

A background image of a businessman in a suit holding a large, transparent, 3D-rendered gear. The gear is part of a complex mechanical structure that appears to be floating or being assembled. The scene is set in a modern office environment with blurred background elements like a laptop and office furniture.

# Обзор новых версий продуктов ViPNet IDS HS и ViPNet SafeBoot

Иван Кадыков

# ViPNet SafeBoot

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



# Решаемые задачи ViPNet SafeBoot

## Организация доверенной загрузки

Контроль целостности

Разграничение  
доступа

UEFI BIOS

MBR

Таблицы ACPI,  
SMBIOS, карты  
распределения  
памяти

Файлов

CMOS

Двухфакторная  
аутентификация

Токены:  
JaCarta  
Rutoken  
Guradant ID

# Возможности текущей сертифицированной версии 1.3

Авторизация на LDAP/AD

Контроль целостности реестра

Автоматическое построение списков контроля для ОС Windows

Поддержка режима защиты BIOS для новых платформ

Средства диагностики UEFI BIOS на предмет возможности установки VIPNet SafeBoot

# Сертифицировано



Средство доверенной загрузки уровня базовой системы ввода-вывода **2 класса**

Какие меры приказов закрывает?

- (ГЛАВНОЕ) УПД.17 для 17,21,31 приказов и УПД.3 для 239 приказа – «Обеспечение доверенной загрузки средств вычислительной техники» - актуально для классов 1-2 ИСПДн, ГИС, АСУ ТП и КИИ
- ИАФ.1, ИАФ.3, ИАФ.4, ИАФ.5, УПД.1, УПД.4, УПД.6, РСБ.1, РСБ.3, РСБ.4, РСБ.5, РСБ.7, ОЦЛ.1



## 29 УГРОЗ в полной или косвенной мере относящиеся к угрозам BIOS/UEFI BIOS

### Угроза

УБИ.004: Угроза аппаратного сброса пароля BIOS  
УБИ.005: Угроза внедрения вредоносного кода в BIOS  
УБИ.008: Угроза восстановления аутентификационной информации  
УБИ.006: Угроза внедрения кода или данных  
УБИ.009: Угроза восстановления предыдущей уязвимой версии BIOS  
УБИ.013: Угроза деструктивного использования декларированного функционала BIOS  
УБИ.018: Угроза загрузки нештатной операционной системы  
УБИ.023: Угроза изменения компонентов системы  
УБИ.024: Угроза изменения режимов работы аппаратных элементов компьютера  
УБИ.030: Угроза использования информации идентификации/аутентификации, заданной по умолчанию  
УБИ.032: Угроза использования поддельных цифровых подписей BIOS  
УБИ.035: Угроза использования слабых криптографических алгоритмов BIOS  
УБИ.039: Угроза исчерпания запаса ключей, необходимых для обновления BIOS  
УБИ.045: Угроза нарушения изоляции среды исполнения BIOS

### Угроза

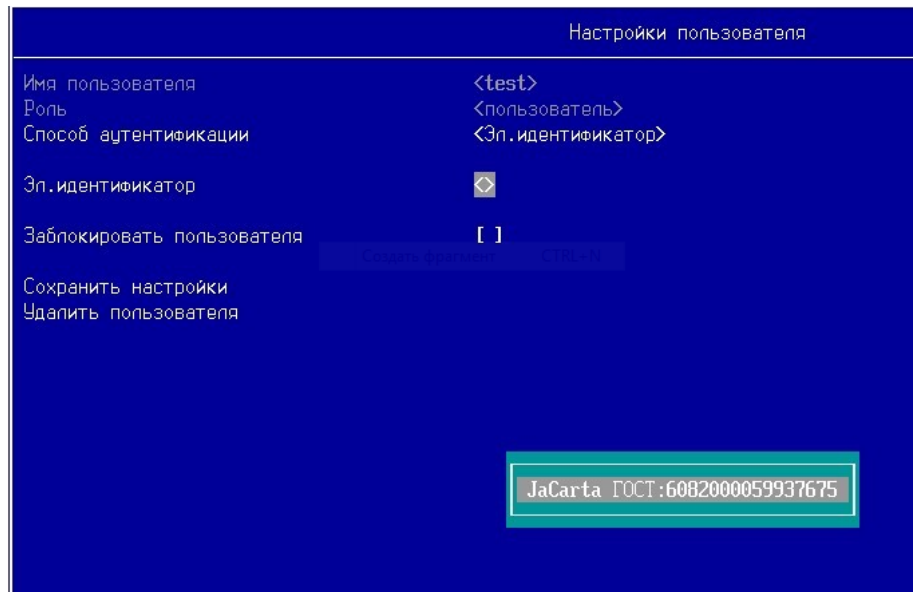
УБИ.053: Угроза невозможности управления правами пользователей BIOS  
УБИ.072: Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS  
УБИ.087: Угроза несанкционированного использования привилегированных функций BIOS  
УБИ.090: Угроза несанкционированного создания учётной записи пользователя  
УБИ.108: Угроза ошибки обновления гипервизора  
УБИ.121: Угроза повреждения системного реестра  
УБИ.123: Угроза подбора пароля BIOS  
УБИ.124: Угроза подделки записей журнала регистрации событий  
УБИ.129: Угроза подмены резервной копии программного обеспечения BIOS  
УБИ.144: Угроза программного сброса пароля BIOS  
УБИ.145: Угроза пропуска проверки целостности программного обеспечения  
УБИ.150: Угроза сбоя процесса обновления BIOS  
УБИ.152: Угроза удаления аутентификационной информации  
УБИ.154: Угроза установки уязвимых версий обновления программного обеспечения BIOS  
УБИ.179: Угроза несанкционированной модификации защищаемой информации

A 3D rendered robotic hand in shades of blue and white, reaching out from the right side of the frame. The background is a dark blue grid with faint, glowing icons of various devices and network symbols.

Что нового в  
ViPNet SafeBoot версии 1.4?

# Поддержка JaCarta-2 ГОСТ

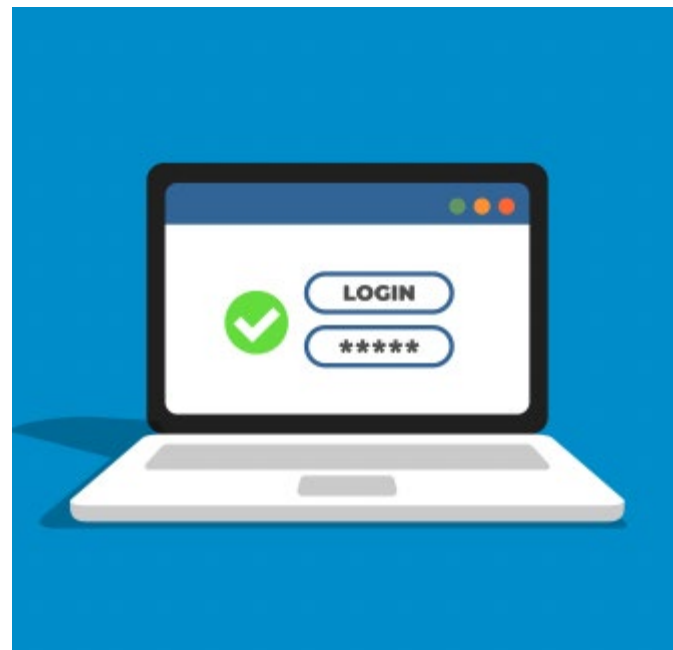
- Поддержка токена JaCarta-2 ГОСТ
- Возможность аутентификации в ViPNet SafeBoot по «сертификату ГОСТ»





# Аутентификация по западным сертификатам в AD

- Зачастую в компаниях развёрнут Microsoft CA
- Для аутентификации используются сертификаты выданные MS CA
- Для входа в SafeBoot или аутентификации на LDAP через SafeBoot имеется возможность использовать западные сертификаты выданные MS CA



# Режим неактивности

Режим неактивности -  
специализированная  
возможность средства  
доверенной загрузки(СДЗ)  
ViPNet SafeBoot для OEM  
поставок в составе платформ  
различных производителей

Продукт не зарегистрирован  
Демонстрационный режим: 1, осталось (дней) : 30

(с) 2019, ОАО "ИнфоТеКс"  
Веб-сайт: [www.infotecs.ru](http://www.infotecs.ru)  
E-mail: [soft@infotecs.ru](mailto:soft@infotecs.ru)  
Телефон для регионов России: 8 800 250-0-260  
Телефон для Москвы: +7 495 737-61-92

Лицензионная информация

Серийный номер

Импортировать серийный номер

Создать запрос на регистрацию

Код регистрации

Импортировать код регистрации

Демо-период использования **ViPNet SafeBoot** завершен  
**ViPNet SafeBoot** выключен  
Нажмите любую клавишу для перезагрузки системы

# Планы по SafeBoot версии 1.4

- Релиз ожидается в начале июня
- ViPNet SafeBoot версии 1.4 будет передан на инспекционный контроль(ИК)
- Срок окончания ИК – октябрь 2019



# Новый интерфейс в Q3

The screenshot displays the VIPNet SafeBoot interface. On the left is a dark grey login screen with the text "VIPNet SafeBoot" and "Введите имя пользователя или подключите идентификатор:". Below this is a "Далее" button and the text "© 2018, ОАО «ИнфоТекс»". On the right, a system log window is open, showing a table of events. The table has two columns: "Время" (Time) and "Событие" (Event). The log entries are as follows:

Время	Событие
2019-02-08 16:48:59	Свободное место в NVRAM распределено [журнал: 11201, БД: 11201]
2019-02-08 16:48:59	Рабочая директория инициализирована
2019-02-08 16:49:06	Вход в режим настроек BIOS заблокирован [раз: 3, последний: 2019-02-08 16:42:31]
2019-02-08 16:49:06	Режим ограниченного функционирования
2019-02-08 16:49:06	Параметры загрузки должны быть настроены
2019-02-08 16:52:05	Администратор аутентифицирован [Admin]

Below the log window, a menu is visible with the following options:

- Контроль целостности
- Автоопределение компонентов загрузки ОС
- Контроль файлов
- Контроль CMOS
- Контроль конфиг. пространства PCI
- Контроль таблиц ACPI
- Контроль таблиц SMBIOS
- Контроль карты распределения памяти
- Контроль модулей UEFI
- Контроль загрузочных секторов
- Контроль реестра Windows
- Контроль журнала транзакций ФС
- Режим обучения
- Проверить целостность
- Перерасчитать эталоны КЦ

# ViPNet IDS HS

ViPNet IDS HS - система обнаружения вторжений, осуществляющее мониторинг и обработку событий внутри хоста, с применением сигнатурного и эвристического метода анализа атак, используя отечественные правила и сигнатуры



# Как выявляются атаки?

## Сигнатурный анализ

Выявление характерных идентифицирующих свойств атаки

## Эвристический анализ

Это совокупность функций нацеленных на обнаружение неизвестных атак

# Ключевая функциональность



Анализ системных журналов и логов ОС и приложений



Мониторинг файловой активности и реестра



Различные источники событий

Результаты выполнения команд или изменений результатов команд

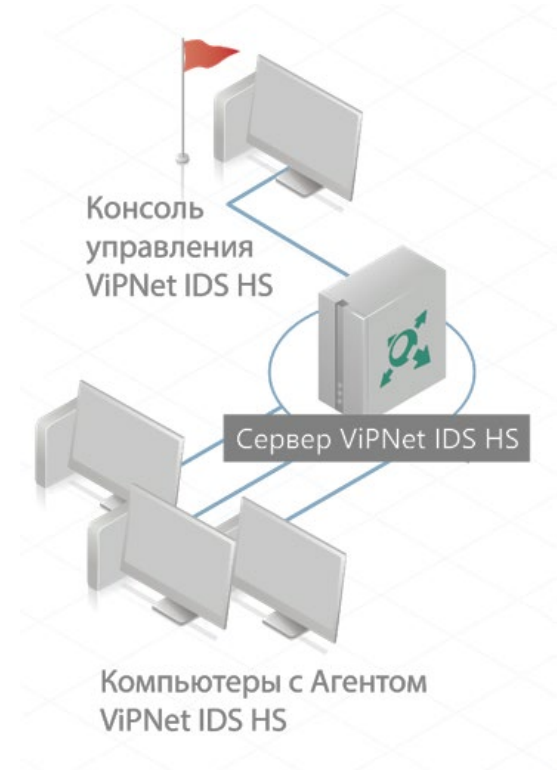


Анализ трафика проходящего через хост



# Архитектура

- Агент - собирает необходимую информацию о функционировании хостов и выполняет первичный анализ данных
- Сервер — получает, хранит и анализирует информацию от Агентов, хранит правила, команды и параметры, и передаёт их на Агенты.
- Консоль управления — предоставляет графический интерфейс для управления Агентами и мониторинга их состояния





# Сертифицировано



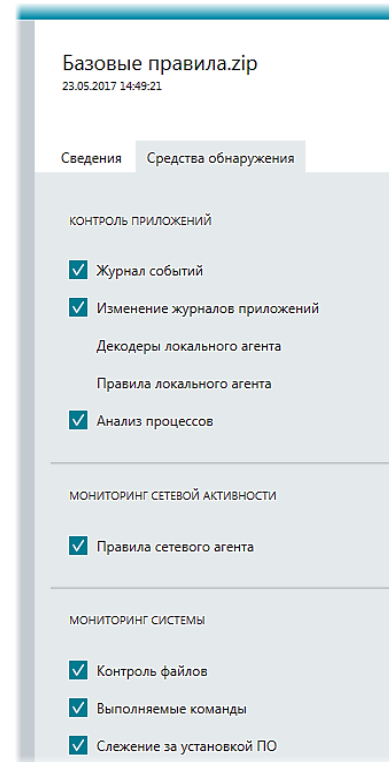
- Сертификат ФСТЭК России по требованиям к системам обнаружения вторжения уровня узла 4 класса.
- Список мер из приказов 17,21,31:  
ИАФ.1, ИАФ.5, УПД.4, РСБ.1, РСБ.3, РСБ.4, РСБ.5, РСБ.6, РСБ.7, СОВ.1, СОВ.2, АНЗ.3, ОЦЛ.1, ОЦЛ.3, ИНЦ.2, ИНЦ.3, ИНЦ.4.



# Особенности реализации агента

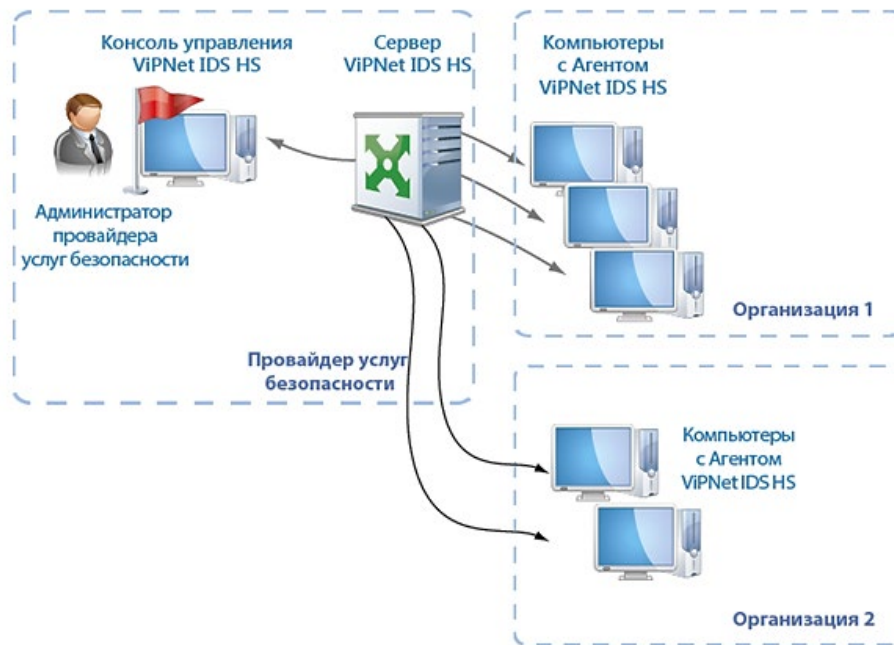
Агент ViPNet IDS HS состоит из двух частей:

- Сетевой агент – осуществляет мониторинг за сетью
- Агент уровня ОС – осуществляет мониторинг за событиями внутри операционной системы



# Мультиарендность

В 2018 удалось реализовать режим Мультиарендности (multitenancy)



# Мультиарендность



Теперь Сервер можно переключить в режим мультиарендности

Агентов подключать к организации

### Организации

Введите название организации для...  [Создать](#) [Удалить](#)

<input type="checkbox"/>	Название
<input type="checkbox"/>	Системная организация
<input type="checkbox"/>	Своя организация
<input type="checkbox"/>	Организация Москва

#### Организация Москва

Идентификатор: 0a370850-3986-452a-9203-ed68bdce0c59

Максимальное количество агентов: 5

Начало действия лицензии: 08.08.2018

Истечение срока действия лицензии: 21.12.2018

Состояние: Активная

Автоподключение агентов

[Приостановить обслуживание](#)

### Устройства

Введите название устройства для п...   [Переместить](#) [Удалить](#)

<input type="checkbox"/>	Название
<input type="checkbox"/>	Системная организация > Запросы на подключение Вернуться в группы
<input checked="" type="checkbox"/>	HS-A1-ЦДА

HS-A1-ЦДА 17.08.20

Своя организация / Запросы на подключение

Организация Москва / Запросы на подключение

Имя агента:

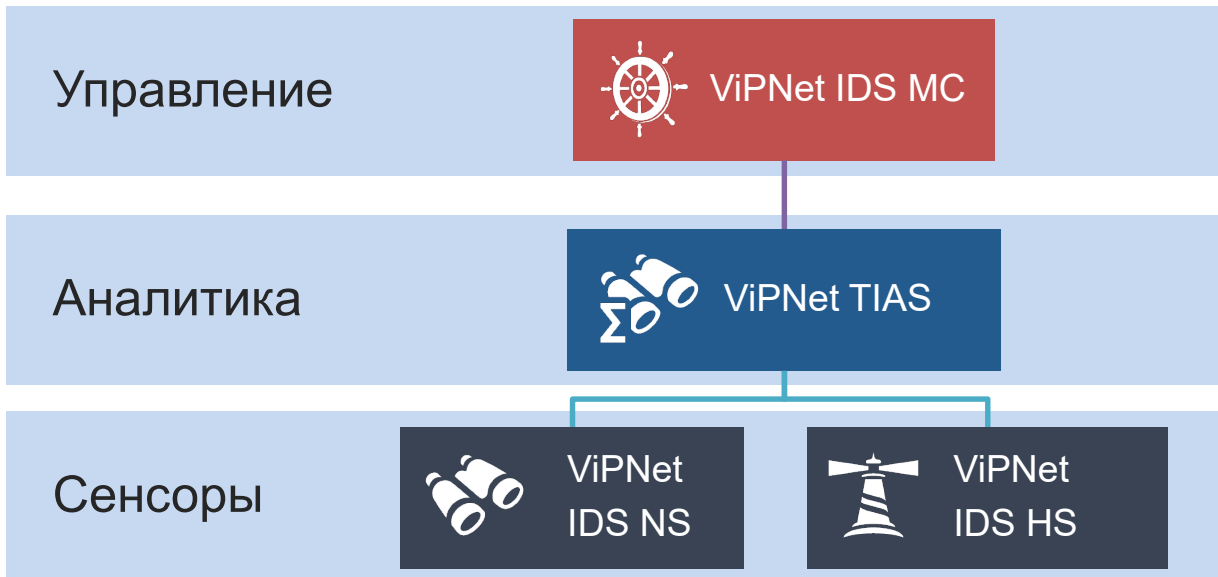
Имя устройс

Адрес устройс

База правил

Назначенная

# Решение по обнаружению компьютерных атак



# Реальная эксплуатация

The screenshot displays the VIPNet IDS HS management console. The interface includes a sidebar with navigation options: Управление (Management), События (Events), Устройства (Devices), Базы правил (Rule Bases), Сервис (Service), Журналы (Logs), Учетные записи (Accounts), and Обнаружение аномалий (Anomaly Detection). The main area is titled 'События' (Events) and contains a search bar, filter, refresh, and delete icons. Below this is a table of events with columns for selection, date/time, description, attempts, identifier, device, and group. The table lists various system events such as logins, session creations, and network connections.

<input type="checkbox"/>	Дата, время	Описание	Попытки	Идентификатор	Устройство	Группа
<input type="checkbox"/>	08.02.19 17:04:43	Вход в систе...	64	500004	10.10.10.10	10.10.10.10
<input type="checkbox"/>	08.02.19 17:04:43	Создание пр...	30	300001	10.10.10.10	10.10.10.10
<input type="checkbox"/>	08.02.19 17:04:43	Изменение ф...	39	200000	10.10.10.10	10.10.10.10
<input type="checkbox"/>	08.02.19 17:04:43	Блокировка...	1	600006	10.10.10.10	10.10.10.10
<input type="checkbox"/>	08.02.19 17:04:43	Получение д...	1	301048	10.10.10.10	10.10.10.10
<input type="checkbox"/>	08.02.19 17:04:43	Создание слу...	1	100017	10.10.10.10	10.10.10.10
<input type="checkbox"/>	08.02.19 17:04:24	Изменение р...	1	100000	10.10.10.10	10.10.10.10
<input type="checkbox"/>	08.02.19 17:04:24	ET INFO Sessi...	1	2018904	10.10.10.10	10.10.10.10
<input type="checkbox"/>	08.02.19 17:04:22	Сетевой вход...	21	500009	10.10.10.10	10.10.10.10
<input type="checkbox"/>	08.02.19 17:04:22	Изменение ф...	31	200000	10.10.10.10	10.10.10.10
<input type="checkbox"/>	08.02.19 17:04:22	Создание пр...	23	300001	10.10.10.10	10.10.10.10
<input type="checkbox"/>	08.02.19 17:04:22	Изменение р...	4	100000	10.10.10.10	10.10.10.10
<input type="checkbox"/>	08.02.19 17:04:18	Изменение ф...	156	210000	10.10.10.10	10.10.10.10
<input type="checkbox"/>	08.02.19 17:04:18	Создание пр...	156	310000	10.10.10.10	10.10.10.10
<input type="checkbox"/>	08.02.19 17:04:17	Вход в систе...	3	500004	10.10.10.10	10.10.10.10

A detailed 3D rendering of a white robotic hand, shown from a side-on perspective. The hand is composed of various mechanical joints and segments, with a blue-tinted inner structure visible at the wrist and fingers. The background is a dark, textured blue with faint, glowing icons of a smartphone, a laptop, and a network diagram, suggesting a digital or technological environment.

Что нового в ViPNet IDS HS  
версии 1.4?

# Политики аудита

**ViPNet IDS HS**

← Политика аудита по умолчанию

Аутентификация Реестр **Файловая система** Управление

КОНТРОЛЬ ВХОДА УЧЕТНОЙ ЗАПИСИ

- Проверка учетных данных  Успех
- Служба проверки подлинности Kerberos  Успех
- Операции с билетами службы Kerberos  Успех

КОНТРОЛЬ ВХОДА И ВЫХОДА

- Вход в систему  Успех
- Выход из системы  Успех
- Специальный вход  Успех
- Другие события входа и выхода  Успех

**ViPNet IDS HS**

← Политика аудита по умолчанию

Аутентификация Реестр **Файловая система** Управление учетными записями Прочие

Аудируемые пути:

- HKKEY\_LOCAL\_MACHINE\SOFTWARE
- HKKEY\_LOCAL\_MACHINE\SYSTEM

Добавить

ОТСЛЕЖИВАЕМЫЕ ОПЕРАЦИИ

<input type="checkbox"/> Полный доступ	<input type="checkbox"/> Запрос значения	<input checked="" type="checkbox"/> Задание значения
<input checked="" type="checkbox"/> Создание подразделов	<input type="checkbox"/> Перечисление подразделов	<input type="checkbox"/> Уведомление
<input type="checkbox"/> Создание связи	<input checked="" type="checkbox"/> Удаление	<input type="checkbox"/> Запись DAC
<input type="checkbox"/> Смена владельца	<input type="checkbox"/> Чтение разрешений	

ОБЛАСТЬ ПРИМЕНИМОСТИ

Этот раздел  Этот раздел и его подразделы  Только подразделы

ИСКЛЮЧЕНИЯ

Добавить

**ViPNet IDS HS**

← Политика аудита по умолчанию

Реестр **Файловая система** Управление учетными записями Прочие

ЛЕЖИВАНИЕ

процессов: детальный аудит

ГЛМ

об общем файловом ресурсе

ытия доступа к объекту

бъектам ядра

ность

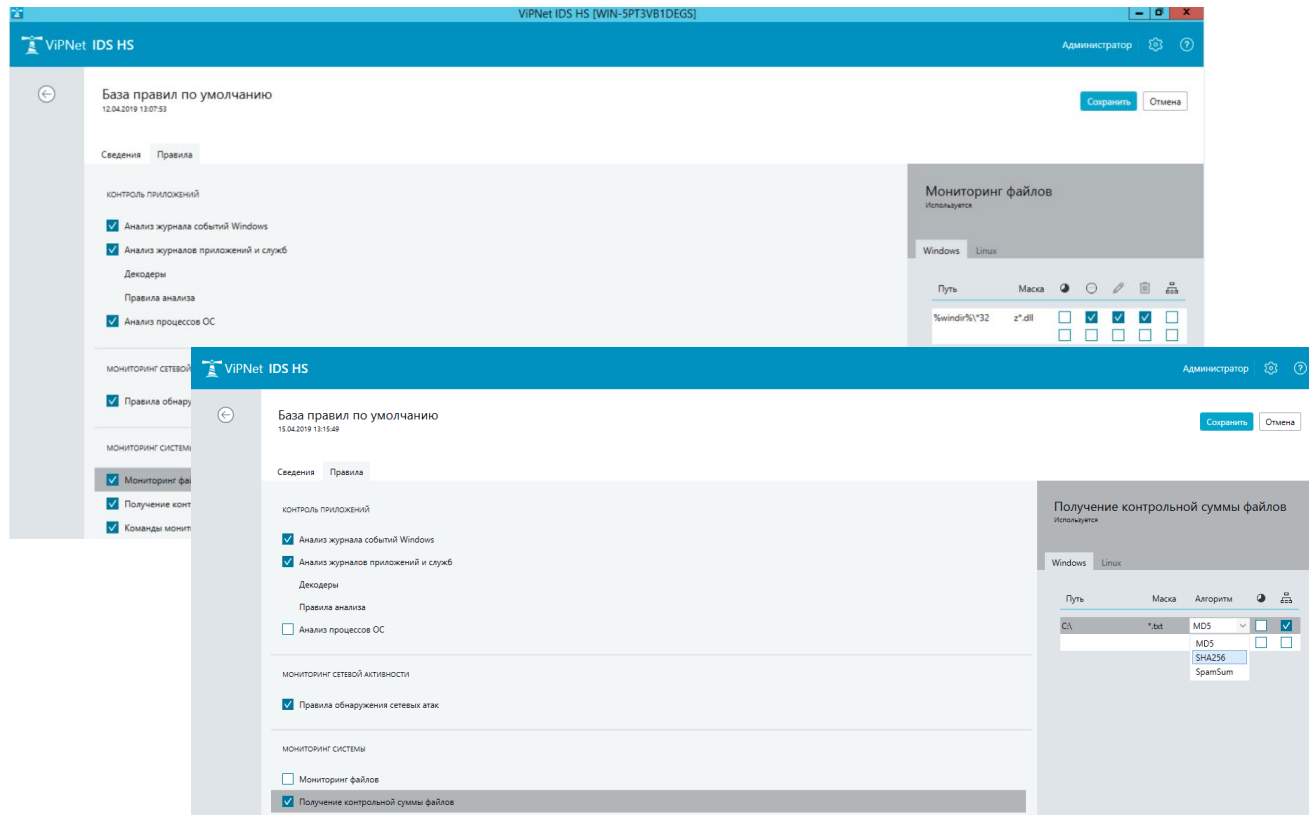
состояния безопасности

е системы безопасности



# Мониторинг и ХЭШ MD5

- Контроль директорий по маске
- Расчёт КС файлов для дальнейшего анализа и сравнение с базой «зловредов»



# Контроль обновлений Windows

The screenshot displays the ViPNet IDS HS interface. The top window shows the configuration for 'База правил по умолчанию' (Default rule base) with a 'Мониторинг системных обновлений' (Windows update monitoring) panel. The configuration includes: 'Уровень событий' (Event level) set to 'Информационное' (Informational), 'Период выборки (секунд)' (Sampling period) set to 600, and 'Системные обновления' (System updates) set to KB971033. The bottom window shows the 'События' (Events) section with a table of detected events.

Дата, время	Описание	Попытки	Идентификатор	Устройство	Группа
12.04.2019 11:34:46	Мониторинг системных обновлений	1	780000	DESKTOP-FGTGLTP	Главная
12.04.2019 11:34:46	Создание процесса (нативный функционал)	1	310000	DESKTOP-FGTGLTP	Главная
12.04.2019 11:34:23	Изменение реестра	2	100000	DESKTOP-FGTGLTP	Главная
12.04.2019 11:31:43	Изменение реестра	2	100000	DESKTOP-FGTGLTP	Главная

Additional details from the interface: The 'Мониторинг системных обновлений' panel shows a status of 'Используется' (Used) and a 'Создаваемые правила' (Generated rules) section with a 'Подробнее' (Details) link. A notification at the bottom right states: 'Системное обновление "KB971033" не установлено' (System update "KB971033" not installed).

# Remsec угрозы

Обнаружение  
RemSec угроз  
(трояны)

The screenshot displays the ViPNet IDS HS interface. The top navigation bar includes the product name, user role (Администратор), and help icons. A left sidebar lists management and service categories. The main area shows a list of events with a table of columns: Date, Description, Attempts, Identifier, and Device. A red alert box highlights a 'RemSec\_Alert: Trojan\_Detected' event from 11.04.2019 17:54:22. A detailed view of this alert is shown on the right, including the rule name, base of rules, and rule type.

Дата, время	Описание	Попытки	Идентификатор	Устройство
11.04.2019 17:54:22	RemSec_Alert...	1	900000	DESKTOP-FG7GL7P
11.04.2019 14:00:28	Установлена...	4	402000	DESKTOP-FG7GL7P
11.04.2019 13:58:08	Установлена...	1	402000	DESKTOP-FG7GL7P
11.04.2019 13:39:07	Контроль уст...	1	750000	DESKTOP-FG7GL7P
11.04.2019 13:38:47	Изменение ф...	3	200000	DESKTOP-FG7GL7P
11.04.2019 13:33:06	Подозрение...	9	403000	DESKTOP-FG7GL7P
11.04.2019 13:33:06	Изменение р...	27	100000	DESKTOP-FG7GL7P
11.04.2019 13:33:06	Регистрация...	2	402021	DESKTOP-FG7GL7P

**RemSec\_Alert: Trojan\_Detected**  
11.04.2019 17:54:22

Сработавшее правило: **Подробнее**

База правил на устройстве: 14  
Тип правил: Обнаружение вредоносной активности RemSec

Сработавшее правило: **Подробнее**

Отображать только важную информацию о событии

C:\Users\Ellidan\AppData\Local\Temp\Temp1\_test\_exe.zip\test.exe

# События от антивируса

Получаем информацию о вредоносных объектах от Антивируса Касперского и Dr. Web

The screenshot displays the ViPNet IDS HS interface, showing a list of security events and a detailed view of a specific event.

**События (Events Table):**

Дата, время	Описание	Попытки	Идентификатор	Устройство
11.04.2019 12:57:53	Изменение р...	3	100000	DESKTOP-ETCL338
11.04.2019 12:53:53	Удаление вр...	1	402014	DESKTOP-ETCL338
11.04.2019 12:53:42	Изменение р...	2	100000	DESKTOP-FG7GL7P
11.04.2019 12:53:33	Изменение р...	11	100000	DESKTOP-ETCL338
11.04.2019 12:51:22	Изменение р...	38	100000	DESKTOP-FG7GL7P

**Обнаружен вредоносный объект (Каспер...)**  
11.04.2019 12:47:42

**Сработавшее правило** | Подробнее

База правил на устройстве: 2  
Тип правил: Системная активность  
Идентификатор правила: 402020  
Уровень события: Критическое  
Описание: Обнаружен вредоносный объект(Касперский)

**Удаление вредоносного объекта DrWeb**  
11.04.2019 12:53:53

**Сработавшее правило** | Подробнее


Отображать только важную информацию о событии

```
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System><Provider Name="DrWebARKDaemon"/><EventID Qualifiers="0">1002</EventID><Level>4</Level><Task>0</Task><Keywords>0a80000000000000</Keywords><TimeCreated SystemTime="2019-04-11T07:53:52.87345200Z"/><EventRecordID>8</EventRecordID><Channel>Doctor Web</Channel><Computer>DESKTOP-ETCL338</Computer><Security/></System><EventData><Data>Neutralized object: I:\Device\HarddiskVolume2\Users\Ellidan\Desktop\icar.zip - deleted (threat name: [ICAR] Test File (NOT a Virus)!), action: 2, type: 0, ret: 0</Data></EventData></Event>
```

# Планы по IDS HS версии 1.4

- Релиз версии 1.4. – май 2019
- Подача на сертификацию ФСБ России по требованиям СОА класс В



The background of the slide is a photograph of a wind farm at sunset. Several wind turbines are silhouetted against a bright, orange, and cloudy sky. In the foreground, there are several high-voltage power line towers and their associated cables, also silhouetted against the sunset. The overall scene conveys a message of clean energy and power infrastructure.

Благодарю  
за внимание!