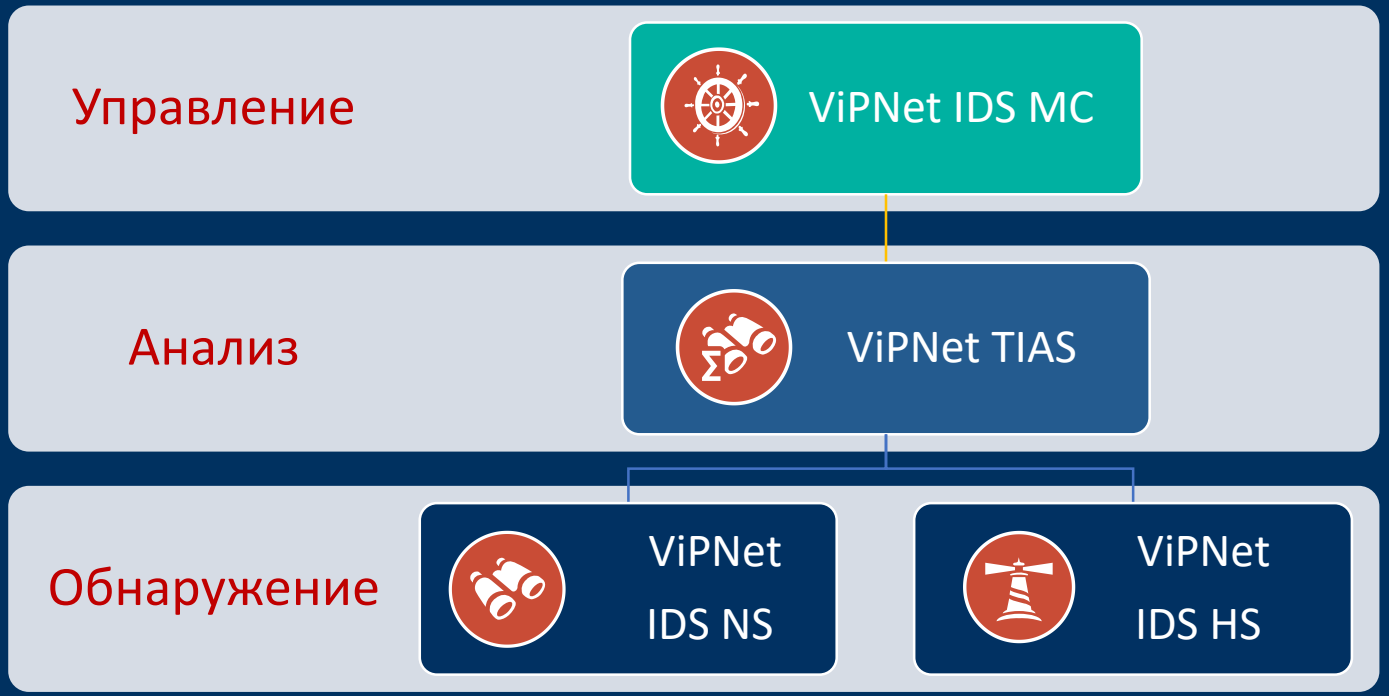

техно
2019
infotecs
фест
ТЕХНИЧЕСКАЯ
КОНФЕРЕНЦИЯ
12
09
2019
Обнаружение атак, обеспечение актуальных мер и требований практической безопасности на примере решения ViPNet ITDP и аналитической системы принятия решений ViPNet TIAS

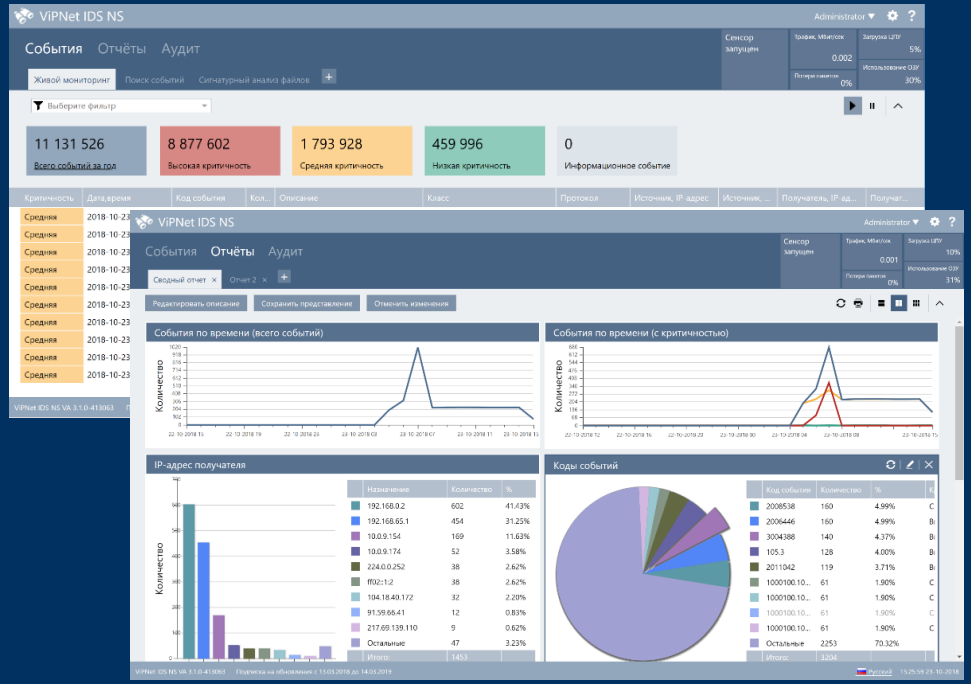
Решение ViPNet ITDP

Состав решения ITDP



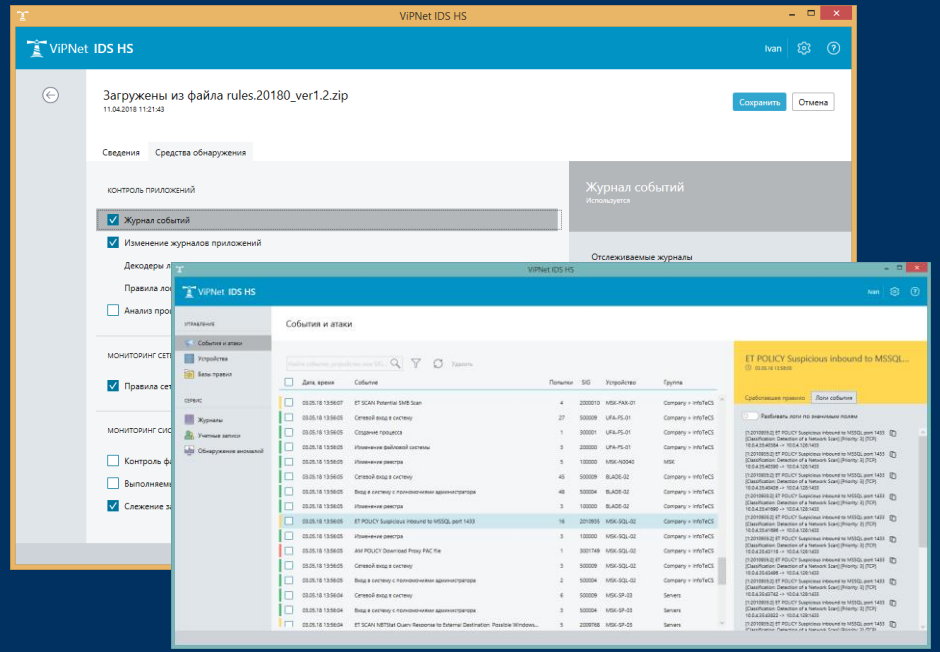
ViPNet IDS NS

- обнаруживать события ИБ в трафике;
- оповещать о событиях;
- хранить события;
- работать с событиями;
- управлять правилами и настройкой сигнатур



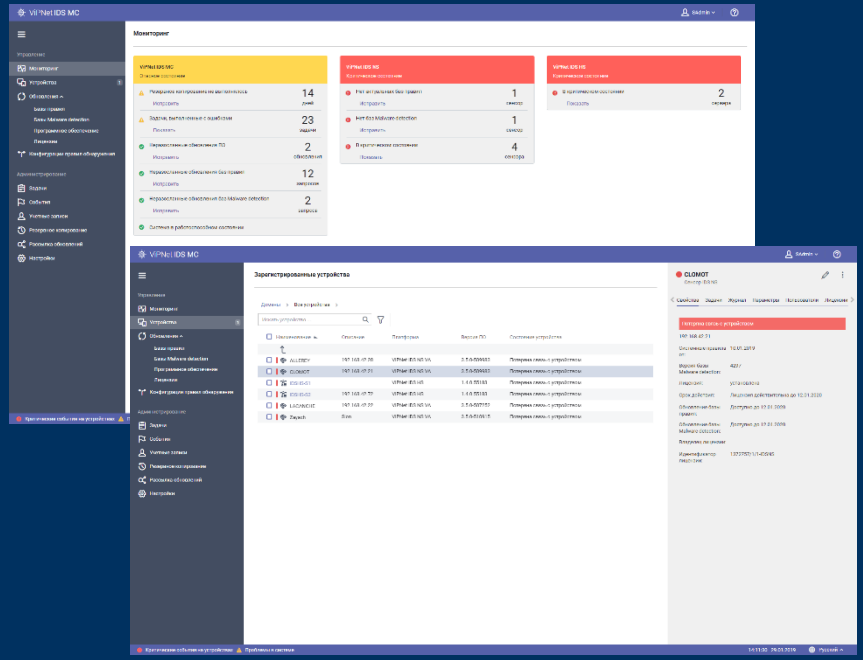
ViPNet IDS HS

- выявлять подозрительную активность внутри ОС:
  - файловая активность,
  - изменения в реестре,
  - неизвестные процессы.
- определять атаки, которые “не видит” сетевой сенсор;
- обнаруживать атаки после расшифровки входящего трафика



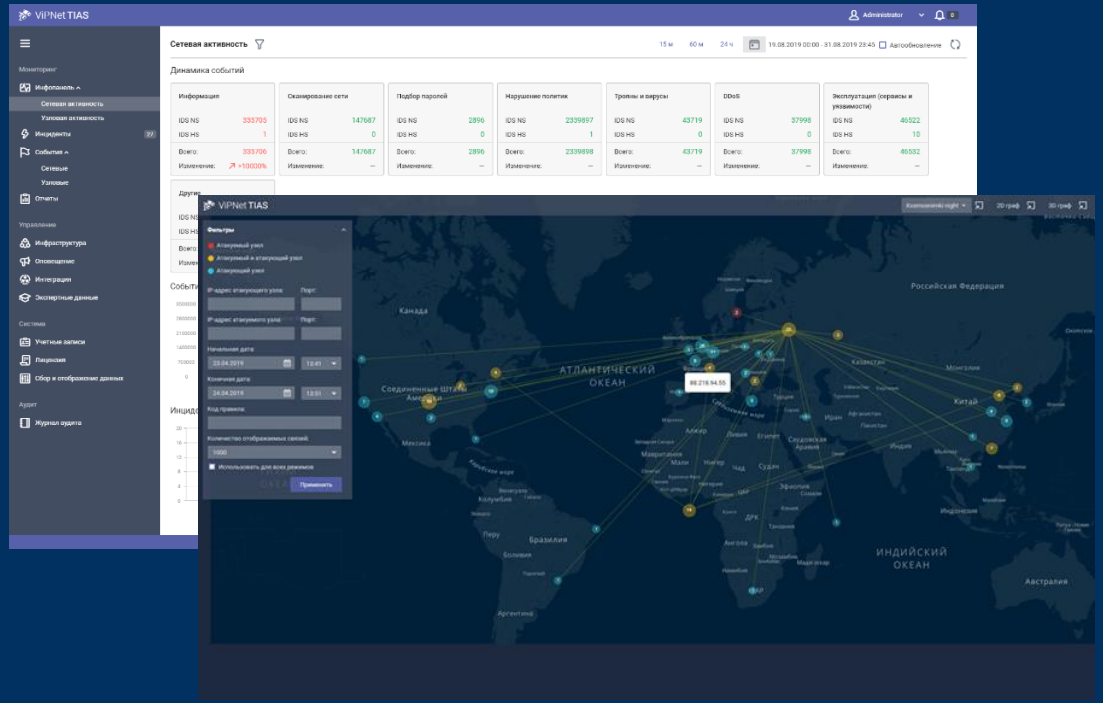
ViPNet IDS MC

- настраивать структуру и параметры сенсоров;
- управлять конфигурациями правил;
- мониторить работоспособность сенсоров;
- обновлять:
  - базы решающих правил;
  - базы сигнатур вредоносного ПО;
  - экспертные данные;

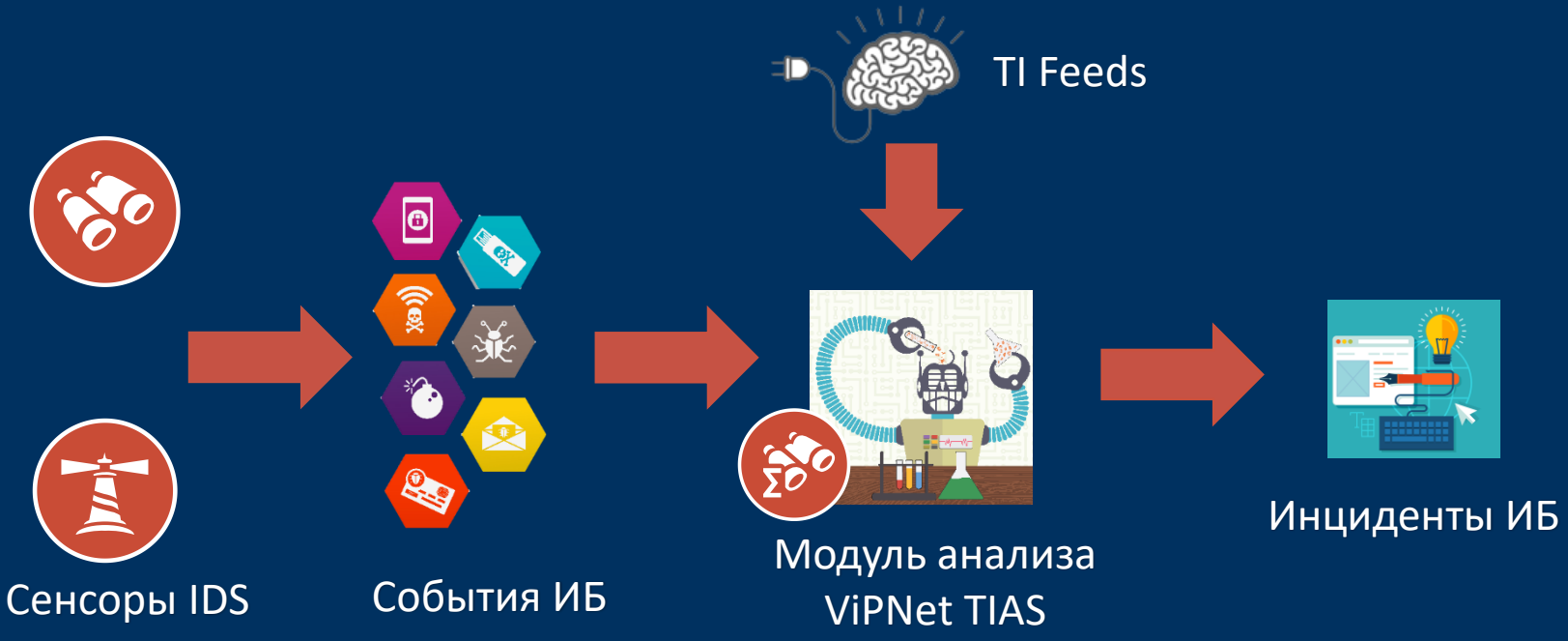


ViPNet TIAS

- анализировать события от сенсоров ViPNet IDS;
- выявлять инциденты;
- оповещать об инцидентах;
- проводить расследования;
- давать рекомендации;
- формировать отчеты.

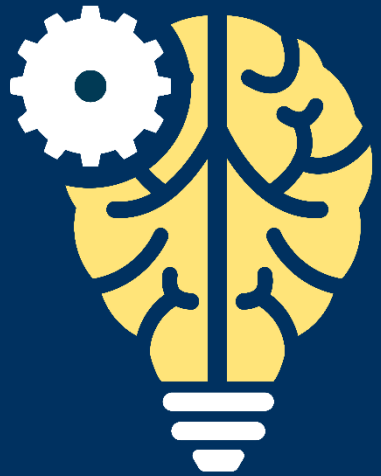


Как это работает?



Отличительные особенности

Machine Learning

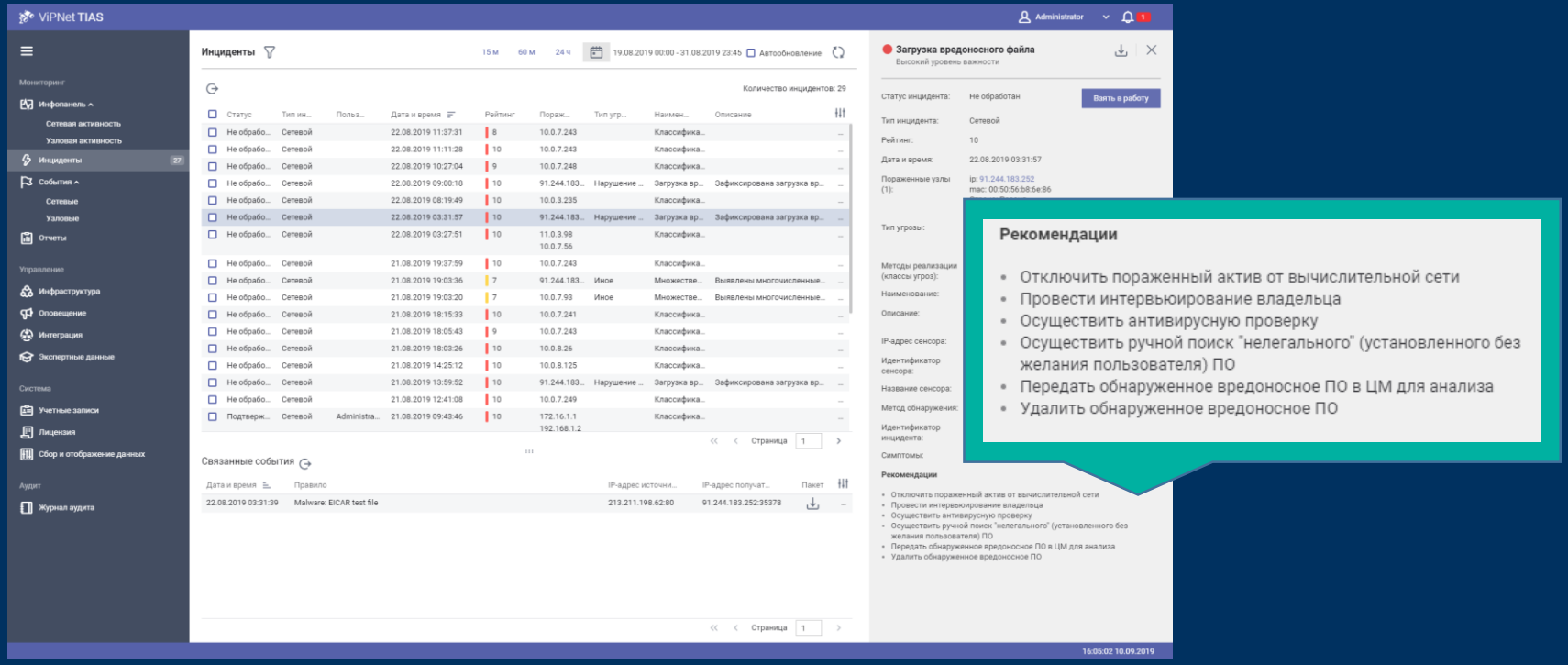


- математическая модель принятия решений;
- алгоритмы машинного обучения;
- ежемесячное переобучение;
- выявление атак нулевого дня

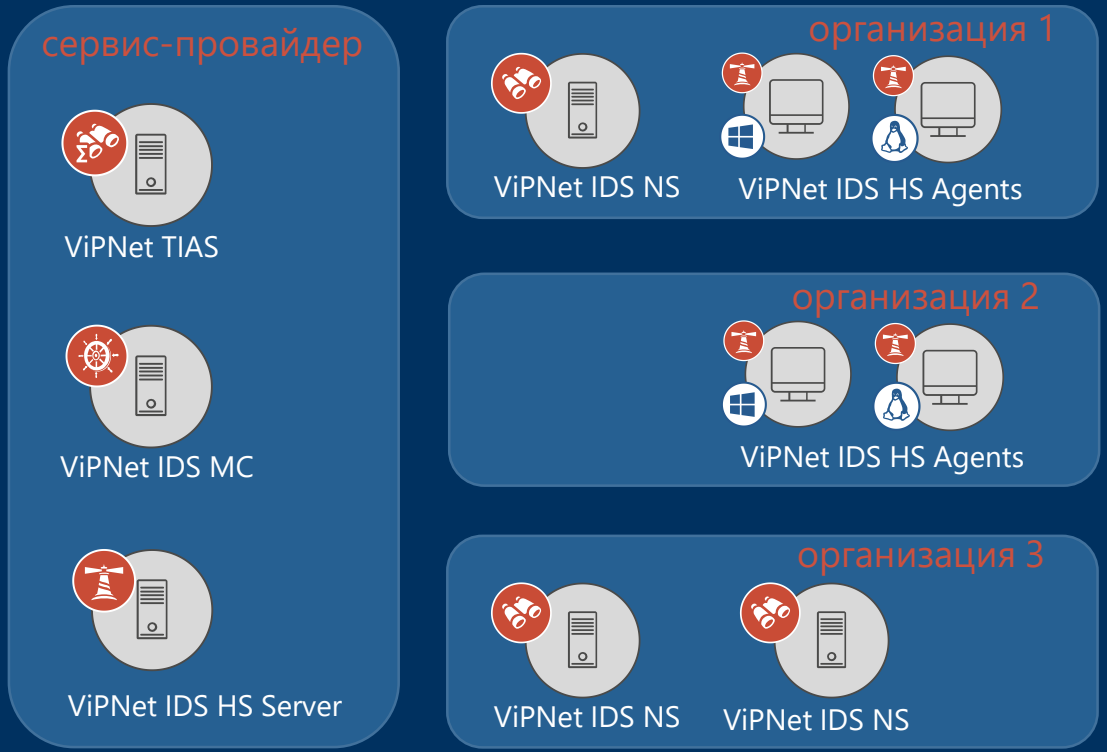
Threat Intelligence

- индикаторы атак и компрометации;
- ТТП - тактики, техники, процедуры;
- информационный обмен:
  - СОПКА,
  - ФСТЭК,
  - RU-CERT;
- опыт клиентов - верифицированная и обезличенная информация

Готовые планы реагирования



Облачный сервис на базе решения



- мастер подключения организации;
- активация и настройка сенсоров из IDS MC;
- мульти-арендный доступ к IDS MC;
- учет лицензий по организациям

Варианты исполнения

Сервер 1U

- ViPNet IDS NS 1000-2000
- ViPNet TIAS 1000-5000

Desktop

- ViPNet IDS NS 100

Virtual Appliance

- ViPNet IDS NS VA
- ViPNet TIAS VA

Software

- ViPNet IDS HS Server
- ViPNet IDS HS Agent

Сертификаты

- ViPNet IDS 2. Сертификат ФСТЭК России СОВ 4 класс
- ViPNet IDS 2. Сертификат ФСБ России СОА класс класса В
- ViPNet IDS HS. Сертификат ФСТЭК России СОВ уровня узла 4 класс
- ViPNet TIAS. Сертификат ФСТЭК России. НДВ 4 уровень, соответствие ТУ

Актуальные меры безопасности. Требования регуляторов

Меры по обеспечению безопасности ИСПДн и ГИС (приказы ФСТЭК России 17, 21)

	Содержание мер	Обеспечение мер с помощью решения ITDP
СОВ.1	Обнаружение вторжений	Все требования ФСТЭК России к СОВ сетевого уровня и уровня узла обеспечиваются ViPNet IDS NS и ViPNet IDS HS и подтверждаются сертификатами
СОВ.2	Обновление базы решающих правил	Автоматическое централизованное обновление БРП на всех сенсорах с помощью ViPNet IDS MC или локально на сенсоре
ИНЦ.1	Определение лиц, ответственных за выявление инцидентов и реагирование на них	Реализовано в ViPNet TIAS с помощью функции управления пользователями с настройкой ролевого доступа к информации об инцидентах
ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов	Реализовано в ViPNet TIAS. Инциденты определяются автоматически и регистрируются в системе
ИНЦ.3	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами	Реализовано в ViPNet TIAS. Способы оповещения: через web-Ui, по e-mail, передача информации об инциденте во внешнюю систему по протоколу syslog
ИНЦ.4	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий	ViPNet TIAS позволяет проводить полноценный анализ инцидентов, определяет источники и причины возникновения инцидентов, предоставляет функции поиска информации в исходных событиях а так же предоставление образцов трафика для сбора доказательств
ИНЦ.5	Принятие мер по устранению последствий инцидентов	ViPNet TIAS по каждому из выявленных инцидентов предоставляет рекомендации по реагированию и устранению последствий
ИНЦ.6	Планирование и принятие мер по предотвращению повторного возникновения инцидентов	ViPNet TIAS позволяет накапливать статистику и строить отчеты по угрозам и инцидентам, на основании которых могут планироваться мероприятия, направленные на предотвращение повторного возникновения инцидентов

Требования по обеспечению безопасности значимых объектов КИИ (приказ ФСТЭК России 239)

Содержание мер		Обеспечение мер с помощью решения ITDP
СОВ.1	Обнаружение и предотвращение компьютерных атак	Все требования ФСТЭК России к СОВ сетевого уровня и уровня узла обеспечиваются ViPNet IDS NS и ViPNet IDS HS и подтверждаются сертификатами. Требование к СОА подтверждены сертификатами ФСБ России
СОВ.2	Обновление базы решающих правил	Автоматическое централизованное обновление БРП на всех сенсорах с помощью ViPNet IDS MC или локально на сенсоре
ИНЦ.1	Выявление компьютерных инцидентов	Является основной целевой функцией ViPNet TIAS
ИНЦ.2	Информирование о компьютерных инцидентах	Реализовано в ViPNet TIAS. Способы оповещения: через web-Ui, по e-mail, передача информации об инциденте во внешнюю систему по протоколу syslog
ИНЦ.3	Анализ компьютерных инцидентов	ViPNet TIAS позволяет проводить глубокий анализ компьютерных инцидентов, предоставляя инструменты поиска и фильтрации данных в событиях, связанных с инцидентом, а так же предоставляя образцы исходного трафика и описания сработавших правил выявления событий безопасности
ИНЦ.4	Устранение последствий компьютерных инцидентов	Карточка инцидента в ViPNet TIAS содержит информацию о пострадавших в результате компьютерного инцидента активах, а так же рекомендации по устранению его последствий
ИНЦ.5	Принятие мер по предотвращению повторного возникновения компьютерных инцидентов	ViPNet TIAS позволяет накапливать статистику и строить отчеты по угрозам и инцидентам, на основании которых могут планироваться мероприятия, направленные на предотвращение повторного возникновения инцидентов
ИНЦ.6	Хранение и защита информации о компьютерных инцидентах	ViPNet TIAS позволяет хранит информацию обо всех обнаруженных компьютерных инцидентах и связанных с ними событий в течении 3 лет. Защита данных при хранении подтверждается сертификатом ФСТЭК России на отсутствие НДВ и соответствие ТУ. Защита при передаче информации об инцидентах должна обеспечиваться сертифицированным СКЗИ

Мониторинг информационной безопасности средств и систем информатизации

	Наименование оборудования	Технические и (или) функциональные характеристики
22	Средства (системы) контроля (анализа) защищенности информационных систем	Автоматизированная инвентаризация ресурсов информационных систем (сбор информации об узлах информационных систем и об используемом в них программном обеспечении), выявление уязвимостей (кода, конфигурации и архитектуры) в них, анализ и управление выявленными уязвимостями с учетом угроз. Должны иметь сертификаты соответствия ФСТЭК России
24.	Средства управления информацией об угрозах безопасности информации	Автоматизированный сбор и анализ информации, поступающей из различных источников, об угрозах безопасности информации. Должны иметь формуляры, оформленные разработчиками (производителями) данных средств. В случае невозможности оформления формуляров разработчиками (производителями) данных средств (свободнораспространяемое программное обеспечение) формуляры оформляются лицензиатами (соискателями лицензии)
25.	Средства управления событиями безопасности информации	Автоматизированный сбор, анализ и корреляция данных о событиях безопасности информации, регистрируемых компонентами информационных систем, идентификация по заданным индикаторам типовых инцидентов информационной безопасности и их локализация. Должны иметь сертификаты соответствия ФСТЭК России

Положение о лицензировании деятельности по технической защите конфиденциальной информации, утвержденное постановлением Правительства Российской Федерации от 3 февраля 2012 г. N 79
Перечень утвержден директором ФСТЭК России 19 апреля 2017 г.

Мониторинг информационной безопасности средств и систем информатизации

	Наименование оборудования	Технические и (или) функциональные характеристики
26.	Средства управления инцидентами информационной безопасности	Автоматизированная регистрация информации об инцидентах информационной безопасности информационных систем, предоставление рекомендаций по реагированию на них, формирование и модификация шаблонов инцидентов информационной безопасности, в том числе рекомендаций по реагированию на них. Должны иметь формуляры, оформленные разработчиками (производителями) данных средств. В случае невозможности оформления формуляров разработчиками (производителями) данных средств (свободнораспространяемое программное обеспечение) формуляры оформляются лицензиатами (соискателями лицензии)
27.	Средства защиты каналов передачи данных	Должны обеспечивать конфиденциальность и целостность данных, передаваемых по каналам связи между информационной системой, используемой для управления информационной безопасностью, и информационными системами, в отношении которых осуществляется мониторинг. Должны иметь сертификаты соответствия ФСБ России
28.	Системы защиты информации информационных систем, используемых для мониторинга информационной безопасности	Системы защиты информации информационных систем, используемых для оказания услуг по мониторингу информационной безопасности информационных систем, должны соответствовать Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденным приказом ФСТЭК России от 11 февраля 2013 г. N 17, применительно к первому классу защищенности государственных информационных систем

ГосСОПКА

Структура ГосСОПКА

В 2018 году средствами ГосСОПКА было выявлено более 4,3 млрд компьютерных воздействий на критическую информационную инфраструктуру, из них более 17 тысяч наиболее опасных компьютерных атак

Мурашов Н.Н

Приказы ФСБ России

- Перечень информации, предоставляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка предоставления информации в ГосСОПКА (Приказ № 367 от 24 июля 2018 года);
- Порядок обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации… (Приказ от 24 июля 2018 г. N 368);
- Требования к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты (Приказ от 06.05.2019 №196)
- Порядок информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации (Приказ ФСБ России от 19.06.2019 N 282)

Приказ ФСБ России №282 от 19.06.2019

- Информация о компьютерном инциденте, связанном с функционированием значимого объекта критической информационной инфраструктуры, направляется субъектом критической информационной инфраструктуры в НКЦКИ **в срок не позднее 3 часов** с момента обнаружения компьютерного инцидента, а в отношении иных объектов критической информационной инфраструктуры — **в срок не позднее 24 часов** с момента его обнаружения
- Информирование осуществляется путем направления информации в Национальный координационный центр по компьютерным инцидентам в соответствии с определенными НКЦКИ форматами

Проект ФЗ о внесении изменений в КОАП:

Непредставление или нарушение порядка либо сроков представления в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации информации, предусмотренной законодательством в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, – влечет наложение административного штрафа:

- на должностных лиц в размере от десяти тысяч до пятидесяти тысяч рублей;
- на юридических лиц – от ста тысяч до пятисот тысяч рублей

Перечень мероприятий

Класс В

ТЕХНО infotecs 2019 фест

- Взаимодействие с НКЦКИ
- Разработка регламентирующих документов
- Эксплуатация средств ГосСОПКА
- Прием сообщений об инцидентах
- Регистрация атак и инцидентов
- Анализ событий ИБ
- Инвентаризация
- Анализ угроз ИБ
- Составление и актуализация перечня угроз
- Выявление уязвимостей
- Подготовка предложений по повышению уровня защищенности
- Составление перечня инцидентов
- Ликвидация последствий
- Анализ результатов ликвидации последствий

Варианты подключения

Самостоятельное подключение

ГОССОПКА

Субъект ГосСОПКА

- Заключить соглашение с 8Ц ФСБ России
- Выполнить организационные и технологические требования к центру ГосСОПКА
- Обеспечить взаимодействие с технической инфраструктурой НКЦКИ

НКЦКИ

Объект КИИ

Подключение через корпоративный центр

ГОССОПКА

Корпоративный центр ГосСОПКА

- Заключить соглашение с корпоративным (ведомственным) центром ГосСОПКА
- Уведомить НКЦКИ о включении своих ресурсов в зону ответственности цента

О решении ITDP в цифрах

Производительность и потребность в ресурсах

ТЕХНО 2019 infotecs ФЕСТ

ViPNet IDS NS

анализ трафика
до 6 Гбит/с

ViPNet TIAS

анализ до 5 000 событий/с

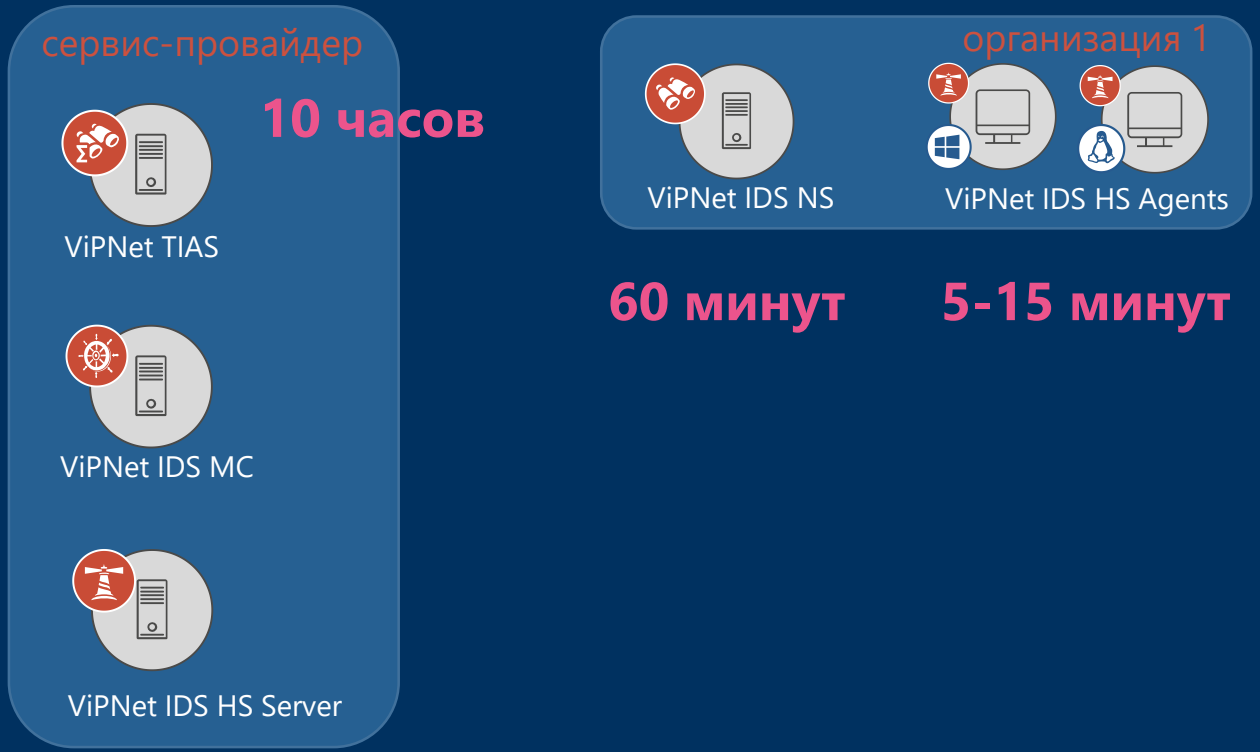
подключение до 50 IDS NS

подключение до 5000 IDS HS Agents

ViPNet IDS HS Agent

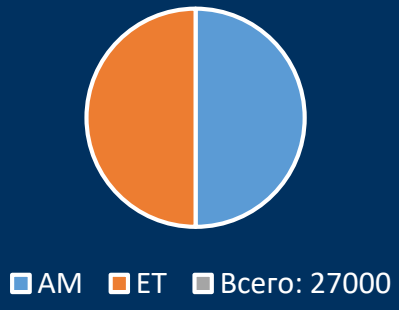
потребляет ~ 60 Мбайт
оперативной памяти

Внедрение решения

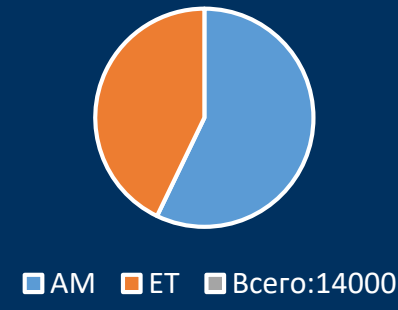


Обновление правил и экспертных данных

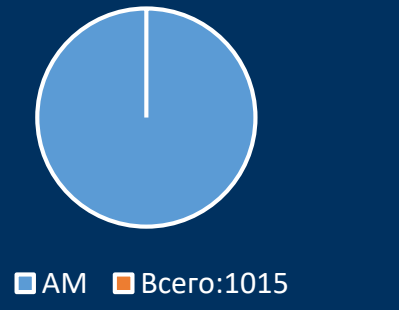
Правила IDS NS



Правила IDS HS



Правила TIAS



- Ежедневное обновление правил
- Ежемесячное переобучение математической модели

Центр мониторинга

894 инцидента
за 2018 год

<60 мин.
на реагирование

более 30
операторов,
исследователей,
аналитиков

ФСК ЕЭС

И ещё более 40 организаций подключались на мониторинг за последние 3 года

Учебный центр

237 человек обучено на курсе «Администрирование IDS и TIAS»

12 ВУЗов имеют лаборатории, оснащенные ViPNet IDS и TIAS

Спойлер

Мастер-класс проведение атаки

ТЕХНО 2019 infotecs Фест

Спасибо
за внимание!