Содержание:

ВВЕДЕНИЕ

В наше время существует немало программ для электронного документооборота. Электронный документооборот позволяет экономить время, повышает комфорт и удобство работы, снижает трудоемкость, а вероятность ошибки по причине пресловутого человеческого фактора стремится к нулю. При этом требования к аппаратному парку предъявляются вполне приемлемые, а уровень компьютерной грамотности пользователей может находиться где-то в пределах среднего. Жизненный цикл любого документа состоит из нескольких этапов: создание, оформление, регистрация, согласование, обсуждение, утверждение, принятие к исполнению, проведение, сдача в архив и т.д. Причем их перечень может меняться в зависимости от конкретной ситуации. Каждый этап в обязательном порядке фиксируется, и в пределах своей компетенции его санкционируют конкретные люди — на практике это оформляется визированием (подписью). Хранение документации должно быть систематизировано — в зависимости от специфики, назначения и прочих факторов. Обычно для этого используются папки, каталоги, разделы и т.п. И, безусловно, одной из важнейших функций делопроизводства является обеспечение сохранности документации.

Все перечисленные, а также многие другие задачи успешно решаются с помощью специализированных программных средств, которые в широком ассортименте представлены на рынке. Сегодня мы рассмотрим такую программу электронного документа оборота как «ИнфоТеКС».

ГЛАВА 1.ПРОГРАММА ИНФОТЕКС

1.1ViPNet IDS HS

ИнфоТеКС (Информационные Технологии и Коммуникационные Системы) — российский разработчик программно-аппаратных VPN-решений и СКЗИ. Группа компаний ИнфоТеКС была основана в 1991 году группой специалистов по информационной безопасности во главе с Андреем Чапчаевым. Согласно рейтингу CNews Analytics, ИнфоТеКС заняла 6-е место среди крупнейших компаний России в сфере защиты информации в 2016 году.

Основной разработкой компании является технология **ViPNet** — гибкое VPN-решение, которое позволяет осуществлять безопасную передачу данных в защищенной сети.

ViPNet®

Virtual Private Network

В состав **ГК ИнфоТеКС** также входят три дочерние компании: ОАО «ИнфоТеКС Интернет Траст», ЗАО «Перспективный мониторинг» и НОЧУ ДПО «Учебный центр ИнфоТеКС». В ГК ИнфоТеКС работает более 800 сотрудников.

ИНФОТЕКС ТРАСТ

infotecs

ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

ViPNet IDS HS — система обнаружения вторжений, осуществляющая мониторинг и обработку событий внутри хоста.

Наблюдение за всеми активностями, происходящими в операционной системе, такими как файловая или сетевая активность, изменения в реестре, процессах или ключевых логах.

Оповещение: по результатам наблюдения система выявляет атаки и незамедлительно оповещает об этом администратора. Администратор получает оповещения в интерфейсе управляющего приложения или по email.

Главное — всегда быть в курсе, что происходит на хосте.

ViPNet IDS HS отлично дополнит Вашу систему безопасности за счёт:

- эвристического анализа - способного обнаружить атаки, для которых еще нет антивирусных сигнатур;
- удобного расположения - так как приложение на хосте способно обнаруживать сетевые атаки, которые не видны сетевым IDS (например, атаки в зашифрованном трафике).

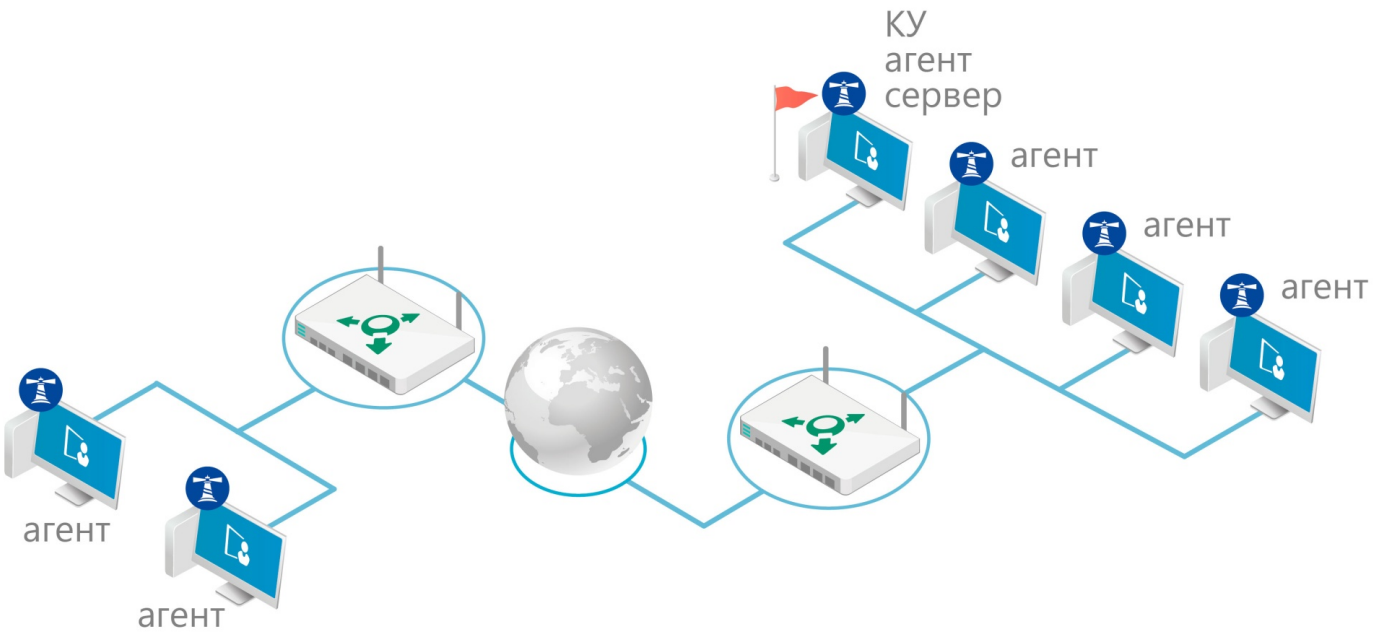
Эвристический анализ (эвристическое сканирование) — это совокупность функций антивируса, нацеленных на обнаружение неизвестных вирусным базам вредоносных программ, но в то же время этот же термин обозначает один из конкретных способов.

Практически все современные антивирусные средства применяют технологию эвристического анализа программного кода. Эвристический анализ нередко используется совместно с сигнатурным сканированием для поиска сложных

шифрующихся и полиморфных вирусов. Методика эвристического анализа позволяет обнаруживать ранее неизвестные инфекции, однако, лечение в таких случаях практически всегда оказывается невозможным. В таком случае, как правило, требуется дополнительное обновление антивирусных баз для получения последних сигнатур и алгоритмов лечения, которые, возможно, содержат информацию о ранее неизвестном вирусе. В противном случае, файл передается для исследования антивирусным аналитикам или авторам антивирусных программ.

1.2 Архитектура продукта

- Агент — собирает информацию о функционировании хостов и выполняет ее первичный анализ. Агент представляет собой ПО, которое устанавливается на хостах.
- Сервер — получает, хранит и анализирует информацию от Агентов.
- Консоль управления — предоставляет графический интерфейс для управления Агентами и мониторинга их состояния.



Поддерживаемые ОС

- MS Windows 10 (32/64), 8.1 (32/64), 8 (32/64), 7 SP1 (32/64).
- MS Windows Server 2012 R2, 2012, 2008 R2, 2008 (32/64).

Базы правил разрабатываются российской компанией ЗАО «Перспективный мониторинг»

1.3 Функциональное описание продукта

Основные задачи:

- Обнаружение атак на информационную систему и их оперативное предотвращение.
- Повышение уровня защищенности информационных систем, центров обработки данных, рабочих станций пользователей, серверов и

телекоммуникационного оборудования.
- Помощь в расследовании инцидентов безопасности за счет агрегирования и журналирования событий.

Преимущества

- Система и базы правил разработаны в России.
- Обнаружение сетевых атак, которые не видны сетевым IDS (атаки в шифрованном трафике).
- Централизованное управление продуктом.

Угрозы(недостатки):

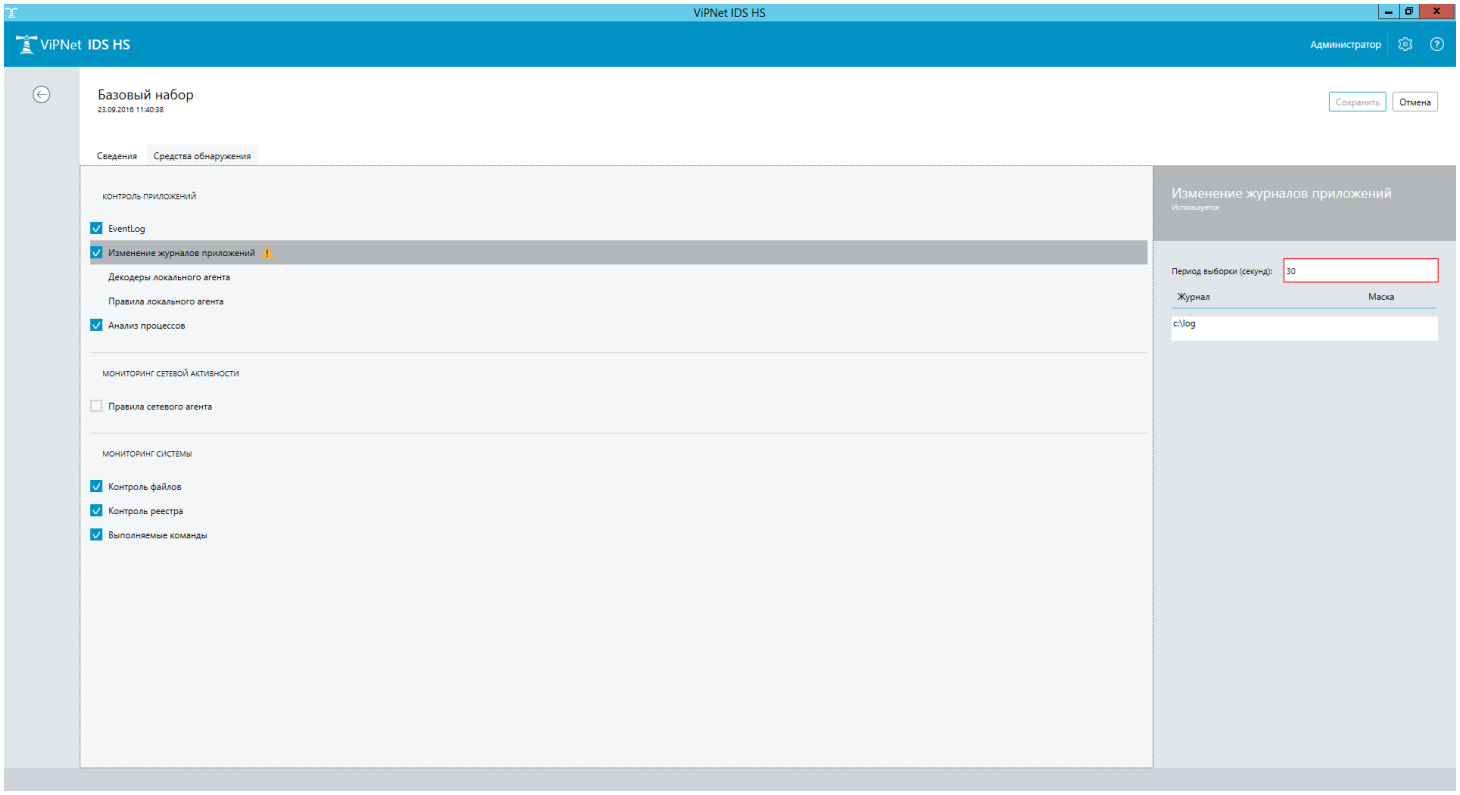
- Прослушивание трафика;
- Изменение содержания трафика;
- Атаки типа "отказ в обслуживании".

Методы защиты:

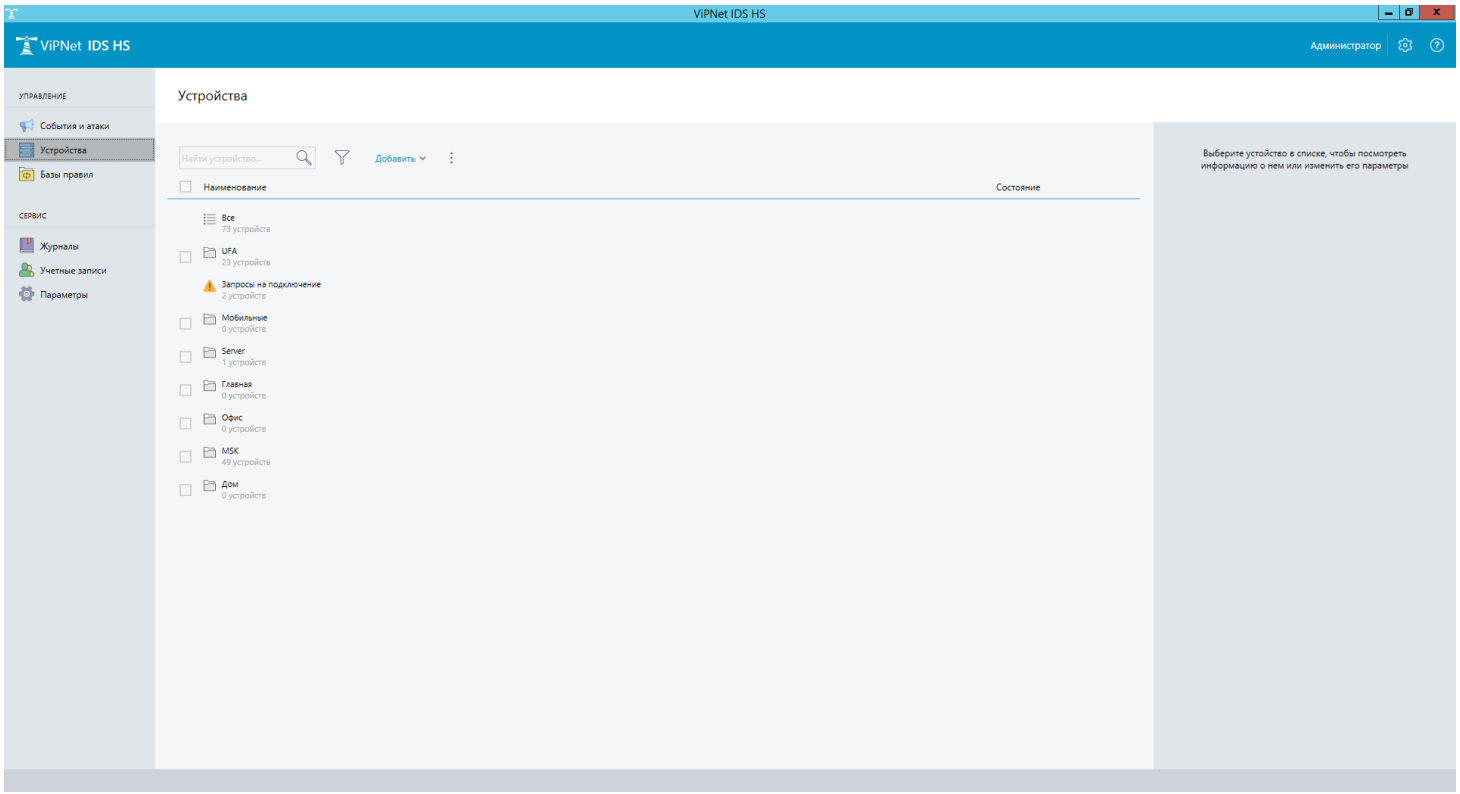
- Использование патентованных (закрытых) кодеков;
- Применение технологии VLAN;
- Внедрение криптографической защиты сетевого трафика.
- Стоимость программы ИнфоТеКС- 345 000 рублей

ГЛАВА 2.ИНТЕРФЕЙС ПРОГРАММЫ

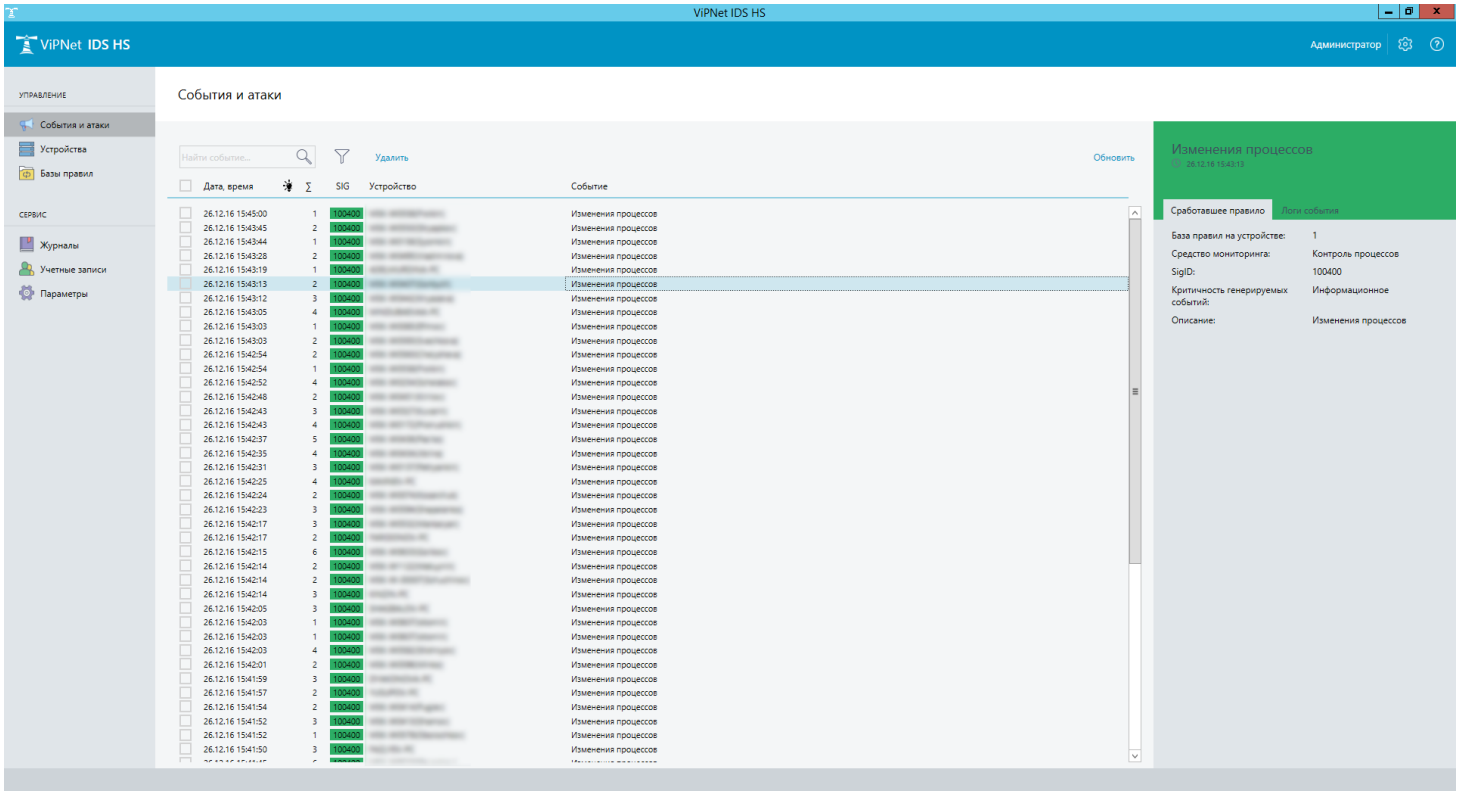
Редактор базы решающих правил



Окно списка устройств



Окно просмотра событий



ЗАКЛЮЧЕНИЕ

Таким образом, сегодня проблема информационной безопасности чрезвычайно важна, а роль решений для ее обеспечения очень существенна, но, к сожалению, рынком пока ещё недооценена. Роль IT-систем постоянно растет, мы передаем в информационные системы все больше и больше задач, которые непосредственно касаются жизни человека: это и управление отоплением, поездами, полетами и многое другое. Критические сбои таких систем могут привести даже к тому, что человечество совсем откажется от информационных технологий, футурологи, к примеру, рассматривают и такую вероятность. В классическом определении безопасность функционирования — это „конфиденциальность — целостность — доступность“, именно это позволяет говорить о том, что мы строим не просто информационные системы, а информационные системы, которым можно доверять.

Однако, «ИнфоТеКС» является весьма перспективной программой с удобным для пользователей интерфейсом, а так же позволяет защищать персональные данные пользователей, что приумножает её достоинства и помогает ей развиваться.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. https://infotecs.ru/about/press-centr/publikatsii/bezopasnost-sistem-bezopasnosti-zashchita-informatsii-ip-videonablyudeniya.html
2. https://infotecs.ru/product/setevye-komponenty/vipnet-ids/
3. http://www.hardnsoft.ru/soft/ofisnyy-soft/20183/
4. https://ru.wikipedia.org/wiki/ИнфоТеКС