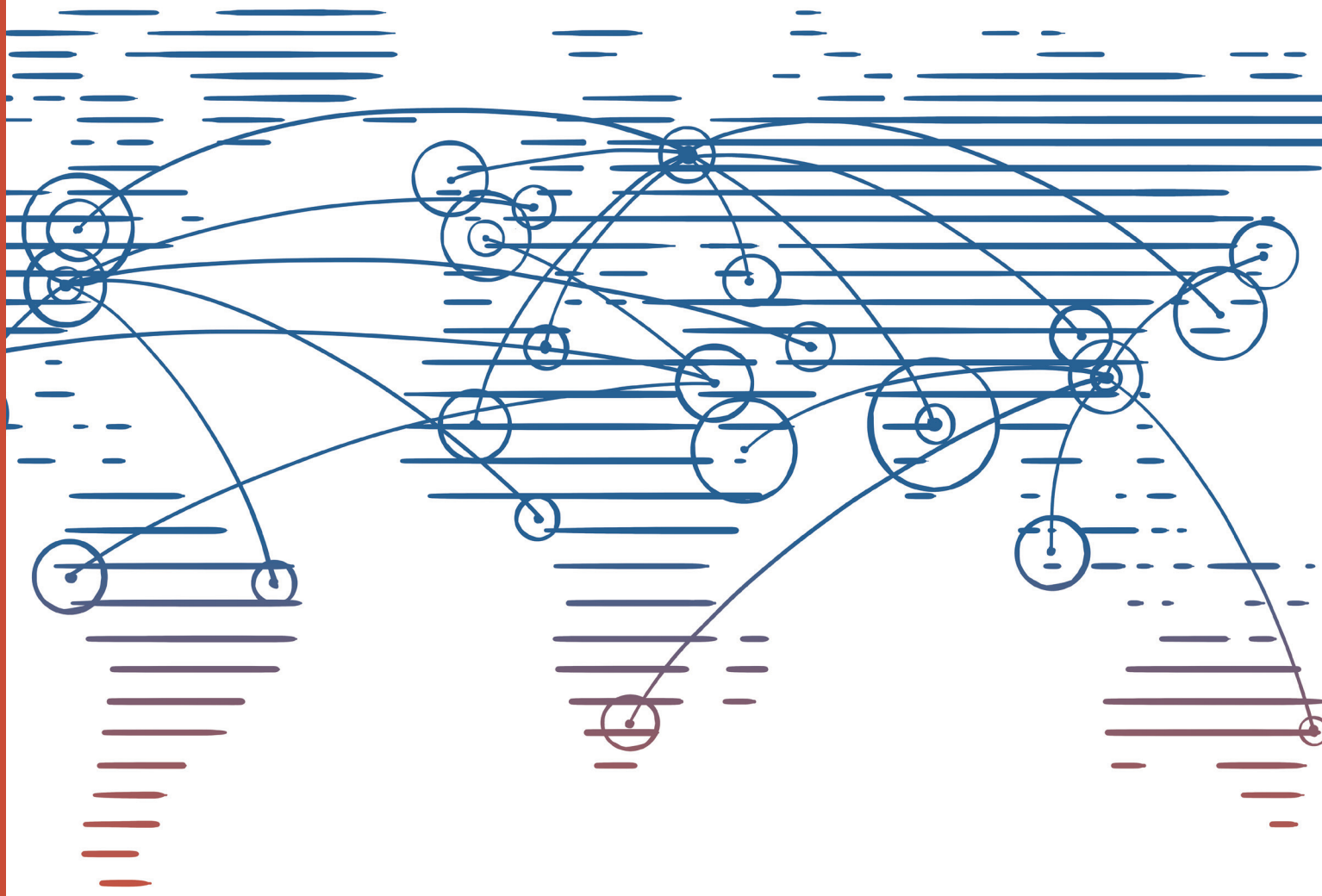
инфотекс

ViPNet TDR

Решение по обнаружению и предотвращению компьютерных атак



Продукты
с искусственным
интеллектом

Ландшафт киберугроз характеризуется усилением существующих и появлением новых векторов атак, связанных с развитием технологий и геополитической обстановкой.

Среди наиболее актуальных угроз можно выделить использование искусственного интеллекта (ИИ) в кибератаках. ИИ стал ключевым инструментом злоумышленников для планирования атак, сбора информации, поиска уязвимостей, подбора паролей и генерации фишинговых писем. Появились автономные ИИ-агенты, способные проводить многоступенчатые атаки без постоянного контроля человека. Нейросети используются для генерации вредоносного кода и управления ботнетами. Компьютеры, рабочие ноутбуки, домашние роутеры и IoT-устройства могут быть скомпрометированы и использоваться для майнинга, участия в ботнетах или как промежуточная инфраструктура атак. Пользователь при этом может не замечать явных признаков проблемы.

Для защиты от этих угроз требуется комплексный подход, включающий разные инструменты и методы обнаружения и предотвращения компьютерных атак.

Решение ViPNet TDR — это интеллектуальная система обнаружения компьютерных атак, которая:

1. Анализирует сетевой трафик и действия пользователей на конечных узлах в режиме реального времени
2. Использует машинное обучение для выявления аномалий и неизвестных угроз
3. Сопоставляет события с базой техник и тактик проведения атак, обогащает их данными об индикаторах компрометации и выдает вердикт об обнаруженной угрозе
4. Предоставляет администратору четкие рекомендации по реагированию

ПРЕИМУЩЕСТВА

- Сокращение времени обнаружения угрозы с нескольких часов до двух минут за счет автоматизации всего процесса обнаружения
- Снижение требований к персоналу за счет использования в решении экспертных данных от наших специалистов
- Большое покрытие разных векторов атак, включая атаки нулевого дня за счет комбинирования сигнатурных, эвристических методов и использования искусственного интеллекта
- Простой ввод решения в эксплуатацию
- Соответствие требованиям регуляторов

ПРЕДОСТАВЛЯЕМЫЕ ВОЗМОЖНОСТИ

- Обеспечение непрерывного процесса мониторинга угроз информационной безопасности и обнаружения компьютерных атак
- Выявление угроз в реальном времени с рекомендацией по их оперативному устранению и проведение ретроспективного анализа
- Поддержка процесса проведения расследований по инцидентам и помощь в принятии решения специалистам по информационной безопасности
- Извлечение полезных уроков из инцидентов и предотвращение их повторения с помощью накопленных знаний об инцидентах
- Предоставление руководству и контролирующим органам сводных отчетов по обнаруженным угрозам и инцидентам
- Передача информации о компьютерных инцидентах в НКЦКИ ГосСОПКА

СОСТАВ РЕШЕНИЯ

ViPNet IDS NS
система обнаружения вторжений уровня сети

ViPNet IDS HS
система обнаружения вторжений уровня узла

ViPNet TIAS
система интеллектуального анализа событий и автоматического выявления инцидентов

ViPNet IDS MC
централизованная консоль управления компонентами решения

СХЕМА ПОДКЛЮЧЕНИЯ В ФИЗИЧЕСКИХ И ВИРТУАЛЬНЫХ СЕТЯХ

Схема подключения в физической сети

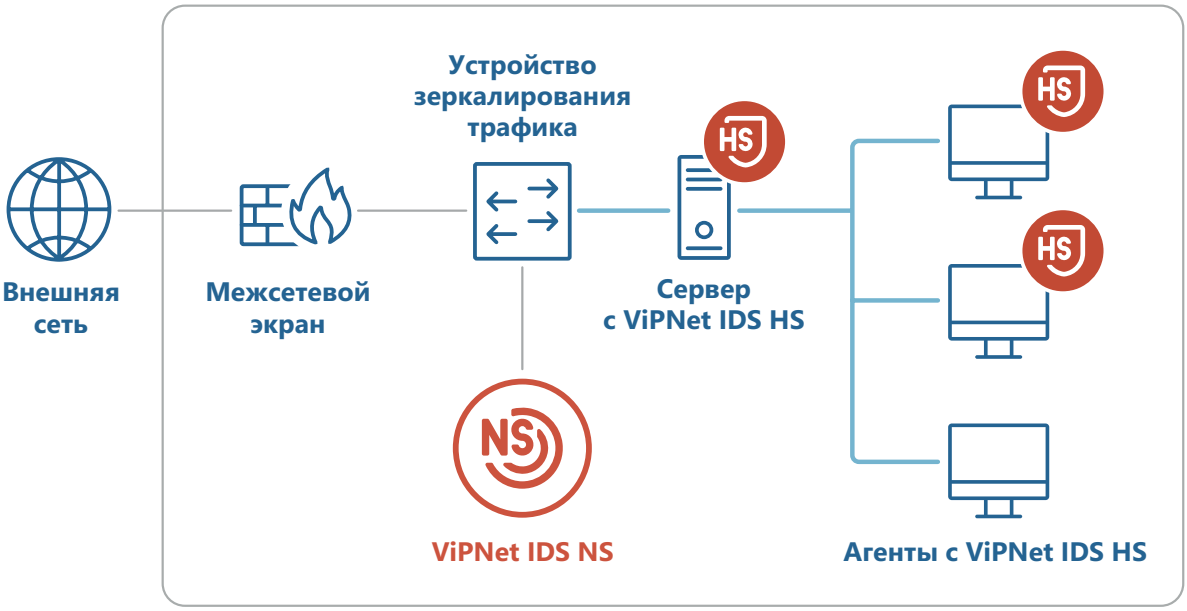
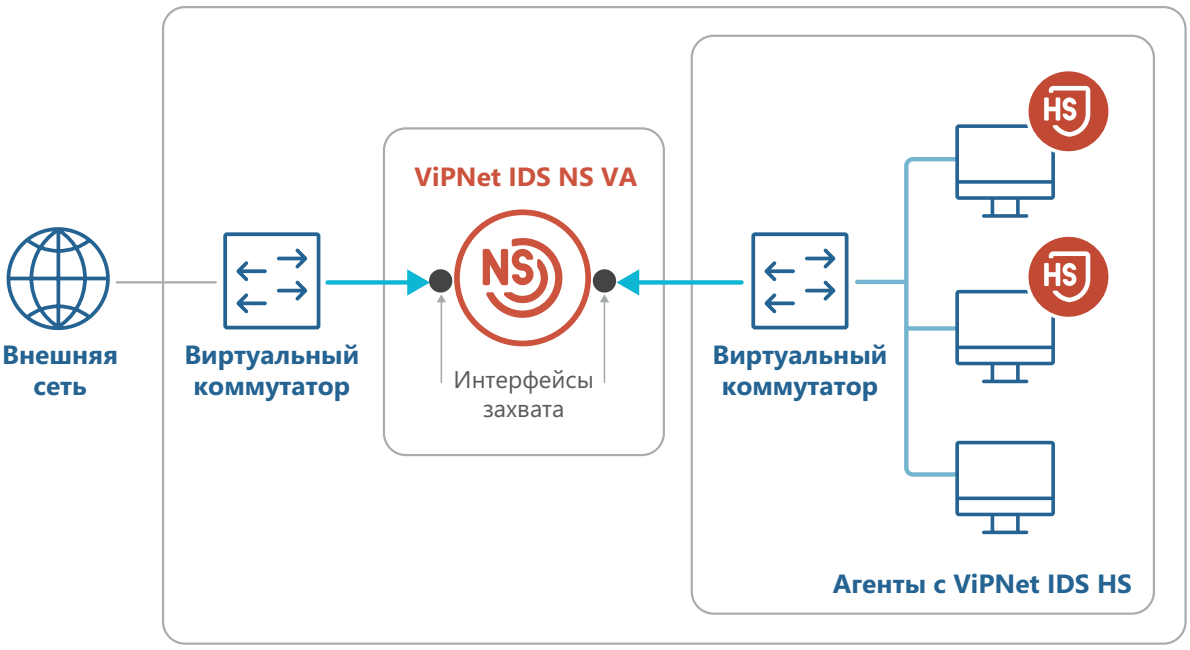


Схема подключения в виртуальной сети



СЦЕНАРИЙ РАБОТЫ

01. Сенсоры систем обнаружения вторжений на основе анализа трафика в сети и событий на конечных устройствах регистрируют события информационной безопасности и отправляют информацию о них в ViPNet TIAS

02. ViPNet TIAS агрегирует информацию о событиях сенсоров, нормализует и сохраняет их в БД

03. ViPNet TIAS с помощью метаправил и обученной математической модели принятия решений анализирует весь поток входящих событий и выявляет действительно значимые угрозы, с большой долей вероятности являющиеся инцидентами информационной безопасности

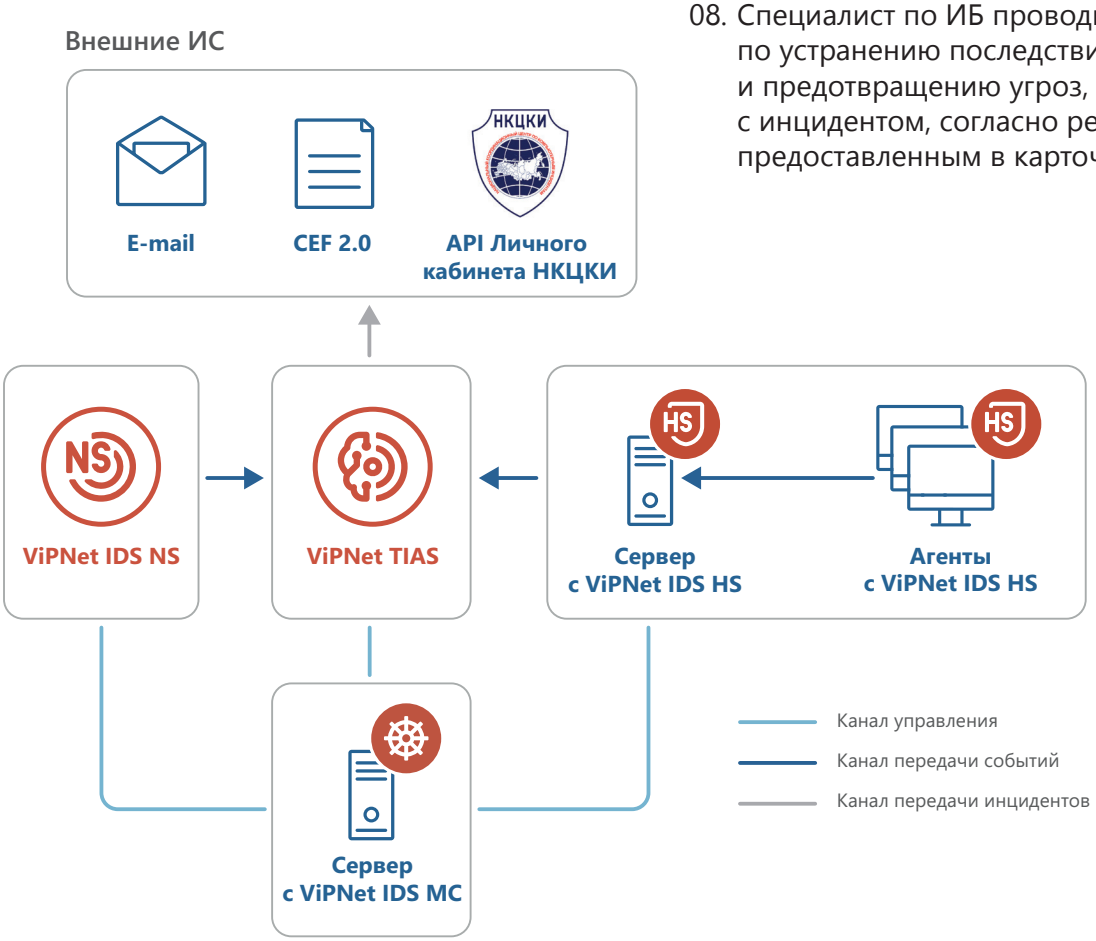
04. При обнаружении подозрений на инцидент ViPNet TIAS:
    > регистрирует данный факт в виде карточки инцидента
    > определяет все связанные с инцидентом события и привязывает их к карточке инцидента
    > оповещает о факте подозрения на инцидент заинтересованных лиц по электронной почте
    > предоставляет инструменты и средства для проведения расследования по инциденту

05. Специалист по ИБ расследует выявленные системой инциденты

06. Специалист по ИБ принимает решение о подтверждении инцидента или о факте ложного срабатывания

07. После подтверждения информация об инциденте передается во внешние системы, в т.ч. в ГосСОПКА

08. Специалист по ИБ проводит мероприятия по устранению последствий инцидента и предотвращению угроз, связанных с инцидентом, согласно рекомендациям, предоставленным в карточке инцидента



ViPNet IDS NS

Система анализа сетевого трафика и обнаружения компьютерных атак (вторжений). Анализирует сетевой трафик и выявляет события информационной безопасности и аномалии в сетевой телеметрии

РЕШАЕМЫЕ ЗАДАЧИ

01. Непрерывно анализирует сетевой трафик, получаемый через SPAN-порт или TAP-устройство.

02. Выявляет события информационной безопасности используя для этого:
    > базы решающих правил;
    > сигнатуры вредоносного ПО и индикаторы компрометации;
    > эвристические методы анализа.

03. Все события фиксируются в локальном хранилище и могут передаваться во внешние системы. При необходимости может быть записан PCAP-файл трафика с потенциальной атакой.

Дополнительно может:
> собирать и хранить данные о сетевых потоках и сессиях;
> анализировать сетевую телеметрию с помощью моделей машинного обучения;
> отображать информацию о сетевых потоках и сессиях в разных представлениях;
> связывать информацию о потоках и выявленных событиях.

04. Предоставляет инструменты построения отчетов по трафику, событиям, сетевым потокам и сессиям.

ViPNet IDS HS

Программный комплекс, который предназначен для обнаружения вторжений на узле на основе сигнатурного и эвристического методов анализа информации.

ViPNet IDS HS используется для повышения уровня защищенности информационных систем, центров обработки данных, рабочих станций пользователей, серверов и коммуникационного оборудования.

ViPNet IDS HS позволяет обнаружить сетевые атаки (DoS- и DDoS-атаки, работу троянских программ и другие) и атаки уровня узла (установку и запуск вредоносного программного обеспечения, компрометацию учетных записей пользователей, наличие вредоносных файлов на узле и другие)

Агент – собирает информацию о функционировании хостов и выполняет ее первичный анализ. Агент представляет собой ПО, которое устанавливается на компьютерах пользователей и серверах

Сервер – получает, хранит и анализирует информацию от агентов

Консоль управления – графический интерфейс для управления агентами и мониторинга их состояния

ФУНКЦИИ

> Производит автоматическое обнаружение компьютерных атак в сетевом трафике и локальных атак на уровне контролируемого узла

> Оповещает администратора о событиях, свидетельствующих о наличии атак, выявленных в результате анализа сетевого трафика и поведения контролируемых узлов

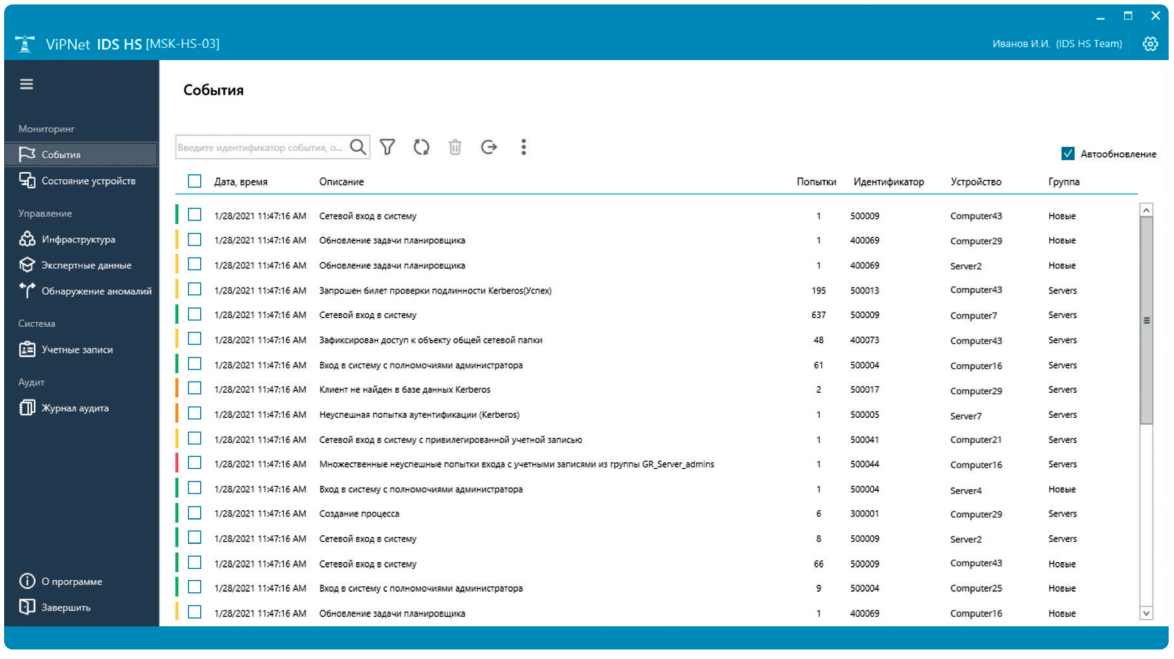
> Отображает список обнаруженных событий в журнале событий и атак ViPNet IDS HS в режиме реального времени

> Производит поиск событий в соответствии с заданными фильтрами

> Позволяет администратору производить настройки для обеспечения оптимальной работы ViPNet IDS HS по выявлению атак

> Обновляет базу решающих правил обнаружения вторжений на узле

> Настраивает и добавляет правила для анализа поведения контролируемых узлов и сетевого трафика



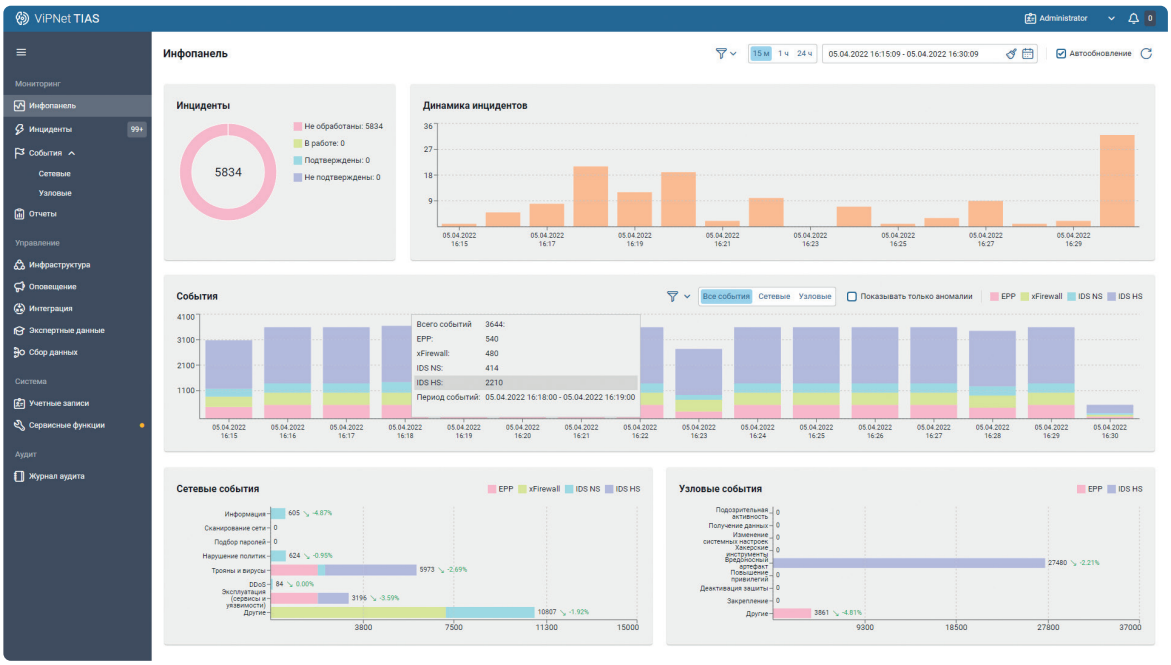
ViPNet TIAS

Программно-аппаратный комплекс, предназначенный для анализа событий информационной безопасности, зарегистрированных сенсорами ViPNet IDS, автоматического выявления инцидентов информационной безопасности на основании потока этих событий и проведения расследований по выявленным инцидентам

ПРИНЦИП РАБОТЫ

1 Метод, основанный на использовании правил и знаний об угрозах

2 Метод машинного обучения математической модели принятия решений



ФУНКЦИИ

> Выполняет сбор событий от сенсоров систем обнаружения вторжений ViPNet IDS. Кроме того, в качестве источников событий могут быть подключены: ViPNet xFirewall, ViPNet EndPoint Protection, ViPNet Coordinator HW5

> Анализирует поступающие события и выявляет инциденты

> Оповещает об инцидентах через веб-интерфейс и по электронной почте

> Предоставляет инструменты для проведения расследований по инцидентам и самостоятельного анализа событий

> Позволяет формировать сводные отчеты по событиям и инцидентам

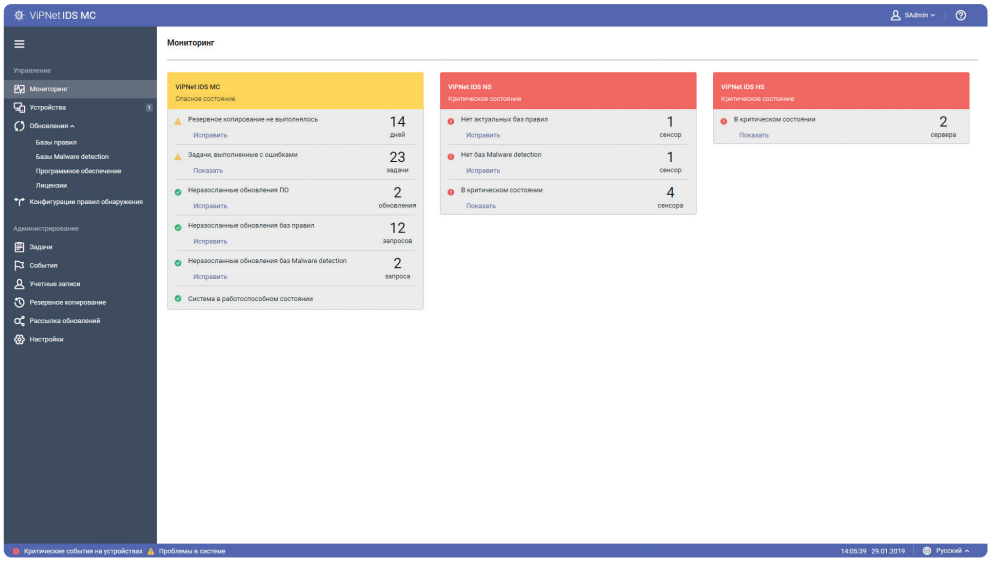
> Позволяет передавать информацию об инцидентах во внешние системы

ViPNet IDS MC

Система централизованного управления и мониторинга состояния сенсоров. Предоставляет возможность управлять всеми компонентами решения

ФУНКЦИИ

> Управление конфигурацией правил обнаружения атак сенсоров
> Управление политиками обнаружения событий на ViPNet IDS HS
> Обновление баз решающих правил на сенсорах
> Мониторинг работоспособности сенсоров
> Обновление программного обеспечения сенсоров
> Управление структурой сенсоров
> Обновление базы сигнатур вредоносного ПО
> Обновление экспертных данных ViPNet TIAS



ПРЕИМУЩЕСТВА

Простота и удобство использования:

> Автоматизация типовых задач по управлению компонентами решения TDR
> Быстрый ввод в эксплуатацию компонентов решения TDR
> Сокращение издержек на развертывание и эксплуатацию решения

Мультиарендный режим эксплуатации позволяет:

> Обеспечить одновременное независимое управление сетевыми и хостовыми сенсорами, принадлежащих различным организациям при помощи личного кабинета администратора организации
> Создавать для каждого домена (организации) уникальные конфигурации правил и автоматически рассылать эти конфигурации
> Вести учет использования обслуживаемых устройств и формировать отчет для систем биллинга

Меры по обеспечению безопасности для значимого объекта КИИ, реализуемые с помощью решения (Приложение к Требованиям по обеспечению безопасности значимых объектов КИИ Российской Федерации, утвержденное приказом ФСТЭК России от 25 декабря 2017 г. N 239)

VII. Предотвращение вторжений (компьютерных атак) (СОВ)

СОВ.0	Разработка политики предотвращения вторжений (компьютерных атак)	Политики предотвращения вторжений разрабатываются компанией «Перспективный мониторинг» и поставляются в решение в виде баз решающих правил для сенсоров и экспертных данных для ViPNet TIAS. В ViPNet IDS NS и ViPNet IDS HS есть возможность создания собственных (пользовательских) правил и политик.
СОВ.1	Обнаружение и предотвращение компьютерных атак	Все требования ФСТЭК России к СОВ и ФСБ России к СОА сетевого уровня и уровня узла выполняются ViPNet IDS NS и ViPNet IDS HS и подтверждаются сертификатами ФСТЭК России и ФСБ России.
СОВ.2	Обновление базы решающих правил	Выполняется процедура выпуска и автоматического централизованного обновления БРП для всех компонентов решения с помощью ViPNet IDS MC.

XII. Реагирование на компьютерные инциденты (ИНЦ)

ИНЦ.0	Разработка политики реагирования на компьютерные инциденты	Политики реагирования на компьютерные инциденты разрабатываются экспертами компании «Перспективный мониторинг» на основе анализа актуальных данных об угрозах, уязвимостях, инструментов и техник проведения атак. В ViPNet TIAS происходит выявление инцидентов и даются рекомендации по реагированию на них.
ИНЦ.1	Выявление компьютерных инцидентов	Реализовано в ViPNet TIAS. Инциденты выявляются автоматически с помощью правил обнаружения инцидентов и математической модели принятия решений. Инциденты однозначно идентифицируются и регистрируются в системе.
ИНЦ.2	Информирование о компьютерных инцидентах	Реализовано в ViPNet TIAS настройкой оповещения заинтересованных лиц о произошедших инцидентах по электронной почте либо передачей информации об инциденте во внешние системы. Есть возможность настройки информирования в зависимости от критичности инцидента, его статуса, а также контролируемого сегмента.
ИНЦ.3	Анализ компьютерных инцидентов	ViPNet TIAS позволяет проводить глубокий анализ компьютерных инцидентов с возможностью поиска и фильтрации данных в событиях, связанных с инцидентом, а также предоставляя образцы исходного трафика и описания 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 также рекомендации по устранению его последствий.
ИНЦ.5	Принятие мер по предотвращению повторного возникновения компьютерных инцидентов	ViPNet TIAS позволяет создавать сводные 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 обеспечивает хранение информации об инцидентах и связанных с инцидентом событиях в течение трех лет. Реализованы все функции защиты информации, предъявляемые к системам обнаружения вторжений.

Меры по защите информации в ГИС и ИСПДН ФСТЭК России, описанные в приказах №17 от 11.02.2013 и №21 от 18.02.2013, обеспечиваемые с помощью решения

VII. Обнаружение вторжений (СОВ)

СОВ.0	Разработка правил и процедур (политик) обнаружения вторжений	Для решения ITDP правила разрабатываются лабораторией АО «Перспективный Мониторинг», имеющей лицензию ФСТЭК России. В IDS NS и IDS HS есть возможность написания собственных правил и политик.
СОВ.1	Обнаружение вторжений	Все требования ФСТЭК России к СОВ и ФСБ России к СОА сетевого уровня и уровня узла выполняются ViPNet IDS NS и ViPNet IDS HS и подтверждаются сертификатами ФСТЭК России и ФСБ России.
СОВ.2	Обновление базы решающих правил	Реализована процедура автоматического централизованного обновления БРП для всех компонентов решения. БРП поставляются лабораторией АО «Перспективный Мониторинг».

XIV. Выявление инцидентов и реагирование на них (ИНЦ)

ИНЦ.0	Разработка правил и процедур (политик) выявления инцидентов и реагирования на них	Правила выявления инцидентов и рекомендации по реагированию на них разрабатываются экспертами компании АО «Перспективный мониторинг» на основе анализа актуальных данных об угрозах, уязвимостях, инструментов и техник проведения атак. Разработанные правила и рекомендации по реагированию применяются в ViPNet TIAS.
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 с помощью правил обнаружения инцидентов и математической модели принятия решений. Инциденты однозначно идентифицируются 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 настройкой оповещения заинтересованных лиц о произошедших инцидентах по электронной почте.
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, предоставляя функции полноценного поиска информации в исходных событиях (в т.ч. с использованием регулярных выражений), а также предоставлением образцов трафика и описания правил выявления событий безопасности.
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 строить отчеты по угрозам и инцидентам, на основании которых могут планироваться мероприятия, направленные на предотвращение повторного возникновения инцидентов.

СЕРТИФИКАЦИЯ

ФСТЭК России

ViPNet IDS 3 в составе ViPNet IDS NS, ViPNet IDS MC, ViPNet IDS TIAS
Сертификат ФСТЭК России на соответствие требованиям к СОВ 4 класса и ТДБ по 4 уровню доверия

ViPNet IDS HS
Сертификат ФСТЭК России на соответствие требованиям СОВ 4 класса защиты

ФСБ России

ViPNet IDS 3 в составе ViPNet IDS NS, ViPNet IDS MC, ViPNet IDS TIAS
Сертификат ФСБ России на соответствие требованиям к СОА класса В

ViPNet IDS HS
Сертификат ФСБ России на соответствие требованиям к СОА класса Б

Свидетельства

> В реестре российского ПО
> В реестре Минпромторга

инфотекс

+7 495 737-61-92
8 800 250-0-260 (бесплатный звонок по России)

soft@infotecs.ru
hotline@infotecs.ru

www.infotecs.ru

TDR26_00RU

ViPNet Virtual Private Network