

Обзор новых версий продуктов  
для защиты рабочих станций  
и серверов от компании ИнфоТеКС

A decorative graphic on the right side of the page, consisting of two overlapping orange semi-circles.



## 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

# 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

# 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

**СИСТЕМА СЕРТИФИКАЦИИ  
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ**

 **ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ  
№ РОСС RU.0001.01БН00**

---

**СЕРТИФИКАТ СООТВЕТСТВИЯ  
№ 3802**

Выдан 12 октября 2017 г.  
Действителен до 12 октября 2020 г.

Настоящий сертификат удостоверяет, что система обнаружения вторжений VIPNet IDS HS, разработанная и производимая ОАО «ИнфоТекс» в соответствии с техническими условиями ФРКЕ.00177-01 97 01, является системой обнаружения вторжений уровня узла, соответствует требованиям документов «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011) и «Профиль защиты системы обнаружения вторжений уровня узла четвертого класса защиты, ИТ.СОВ.У4.ПЗ» (ФСТЭК России, 2012).

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ООО «ЦНИ» (аттестат аккредитации от 11.04.2016 № СИ RU.0001.01БН00.Б004) - техническое заключение от 23.05.2017, экспертного заключения от 23.08.2017 органа по сертификации ФАУ «ТННИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СИ RU.0001.01БН00.А002).

Заявитель: ОАО «ИнфоТекс» (ИНН 7710013769)  
Адрес: 127287, г. Москва, Старый Петровско-Разумовский проезд, д. 1/23, стр. 1  
Телефон: (495) 737-6192

Контроль маркирования знаками соответствия сертифицированной продукции и инспекционный контроль её соответствия требованиям документов, указанных в настоящем сертификате, осуществляется испытательной лабораторией ООО «ЦНИ».

**ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ**

В. Лютиков

---

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации  
12 октября 2017 г.



Что нового в ViPNet IDS HS  
версии 1.4?

# Политики аудита

**ViPNet IDS HS**

## ← Политика аудита по умолчанию

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

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:

- 
- 

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

**ViPNet IDS HS**

## ← Политика аудита по умолчанию

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

ОТСЛЕЖИВАНИЕ

- Запись событий
- Процессы: детальный аудит

ГЛМ

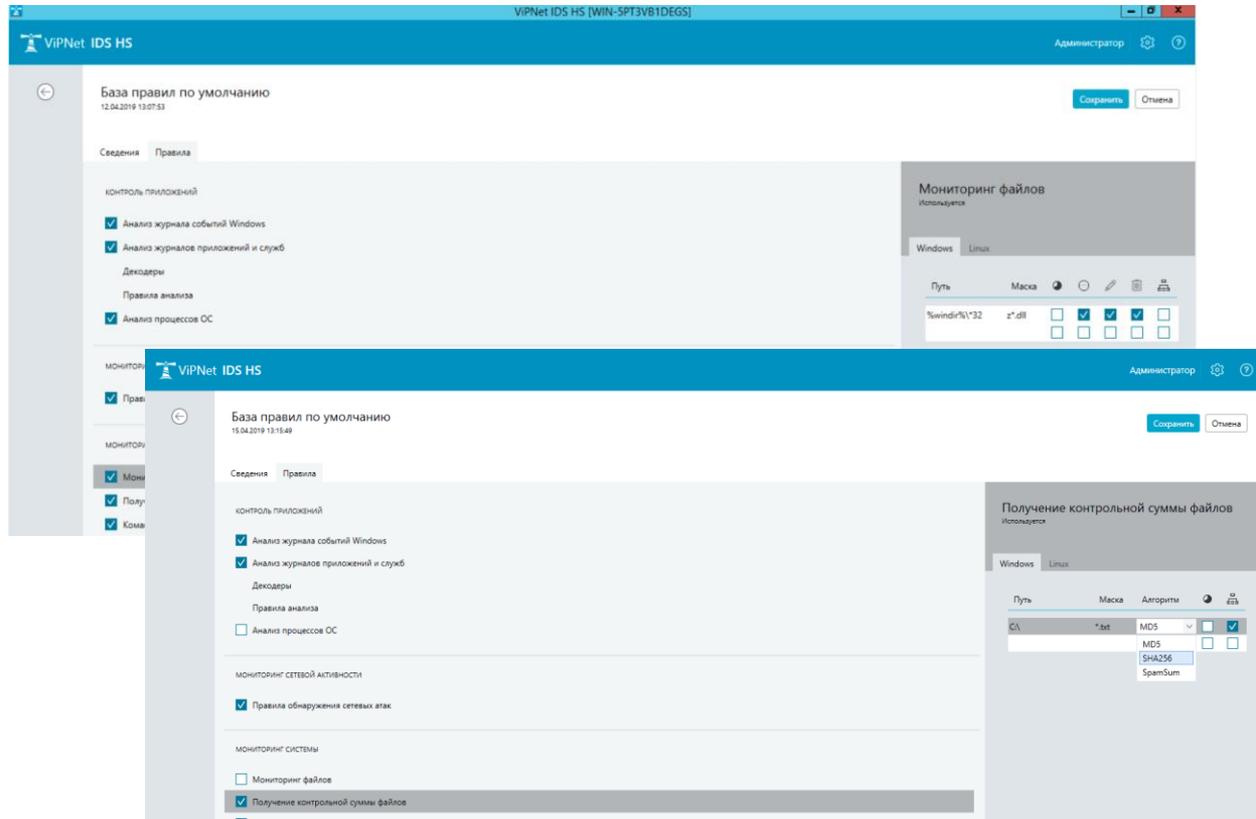
- Общем файловом ресурсе
- Изменения доступа к объекту
- Объектам ядра

ОТСЛЕЖИВАНИЕ

- Состояния безопасности
- 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, which is used for monitoring system updates. The main window is titled "База правил по умолчанию" (Default rule base) and shows a configuration page for "Мониторинг системных обновлений" (System update monitoring). The configuration includes a search for event identifiers, a search filter, and a table of events. The table has columns for "Дата, время" (Date, time), "Описание" (Description), "Попытки" (Attempts), "Идентификатор" (Identifier), "Устройство" (Device), and "Группа" (Group). The events listed are:

Дата, время	Описание	Попытки	Идентификатор	Устройство	Группа
12.04.2019 11:34:46	Мониторинг системных обновлений	1	780000	DESKTOP-FGTGL7P	Главная
12.04.2019 11:34:46	Создание процесса (пассивный функционал)	1	310000	DESKTOP-FGTGL7P	Главная
12.04.2019 11:34:23	Изменение реестра	2	100000	DESKTOP-FGTGL7P	Главная
12.04.2019 11:31:43	Изменение реестра	2	100000	DESKTOP-FGTGL7P	Главная

The interface also shows a sidebar with navigation options: "УПРАВЛЕНИЕ" (Management) with "События" (Events) selected, "Устройства" (Devices), and "Базы правил" (Rule bases); "СЕРВИС" (Service) with "Журналы" (Logs), "Учетные записи" (Accounts), and "Обнаружение аномалий" (Anomaly detection). A right-hand panel shows the "Мониторинг системных обновлений" configuration with "Уровень событий" (Event level) set to "Информационное" (Informational), "Период выборки (секунд)" (Sampling period) set to 600, and "Системные обновления" (System updates) set to KB971033. A bottom-right panel shows a notification for the update KB971033, which is marked as "не установлено" (not installed).

# Remsec угрозы

## Обнаружение RemSec угроз (трояны)

The screenshot displays the VIPNet IDS HS web interface. The main window shows a list of events under the 'События' (Events) tab. A detailed view of a specific event is shown on the right, titled 'RemSec\_Alert: Trojan\_Detected'.

**Event List:**

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

**Alert Details:**

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

Сработавшее правило: [Подробнее](#)

База правил на устройстве: 14

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. The top navigation bar includes the product name, user role (Администратор), and system status icons. The left sidebar contains navigation options for management, events, devices, rules, services, logs, accounts, anomaly detection, and monitoring.

The main area shows a list of security events under the heading "События". The table below summarizes the visible events:

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

A detailed view of a specific event is shown on the right, titled "Удаление вредоносного объекта DrWeb". The event details include:

- База правил на устройстве: 2
- Тип правил: Системная активность
- Идентификатор правила: 402020
- Уровень события: Критическое

The event XML data is displayed at the bottom of the detailed view:

```
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event" ><System><Provider Name="DrWebARC Daemon" /><EventID Qualifiers="0">1002</EventID><Level>4</Level><Task>0</Task><Keywords>0x0000000000000000</Keywords><TimeCreated SystemTime="2019-04-11T07:53:52.873845200Z" /><EventRecordID>8</EventRecordID><Channel>Doctor Web</Channel><Computer>DESKTOP-ETCL338</Computer><Security></Security></System><EventData><Data>Neutralized object: {Device\HarddiskVolume2\Users\Ellidan\Desktop\leicar.zip - deleted [threat name: {EICAR Test File (NOT A Virus!); action: 2, type: 0, ret: 8}</Data></EventData></Event>
```





## 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 атаками на сам BIOS

## Организация доверенной загрузки

Контроль целостности

Разграничение доступа

UEFI BIOS

MBR

Таблицы ACPI,  
SMBIOS, карты  
распределения  
памяти

Файлов

CMOS

Двухфакторная  
аутентификация

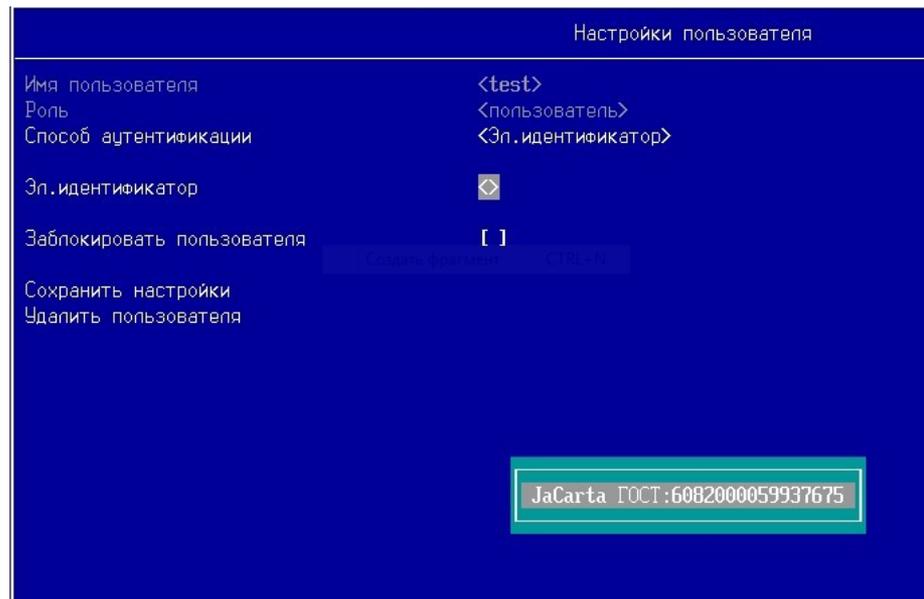
Токены:  
JaCarta  
Rutoken  
Guradant ID



Что нового в ViPNet  
SafeBoot версии 1.4?

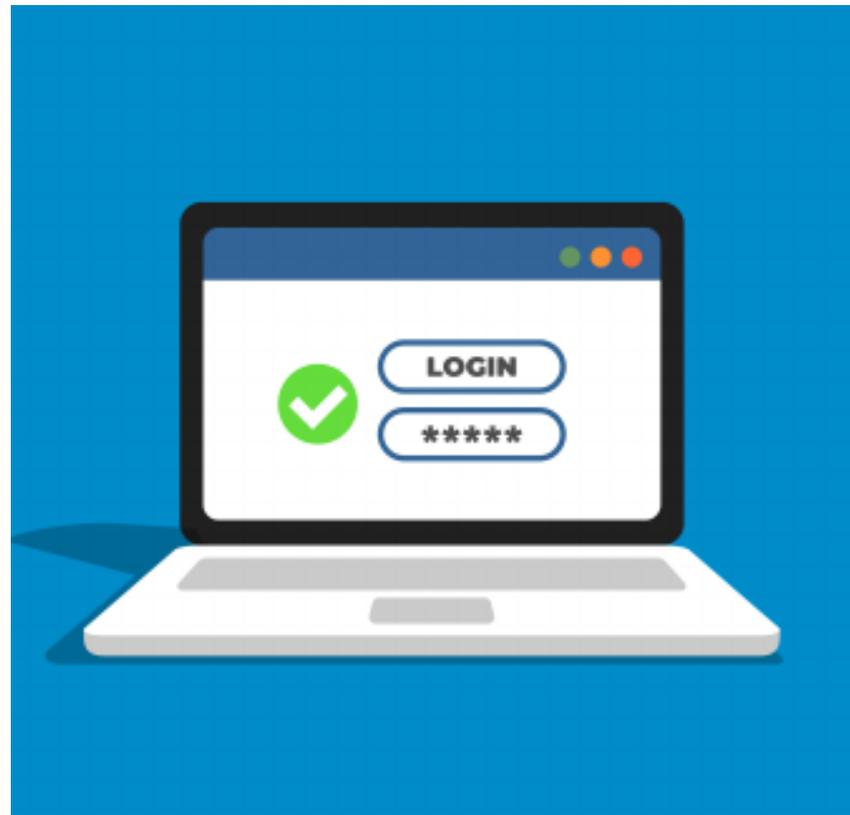
# Поддержка JaCarta-2 ГОСТ

- 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

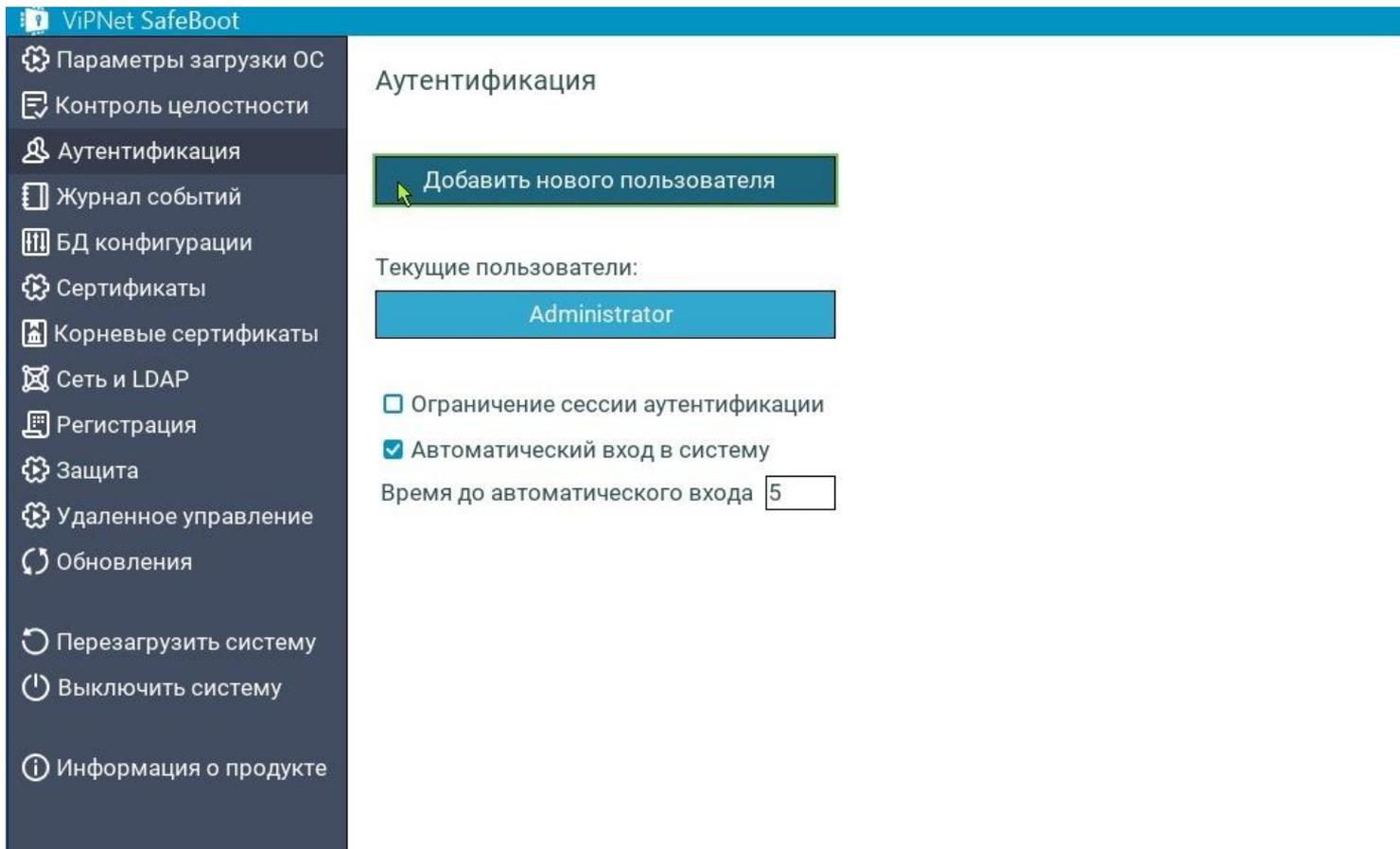
Создать запрос на регистрацию

Код регистрации

Импортировать код регистрации

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

# В ноябре обновлённый интерфейс!



The screenshot displays the management interface for VIPNet SafeBoot. On the left is a dark sidebar with a menu of options, and on the right is the main content area for the 'Аутентификация' (Authentication) settings.

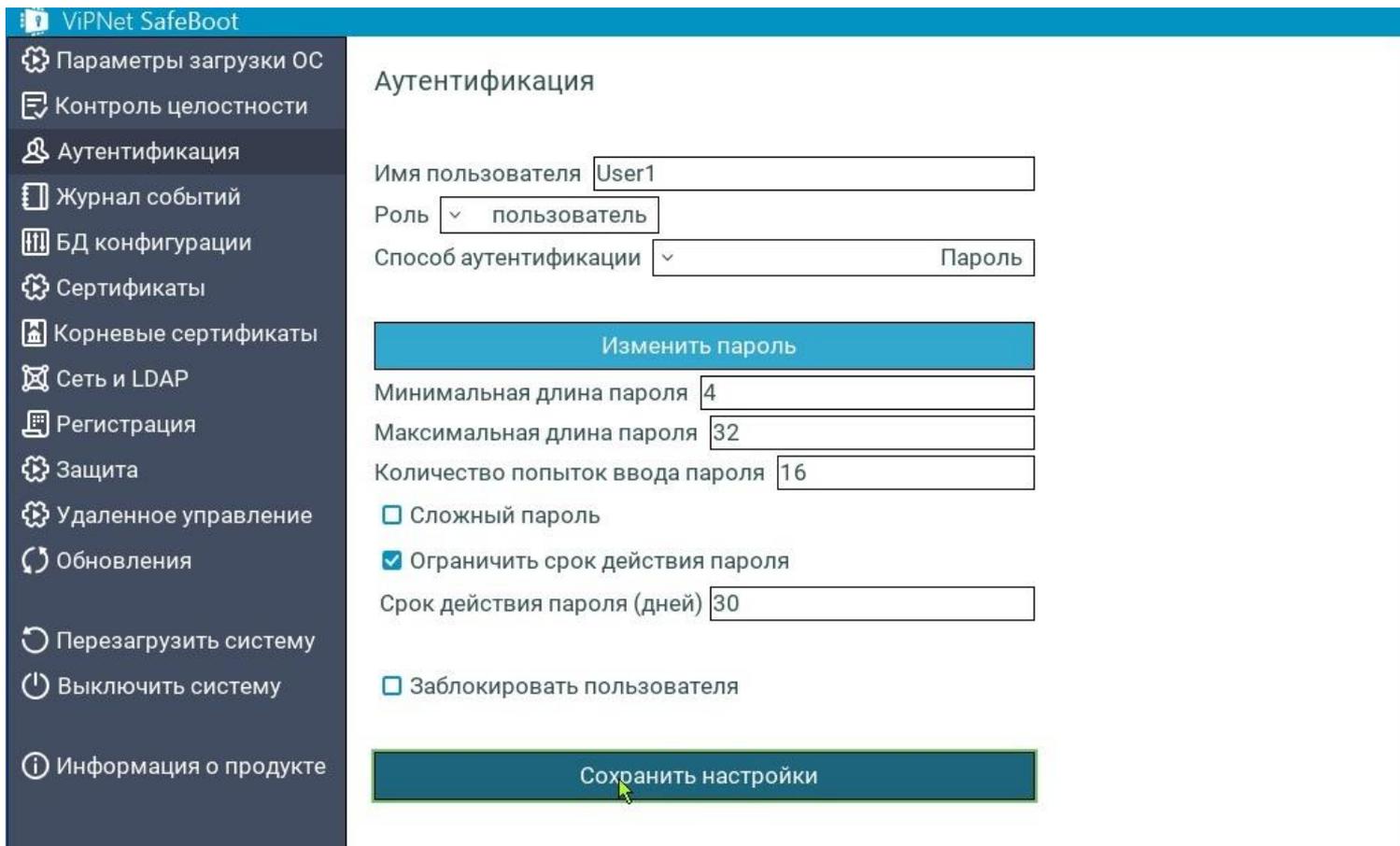
**Menu items (left sidebar):**

- Параметры загрузки ОС
- Контроль целостности
- Аутентификация**
- Журнал событий
- БД конфигурации
- Сертификаты
- Корневые сертификаты
- Сеть и LDAP
- Регистрация
- Защита
- Удаленное управление
- Обновления
- Перезагрузить систему
- Выключить систему
- Информация о продукте

**Main content area (Аутентификация):**

- Аутентификация
- Добавить нового пользователя (button)
- Текущие пользователи:
  - Administrator (button)
- Ограничение сессии аутентификации
- Автоматический вход в систему
- Время до автоматического входа

# В ноябре обновлённый интерфейс!



**ViPNet SafeBoot**

- Параметры загрузки ОС
- Контроль целостности
- Аутентификация**
- Журнал событий
- БД конфигурации
- Сертификаты
- Корневые сертификаты
- Сеть и LDAP
- Регистрация
- Защита
- Удаленное управление
- Обновления
- Перезагрузить систему
- Выключить систему
- Информация о продукте

### Аутентификация

Имя пользователя

Роль

Способ аутентификации

**Изменить пароль**

Минимальная длина пароля

Максимальная длина пароля

Количество попыток ввода пароля

Сложный пароль

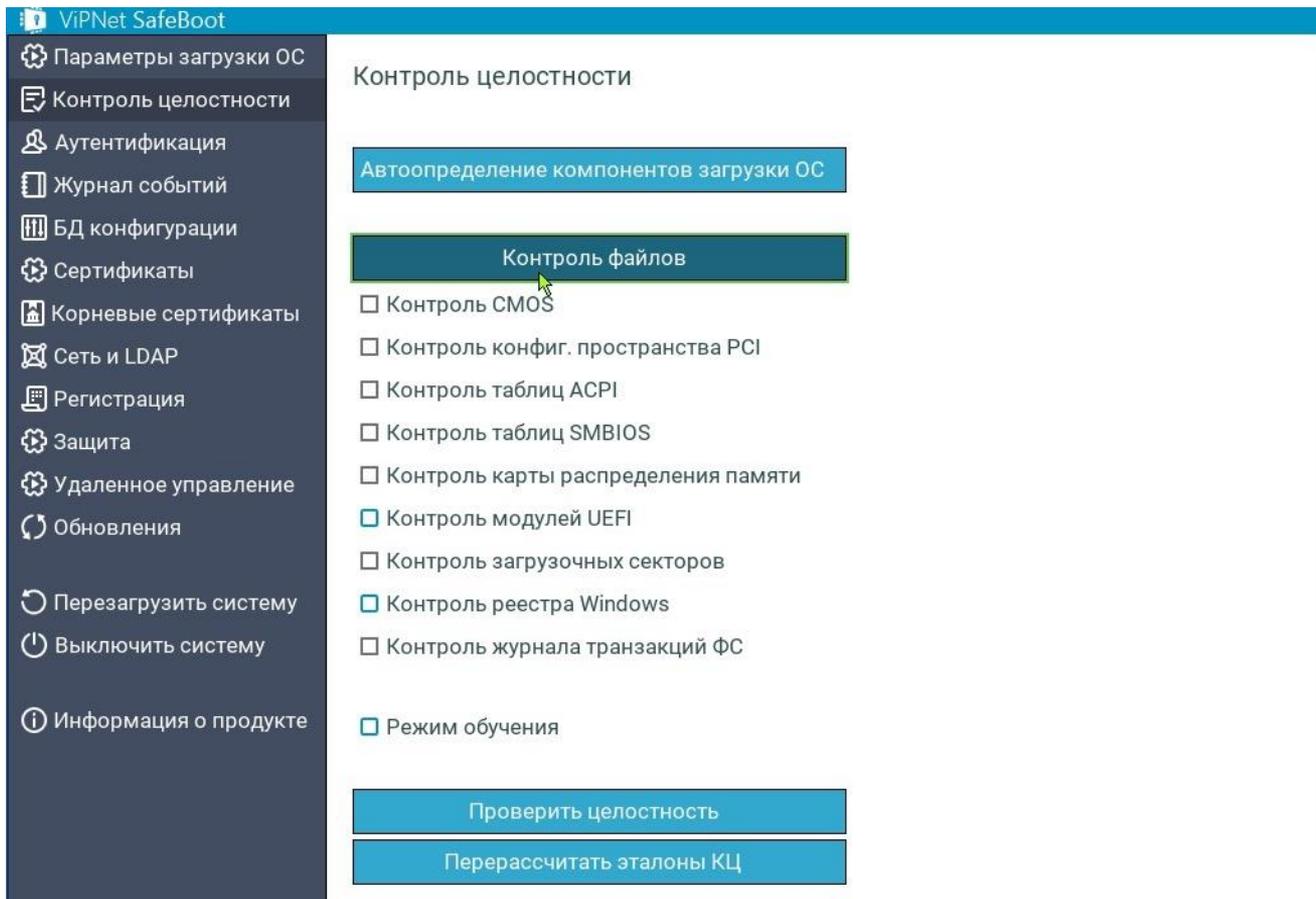
Ограничить срок действия пароля

Срок действия пароля (дней)

Заблокировать пользователя

**Сохранить настройки**

# В ноябре обновлённый интерфейс!



The screenshot displays the 'ViPNet SafeBoot' application interface. On the left is a dark sidebar with a list of settings categories, including 'Parameters of OS loading', 'Control integrity', 'Authentication', 'Event log', 'Configuration database', 'Certificates', 'Root certificates', 'Network and LDAP', 'Registration', 'Protection', 'Remote management', 'Updates', 'Restart system', 'Turn off system', and 'Product information'. The main area is titled 'Control integrity' and contains several buttons and a list of checkboxes. A mouse cursor is pointing at the 'Control files' button, which is highlighted with a green border. Below it, a list of system components has checkboxes for integrity control, with 'Control UEFI modules' and 'Control Windows registry' checked. At the bottom, there are two large buttons: 'Check integrity' and 'Recalculate hashes'.

ViPNet SafeBoot

- Параметры загрузки ОС
- Контроль целостности
- Аутентификация
- Журнал событий
- БД конфигурации
- Сертификаты
- Корневые сертификаты
- Сеть и LDAP
- Регистрация
- Защита
- Удаленное управление
- Обновления
- Перезагрузить систему
- Выключить систему
- Информация о продукте

### 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

Перерассчитать эталоны КЦ





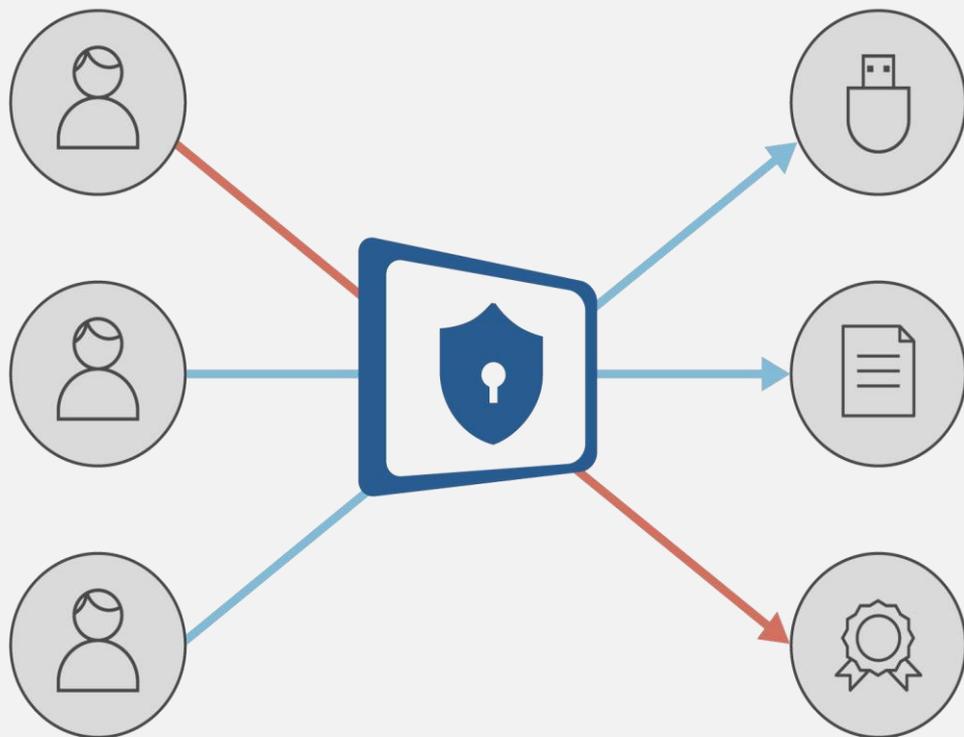
## ViPNet SafePoint

Средство защиты информации от несанкционированного доступа, устанавливаемое на рабочие станции и сервера, предназначенное для мандатного и дискреционного разграничения доступа к критически важной информации. Реализована разграничительная (пользователя к объектам) и разделительная (между пользователями) политика доступа, основанная на автоматической разметке создаваемых файлов.

# Идентификация и аутентификация

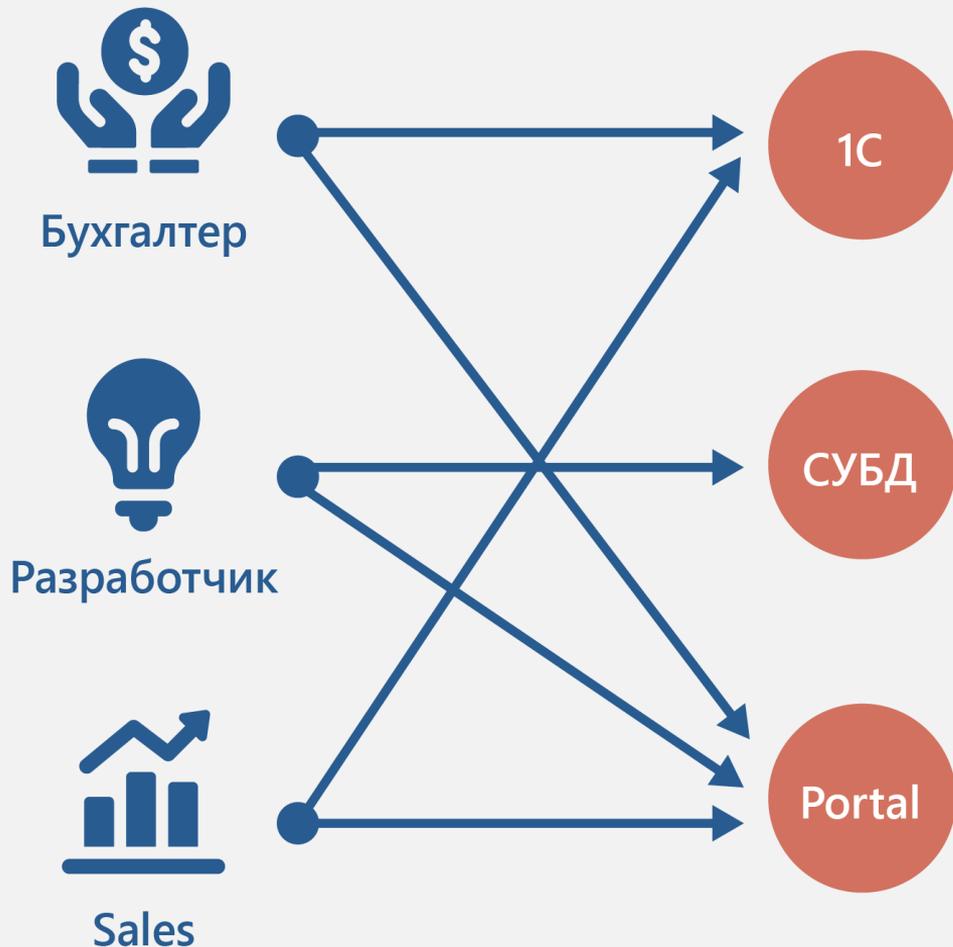


- Двухфакторная аутентификация пользователей
- Поддержка USB-токенов и смарт-карт:
  - JaCarta ГОСТ
  - JaCarta PKI
  - JaCarta LT
  - Rutoken S
  - Rutoken Lite
  - Rutoken ЭЦП



## Дискреционный контроль доступа пользователей

Разграничительная политика на основе матрицы доступа



Мандатный контроль  
доступа пользователей  
и процессов

Разграничительная политика  
на основе меток безопасности

# Замкнутая программная среда

- Защита от модификации запускаемых модулей
- Контроль запуска скриптов Active Scripts
- Контроль запуска задач



## Контроль устройств

- Контроль и разграничения доступа к подключаемым внешним устройствам
- Разграничение доступа к принтерам

# Создание правила доступа

Управление настройками клиента "Новый клиент, IP: 127.0.0.1"

Профиль: Программисты

Правила доступа для выбранного профиля

Тип	Объект файлово	Режим доступа	Режим аудита
★	\\*	+Ц+Э+И+У+П	-----:-----

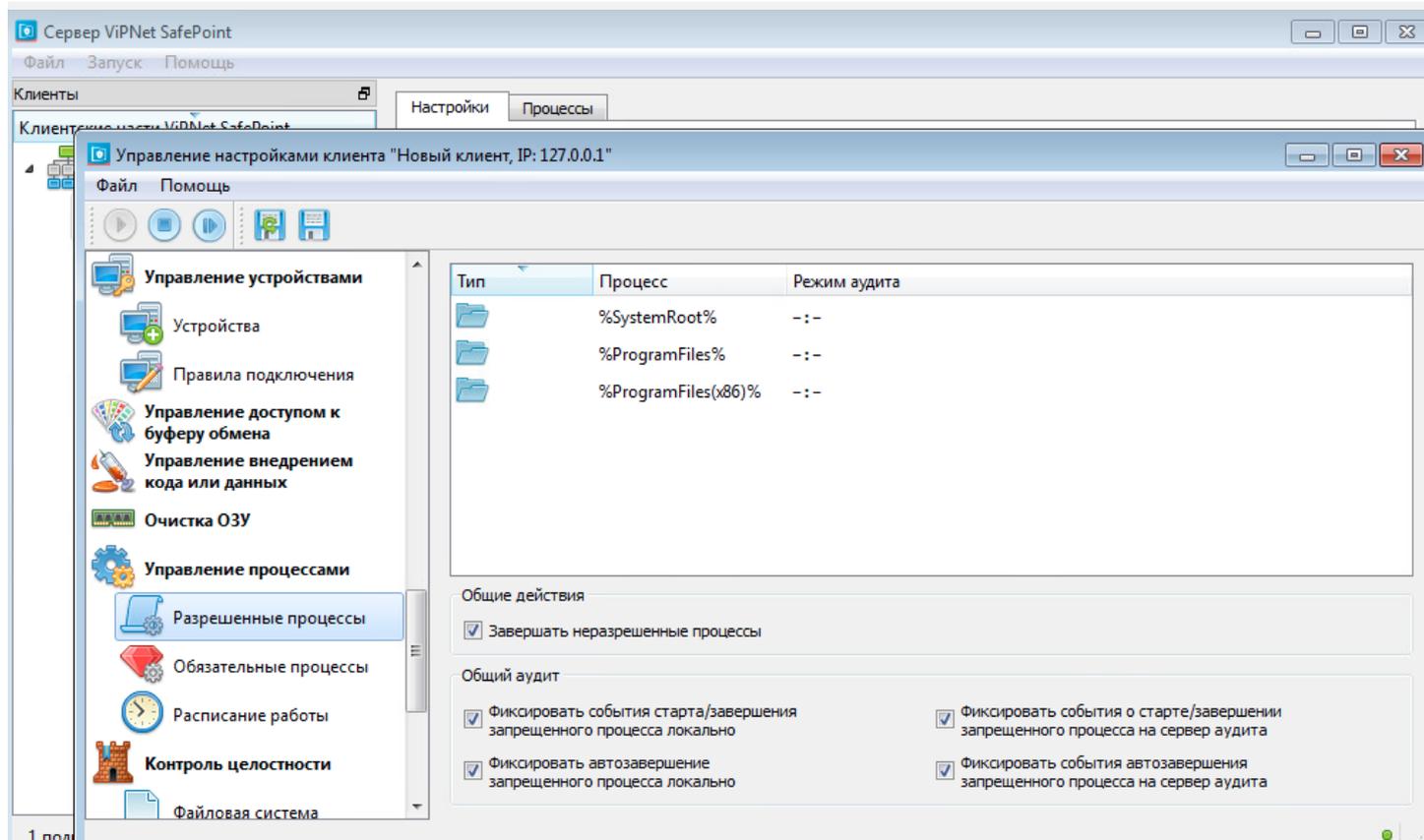
Добавить новое правило

C:\Program Files (x86)

Режим доступа

Чтение:	<input checked="" type="checkbox"/> Разрешить <input type="checkbox"/> Запретить	<input type="checkbox"/> Фиксировать чтение локально	<input checked="" type="checkbox"/> Фиксировать чтение на сервере аудита
Запись:	<input type="checkbox"/> Разрешить <input checked="" type="checkbox"/> Запретить	<input type="checkbox"/> Фиксировать запись локально	<input checked="" type="checkbox"/> Фиксировать запись на сервере аудита
Исполнение:	<input checked="" type="checkbox"/> Разрешить <input type="checkbox"/> Запретить	<input type="checkbox"/> Фиксировать исполнение локально	<input checked="" type="checkbox"/> Фиксировать исполнение на сервере аудита
Удаление:	<input type="checkbox"/> Разрешить <input checked="" type="checkbox"/> Запретить	<input type="checkbox"/> Фиксировать удаление локально	<input checked="" type="checkbox"/> Фиксировать удаление на сервере аудита
Переименование:	<input type="checkbox"/> Разрешить <input checked="" type="checkbox"/> Запретить	<input type="checkbox"/> Фиксировать переименование локально	<input checked="" type="checkbox"/> Фиксировать переименование на сервере аудита

# Настройка разрешённых процессов



Сервер VIPNet SafePoint

Файл Запуск Помощь

Клиенты

Настройки Процессы

Управление настройками клиента "Новый клиент, IP: 127.0.0.1"

Файл Помощь

Управление устройствами

- Устройства
- Правила подключения

Управление доступом к буферу обмена

Управление внедрением кода или данных

Очистка ОЗУ

Управление процессами

- Разрешенные процессы**
- Обязательные процессы
- Расписание работы

Контроль целостности

- Файловая система

Тип	Процесс	Режим аудита
Папка	%SystemRoot%	--
Папка	%ProgramFiles%	--
Папка	%ProgramFiles(x86)%	--

Общие действия

- Завершать неразрешенные процессы

Общий аудит

- Фиксировать события старта/завершения запрещенного процесса локально
- Фиксировать события о старте/завершении запрещенного процесса на сервер аудита
- Фиксировать события автозавершения запрещенного процесса локально
- Фиксировать события автозавершения запрещенного процесса на сервер аудита

# Ожидание по сертификации



Продукт будет передан на сертификацию по линии ФСТЭК России по требованиям к:

- 5 классу защищенности СВТ
- 4 классу защиты СКН (ИТ.СКН.П4.ПЗ)
- 4 классу ТДБ



Спасибо  
за внимание!