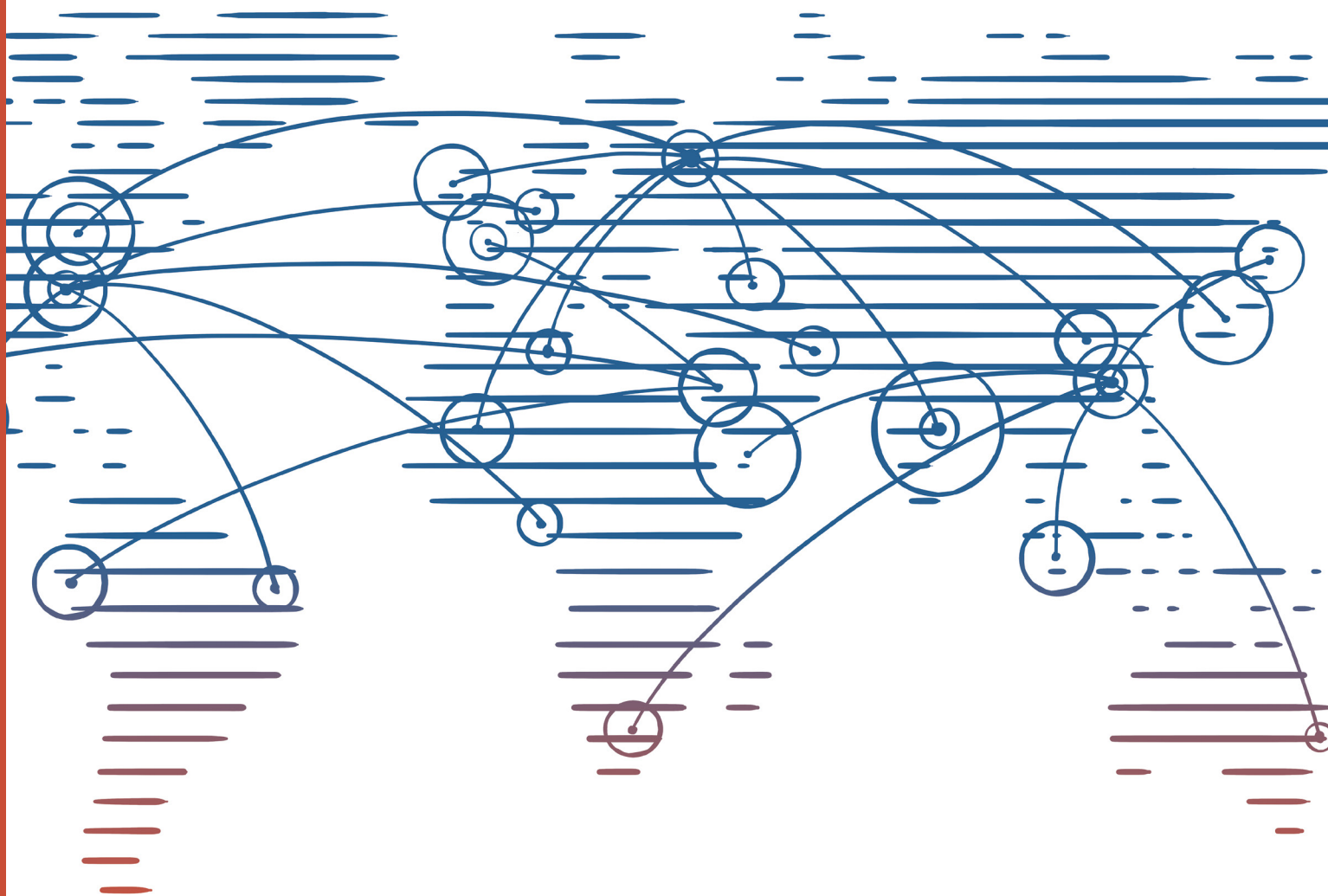


# VIPNet TDR

Решение по обнаружению  
и предотвращению компьютерных атак



>> Массовое использование мобильных устройств, интернета вещей и облачных ресурсов изменило подходы к защите информации. Традиционных мер недостаточно для того, чтобы не только защитить, но даже определить защищаемый периметр. При этом количество и разнообразие угроз информационной безопасности постоянно растет.

Компаниям приходится создавать системы мониторинга и регистрации событий ИБ, а для их эффективной работы необходим штат высококлассных специалистов, способных оперативно реагировать на выявленные угрозы.

Снизить затраты и нагрузку на персонал позволяет ViPNet Threat Detection and Response (TDR). Данное решение способно значительно повысить существующий уровень безопасности информационных систем, центров обработки данных, рабочих станций пользователей, а также серверов и телекоммуникационного оборудования при общем сокращении финансовых и временных затрат на выявление и реагирование на инциденты ИБ.

## ПРЕИМУЩЕСТВА

- > Сокращение среднего времени обнаружения инцидента с 30 до 2 минут по сравнению с ручным анализом событий квалифицированным специалистом
- > Возможность предоставления дополнительных сервисов, в том числе углубленного проведения расследования инцидентов информационной безопасности высококвалифицированными аналитиками компании «Перспективный мониторинг»
- > Снижение затрат на эксплуатацию системы обнаружения вторжений за счет сокращения нагрузки на персонал, обслуживающий систему, и снижения требований к их квалификации
- > Упрощение реагирования на угрозы информационной безопасности благодаря автоматически формируемым рекомендациям и автоматическому сбору связанных с инцидентом событий

## ПРЕДОСТАВЛЯЕМЫЕ ВОЗМОЖНОСТИ

- > Обеспечение непрерывного процесса мониторинга угроз информационной безопасности и обнаружения компьютерных атак
- > Выявление угроз в реальном времени с рекомендацией по их оперативному устранению
- > 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

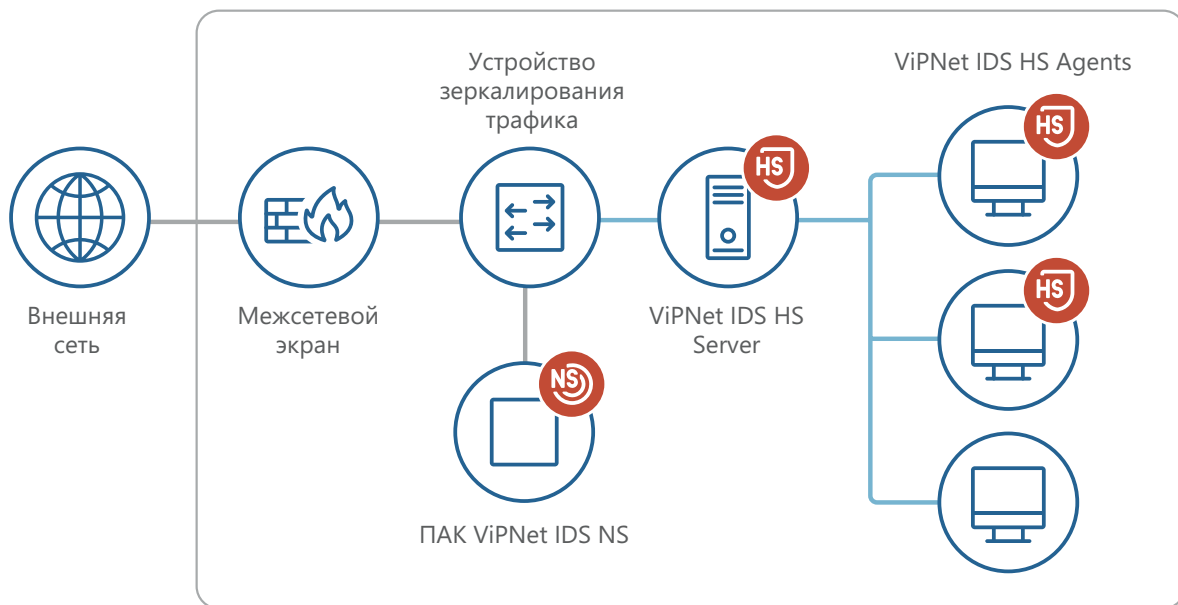
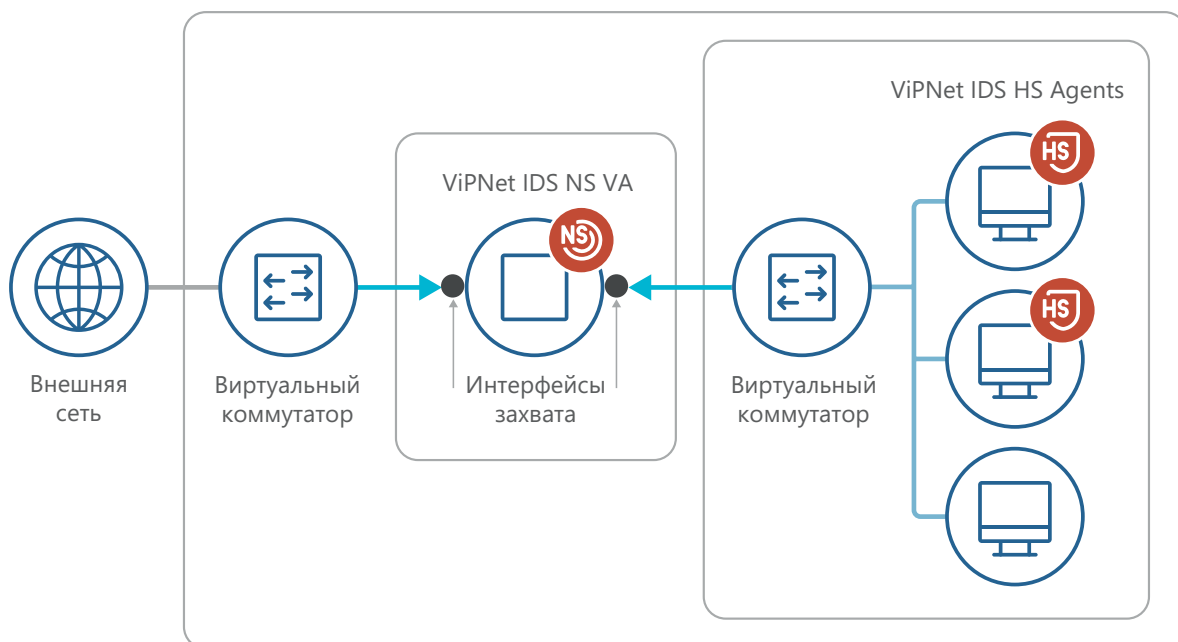
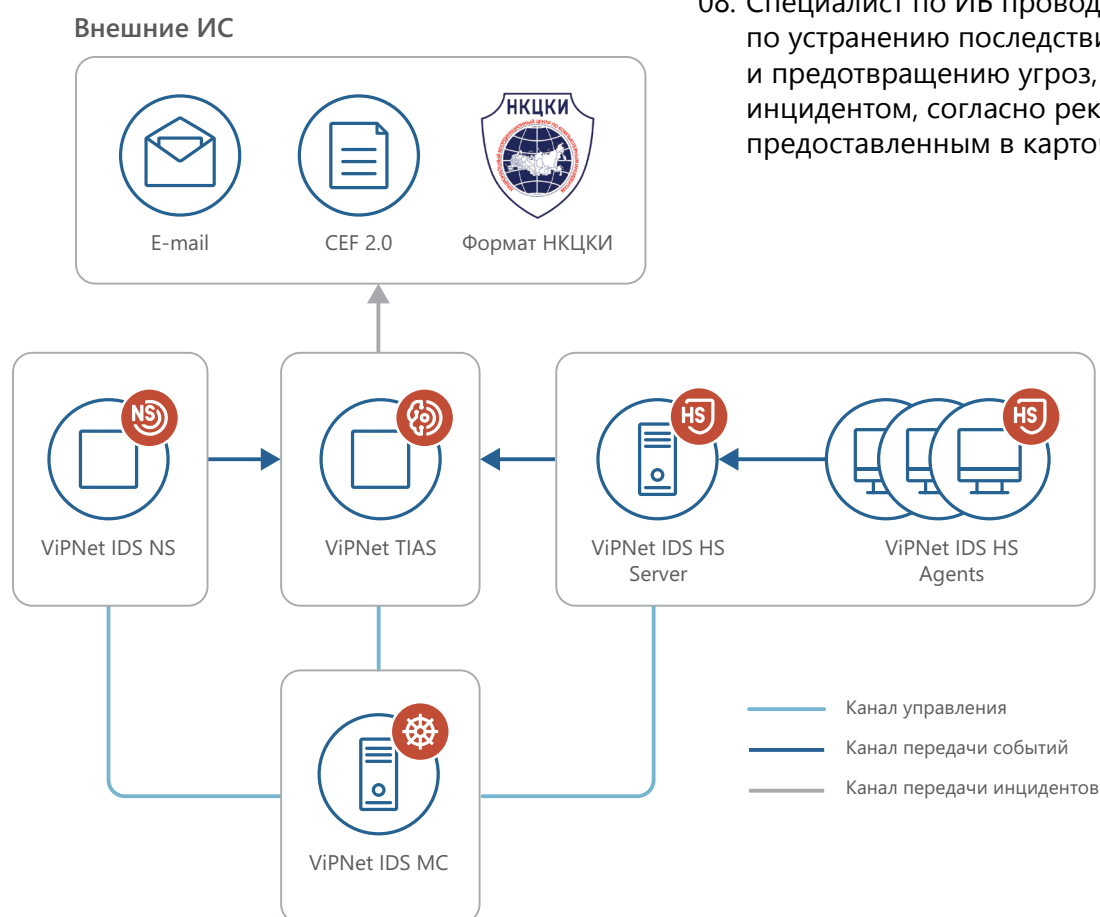


Схема подключения в виртуальной сети



## СЦЕНАРИЙ ИСПОЛЬЗОВАНИЯ

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

Программно-аппаратный комплекс,  
являющийся средством обнаружения атак  
и вредоносного ПО в сетевом трафике.  
ПАК VIPNet IDS NS устанавливается  
на границе сети с целью повышения  
уровня защищенности ИС, ЦОД, серверов  
и коммуникационного оборудования,  
АРМ пользователей



## РЕШАЕМЫЕ ЗАДАЧИ

- > Выполняет автоматическое обнаружение угроз безопасности на основе динамического анализа сетевого трафика, начиная с канального и заканчивая прикладным уровнем модели взаимодействия открытых систем (OSI)
- > Оповещает администратора о событиях, свидетельствующих о наличии атак, выявленных в результате анализа сетевого трафика, а также об обнаружении вредоносного ПО, передаваемого в сетевом трафике
- > Позволяет устанавливать обновления баз правил и сигнатур вредоносного ПО, предоставляемых производителем
- > Ведет журнал регистрации обнаруженных угроз безопасности для последующего анализа, в том числе отображает географическое местоположение атакующего и атакуемого узлов по их IP-адресу с точностью до страны и города
- > Позволяет добавлять собственные пользовательские правила для анализа сетевого трафика
- > Позволяет производить настройку сигнатурных правил обнаружения атак





# 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

The screenshot displays the ViPNet Threat Intelligence Analytics System interface. The main window shows a table of events under the heading 'События IDS HS'. The table has columns for 'Время', 'Наименование', 'Имя узла', 'IP адрес', 'Критично...', 'Категори...', 'Параметры события', and 'Прочее'. The events listed include 'Изменение реестра', 'Установлена задача планировщика', and 'Тестовое событие'. The interface also features a left sidebar with navigation options like 'Мониторинг', 'Инциденты', 'Отчеты', and 'Управление', and a top navigation bar with the system name and user role 'Administrator'.

| Время             | Наименование                    | Имя узла        | IP адрес  | Критично... | Категори...    | Параметры события                                       | Прочее                           |
|-------------------|---------------------------------|-----------------|-----------|-------------|----------------|---|----------------------------------|
| 12.09.2017 10:... | Изменение реестра               | WIN-P4K047H...  | localhost | Низкая      | Подозритель... | Sep 12 07:02:47.012 HS-Server CEF:0[infotecs]/IDS HS... | Тип события = 100000             |
| 12.09.2017 10:... | Установлена задача планировщика | WIN-P4K047H...  | localhost | Средняя     | Подозритель... | Sep 12 07:02:47.012 HS-Server CEF:0[infotecs]/IDS HS... | Тип события = 402000             |
| 12.09.2017 10:... | Изменение реестра               | WIN-P4K047H...  | localhost | Низкая      | Подозритель... | Sep 12 07:02:27.011 HS-Server CEF:0[infotecs]/IDS HS... | Тип события = 100000             |
| 12.09.2017 10:... | Тестовое событие                | Тестовое соо... | localhost | Низкая      | Подозритель... | Sep 12 07:01:33.919 HS-Server CEF:0[infotecs]/IDS HS... | Тип события = 0                  |
| 12.09.2017 05:... | Изменение реестра               | WIN-P4K047H...  | localhost | Низкая      | Подозритель... | Sep 12 07:01:27.539 HS-Server CEF:0[infotecs]/IDS HS... | Тип события = 0                  |
| 12.09.2017 05:... | Изменение реестра               | WIN-P4K047H...  | localhost | Низкая      | Подозритель... | Sep 12 02:58:02.009 HS-Server CEF:0[infotecs]/IDS HS... | Идентификатор сенсора = 742678/1 |
| 12.09.2017 05:... | Изменение реестра               | WIN-P4K047H...  | localhost | Низкая      | Подозритель... | Sep 12 02:57:42.007 HS-Server CEF:0[infotecs]/IDS HS... | Идентификатор сенсора = 742678/1 |
| 12.09.2017 05:... | Изменение реестра               | WIN-P4K047H...  | localhost | Низкая      | Подозритель... | Sep 12 02:43:43.043 HS-Server CEF:0[infotecs]/IDS HS... | Идентификатор сенсора = 742678/1 |
| 12.09.2017 05:... | Изменение реестра               | WIN-P4K047H...  | localhost | Низкая      | Подозритель... | Sep 12 02:43:23.012 HS-Server CEF:0[infotecs]/IDS HS... | Идентификатор сенсора = 742678/1 |
| 12.09.2017 05:... | Изменение реестра               | WIN-P4K047H...  | localhost | Низкая      | Подозритель... | Sep 12 02:43:03.008 HS-Server CEF:0[infotecs]/IDS HS... | Идентификатор сенсора = 742678/1 |
| 12.09.2017 05:... | Изменение реестра               | WIN-P4K047H...  | localhost | Низкая      | Подозритель... | Sep 12 02:42:43.997 HS-Server CEF:0[infotecs]/IDS HS... | Идентификатор сенсора = 742678/1 |
| 12.09.2017 05:... | Изменение реестра               | WIN-P4K047H...  | localhost | Низкая      | Подозритель... | Sep 12 02:42:05.994 HS-Server CEF:0[infotecs]/IDS HS... | Идентификатор сенсора = 742678/1 |
| 12.09.2017 01:... | Изменение реестра               | WIN-P4K047H...  | localhost | Низкая      | Подозритель... | Sep 11 22:00:20.999 HS-Server CEF:0[infotecs]/IDS HS... | Идентификатор сенсора = 742678/1 |
| 12.09.2017 00:... | ET SCAN Potential SMB Scan      | WIN-P4K047H...  | localhost | Низкая      | Подозритель... | Sep 11 21:42:02.998 HS-Server CEF:0[infotecs]/IDS HS... | Идентификатор сенсора = 742678/1 |



# 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



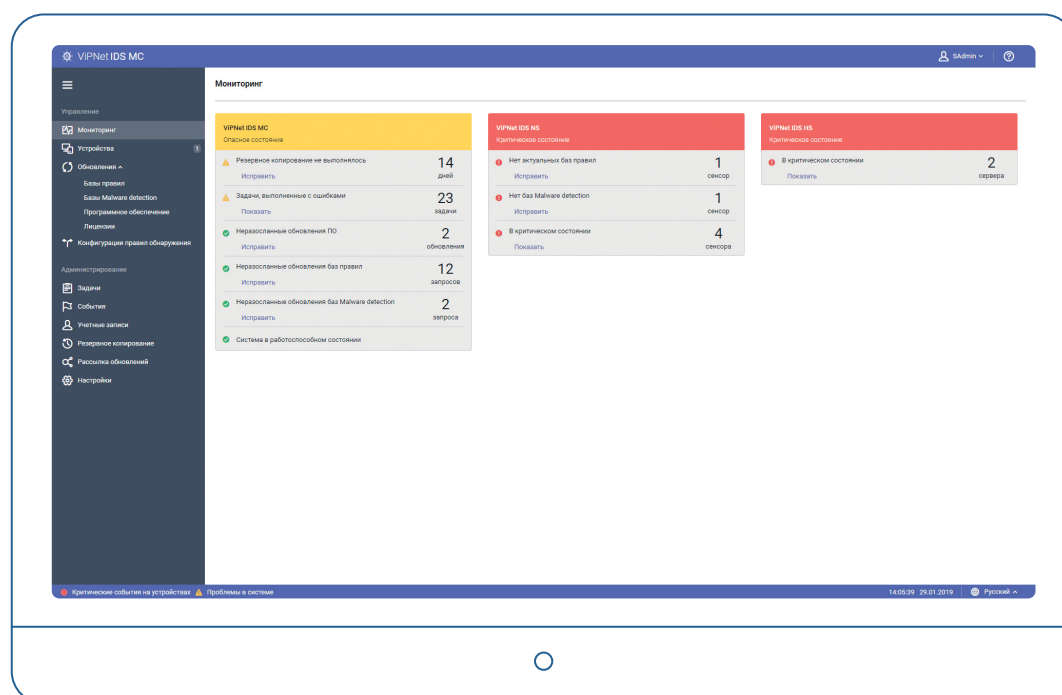


# VIPNet IDS MC

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) (COB)

|       |  |   |
|-------|--|---|
| COB.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. |
| COB.1 | Обнаружение и предотвращение компьютерных атак                   | Все требования ФСТЭК России к COB и ФСБ России к COA сетевого уровня и уровня узла выполняются ViPNet IDS NS и ViPNet IDS HS и подтверждаются сертификатами ФСТЭК России и ФСБ России.  |
| COB.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 (COB)

|       |  |  |
|-------|--|--|
| COB.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. |
| COB.1 | Обнаружение вторжений  | Все требования ФСТЭК России к COB и ФСБ России к COA сетевого уровня и уровня узла выполняются ViPNet IDS NS и ViPNet IDS HS и подтверждаются сертификатами ФСТЭК России и ФСБ России.         |
| COB.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



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

soft@infotecs.ru  
hotline@infotecs.ru

www.infotecs.ru



Содержимое документа носит исключительно информационный характер и не является публичной офертой. Для получения подробной информации об указанных в документе продуктах и услугах вы можете обратиться в АО «ИнфоТекС». Все изображения являются лишь иллюстрациями. Все технические характеристики, внешний вид и комплектность описываемой продукции могут меняться без предварительного уведомления. Символы ™ или ® в документе не используются, однако, если не указано иного, все товарные знаки в данном документе защищены соответствующим правом, которое принадлежит их владельцам.