Coordinator VA2000	Failover2000	7	unlim

- Единый дистрибутив ПО для всех типов лицензий
- Возможность обновления лицензии VA100 → VA500 → VA1000 → VA2000
- Лицензии поддерживаются ПК ViPNet Administrator 4.6.4 и выше

Производительность

- Зависит от конфигурации хостовой машины и гипервизора

Тип лицензии	VA100	VA500	VA1000	VA2000
VPN, Мбит/с	180	580	1 400	4 000
МЭ, Мбит/с	330	940	3 500	5 500
Макс. количество сессий МЭ	150 000	500 000	1 000 000	3 000 000
Рекомендуемое число VPN-клиентов	100	500	1 000	2 000

*Условия измерений: VMware ESX 6.7, CPU Xeon E-2278GE

Комплект поставки

- Файл с образом виртуальной машины:
  - va_vipnet_**vhd**.tar.gz (для Microsoft Hyper-V)
  - va_vipnet_**raw**.tar.gz
  - va_vipnet_**qcow2**.tar.gz } (для развертывания в среде KVM)
  - va_vipnet_.**ova** (для в ESXi и остальных сред виртуализации)
- Файл обновления в формате LZH
- Документация в формате PDF
- Формуляр (в печатном виде)

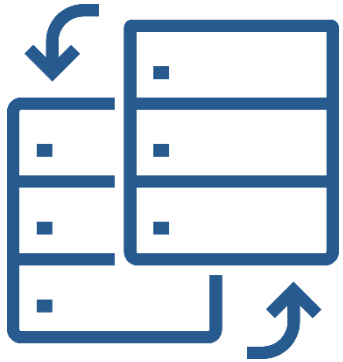
Новые версии

ViPNet Coordinator VA 4.5.2

- Кластер высокой доступности
- Новые возможности мониторинга
- Повышение безопасности сетевых протоколов
- Новые сервисные функции
- Улучшения веб-интерфейса

Кластер высокой доступности

- Быстрое переключение кластера по потере связи и питания
- Синхронизация сессий МЭ в кластере
- Виртуальный MAC-адрес для кластера
- Синхронизация времени пассивного узла кластера
- **Минимальное время переключения кластера сократилось до 1 секунды**

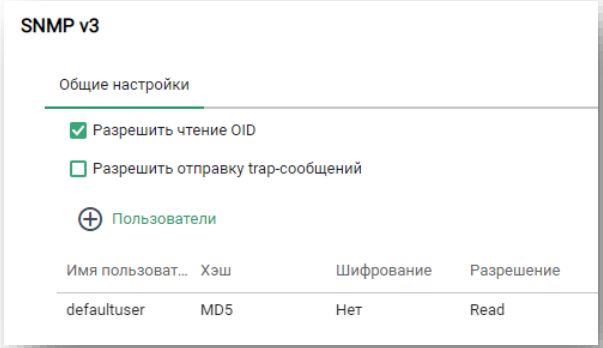


Новые возможности мониторинга

- Поддержка протокола SNMPv3 (+INFORM)
- Мониторинг пассивного узла кластера через SNMP
- Интеграция базы SNMP MIB в WebUI
- Утилизация сетевых интерфейсов в WebUI

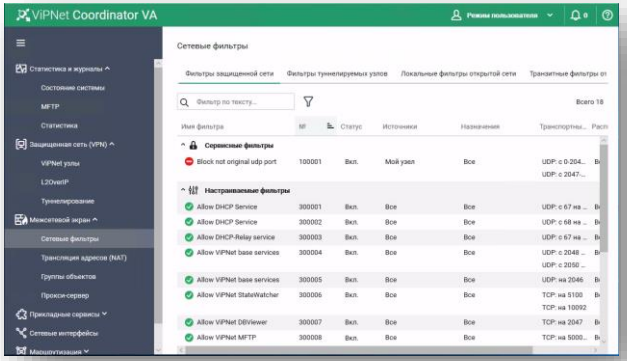
Повышение безопасности сетевых протоколов

- Поддержка протокола SNMPv3
  - Аутентификация и шифрование
- Работа веб-интерфейса по HTTPS (AES)
  - Самоподписанные и внешние сертификаты
- Поддержка аутентификации OSPFv2
  - Парольная и криптографическая аутентификация



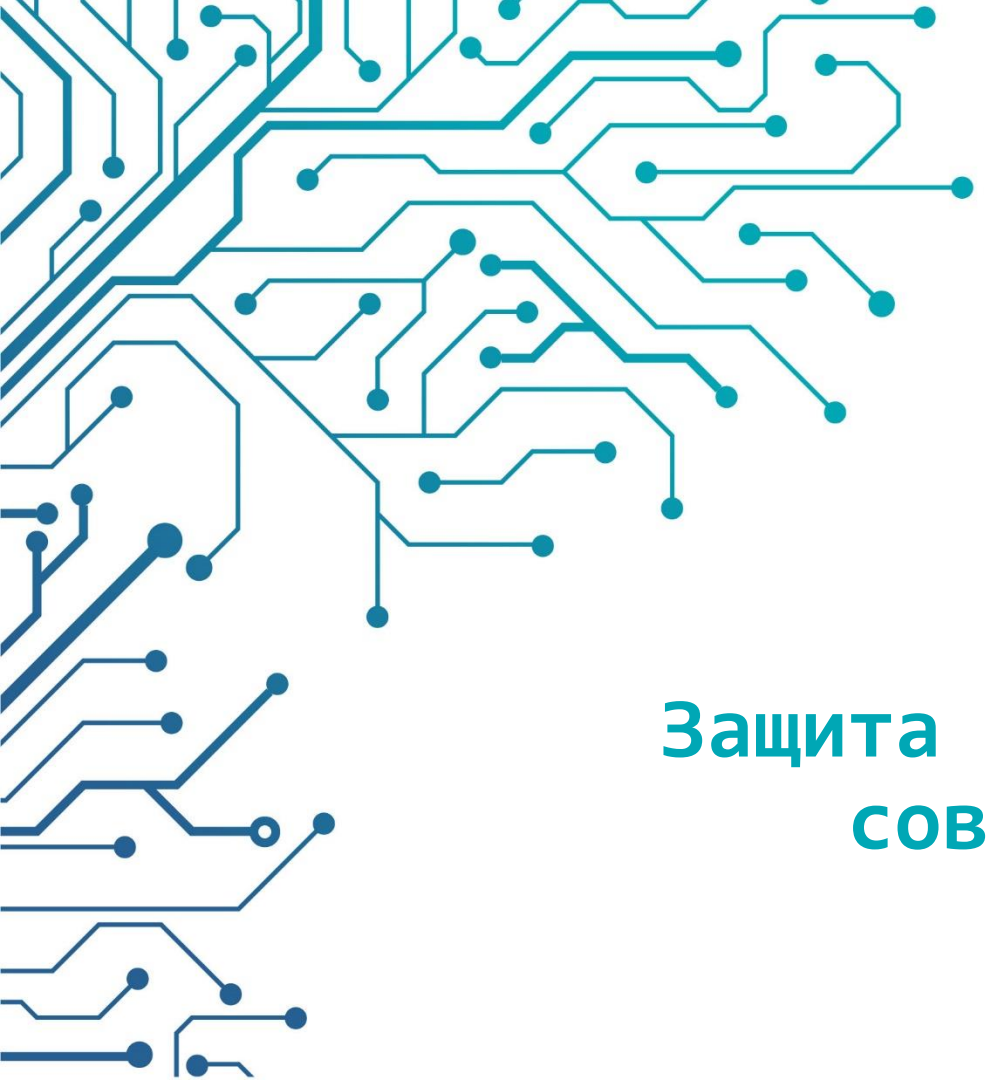
Улучшения веб-интерфейса

- Настройка видимости адресов
- Настройка туннелирования локальных адресов
- Настройка журнала регистрации IP-пакетов
- Проверка доступности сетевых адресов



Сервисные функции

- Возврат к заводским настройкам
- Отложенный старт основных служб
- Управление отпечатками SSH-ключей
- Локальное обновление справочников и ключей
- Управление перезагрузкой и службами ALG в WebUI



infotecs

Защита рабочих станций в современных условиях

Кадыков Иван
Руководитель направления

Доверие

Доверие – это убежденность в чьей-нибудь честности, порядочности, веры в искренность и добросовестность кого-нибудь.

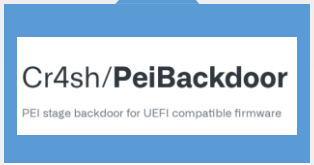
Доверие к платформе и загружаемой операционной системе

- Уверенность в платформе:
  - Неизменность BIOS
  - Аппаратных составляющих
  - Защита от bootkit и rootkit
- Доступ к платформе должен получить только легитимный пользователь
- Должна загружаться только доверенная операционная система с установленными СЗИ

Зловреды, атаки, уязвимости…

infotecs

2016



PeiBackdoor – один из первых «зловредов» для UEFI

2018

Lojax – первый rootkit найденный сотрудниками компании ESET в «дикой среде».

2020

MosaicRegressor – bootkit найденный сотнудниками «Лаборатории Касперского», предназначенный для шпионажа

BootHole - уязвимость в загрузчике

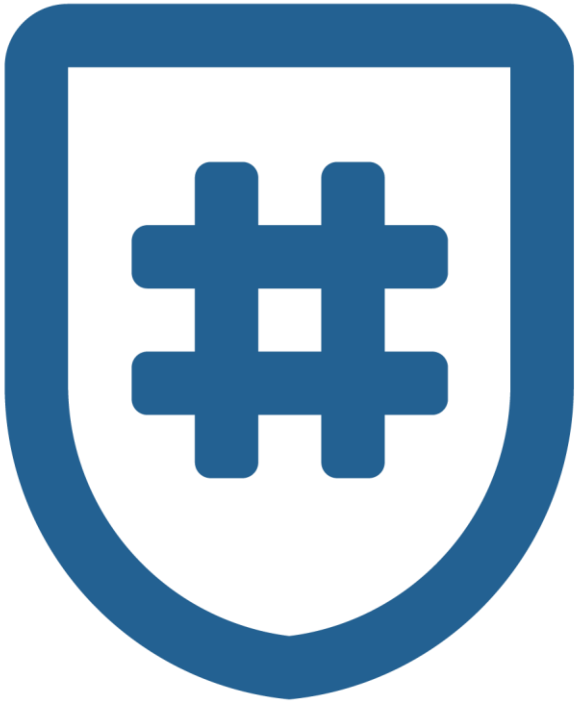
2021

ESPecter bootkit предназначенный для целевых атак и шпионажа (найден сотрудниками ESET)

2022

MoonBounce – позволяет изменить цепочку выполнения команд в UEFI BIOS и осуществить внедрение вредоносного кода, который запуститься при старте машины.

ViPNet SafeBoot

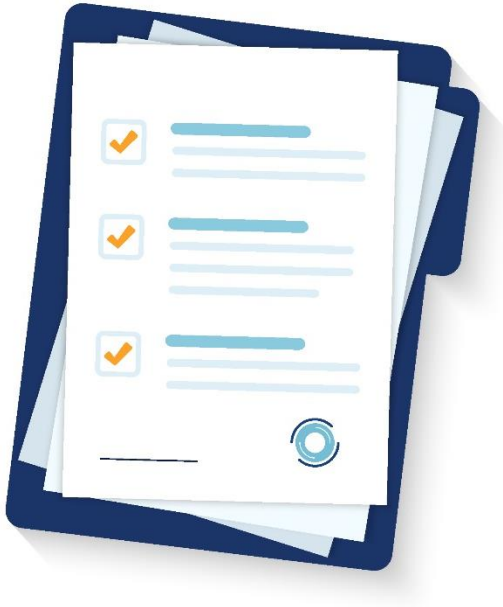


Высокотехнологичный программный модуль доверенной загрузки, устанавливаемый в UEFI BIOS различных производителей. Предназначен для защиты компьютеров и серверов (в т.ч. и серверов виртуализации) от современных угроз НСД, связанных с загрузкой ОС и атак на сам BIOS.

Решаемые задачи ViPNet SafeBoot

Доверие к операционной системе и пользователю

- Каждый пользователь должен работать только в созданном информационном пространстве, в соответствии со своей матрицей доступа
- Исключение злонаправленных действий пользователей (хищение данных, с целью передачи третьим лицам)
- Контроль подключения внешних устройств
- Регулярный контроль целостности критически важных объектов ОС
- Контроль службы обновлений операционной системы и программного обеспечения



ViPNet SafePoint

Средство защиты информации от несанкционированного доступа, устанавливаемое на рабочие станции и сервера, предназначенное для мандатного и дискреционного разграничения доступа к критически важной информации.

Реализована разграничительная (пользователя к объектам) и разделительная (между пользователями) политика доступа, основанная на автоматической разметке создаваемых файлов.

Ключевые решаемые задачи

Идентификация и аутентификация пользователей

Дискреционный контроль доступа пользователей

Замкнутая программная среда

Контроль подключаемых устройств

Контроль целостности программной среды

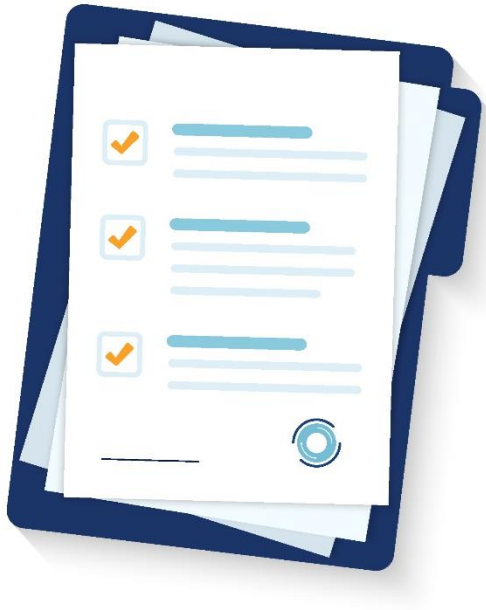
СЗИ от НСД может заменить

infotecs

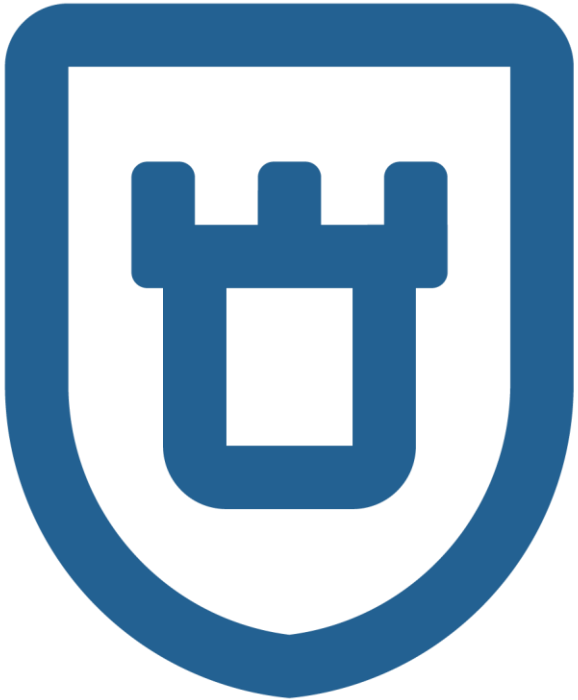
- Application Control
- Device Control
- Identity and Access Management
- Privileged users management (PUM)
- Data Integrity Control

Защита от внешних нарушителей и угроз

- Мониторинг и противодействие подозрительной активности на хосте
- Защита и предотвращение сетевых атак
- Защита от внедрения и выполнения вредоносных программ и кода
- Защита легитимных процессов



ViPNet EndPoint Protection



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

Ключевые защитные механизмы

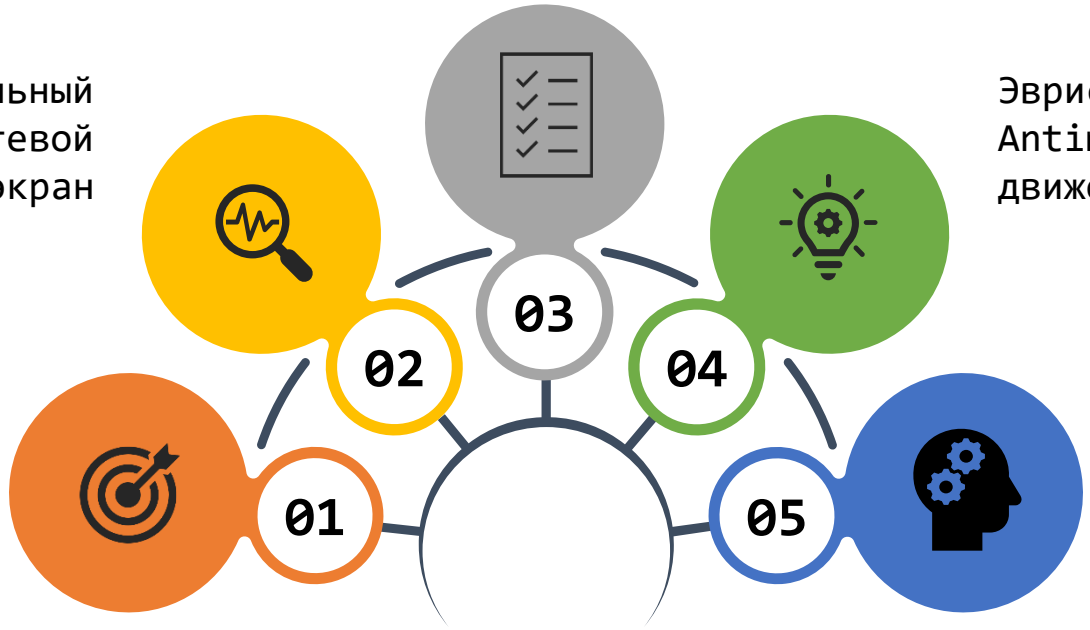
Контроль приложений

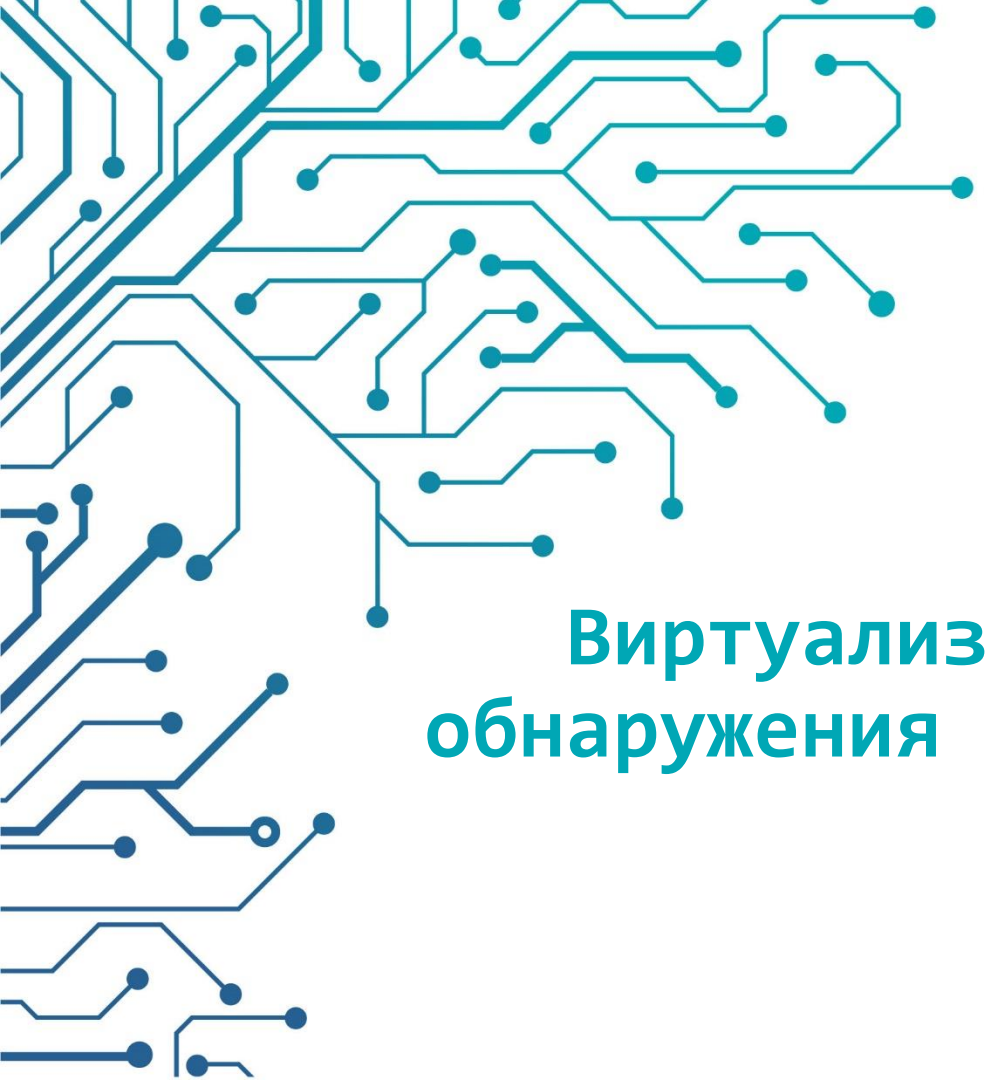
Персональный межсетевой экран

Эвристический Antimalware движок

Система обнаружения и предотвращения вторжений

Модуль поведенческого анализа





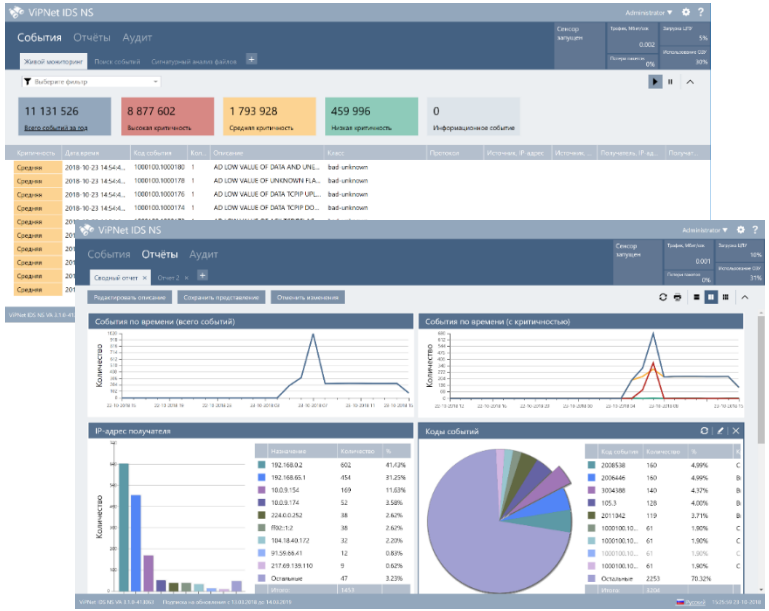
Виртуализированная система обнаружения компьютерных атак (вторжений)

Старовойт Светлана

infotecs

ViPNet IDS NS VA

ViPNet IDS NS VA



Сигнатурные методы анализа:

- Анализ трафика с помощью баз решающих правил (SNORT)
- Анализ трафика на наличие вредоносных файлов (Malware detection)

Эвристический анализ:

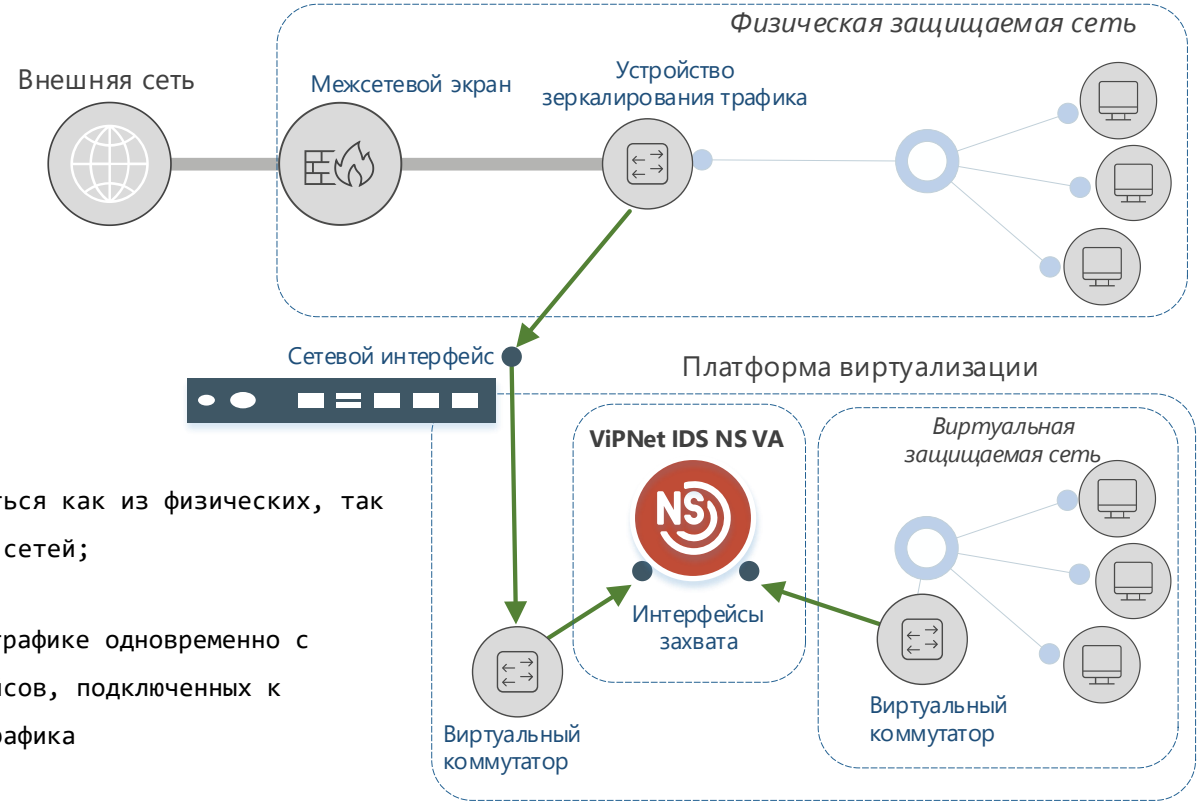
- отслеживание отклонений параметров сетевого трафика от эталонной модели.
- анализ служебных полей заголовков протоколов на наличие аномалий (RPC, HTTP, SMTP, FTP, SSH, MODBUS, GTP, SIP, Telnet, TCP, SSL, IMAP, DNS, DNP3, MODBUS, POP),
- отслеживание ARP-spoofing

Передача данных во внешние системы:

- CEF 2.0
- Syslog (RFC 5424)
- Netflow
- SNMP v2, v3

ViPNet IDS NS VA = ПАК ViPNet IDS NS

Анализ трафика физической и виртуальной сети



- сбор трафика может выполняться как из физических, так и из виртуальных локальных сетей;
- сбор информации о сетевом трафике одновременно с нескольких сетевых интерфейсов, подключенных к устройствам дублирования трафика

Поддерживаемые платформы виртуализации

- VMware ESXi / vSphere – версия 6.7.
- VMware Workstation Pro – версия 15.5.6.
- Oracle VM VirtualBox – версия 6.0.14.
- Oracle Virtual Server 3.4.6
- Платформы виртуализации на базе KVM, XEN

Особенности развертывания и эксплуатации

! Для Microsoft Hyper-V необходимо создать новую виртуальную машину и установить на нее ViPNet IDS NS из образа в формате ISO

! Для поддержки USB-устройств в Oracle VM VirtualBox используйте пакет расширений Oracle VM VirtualBox Extension Pack

! Не рекомендуется использовать Microsoft Hyper-V для исполнений ViPNet IDS NS VA 2000 и ViPNet IDS NS VA 5000

Конфигурация виртуальных машин по исполнениям

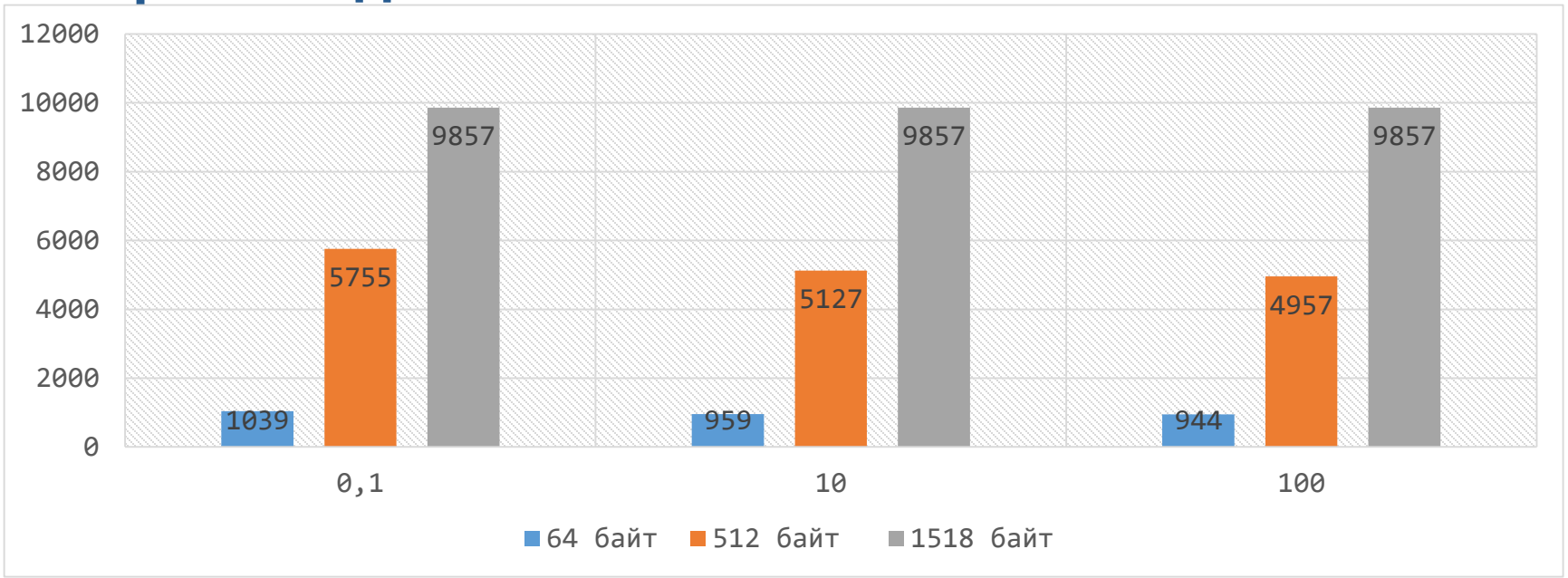
Исполнение	Количество процессоров, шт.	Объем оперативной памяти, Гбайт	Объем жесткого диска, Гбайт
ViPNet IDS NS VA 100	2	4	500
ViPNet IDS NS VA 1000	4	4	500
ViPNet IDS NS VA 2000	6	8	500
ViPNet IDS NS VA 5000	12	16	500

- Один образ виртуальной машины для всех исполнений;
- Разные лицензии

! Избыточное аппаратное обеспечение после установки и активации лицензии не будет задействовано в работе ViPNet IDS NS VA.

! Корректная работы ViPNet IDS NS VA не гарантируется на виртуальной машине с недостаточными аппаратными ресурсами

Производительность ViPNet IDS VA



Гипервизор: Oracle VM Server 3.4.6
Трафик: UDP
Включенных правил: 28601
Маска/кол-во адресов источника: 24/256
Snort instances: 8

Аппаратная платформа:
Processor model: Intel(R) Xeon(R) E-2278GE CPU @ 3.30GHz
Number cores: 12

Решение ViPNet TDR

infotecs

ViPNet IDS MC

- Управлять инфраструктурой сенсоров
- Осуществлять мониторинг состояния сенсоров

ViPNet TIAS

- Анализировать события ИБ от сетевых и хостовых сенсоров и выявлять инциденты ИБ

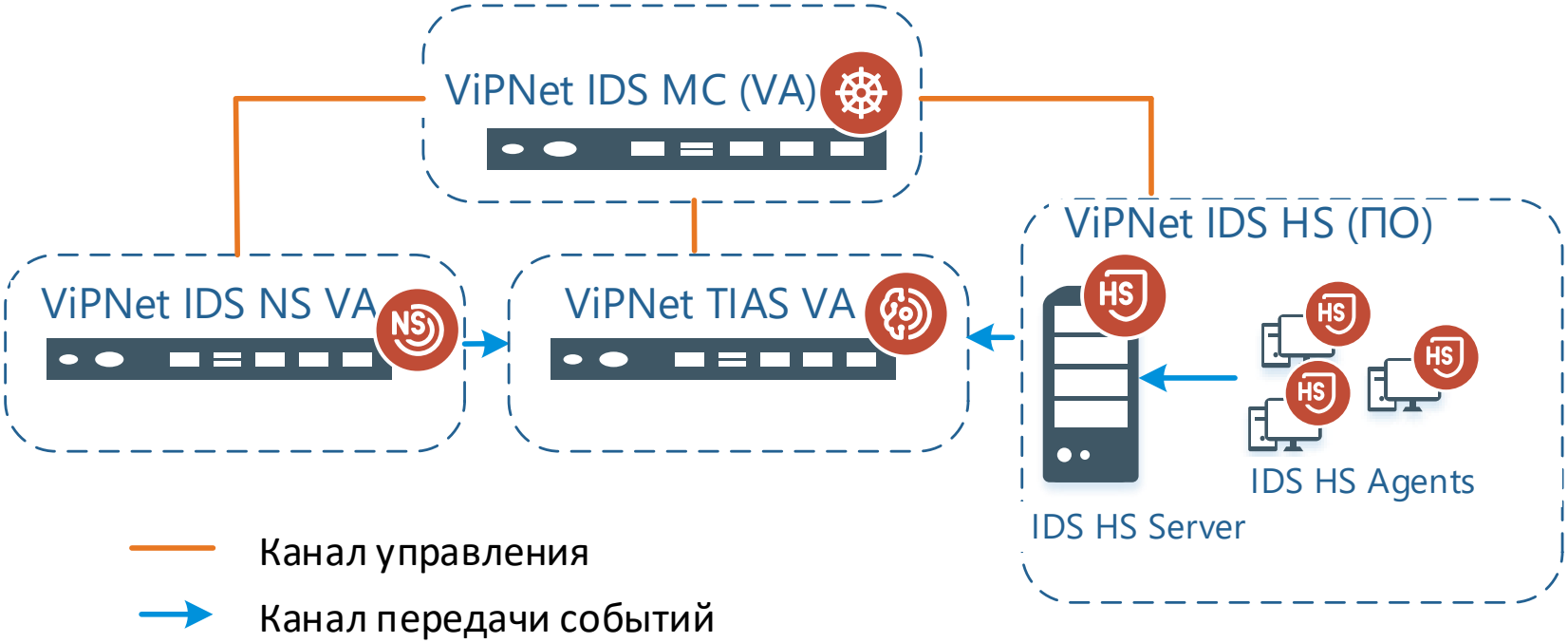
ViPNet IDS NS

- Выявлять события, связанные с ИБ в сетевом трафике

ViPNet IDS HS

- Выявлять события ИБ и аномалии поведения на конечных узлах

Программные исполнения компонентов решения ViPNet TDR



Лицензирование ViPNet TIAS

Исполнение	Что входит	Ограничения
Базовая лицензия ViPNet TIAS VA	Лицензии на подключение : 1 IDS NS 1 IDS HS Server 10 IDS HS Agent Сервис технической поддержки уровня Базовый на 1 год Сервис обновления экспертных данных на срок 1 год	до 300 событий ИБ за 1 секунду
Расширение лицензии на подключение в качестве источника 1 IDS NS	Лицензия на подключение 1 IDS NS	до 100 IDS NS
Расширение лицензии на подключение в качестве источника 1 IDS HS Server	Лицензия на подключение 1 IDS HS Server	до 5 IDS HS Server
Расширение лицензии на подключение в качестве источника 1 IDS HS Server Agent	Лицензия на подключение 1 IDS HS Agent	до 5000 IDS HS Agent
Расширение функционала производительности TIAS VA	Лицензия расширения производительности TIAS VA на 300 EPS (количество обрабатываемых событий ИБ в секунду)	до 5000 событий ИБ за 1 секунду

Сертифицированные версии

СОА класса В

Система IDS 3 в составе:

- ПАК ViPNet IDS NS 3.6.0
- ПО ViPNet IDS MC 1.6.0
- ПАК ViPNet TIAS 3.5.1

СЗИ

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, № РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ

№ СФ/СЗИ-0394

Выдан "22" июня 2020 г. Действителен до "30" июня 2023 г.

Настоящий сертификат удостоверяет, что:

1. Средство защиты информации «Система обнаружения компьютерных атак (сетевой) ViPNet IDS 3» (сокращенное наименование: ViPNet IDS NS3100, ViPNet IDS NS3000, ViPNet IDS NS VA в комбинации со средством централизованного управления и мониторинга ViPNet IDS MC; средством анализа событий информационной безопасности ViPNet TIAS (исполнение: TIAS 1000, TIAS 2000, TIAS 5000, TIAS VA)), изготовленная в соответствии с техническими условиями ФПРК.00211-01 ТУ 01, ТУ...

соответствует требованиям ФСБ России к средствам обнаружения компьютерных атак класса В и может использоваться для обнаружения в автоматическом режиме компьютерных атак (вторжений) по сетевым каналам сетевого трафика в автоматизированных информационных системах, обрабатывающих информацию, не содержащую сведений, составляющих государственную тайну, при условии выполнения требований эксплуатационной документации согласно формуляру ФПРК.00211-01 30 01, ФО...

2. Сертификат соответствия выдан на основании экспертного заключения Центра защиты информации и специальной связи Федеральной службы безопасности Российской Федерации № 149/2/2-162 от 20 января 2020 г. и результатов испытаний, проведенных испытательной лабораторией ...

3. Заявитель, изготовитель: Открытое акционерное общество «Информационные технологии и коммуникационные системы» (ОАО «ИнфоТеКС»); 127287, г. Москва, Старый Петровско-Разумовский проезд, д. 1/23, стр. 1

4. Заявитель, изготовитель: Общество с ограниченной ответственностью «Линия защиты» (ООО «Линия»); 127083, г. Москва, ул. Мишина, дом 56, строение 2, офис 10.

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России — О.В. Скребнев

Сертификат имеет юридическую силу на всей территории Российской Федерации

Заместитель начальника Центра по лицензированию, сертификации и защите государственной тайны ФСБ России — Д.А. Кругляк

СОВ 4 класс, ТДБ 4 уровень

Система IDS 3 в составе:

- ПО ViPNet IDS NS 3.6.0
- ПО ViPNet IDS MC 1.6.0
- ПО ViPNet TIAS 3.5.1

СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ

№ 4329

Внесен в государственный реестр системы сертификации средств защиты информации по требованиям безопасности информации 24 ноября 2020 г.

Выдан: 24 ноября 2020 г.

Действителен до: 24 ноября 2025 г.

Настоящий сертификат удостоверяет, что система обнаружения компьютерных атак (вторжений) ViPNet IDS 3, разработанная и производимая АО «ИнфоТеКС», является системой 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 системам обнаружения вторжений» (ФСТЭК России, 2011) и «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ» (ФСТЭК России, 2012).

Сертификат выдан на основании технического заключения от 30.09.2020, оформленного по результатам сертификационных испытаний испытательной лабораторией МЦУ «ИНФО» (аттестат аккредитации от 18.11.2016 № СЗИ RU.0001.01БИ00.БЛ12), и экспертного заключения от 27.10.2020, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002).

Заявитель: АО «ИнфоТеКС»
Адрес: 127287, г. Москва, Старый Петровско-Разумовский проезд, д. 1/23, стр. 1
Телефон: (495) 737-6192

НАЧАЛЬНИК 2 УПРАВЛЕНИЯ ФСТЭК РОССИИ — Д.Шевцов

Официальные версии

- ViPNet IDS NS 3.8
- ViPNet IDS HS 1.5
- ViPNet TIAS 3.7
- ViPNet IDS MC 3.8

infotecs

Новое в версиях

ViPNet IDS NS 3.8

Методы захвата трафика по умолчанию

Аппаратная платформа	Метод по умолчанию	Возможность смены метода
ViPNet IDS NS100 X1/N1	PF_RING	–
ViPNet IDS NS1000 Q1	PF_RING	–
ViPNet IDS NS1000 Q2/Q3	PF_RING	✓
ViPNet IDS NS2000 Q1/Q2/Q3	PF_RING	✓
ViPNet IDS NS2000 Q4	DPDK	✓
ViPNet IDS NS10000 Q1	DPDK	✓
ViPNet IDS NS VA 100	PF_RING	–
ViPNet IDS NS VA 1000/2000/5000	PF_RING	✓

Внимание! Метод сбора и обработки сетевого трафика с помощью интерфейса DPDK не поддерживается для исполнений ViPNet IDS NS VA, развернутых на платформах виртуализации Microsoft Hyper-V Server 2019 и Microsoft Hyper-V (роль в составе Windows Server 2016).

Новый метод сбора и обработки сетевых пакетов (DPDK)

- DPDK обеспечивает лучшие, по сравнению с интерфейсом PF_RING, показатели по обработке трафика на высокопроизводительных аппаратных платформах при захвате пакетов небольших размеров

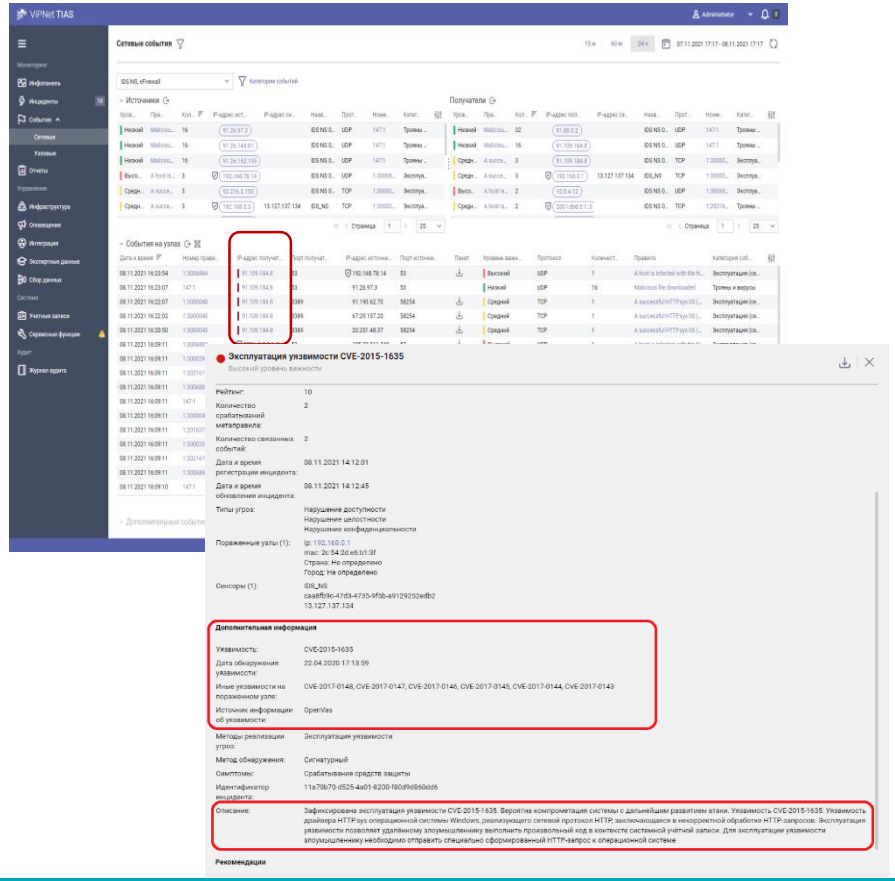
Запись сетевой сессии

- Теперь при расследования сетевой атаки можно выполнить анализ фрагмента сетевой сессии, связанного с зарегистрированным событием.

Увеличение количества пользовательских правил

- Теперь в ViPNet IDS NS можно создавать или загружать до 15000 пользовательских правил

ViPNet TIAS 3.7



Новые источники событий

- в качестве источника событий могут быть подключены ViPNet xFW и ViPNet EPP;

Обогащение информации

- Загрузка и использование данных от сканеров уязвимостей;
- Выявление инцидентов с использованием данных IoC;

Удобство эксплуатации

- Использование NTP-сервера для синхронизации времени;
- Мониторинг состояния TIAS по SNMP;

infotecs

Спасибо за внимание!

Подписывайтесь на наши соцсети

https://vk.com/infotecs_news

https://t.me/infotecs_news