

Программно-аппаратные комплексы ViPNet IDS

НОЧУ ДПО ЦПК «Учебный центр «ИнфоТекС»
education@infotecs.ru

ОАО «ИнфоТекС», Москва
(495) 737-61-92
www.infotecs.ru

- **Критическая информационная инфраструктура (КИИ)** - объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов
- **Объекты критической информационной инфраструктуры** - информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры
- **Безопасность критической информационной инфраструктуры** - состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак
- **Компьютерная атака** - целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации
- **Компьютерный инцидент** - факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки

(Федеральный закон от 26 июля 2017 г. N 187-ФЗ)

- **Субъекты критической информационной инфраструктуры** - государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.
- **Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА)** на информационные ресурсы Российской Федерации представляет собой единый территориально распределенный комплекс, включающий силы и средства, предназначенные для **обнаружения**, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты. В целях настоящей статьи под информационными ресурсами Российской Федерации понимаются информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления, находящиеся на территории Российской Федерации, в дипломатических представительствах и (или) консульских учреждениях Российской Федерации.


Internal_ViPNe VIPNet IDS Ad Internal_ViPNe Системы Прак Новое издани госсопка — Я! ГосСОПКА X + - □ X

← → ↻ 🏠 gossopka.ru/ 📄 ☆ ⚙️ 🖨️ 📧 ⋮

ГосСОПКА

[Главная](#) [ЧаВО \[FAQ\]](#) [Законодательство](#) [Перечень средств защиты](#) [Судебная практика](#) [Публикации](#)

[Форум](#)



РОСТЕХ ОТРАЗИЛ БОЛЕЕ 300 КИБЕРАТАК В 2018 ГОДУ

🕒 26.03.2019 | ✎ admin |

«РТ-Информ», входящая в Ростех, в 2018 году предотвратила 322 хакерские атаки на предприятия госкорпорации. Всего в прошлом году было зафиксировано более 1,5 млн инцидентов в сфере информационной безопасности. Попытки нападений выявлены и отражены корпоративным центром по обнаружению, предупреждению и ликвидации последствий компьютерных атак (КЦОПЛ), действующим на базе «РТ-Информ». Центр обладает экспертизой в области ИТ-безопасности и

[Read More](#)

Основные понятия и определения

- **Вторжение (атака)** – действие, целью которого является осуществление несанкционированного доступа к информационным ресурсам
- **Система обнаружения вторжений (СОВ)** – программное или программно-техническое средство, реализующие функции автоматизированного обнаружения (блокирования) действий в информационной системе, направленных на преднамеренный доступ к информации, специальные воздействия на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней

Англоязычный термин – Intrusion Detection System (IDS)

- **Администратор СОВ** – уполномоченный пользователь, ответственный за установку, администрирование и эксплуатацию СОВ.
- **Анализатор СОВ** – программный или программно-технический компонент СОВ, предназначенный для сбора информации от сенсоров (датчиков) СОВ, ее итогового анализа на предмет обнаружения вторжения (атаки) на контролируемую ИС
- **База решающих правил** - составная часть СОВ, содержащая информацию о вторжениях (сигнатуры), на основе которой СОВ принимает решение о наличии вторжения (атаки)
- **Данные СОВ** – данные, собранные или созданные СОВ в результате выполнения своих функций
- **Датчик (сенсор) СОВ** – программный или программно-технический компонент

Система обнаружения вторжений (атак) (СОВ, IDS) - один из важнейших элементов обеспечения безопасности КИИ

Защита информации наиболее эффективна, когда в системе поддерживается многоуровневая защита (эшелонированная оборона).

Она складывается из следующих компонент:

- политика безопасности интрасети организации;
 - система защиты хостов в сети;
 - сетевой аудит;
 - защита на основе маршрутизаторов;
 - межсетевые экраны;
 - **системы обнаружения вторжений;**
 - план реагирования на выявленные атаки.
-
- Система обнаружения вторжений - **одна из компонент** обеспечения безопасности сети в многоуровневой стратегии её защиты.
 - СОВ **не должна** рассматриваться как **замена** *любого* из других средств обеспечения безопасности.

Основными причинами наличия возможностей проведения атак в отношении компьютерных систем являются следующие:

- Во многих наследуемых системах не могут быть установлены все необходимые обновления и модификации, связанные с безопасностью.
- Пользователям могут требоваться функциональности сетевых сервисов и протоколов, которые имеют известные уязвимости.
- Как пользователи, так и администраторы делают ошибки при конфигурировании и использовании систем.
- При конфигурировании системных механизмов управления доступом для реализации конкретной политики всегда могут существовать определенные ошибки. Пользователям могут требоваться функциональности сетевых сервисов и протоколов, которые имеют известные уязвимости.

Источники информации

- сетевые СОВ
- хостовые (системные)
- уровня приложений

Метод анализа

- определение допустимого порога
- статистические метрики
- метрики, основанные на правилах
- другие метрики

Режим работы

- пассивные действия при обнаружении атаки
- активные действия при обнаружении атаки

Реакция на выявленное вторжение

- сбор дополнительной информации
- изменение окружения
- выполнение действия против атакующего
- использование SNMP Traps

Варианты развертывания

- позади внешней системы сетевой защиты (межсетевых экранов)
- впереди внешней системы сетевой защиты
- на опорных сетевых каналах
- в критической подсети

Типовая архитектура

- множество сенсоров (средства сбора информации)
- анализатор (средство анализа информации)
- средства реагирования
- средства управления

Стратегия управления

- связи для передачи отчетов
- связи для мониторинга хостов и сетей
- связи для реализации реакций СОВ

Варианты организации управления

- централизованное управление
- частично распределенное управление
- полностью распределенное управление

infotecs Проблема СОВ - размерность данных

Активность
пользовате
ль

Доступ к
ресурсам

Изменения
политик

Вредоносный
трафик

Эксплуатаци
я
уязвимостей

...



более 10 000 000
исходных событий

более 1 000 000 событий ИБ

порядка 10 инцидентов ИБ



Обзор продуктовой линейки ГК «ИнфоТеКС» в области обнаружения компьютерных атак (вторжений)

- ИнфоТеКС ViPNet IDS версии 2.4 – сертифицированная ФСБ и ФСТЭК СОВ для мониторинга сети
- Новое комплексное решение для сквозного интеллектуального мониторинга информационных ресурсов организации (проходит сертификацию в настоящее время)
 - Сетевой сенсор ViPNet IDS NS – улучшенная версия ViPNet IDS
 - Системный (хостовый) сенсор ViPNet IDS HS
 - Система интеллектуального анализа угроз ViPNet TIAS (*Threat Intelligence Analytics System*)
 - Центр управления ViPNet IDS MC
- Продукты работают не только в сетях VipNet – в любых сетях!
 - Имеются доп.возможности при работе в сетях ViPNet
- Возможна работа как в комплексе, так и по отдельности

Сетевой сенсор системы обнаружения атак программно-аппаратный комплекс *ViPNet IDS NS*

- является программно-техническим средством, предназначенным для сбора, хранения и первичного анализа сетевого трафика сегментов защищаемой информационной системы

ViPNet IDS NS предназначен

- для интеграции в компьютерные сети в целях повышения уровня защищенности информационных систем, центров обработки данных, рабочих станций пользователей, серверов и коммуникационного оборудования

ViPNet IDS NS

Операционная система

модифицированный *Linux*-дистрибутив на пакетной базе *CentOS 7*. Обеспечивает поддержку драйверов устройств, а также реализацию среды исполнения для других модулей ПО

Модуль анализа трафика

решает задачи балансировки входящих сетевых пакетов между потоками обработчиков, предварительную обработку трафика для выявления аномалий в заголовках сетевых протоколов или последовательности команд сетевых протоколов

СУБД

система управления базами данных, решает задачи хранения и доступа к данным сетевого сенсора, включая журнал обнаруженных событий и образцы сетевого трафика

Веб-сервер

предоставляет внешние программные интерфейсы для идентификации и аутентификации администраторов, управления функциями безопасности *ViPNet IDS NS*, просмотра журналов аудита

Подсистема аудита

реализует формирование, регистрацию и защиту записей аудита

Контроль целостности и работоспособности

обеспечивает выполнение пакета тестовых программ для периодического контроля состояния компонентов ПО *ViPNet IDS NS*

Интеграция с внешними системами

обеспечивает поддержку прикладных интерфейсов программирования для взаимодействия с *ViPNet IDS MC*, *ViPNet TIAS* и другими продуктами, входящими в состав защищаемой информационной системы

| № п/п | Метод анализа сетевого трафика | Особенности метода |
|-------|---|--|
| 1 | Анализ сетевого трафика сигнатурным методом | Основывается на выявлении в потоке данных такой последовательности, которая определена как признак атаки (например, сообщения об ошибках, записанные в журнал приложения) |
| 2 | Предварительная обработка сетевого трафика и анализ служебных заголовков протоколов | Основан на использовании препроцессоров модуля обнаружения, под которыми понимаются подключаемые модули обнаружения атак, имеющие расширенную функциональность по сравнению с простейшим методом сигнатурного обнаружения атак |
| 3 | Анализ файлов в сетевом трафике на наличие вредоносного программного обеспечения | Применяется метод сигнатурного анализа файлов, который заключается в определении и сравнении сигнатуры файла, обнаруженного в сетевом трафике, с перечнем известных сигнатур вредоносного программного обеспечения |
| 4 | Выявление аномалий сетевого трафика эвристическим методом | При выявлении аномалий администратор заранее знает, какое поведение системы является стандартным для системы. Администратор может самостоятельно задать параметры для определения аномального поведения |

| № шага | Описание шага | Пояснение к шагу |
|--------|---|---|
| 1 | Информация о параметрах сетевого трафика с заданной периодичностью сохраняется в служебных статистических журналах | По умолчанию статистика регистрируется каждые 10 минут |
| 2 | По факту накопления статистики за заданный временной интервал формируется первоначальная эталонная модель сетевого трафика | В эталонной модели содержатся вычисленные максимальные и минимальные значения контролируемых параметров сетевого трафика. По умолчанию первоначальная эталонная модель формируется на основе статистики, собранной за 40 дней |
| 3 | Для эталонной модели на основе математических алгоритмов рассчитываются прогнозируемые диапазоны значений для каждого контролируемого параметра трафика на период в одну неделю | Фиксированный период в одну неделю связан с необходимостью прогнозировать сетевую активность различным образом для каждого дня недели |
| 4 | Текущий сетевой трафик сравнивается с эталонным с заданной периодичностью | При этом информация о параметрах сетевого трафика продолжает накапливаться в служебных статистических журналах (см. шаг 1). Значение каждого контролируемого параметра сравнивается с эталонным. Сетевой трафик считается аномальным, когда значение одного из параметров вышло за пределы прогнозируемого для него диапазона значений, определенного в эталоне |
| 5 | В случае выявления аномалии в журнале регистрируется событие информационной безопасности | |
| 6 | С заданной периодичностью выполняется перерасчет эталонной модели на основе статистики за указанное количество дней до текущего момента | По умолчанию перерасчет эталонной модели выполняется 1 раз в три недели – каждый 21 день на основе статистики, накопленной за 40 дней до текущего момента |

Системные правила, сформированные специалистами ОАО «ИнфоТеКС»

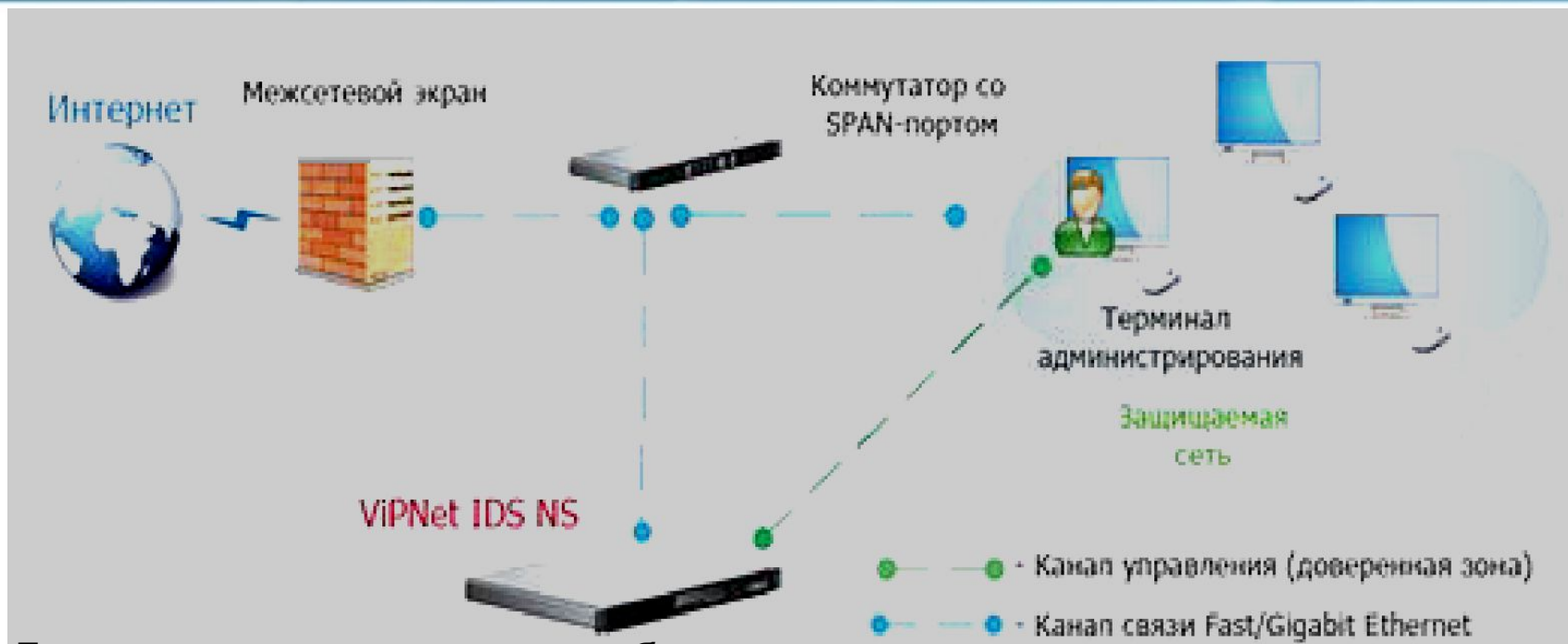
- загружаются в *ViPNet IDS NS* в составе базы правил
- состоят из сигнатурных и препроцессорных правил

Пользовательские правила, созданные администраторами *ViPNet IDS NS*

- создаются вручную с помощью конструктора или загружаются на *ViPNet IDS NS* списком из файла
- можно создать или загрузить не более 1000 пользовательских правил

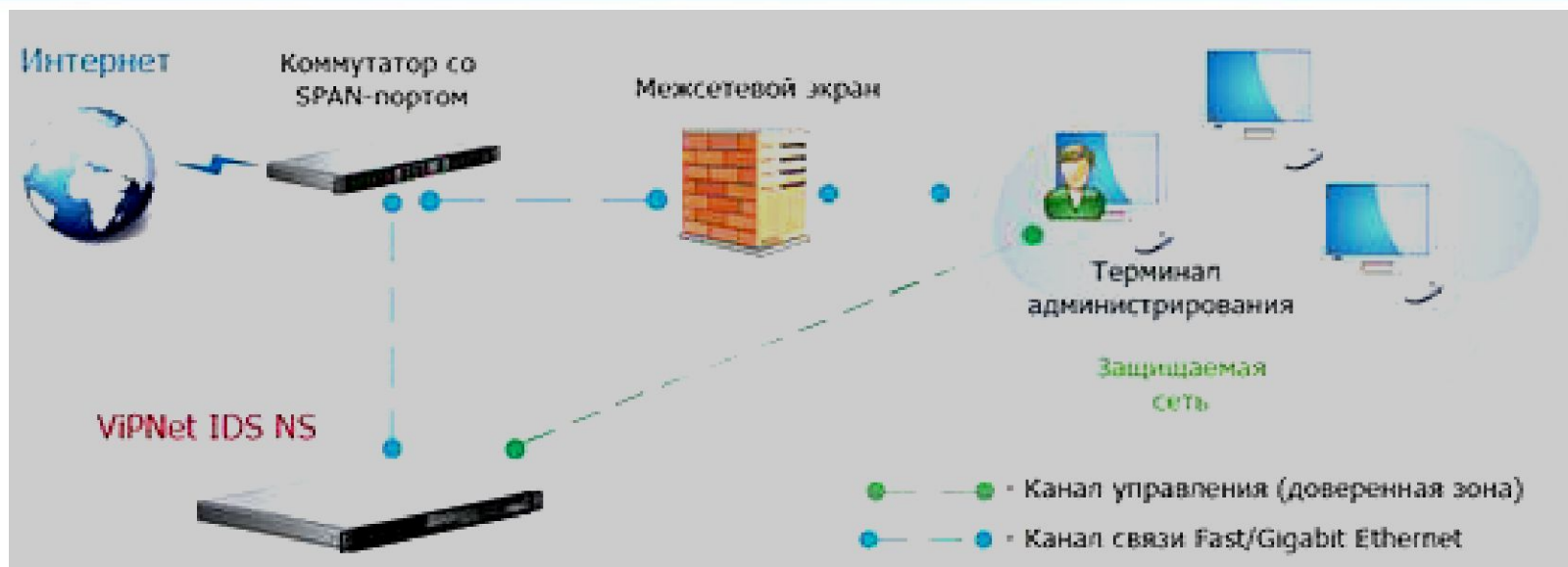
Пользовательские правила, созданные и назначенные *ViPNet IDS NS* Администраторами централизованной системы управления *ViPNet IDS MC*

- Администратор *ViPNet IDS MC* может назначить *ViPNet IDS NS* не более 1000 правил



Достоинствами данного способа подключения являются:

- нагрузка на *ViPNet IDS NS* снижается, так как часть трафика блокируется межсетевым экраном;
- объем информации, поступающей администратору, уменьшается;
- появляется возможность настройки правил на межсетевом экране с целью предотвращения реализации выявленных угроз безопасности информации;
- позволяет выявлять угрозы безопасности, пропущенные межсетевым экраном, внутри защищенного контура как от внешних, так и от внутренних нарушителей (при соответствующих настройках сети)



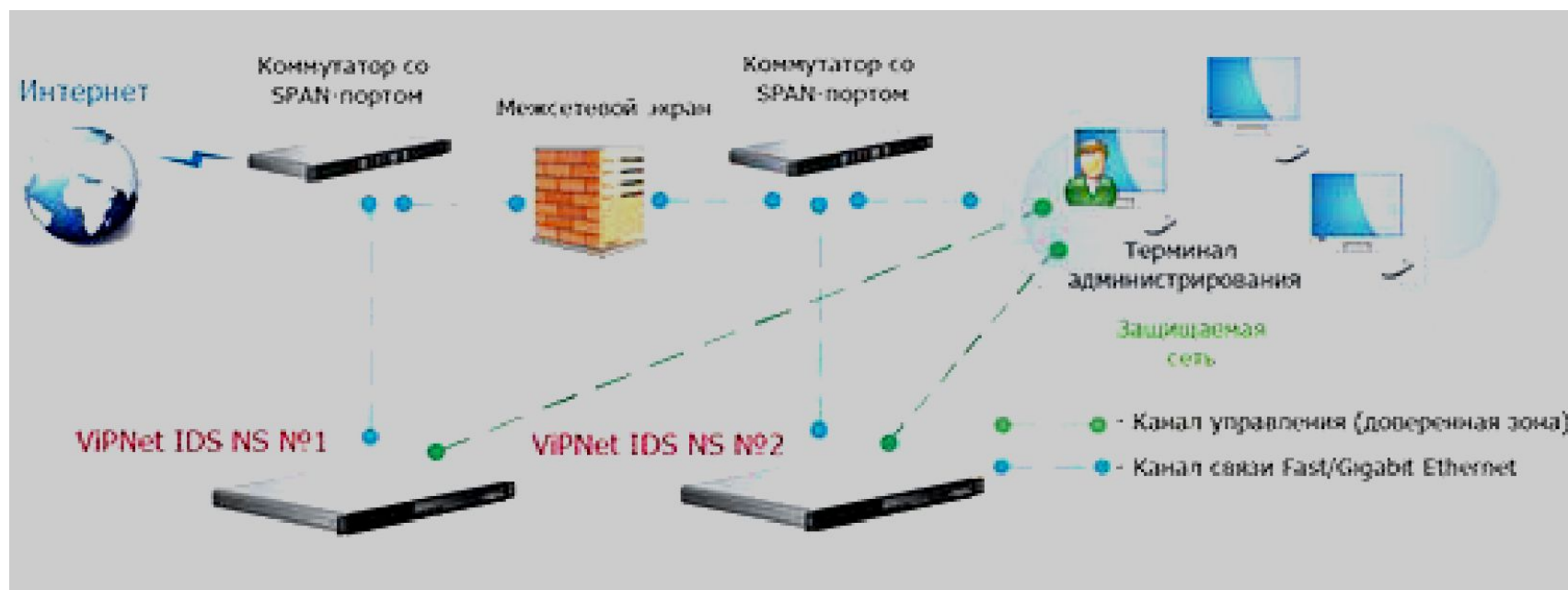
Преимущества данного способа подключения:

- позволяет получать наиболее полную информацию об угрозах безопасности со стороны внешних нарушителей, как проникших в защищаемый контур через межсетевой экран, так и пытавшихся взломать защиту межсетевого экрана.

Недостатки данного способа подключения:

- возрастает нагрузка на *ViPNet IDS NS*;
- исключается возможность анализа трафика внутри защищаемого контура;
- исключается возможность анализа эффективности работы правил блокировки угроз безопасности, настроенных на межсетевом экране.

Подключение *VIPNet IDS NS* до и после межсетевого экрана

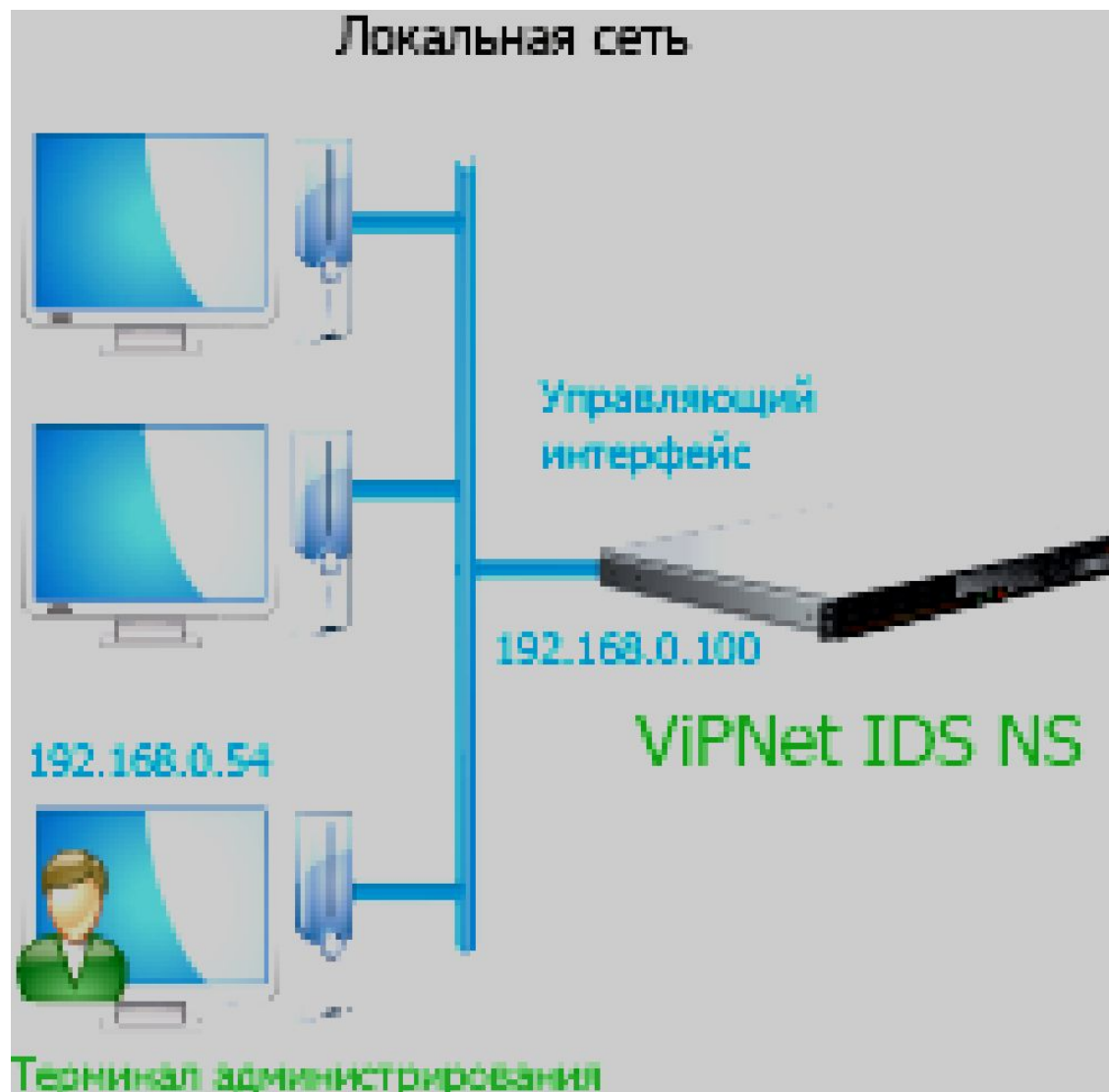


Преимущества данного способа подключения:

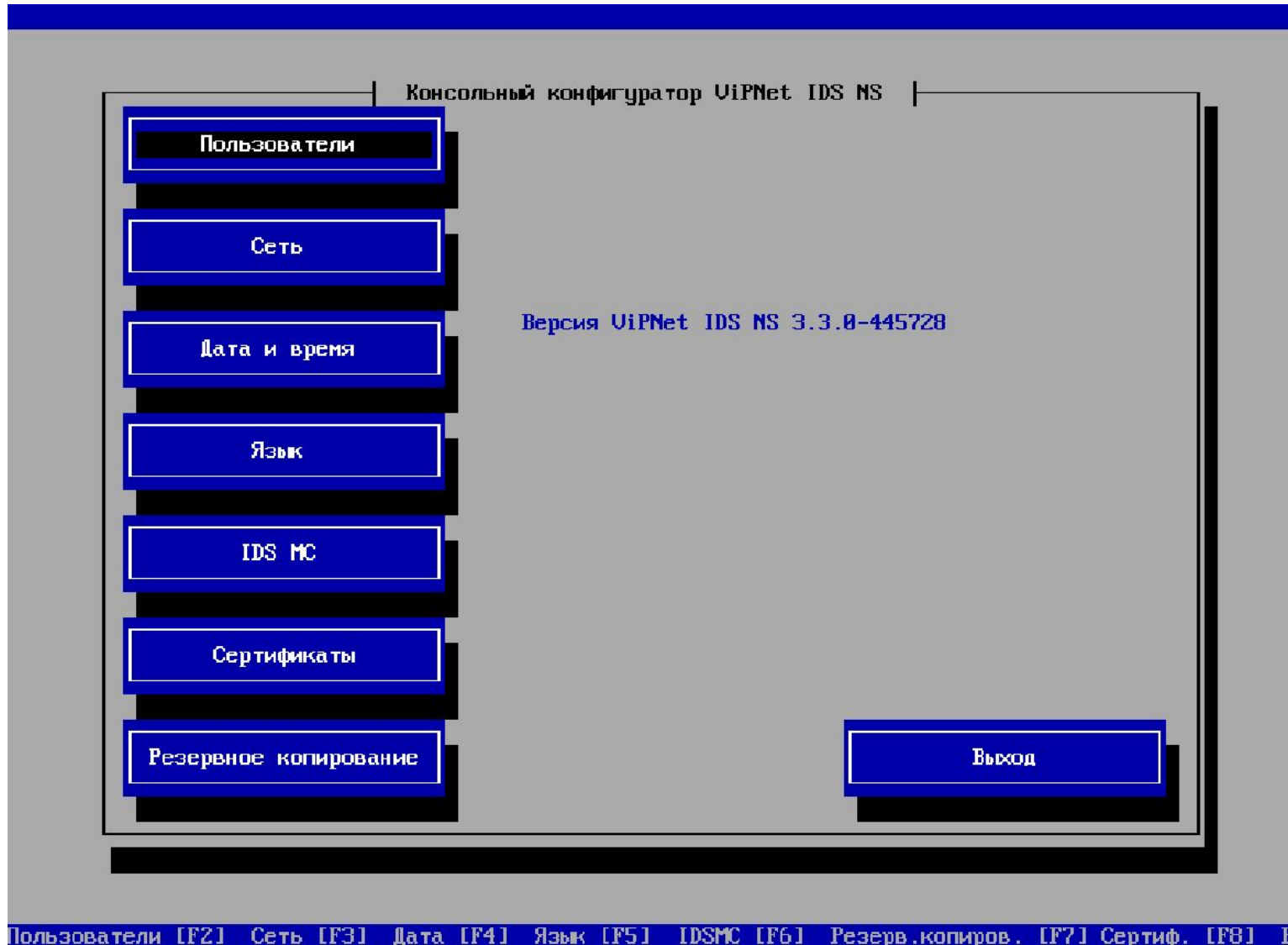
- реализует преимущества и устраняет недостатки двух предыдущих способов подключения.

Недостатки данного способа подключения:

- возрастает стоимость системы.



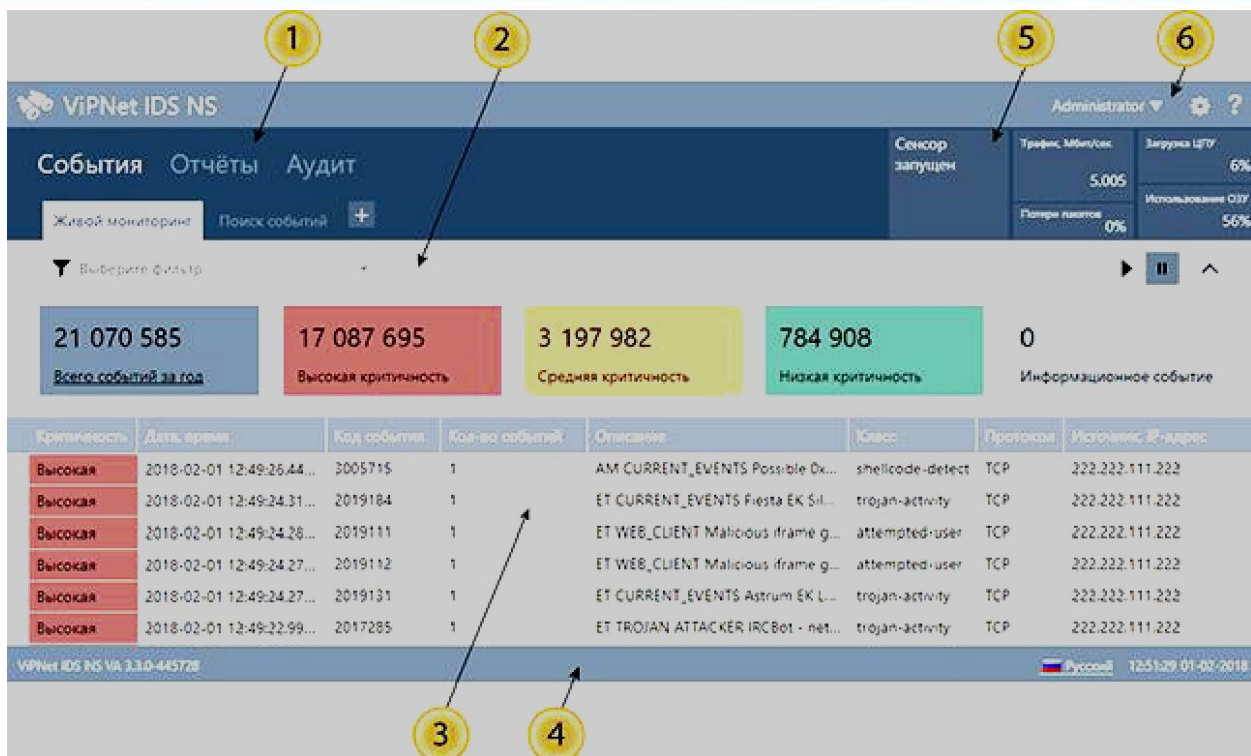
Главное окно программы «Консольный конфигуратор» *ViPNet IDS NS*



Терминал администрирования – это компьютер, предназначенный для управления *VIPNet IDS NS* через веб-интерфейс или с помощью консоли по протоколу *SSH*. При этом терминал администрирования должен иметь сетевой доступ к *VIPNet IDS NS*. Для управления *VIPNet IDS NS* может быть задействовано несколько терминалов администрирования.

| Элемент | Ед. измерения | Характеристика |
|----------------------------------|---------------|--|
| Процессор | | Intel Pentium 4 / AMD Athlon 64 или другой более поздней версии x86-совместимый процессор с поддержкой SSE2 |
| Объем оперативной памяти | Гбайт | не менее 2 |
| Свободное место на жестком диске | Мбайт | не менее 200 |
| Сетевой адаптер | шт. | не менее 1 |
| Операционная система | | семейства Windows (Windows 7/Windows Server 2008R2 и более поздние версии) |
| Веб-браузер | | Mozilla Firefox (версии 58.0 и выше) |
| | | Opera (версии 50.0 и выше) |
| | | Google Chrome (версии 63.0 и выше) |
| SSH-клиент | | с паролем типом аутентификации (например, Bitvise SSH Client или PuTTY), предназначенный для удаленного подключения к консоли <i>VIPNet IDS NS</i> по протоколу <i>SSH</i> |

Начальная страница веб-интерфейса *VIPNet IDS NS*



| Цифра на рисунке | Элемент веб-интерфейса |
|------------------|------------------------|
| 1 | Панель навигации |
| 2 | Панель инструментов |
| 3 | Панель просмотра |
| 4 | Панель состояния |
| 5 | Инфопанель |
| 6 | Панель заголовка |

ViPNet IDS NS Administrator

События Отчёты Аудит

Живой мониторинг Поиск событий +

События за последние 24 часа

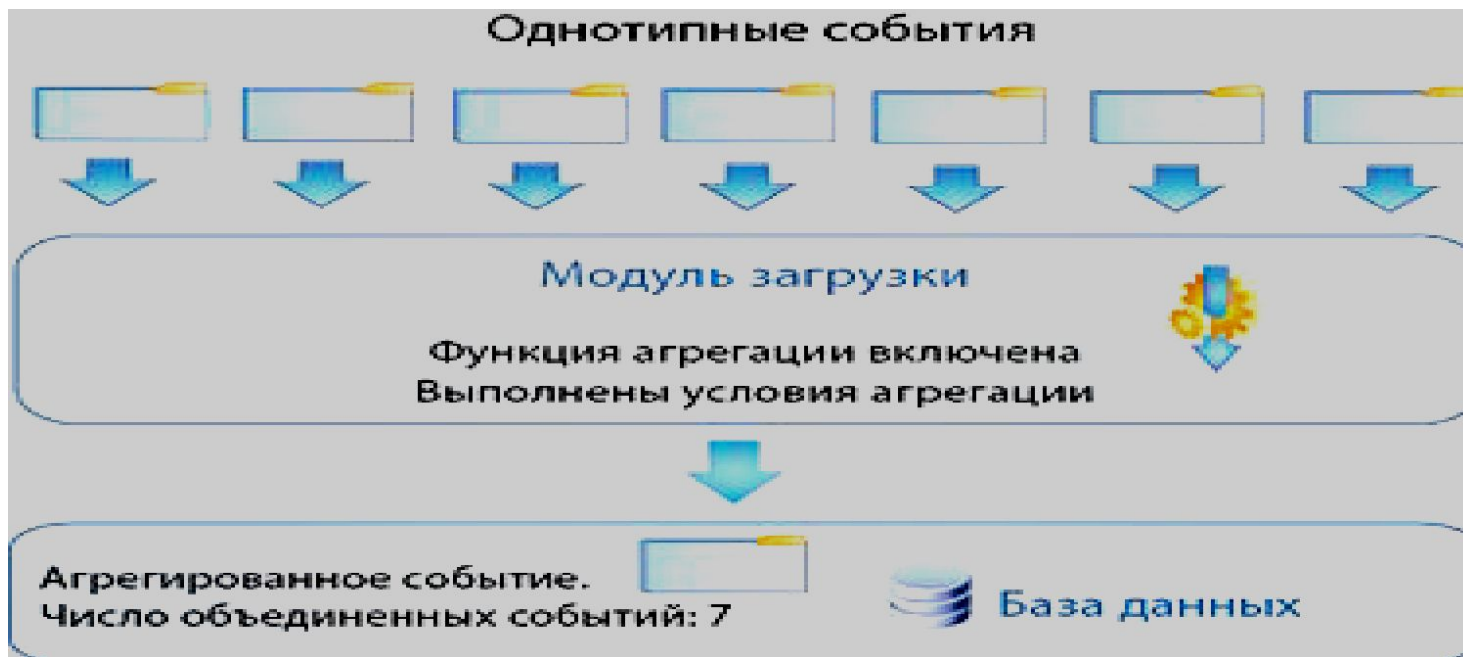
Найдено более 10000 записей: ⚙️ 📄 ↻ ⬇️

| Дата, время | ↑ Критичность | Код события | Тип события | Класс |
|----------------------------|---------------|-------------|---------------------|------------------------|
| 2018-01-25 12:37:19.89043 | Высокая | 2007903 | Сигнатурное событие | web-application-attack |
| 2018-01-25 12:37:19.624902 | Высокая | 2008407 | Сигнатурное событие | web-application-attack |
| 2018-01-25 12:37:19.619876 | Высокая | 2008408 | Сигнатурное событие | web-application-attack |
| 2018-01-25 12:37:19.617484 | Высокая | 2008409 | Сигнатурное событие | web-application-attack |
| 2018-01-25 12:37:19.515186 | Высокая | 2008099 | Сигнатурное событие | web-application-attack |
| 2018-01-25 12:37:19.234419 | Высокая | 2001188 | Сигнатурное событие | policy-violation |
| 2018-01-25 12:37:19.212806 | Высокая | 2001188 | Сигнатурное событие | policy-violation |

Уровни важности событий информационной безопасности

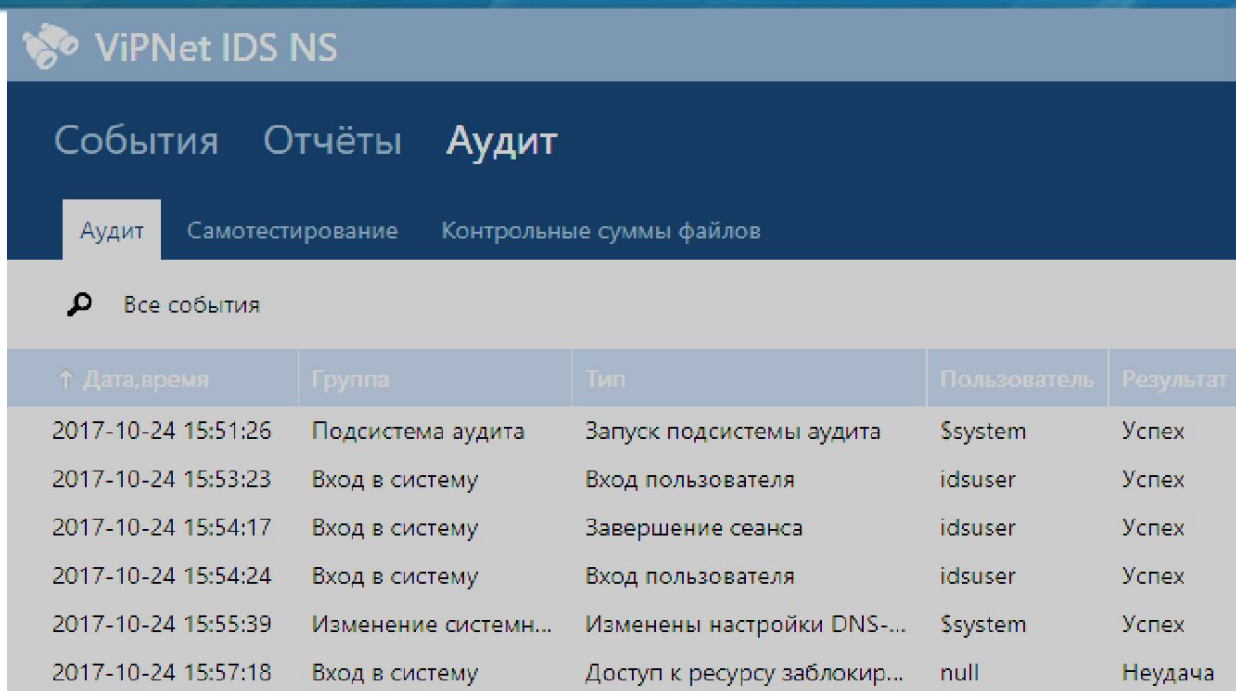
| Уровень важности | Характеристика | Цветовое отображение |
|------------------------|--|----------------------|
| высокий уровень | наиболее опасные события | Красный |
| средний уровень | события средней степени опасности | Желтый |
| низкий уровень | наименее критичные события | Зеленый |
| информационный уровень | события, носящие уведомительный характер | Белый |

Принцип агрегирования однотипных событий в Журнале событий



В механизме агрегации однотипными считаются следующие события:

- события, зарегистрированные при срабатывании правил с одинаковым номером, при этом должны совпадать *ip*-адреса узла-источника и узла-назначения пакета;
- события, зарегистрированные при обнаружении файлов с вредоносным программным обеспечением, имеющих одинаковые сигнатуры, при этом должны совпадать *ip*-адреса узла-отправителя и узла-получателя файла.

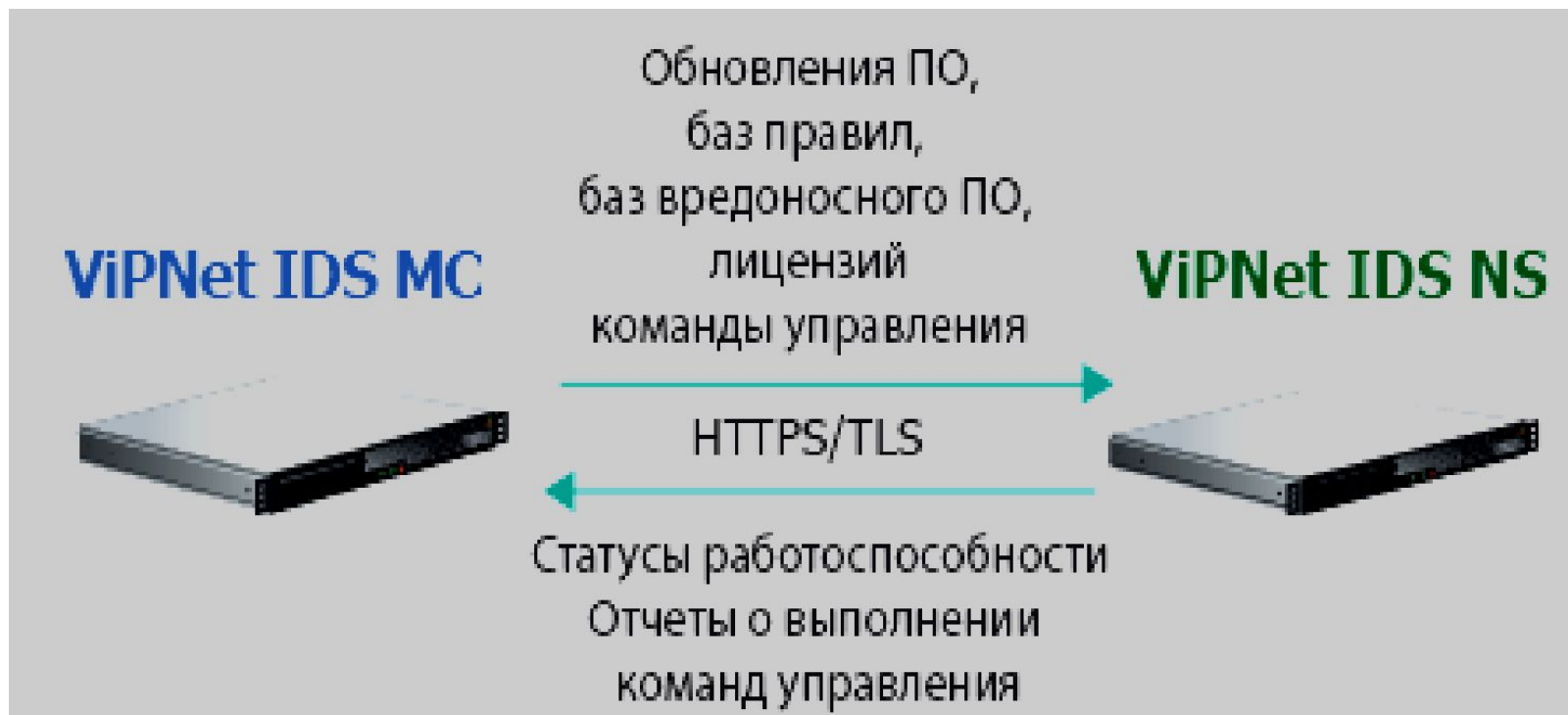


| ↑ Дата, время | Группа | Тип | Пользователь | Результат |
|---------------------|----------------------|------------------------------|--------------|-----------|
| 2017-10-24 15:51:26 | Подсистема аудита | Запуск подсистемы аудита | \$system | Успех |
| 2017-10-24 15:53:23 | Вход в систему | Вход пользователя | idsuser | Успех |
| 2017-10-24 15:54:17 | Вход в систему | Завершение сеанса | idsuser | Успех |
| 2017-10-24 15:54:24 | Вход в систему | Вход пользователя | idsuser | Успех |
| 2017-10-24 15:55:39 | Изменение системн... | Изменены настройки DNS-... | \$system | Успех |
| 2017-10-24 15:57:18 | Вход в систему | Доступ к ресурсу заблокир... | null | Неудача |

Каждая запись в *Журнале аудита* содержит следующую информацию о зафиксированном событии:

- дату и время регистрации с точностью до секунды;
- группу, в которую входит событие данного типа (например, «Вход в систему»);
- тип – описание события (например, «Вход пользователя»);
- имя пользователя, инициировавшего процесс, в результате которого было зарегистрировано событие (например, «*admin*»);
- результат действия, при котором было зарегистрировано событие («Успех» или «Неудача»);
- дополнительные параметры, содержащие уточняющую информацию о событии. Например, для типа события «*Создание резервной копии конфигурации*» в качестве параметра приводится название запущенного задания резервного копирования.

Схема взаимодействия *ViPNet IDS NS* и *ViPNet IDS MC*



Система обнаружения вторжений на хостах ViPNet IDS HS – это 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.

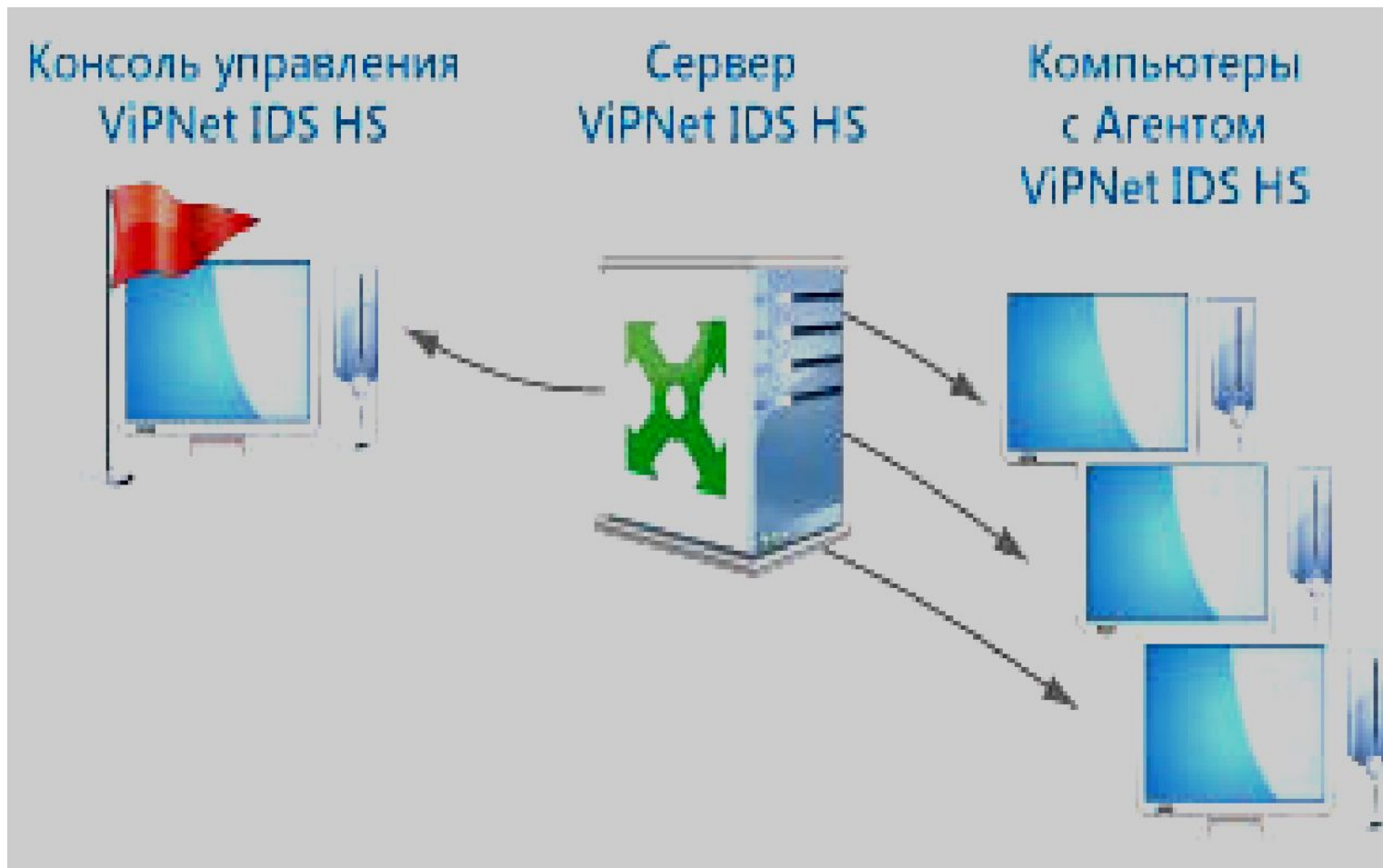
ViPNet IDS HS позволяет обнаружить сетевые атаки (*DoS*- и *DDoS*-атаки, работу троянских программ и др.) и атаки уровня узла (установку и запуск вредоносного программного обеспечения, компрометацию учетных записей пользователей, наличие вредоносных файлов на узле и другие).

В состав *ViPNet IDS HS* входят следующие компоненты:

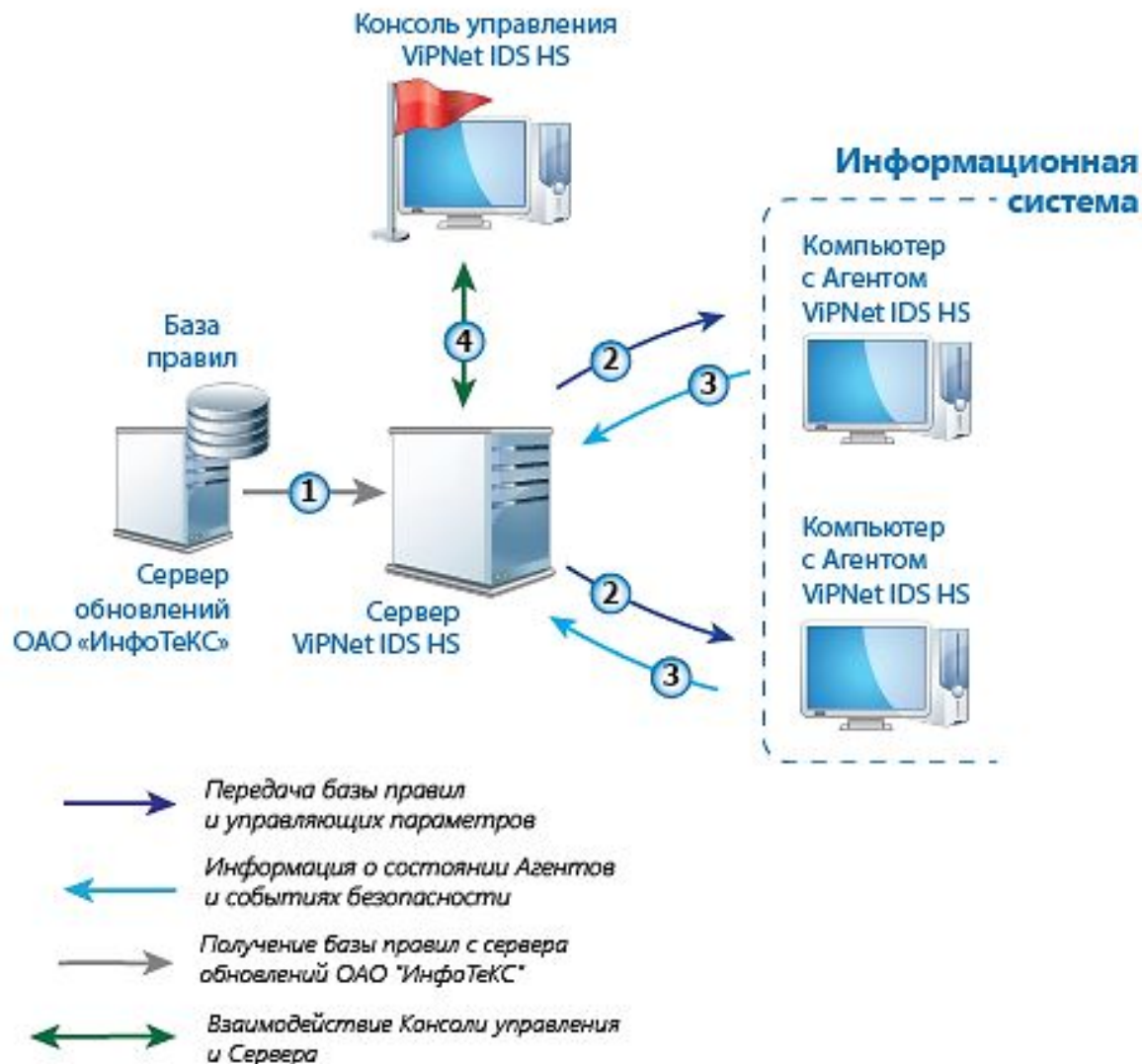
ViPNet IDS HS Агент – компонент устанавливается на узлы, которые нужно контролировать с помощью *ViPNet IDS HS* (*контролируемые узлы*). Выполняет сбор информации и первичную обработку событий на узле, на котором он установлен, и передает информацию на компьютер с установленным ПО *ViPNet IDS HS Сервер*;

ViPNet IDS HS Сервер – компонент служит для получения информации от *Агентов*, её хранения и анализа. С *Сервера* администратор отправляет базу правил на *контролируемые узлы*;

ViPNet IDS HS Консоль управления – компонент представляет собой графический интерфейс для управления *контролируемыми узлами* и контроля их состояния.



Порядок взаимодействия компонентов ViPNet IDS HS



сигнатурный метод

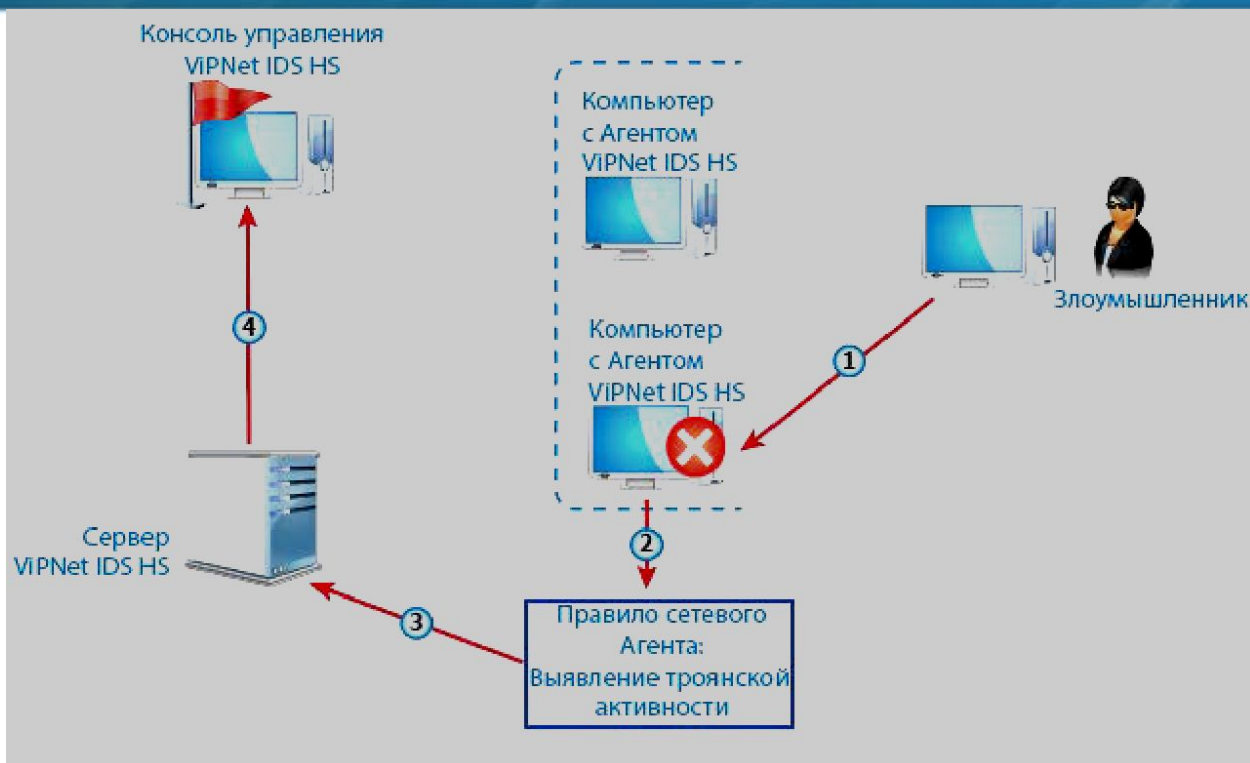
основывается на выявлении в потоке данных такой последовательности, которая определена как признак атаки (например, сообщения об ошибках, записанные в журнал приложения)

эвристический метод выявления аномалий

используется в случае, когда администратор заранее знает, какое поведение системы является стандартным для системы. Администратор может самостоятельно задать параметры для определения аномального поведения. Эвристический метод применяется в *VIPNet IDS HS* для выявления аномалий сетевого трафика и поведения пользователей системы

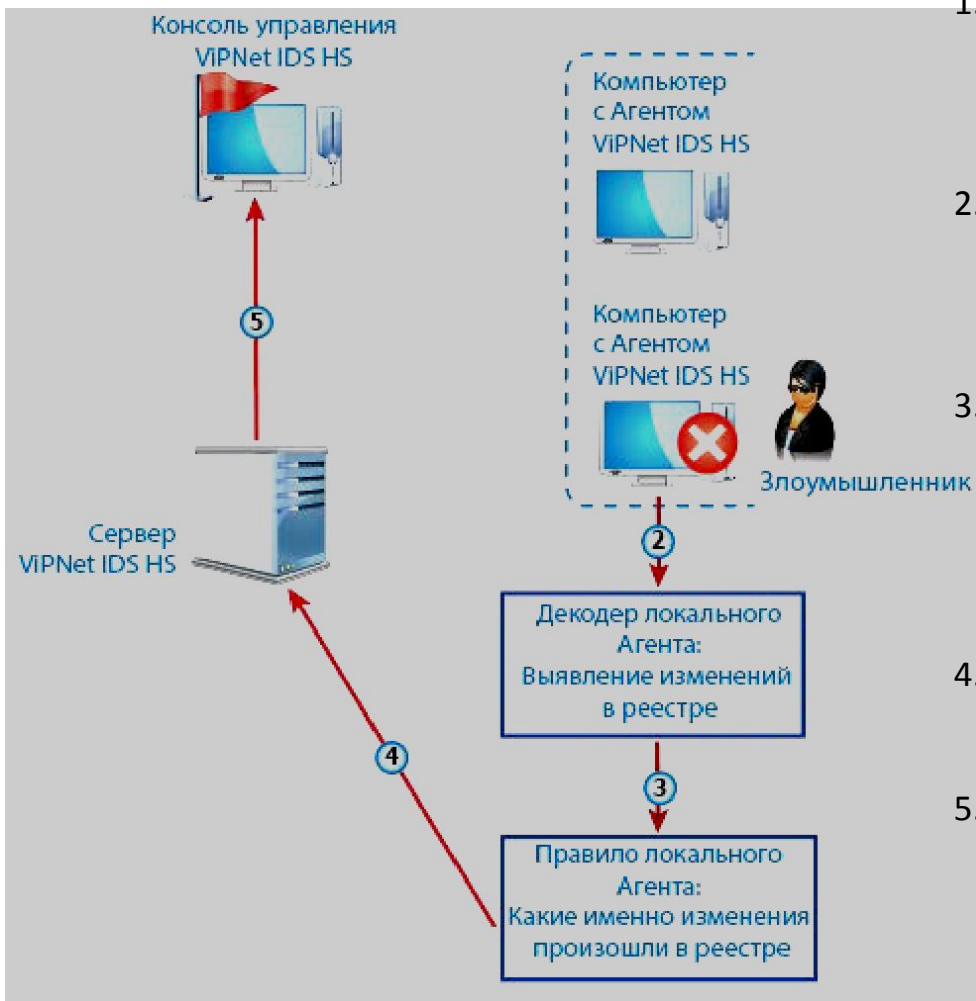
| № п/ п | Уровень критичности события | Пояснение |
|--------------|--------------------------------|--|
| 1 | Критические события | Наиболее опасные события, которые угрожают работоспособности узла и системе в целом. Требуют принятия экстренных мер со стороны администратора |
| 2 | Опасные события | События средней степени опасности, которые могут привести к сбоям в работе системы |
| 3 | Важные события | События, которые могут косвенно свидетельствовать об осуществлении вредоносной активности на узле |
| 4 | Информационные события | Носят уведомительный характер, оповещают о системном событии |

Обнаружение атак сигнатурным методом в *ViPNet IDS HS* на сетевом уровне



1. Злоумышленник получил удаленный доступ к одному из контролируемых узлов и запустил троянскую программу.
2. С помощью правила *Сетевого агента* произошло обнаружение сигнатуры работы троянской программы.
3. Данные об обнаруженной атаке были переданы на *Сервер*.
4. В *Консоли управления* отобразились сведения об обнаруженной атаке.

Обнаружение атак сигнатурным методом в VIPNet IDS HS на локальном уровне



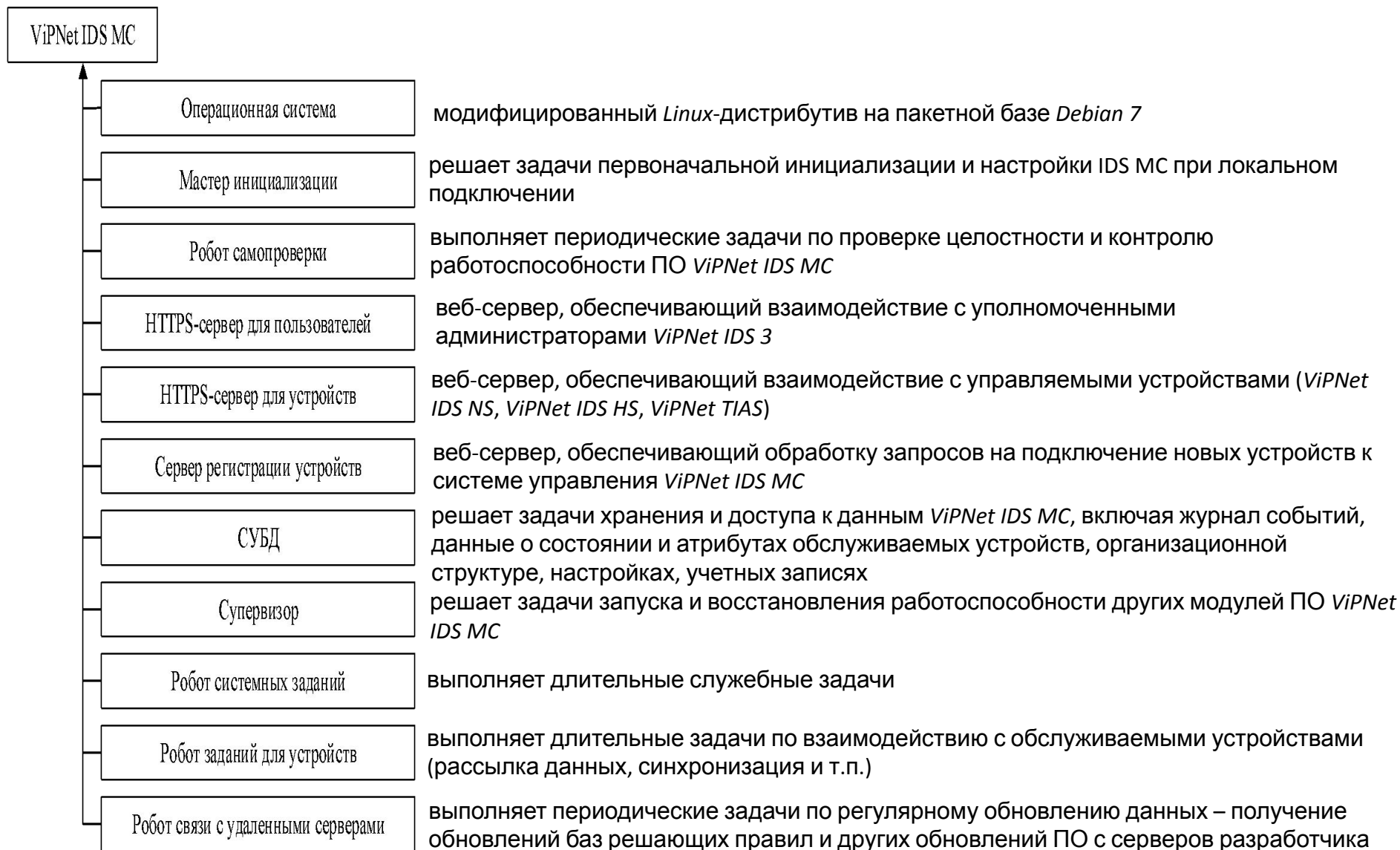
1. Злоумышленник получил удаленный доступ к одному из контролируемых узлов и меняет записи в реестре.
2. С помощью декодера Локального агента произошло обнаружение изменений в реестре.
3. С помощью правила Локального агента было определено, какие именно изменения произошли в реестре: какие ключи, разделы, параметры реестра были изменены.
4. Данные об обнаруженной атаке были переданы на Сервер.
5. В Консоли управления отобразились данные об обнаруженной атаке.

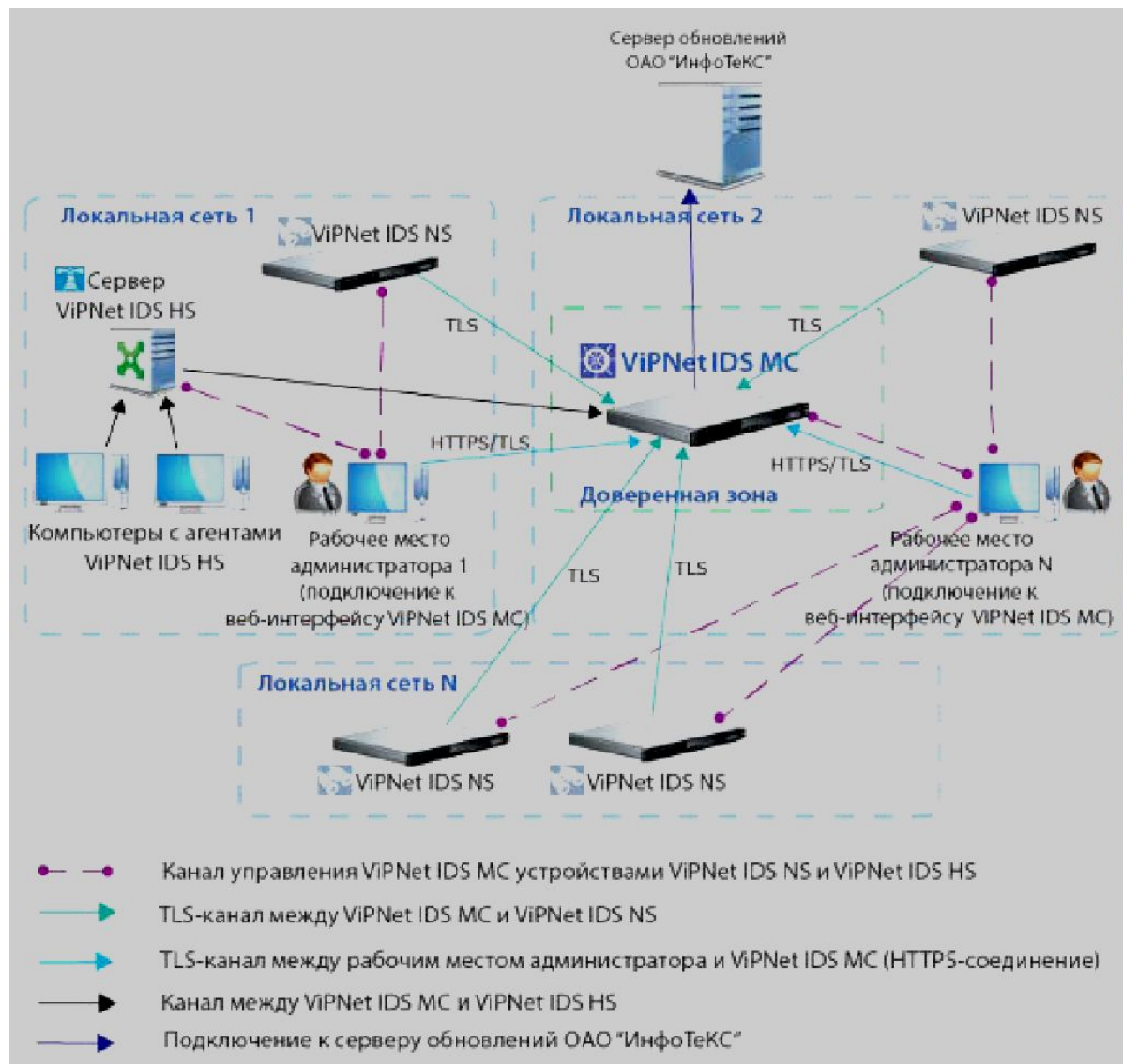
Система централизованного управления и мониторинга *ViPNet IDS MC* – это программное обеспечение, предназначенное для централизованного управления устройствами *ViPNet IDS NS* и *ViPNet IDS HS*, которые обеспечивают обнаружение вторжений в информационные системы и своевременное оповещение администраторов о выявленных событиях информационной безопасности.

ViPNet IDS MC предоставляет администратору возможность управлять конфигурацией правил обнаружения атак на сенсорах *ViPNet IDS NS*, управлять настройками *ViPNet IDS HS*, рассылать на устройства лицензии, базы правил обнаружения атак, базы сигнатур вредоносного программного обеспечения, обновления программного обеспечения, а также осуществлять мониторинг состояния устройств. В составе *ViPNet IDS MC* реализована подсистема управления доступом администраторов к функциям мониторинга и управления путем назначения администраторам определенных ролей. *ViPNet IDS MC* позволяет управлять как отдельными устройствами, так и доменами (группами) устройств.

ViPNet IDS MC функционирует под управлением адаптированной операционной системы *GNU/Linux*.

ViPNet IDS MC поставляется заказчикам в виде образа виртуальной машины в формате *OVA*, предназначенного для развертывания в виртуальной среде.







Классы ролей в *ViPNet IDS MC*, их функционал и функциональные роли

| Классы ролей | Функционал ролей | Функциональные роли |
|--------------------------------------|---|---|
| Роли управления <i>ViPNet IDS MC</i> | Позволяют разграничивать действия администраторов по управлению как <i>ViPNet IDS MC</i> , так и всеми устройствами, подключенными к <i>ViPNet IDS MC</i> | Главный администратор <i>ViPNet IDS MC</i> |
| | | Администратор безопасности <i>ViPNet IDS MC</i> |
| | | Администратор <i>ViPNet IDS MC</i> |
| | | Аудитор <i>ViPNet IDS MC</i> |
| Роли управления устройствами | Позволяют разграничивать действия администраторов по управлению только устройствами, при этом список управляемых устройств для каждого администратора может быть ограничен администратором безопасности <i>ViPNet IDS MC</i> . Управление <i>ViPNet IDS MC</i> этим ролям недоступно. Роли управления устройствами предназначены в основном для передачи управления частью устройств администраторам в другие организации | Главный администратор устройства |
| | | Администратор устройства |
| | | Пользователь устройства |

Журнал событий



| Дата, время | Инициат... | Описание | Объект |
|------------------------|------------|---|-----------|
| 2017-06-22 17:38:31... | IDS MC | На агентах есть опасные или важные с... | HS-S-Ц... |
| 2017-06-22 17:38:31... | IDS MC | Есть необработанные запросы на под... | HS-S-Ц... |
| 2017-06-22 17:38:31... | IDS MC | Сенсор сигнализирует о работоспособ... | HS-S-Ц... |
| 2017-06-22 17:38:16... | IDS MC | Изменения списка баз правил были п... | HS-S-Ц... |
| 2017-06-22 17:38:00... | IDS MC | Ожидание подключения сенсора | HS-S-Ц... |
| 2017-06-22 17:37:30... | IDS MC | Ожидание подключения сенсора | HS-S-Ц... |
| 2017-06-22 17:31:59... | IDS MC | Загрузка действующей, валидной, сов... | IDS MC |
| 2017-06-22 17:31:59... | IDS MC | Запущен системный модуль. | IDS MC |
| 2017-06-22 17:31:58... | IDS MC | Запущен системный модуль. | IDS MC |

На агентах есть опасные или важные события

2017-06-22 17:38:31.032

Дата, время события: 22.06.2017 17:38:31.032

Объект: HS-S-LIDA

Уровень события: **Опасное**

Инициатор события (система): IDS MC

| Категория события | Пояснения |
|---|--|
| | События <i>VIPNet IDS MC</i> |
| общие | общие события <i>VIPNet IDS MC</i> |
| лицензирование | события, связанные с управлением лицензиями в <i>VIPNet IDS MC</i> |
| обновления ПО | события, связанные с обновлениями ПО |
| обновления базы правил | события, связанные с обновлениями базы правил |
| обновления баз сигнатур вредоносного ПО | события, связанные с обновлениями базы сигнатур вредоносного ПО |
| учетные записи | события управления учетными записями |
| домены и группы устройств | события управления доменами и группами устройств |
| ключи и сертификаты | события управления транспортными ключами и сертификатами |
| | События сенсоров <i>VIPNet IDS NS</i> |
| состояние сенсоров <i>VIPNet IDS NS</i> | события, отображающие состояние сенсоров |
| сертификаты <i>VIPNet IDS NS</i> | работа с запросами и сертификатами сенсоров |
| лицензии <i>VIPNet IDS NS</i> | события, связанные с лицензиями на сенсорах |
| обслуживание <i>VIPNet IDS NS</i> | события взаимодействия с сенсорами |
| | События устройств <i>VIPNet IDS HS</i> |
| состояние серверов <i>VIPNet IDS HS</i> | события, отображающие состояние серверов <i>VIPNet IDS HS</i> |
| лицензии <i>VIPNet IDS HS</i> | события, связанные с лицензиями на серверах <i>VIPNet IDS HS</i> |
| обслуживание <i>VIPNet IDS HS</i> | события взаимодействия с серверами <i>VIPNet IDS HS</i> |
| | Другие события |
| служебные события | системные события, не влияющие на состояние системы и устройств |

Схема аутентификации и используемые сертификаты *ViPNet IDS MC*



Программно-аппаратный комплекс ViPNet TIAS (Threat Intelligence Analytics System) (далее – ViPNet TIAS) представляет собой программно-техническое средство, предназначенное для централизованного сбора, хранения и анализа информации о событиях информационной безопасности, обнаруженных сетевыми сенсорами ViPNet IDS NS и серверами ViPNet IDS HS, выявления инцидентов (вторжений, атак) эвристическими методами, оповещения об обнаруженных инцидентах, генерации сводных отчетов об инцидентах.

Под **интеллектуальным анализом данных** понимается совокупность методов обнаружения в данных ранее неизвестных, нетривиальных, практически полезных и доступных интерпретации знаний, необходимых для принятия решений в различных сферах человеческой деятельности.

ViPNet TIAS предназначен для для автоматического выявления и регистрации инцидентов информационной безопасности в информационных системах на основе анализа информации об угрозах безопасности информации и событиях информационной безопасности, полученной от систем обнаружения атак (вторжений) уровней сети и узла

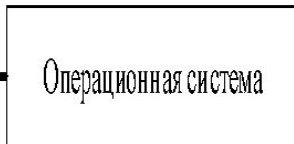
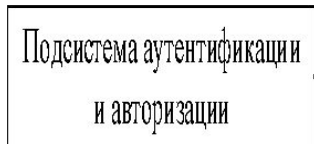
Система интеллектуального анализа угроз безопасности информации *ViPNet TIAS*

ViPNet TIAS предназначен для использования на территории Российской Федерации в государственных и коммерческих организациях, а также физическими лицами в системах защиты информации конфиденциального характера, не содержащей сведений, составляющих государственную тайну, и обеспечивает защиту конфиденциальной информации при выполнении требований и рекомендаций, изложенных в эксплуатационной документации.

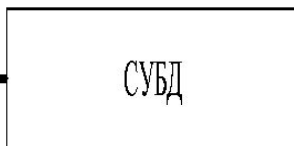
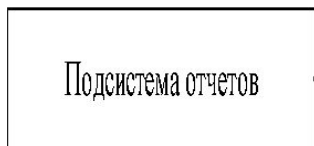
ViPNet TIAS может вывозиться с территории Российской Федерации в соответствии с законодательством Российской Федерации в области экспортного контроля или (и) таможенным законодательством Евразийского экономического союза в составе систем защиты информации или в качестве самостоятельного изделия.

Специализированное программное обеспечение *ViPNet TIAS* представляет собой замкнутую программную среду, состоящую из программных компонентов, функционирующих под управлением адаптированной 64 разрядной операционной системы на базе ядра *Linux*.

По умолчанию *ViPNet TIAS* поставляется с программно выключенной поддержкой приема информации об угрозах и событиях от межсетевых экранов *Cisco ASA*. По запросу Заказчика *ViPNet TIAS* может поставляться с поддержкой данного источника. Включение поддержки данного источника выполняется программно – штатной процедурой обновления программных компонентов СПО *ViPNet TIAS* с помощью файла «*enable cisco asa.tar.gz*», включенного в комплект



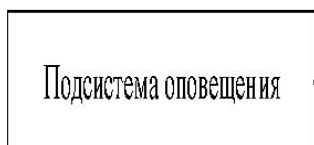
модифицированный *Linux*-дистрибутив на пакетной базе *Debian 7*.
Обеспечивает поддержку драйверов устройств, а также реализацию среды исполнения для других модулей ПО



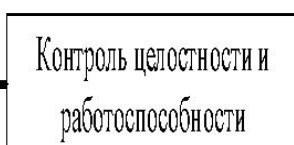
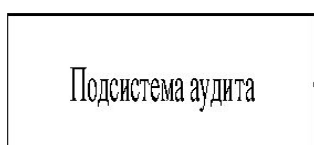
решает задачи хранения и доступа к накопленным данным аудита



отвечает за принятие решений об обнаружении атаки на основании данных сенсоров



реализует программный интерфейс взаимодействия для сбора данных с сетевых сенсоров *ViPNet IDS NS* и серверов *ViPNet IDS HS*



реализует пакет тестовых программ для периодического контроля целостности и работоспособности функций ПО *ViPNet TIAS*

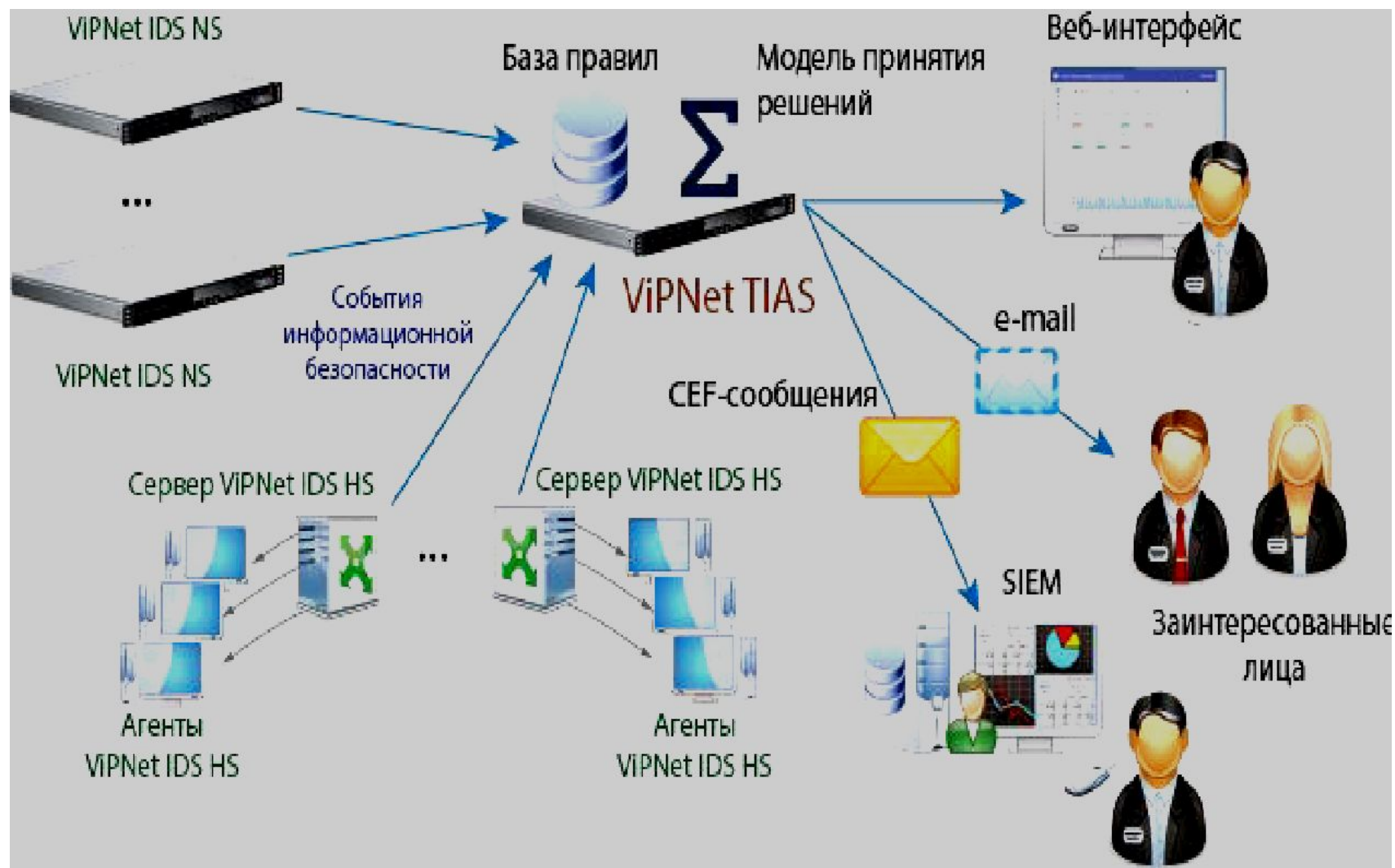
реализует сценарии разграничения и учета попыток доступа к данным *ViPNet TIAS*

отвечает за генерацию и публикацию сводных отчетов о выявленных аномалиях и атаках на защищаемую информационную систему

предоставляет внешние программные интерфейсы для управления функциями безопасности *ViPNet TIAS* и просмотра журналов

реализует настраиваемые администратором политики уведомления об обнаруженных атаках (вторжениях)

обеспечивает генерацию, сбор, хранение, поиск и разграничение доступа к данным внутреннего аудита *ViPNet TIAS*



сигнатурный метод

основан на использовании базы правил обнаружения инцидентов

эвристический метод

основан на использовании математической модели принятия решений, которая разработана на основе алгоритма машинного обучения



Экспертные данные формируются и постоянно актуализируются специалистами ОАО «ИнфоТеКС» по результатам анализа инструментов и техник выполнения сетевых атак. Для своевременного выявления новых типов инцидентов необходимо регулярно обновлять экспертные данные для *ViPNet TIAS*.

Сенсоры регистрируют события информационной безопасности и отправляют информацию о них *ViPNet TIAS* в формате *CEF*

ViPNet TIAS принимает и обрабатывает информацию о событиях только от указанных в настройках сенсоров

ViPNet TIAS анализирует события сигнатурным и эвристическим методами на основе экспертных данных

В результате анализа цепочки событий выявляются инциденты, которые свидетельствуют с большой степенью вероятности о нарушении информационной безопасности или выявленном факте проведенной сетевой атаки

При обнаружении инцидента выполняется его регистрация, формирование карточки инцидента и списка связанных с инцидентом событий

При обнаружении инцидента *ViPNet TIAS* оповещает заинтересованные лица по электронной почте, а также отправляет информацию об инциденте во внешние системы управления событиями информационной безопасности (*SIEM*)

Заинтересованное лицо посредством веб-интерфейса анализирует информацию об инциденте и связанных с ним событиях, проводит расследование инцидента

В случае подтверждения инцидента устанавливаются причины возникновения и устраняются последствия, а также предпринимаются меры по предупреждению возникновения подобных инцидентов в будущем

При этом применяются рекомендации, предоставленные *ViPNet TIAS* в карточке инцидента

Роли, используемые в *ViPNet TIAS* и их характеристики

| Роль <i>ViPNet TIAS</i> | Характеристика роли | Возможности управления <i>ViPNet TIAS</i> |
|-------------------------|--|---|
| Системный администратор | Соответствует одна встроенная учетная запись | Только с помощью консоли <i>ViPNet TIAS</i> |
| | Имя учетной записи – <i>admin</i> | |
| | Пароль учетной записи задается при прохождении первоначальной инициализации <i>ViPNet TIAS</i> | |
| Администратор | Соответствует одна встроенная учетная запись | Только через веб-интерфейс |
| | Имя учетной записи – <i>Administrator</i> | |
| | Пароль по умолчанию – <i>Administrator</i> | |
| Пользователь | Может соответствовать несколько учетных записей | Только через веб-интерфейс |
| | По умолчанию учетные записи пользователей отсутствуют | |
| | Учетными записями пользователей управляет администратор | |

Действия по настройке и управлению *VipNet TIAS*, доступные для каждой из ролей

| Роль <i>VipNet TIAS</i> | Доступные действия по настройке и управлению <i>VipNet TIAS</i> |
|--|--|
| Системный администратор | Установка и активация лицензии |
| | Первоначальная инициализация |
| | Установка системного времени |
| | Настройка сетевых интерфейсов |
| | Управление сертификатами |
| | Обновление программного обеспечения |
| | Резервное копирование и восстановление данных |
| | Восстановление пароля учетной записи администратора |
| | Смена пароля системного администратора |
| | Выгрузка диагностических журналов |
| Запуск проверки целостности программного обеспечения вручную | |
| Администратор | Обладает полными полномочиями в управлении <i>VipNet TIAS</i> через веб-интерфейс |
| Пользователь | Расследование инцидентов и анализ событий информационной безопасности |
| | Имеет доступ к просмотру информации о выявленных инцидентах и событиях информационной безопасности, полученных от сенсоров |
| | Может работать с отчетами |

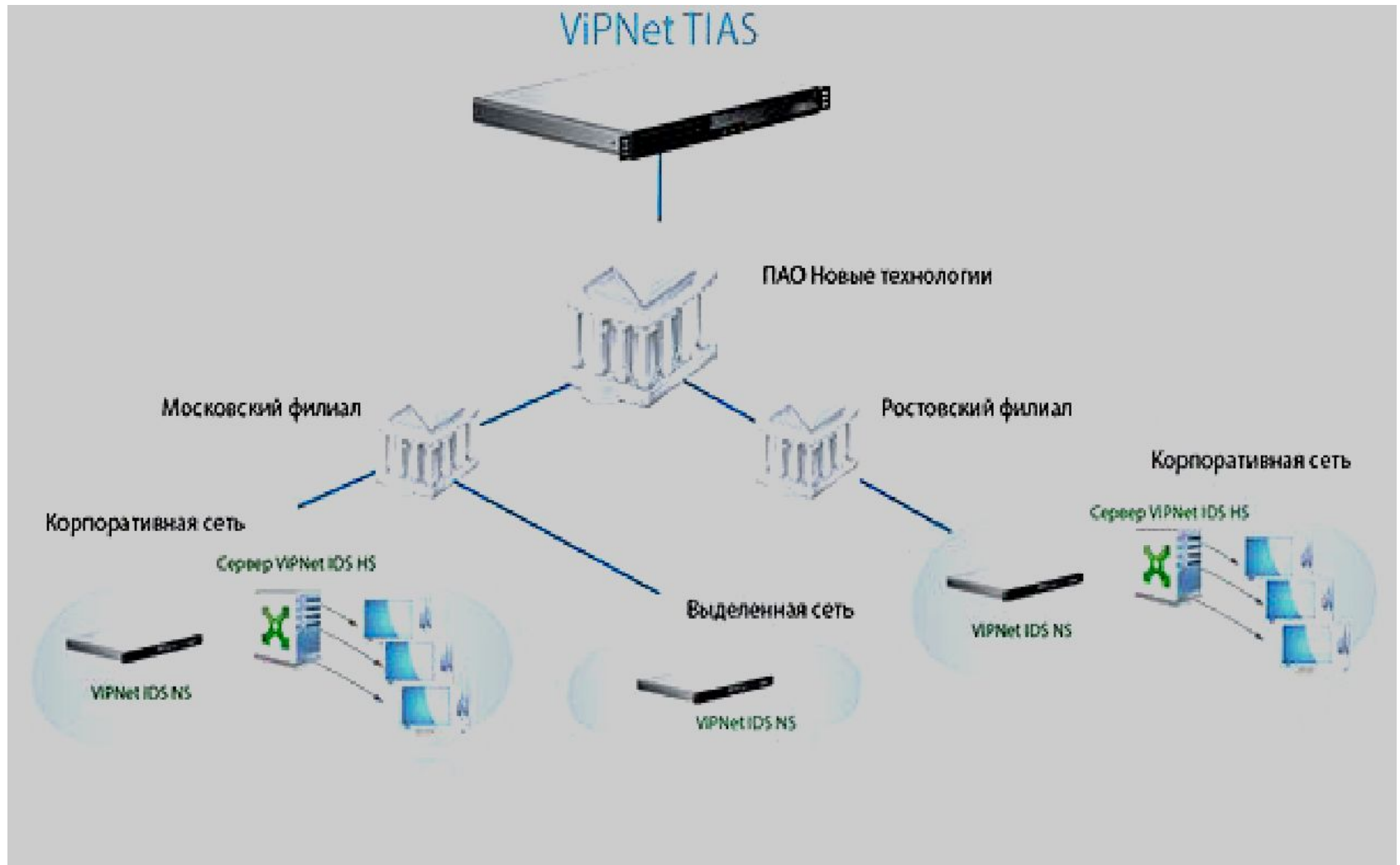
Способы управления *ViPNet TIAS* и их особенности

| Способ управления <i>ViPNet TIAS</i> | Особенности способа управления |
|---|---|
| Удаленно посредством веб-интерфейса | <p>Веб-интерфейс является основным средством управления <i>ViPNet TIAS</i></p> <p>Удаленное подключение к <i>ViPNet TIAS</i> выполняется по сети передачи данных с помощью веб-браузера, установленного на отдельном компьютере – терминале управления</p> <p>Канал передачи данных между <i>Терминалом управления</i> и <i>ViPNet TIAS</i> организован по протоколу <i>HTTPS/TLS</i> с односторонней аутентификацией и шифрованием передаваемых данных</p> |
| Локально или удаленно посредством консоли | <p>Используется в основном при подготовке <i>ViPNet TIAS</i> к эксплуатации, а также в ходе эксплуатации для выполнения системных настроек и служебных операций, недоступных через веб-интерфейс (например, для изменения сетевых настроек или создания резервной копии данных)</p> <p>Выполняется путем подсоединения к аппаратной платформе <i>ViPNet TIAS</i> монитора и клавиатуры или для исполнения <i>TIAS VA</i> – открытием терминального окна виртуальной машины</p> <p>Удаленное подключение к консоли выполняется по сети передачи данных с помощью <i>SSH-клиента</i>, установленного на <i>Терминале управления</i></p> <p>Канал передачи данных между <i>Терминалом управления</i> и <i>ViPNet TIAS</i> организован по протоколу <i>SSH</i> без аутентификации с шифрованием передаваемых данных</p> |

Терминал управления – это компьютер общего назначения, предназначенный для удаленного управления *ViPNet TIAS* посредством веб-интерфейса и/или консоли.

| Элемент | Ед. измерения | Характеристика |
|----------------------------------|---------------|---|
| Процессор | | Intel Pentium 4 / AMD Athlon 64 или другой более поздней версии x86-совместимый процессор с поддержкой SSE2 |
| Объем оперативной памяти | Гбайт | не менее 2 |
| Свободное место на жестком диске | Мбайт | не менее 200 |
| Сетевой адаптер | шт. | не менее 1 |
| Операционная система | | Windows 7/8/8.1/10 (32/64-разрядная) |
| | | Windows Server 2008 R2/2012/2012 R2 (64-разрядная) |

Пример иерархической структуры сенсоров



События на узлах


- список всех событий, полученных от всех сенсоров

Источники

- список событий, отобранных по направлению предполагаемой атаки, для которых узел-источник угрозы находится в защищаемых сенсорами сетях. События индивидуально от каждого сенсора контролируемой сети агрегируются в записи при совпадении *ip*-адреса узла-источника угрозы и сработавшего

Получатели

- список событий, отобранных по направлению предполагаемой атаки, для которых узел-источник находится во внешних для сенсоров сетях. События индивидуально от каждого сенсора контролируемой сети агрегируются в записи при совпадении *ip*-адреса узла-источника угрозы и сработавшего правила

 ViPNet Threat Intelligence Analytics System

События IDS NS Все события Все сенсоры 15 м 60 м 24 ч

Источники Получатели

| Важность | Количество | IP-адрес источника | Код правила | Категория события | Важность |
|-----------|------------|--------------------|-------------|--------------------------|-----------|
| Критичная | 1 | 192.168.27.188 | 1:3000796 | Трояны и вирусы | Средняя |
| Средняя | 1 | 192.168.254.53 | 1:2100366 | Информация | Средняя |
| Критичная | 1 | 192.168.253.60 | 1:2018789 | Нарушение политик | Высокая |
| Критичная | 1 | 192.168.251.236 | 1:2021938 | Трояны и вирусы | Критичная |
| Средняя | 1 | 192.168.250.238 | 112:1 | Другие | Критичная |
| Высокая | 1 | 192.168.248.12 | 1:2011505 | Эксплуатация (сервис...) | Критичная |
| Критичная | 1 | 192.168.247.154 | 1:2009579 | Эксплуатация (сервис...) | Критичная |

События на узлах

| Дата | IP сенсора | IP получателя | IP источника | Пакет | Важность | Количество | Правило |
|---------------------|-----------------|---------------|----------------|-------|----------|------------|---------|
| 21.02.2018 12:27:51 | 123.123.123.123 | 200.168.14.35 | 192.168.152.2 | ↓ | Средняя | 5976 | GPL IC |
| 21.02.2018 12:27:51 | 123.123.123.123 | 200.168.14.35 | 192.168.84.14 | ↓ | Средняя | 5976 | GPL IC |
| 21.02.2018 12:27:51 | 123.123.123.123 | 200.168.14.35 | 192.168.192... | ↓ | Средняя | 5976 | GPL IC |

Заражение хоста вредоносным ПО DealPly ↓ ×

Высокий уровень угрозы

Статус инцидента: Не обработан

Взять в работу

Пользователь:

Рейтинг: 10

Дата фиксации: 22.03.2018 08:58:49

Пораженные узлы (1): ip: 192.168.118.72
mac: 0a:00:27:ab:55:7a

Тип угрозы ИБ: Нарушение конфиденциальности

Наименование: Заражение хоста вредоносным ПО DealPly

Метод: Сигнатурный

Идентификатор: 5ab3461997139608056e240c

Симптомы: Аномальная сетевая активность APM

✓ Рекомендации:

- Отключить пораженный актив от вычислительной сети
- Провести интервьюирование владельца
- Осуществить антивирусную проверку
- Передать обнаруженное вредоносное ПО в ЦМ для анализа
- Удалить обнаруженное вредоносное ПО

Просмотр статистики событий и инцидентов в веб-интерфейсе ViPNet TIAS

Инфопанель

Вопросы

Вопросы

15 м

60 м

24 ч



12.07.2017 18:00 - 13.07.2017 06:20



Автообновление

Динамика событий по угрозам

информация

2455

-18.5%

осаждение

10587

+61.5%

подбор паролей

38

-4021.1%

политицизм

174

-2241.4%

травы и вирусы

5798

+9.1%

ооос

27

+88.7%

атаки

3176

+43.8%

другие

2999

+66.0%

Статистика инцидентов

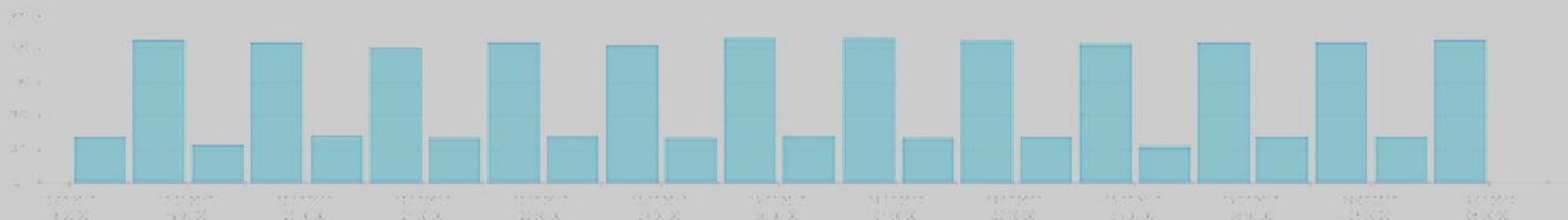
Количество инцидентов

2421

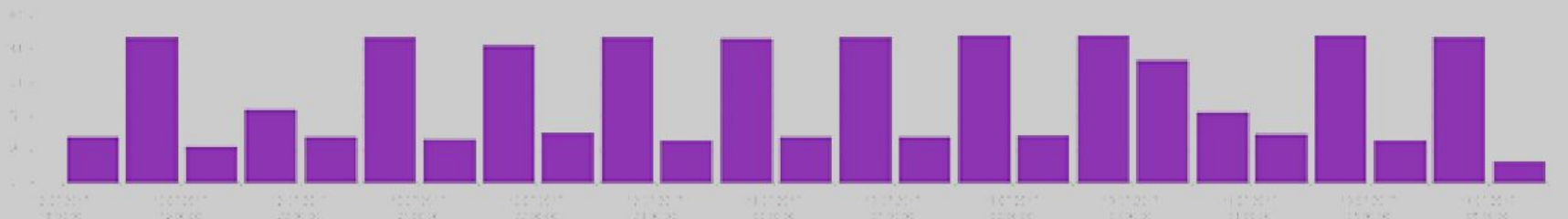
Требующие обработки

2421

События

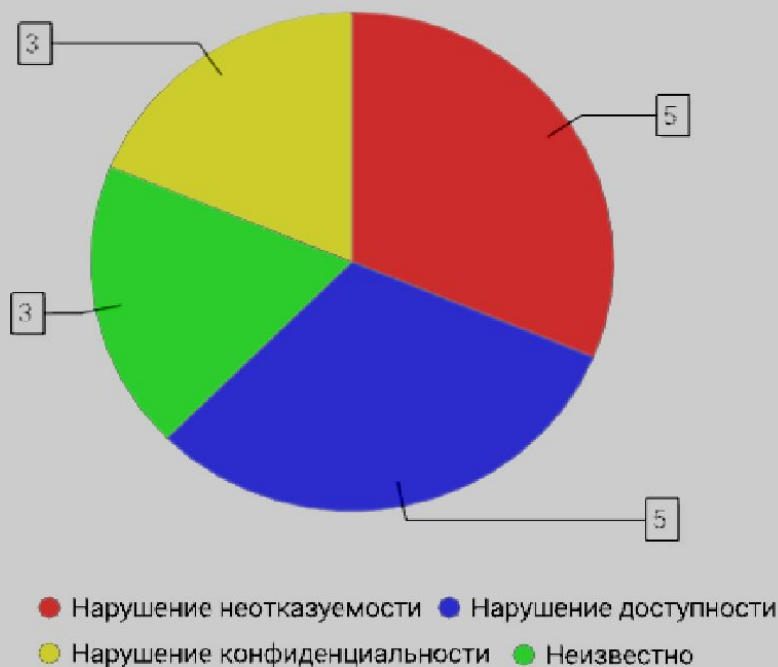


Инциденты



Пример отчета о количестве инцидентов по типам угроз

| Наименование типа угрозы | Количество инцидентов |
|------------------------------|-----------------------|
| Нарушение неотказуемости | 5 |
| Нарушение доступности | 5 |
| Неизвестно | 3 |
| Нарушение конфиденциальности | 3 |

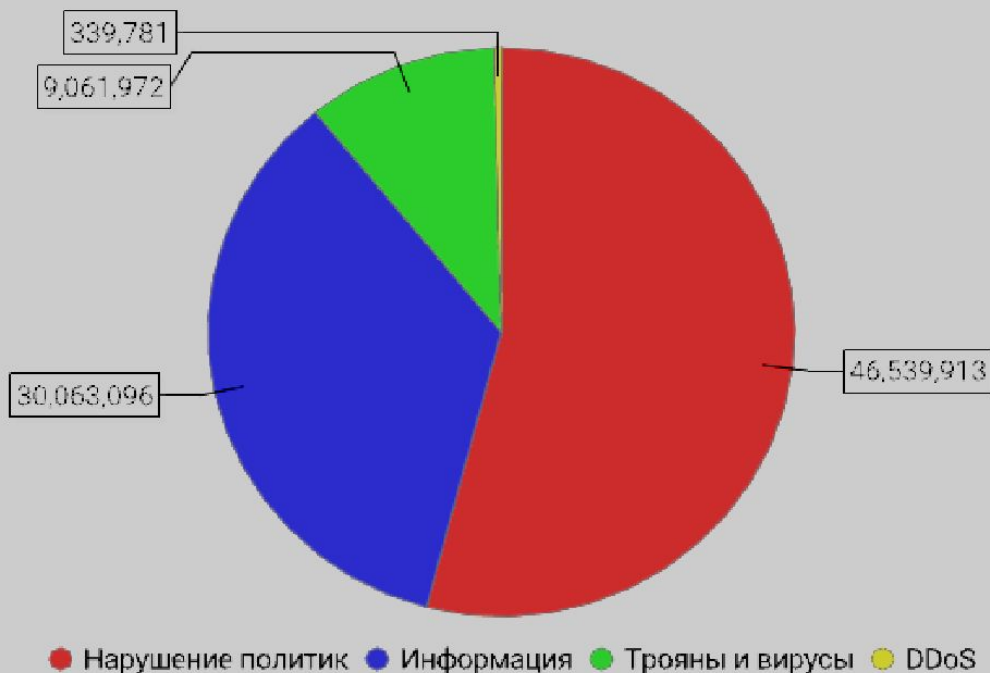


Шаблоны для формирования отчетов по полученным от сенсоров событиям

| № | Вид шаблона | Описание шаблона |
|---|---|---|
| 1 | События информационной безопасности | Статистический отчет, который формируется в виде таблицы и отражает информацию о количестве полученных событий, зарегистрированных на сенсорах при срабатывании правил каждого типа |
| 2 | Источники атак (100 самых атакующих узлов) | Статистический отчет, который формируется в виде таблицы и отражает информацию об <i>ip</i> -адресах 100 узлов-источников (атакующих узлов) пакетов, при анализе которых на сенсорах было зарегистрировано наибольшее количество событий |
| 3 | Цели атак (100 самых атакуемых узлов) | Статистический отчет, который формируется в виде таблицы и отражает информацию об <i>ip</i> -адресах 100 узлов-получателей (атакуемых узлов) пакетов, при анализе которых на сенсорах было зарегистрировано наибольшее количество событий |
| 4 | Категории угроз информационной безопасности | Отчет формируется в виде таблицы и круговой диаграммы и отражает информацию о количестве полученных событий каждой категории угроз |

Пример отчета о количестве событий по категориям угроз

| Наименование категории угроз | Количество сработавших события |
|------------------------------|--------------------------------|
| Нарушение политик | 46 539 913 |
| Информация | 30 063 096 |
| Трояны и вирусы | 9 061 972 |
| DDoS | 339 781 |





Журнал событий



↓ Скачать файл



Аудит × Инциденты × Лицензирование × Обновление × Оповещение × Отчеты × Сертификаты ×



Время регистрации

Категория

Наименование

Инициатор

Статус



27.03.2018 09:22:56

Аудит

Чтение журнала

Administrator

Информация

26.03.2018 11:10:59

Обновление

Загрузка обновления

Administrator

Ошибка



26.03.2018 10:00:50

Аудит

Чтение журнала

Administrator

Информация



26.03.2018 09:13:21

Отчеты

Создание отчета

Administrator

Информация

26.03.2018 09:12:49

Отчеты

Удаление отчета

Administrator

Информация

1. Подключение ПАК ViPNet IDS NS к сети организации (в соответствии с заранее спроектированной схемой!)
2. Настройка системы
 - Вход с технологической учетной записью (логин iduser и пароль vipnet)
 - Смена пароля
 - Должен быть не менее 8 символов, содержащих буквы разных регистров, цифры, специальные символы
 - Надо сделать это быстро 😊
 - Добавление/удаление/изменение учетных записей всех категорий пользователей ПАК
 - Настройка параметров сети
 - Конфигурирование сетевого интерфейса для управления и назначение его параметров
 - Конфигурирование сетевых интерфейсов (до 3-х шт) для захвата и анализа трафика
 - Подключение управляющего компьютера через веб-интерфейс
 - Установка лицензии и активация
 - Обновление базы решающих правил и сигнатур вредоносного ПО
3. Работа с ViPNet IDS в соответствии с политикой информационной безопасности организации

Спасибо за внимание!

Вопросы?

НОЧУ ДПО ЦПК «Учебный центр «ИнфоТеКС»
education@infotecs.ru

ОАО «ИнфоТеКС», Москва
(495) 737-61-92
www.infotecs.ru