# ViPNet IDS HS -

## новая сертифицированная система обнаружения вторжений уровня узла от компании Инфотекс

Иван Кадыков

# Для чего нужны HIDS?

- Определять атаки, которые “не видит” NIDS;
- Обнаружение атаки после расшифровки входящего трафика;
- Обнаруживать подозрительную активность внутри ОС (файловая активность, изменения в реестре и процессах).

# 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 – выявление IoC

# Возможности IDS HS

- Различные методы определения атак
  - Сигнатурный метод
  - Метод аномалий
- Базы правил разрабатываются при участии ЗАО «Перспективный мониторинг»
- 4 уровня критичности событий
- Уведомление администратора по e-mail

# 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

# Поддерживаемые ОС

- Microsoft Windows 10 (32/64-бит);
- Microsoft Windows 8.1 (32/64-бит);
- Microsoft Windows 8 (32/64-бит);
- Microsoft Windows 7 SP1 (32/64-бит);
- Microsoft Windows Server 2012 R2;
- Microsoft Windows Server 2012;
- Microsoft Windows Server 2008 R2 SP1;
- Microsoft Windows Server 2008 SP2 (32/64-бит);

# Сертификат

- Сертификат ФСТЭК России по требованиям к системам обнаружения вторжения уровня узла 4 класса.

- Список мер из приказов №21 и №17:
  - 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.0001.01БИ00

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 систем 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 «ЦБИ» (аттестат аккредитации от 11.04.2016 № СЗИ RU.0001.01БИ00.Б004) - техническое заключение от 23.05.2017, экспертного заключения от 29.08.2017 органа по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.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 «ЦБИ».

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

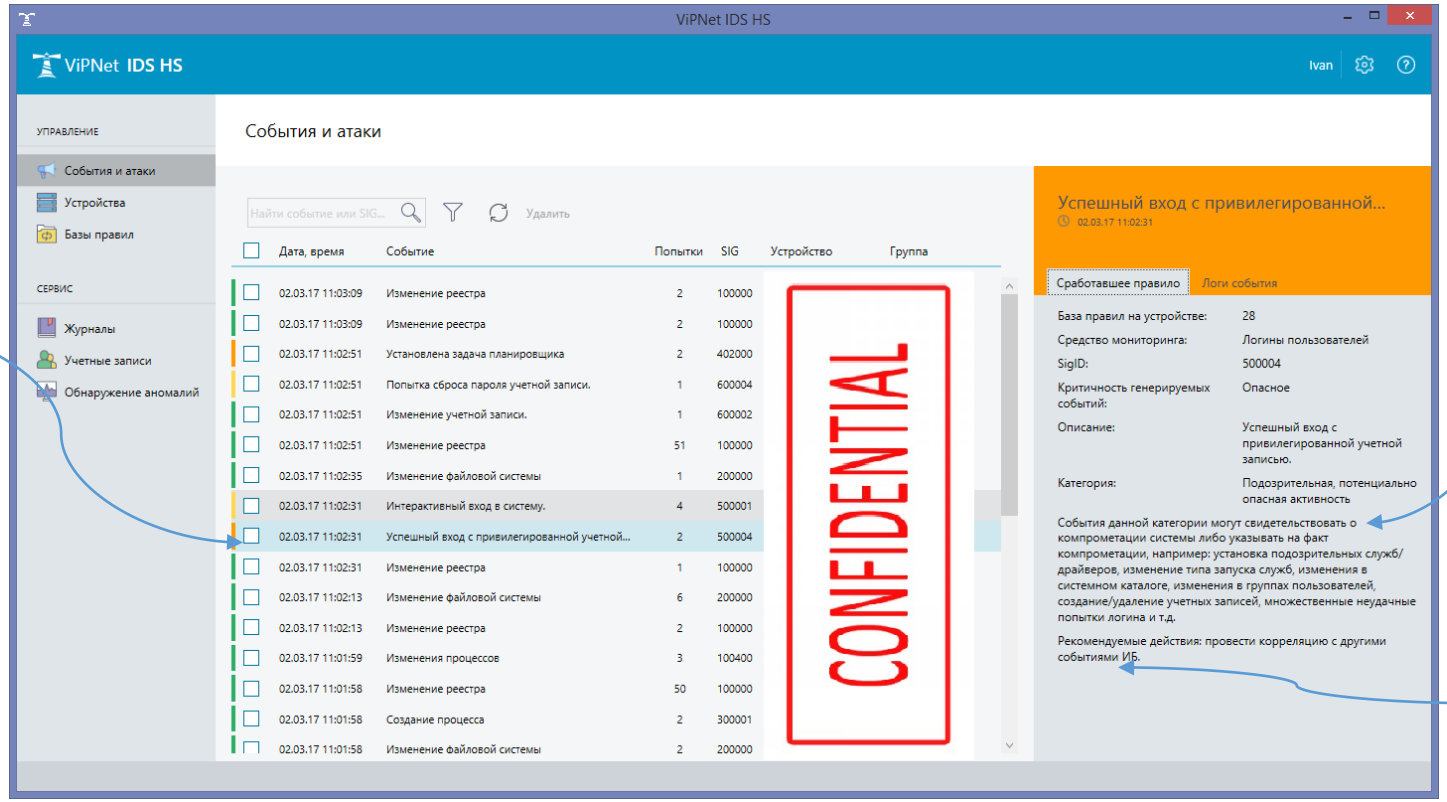
В. Лютиков

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

# Схема лицензирования

Совокупная стоимость продукта складывается из стоимости серверной лицензии(количество подключений агентов), права на подписку БРП на 1 год, сертификата на ТП и установочного комплекта.

# Внешний вид интерфейса




Опасное событие

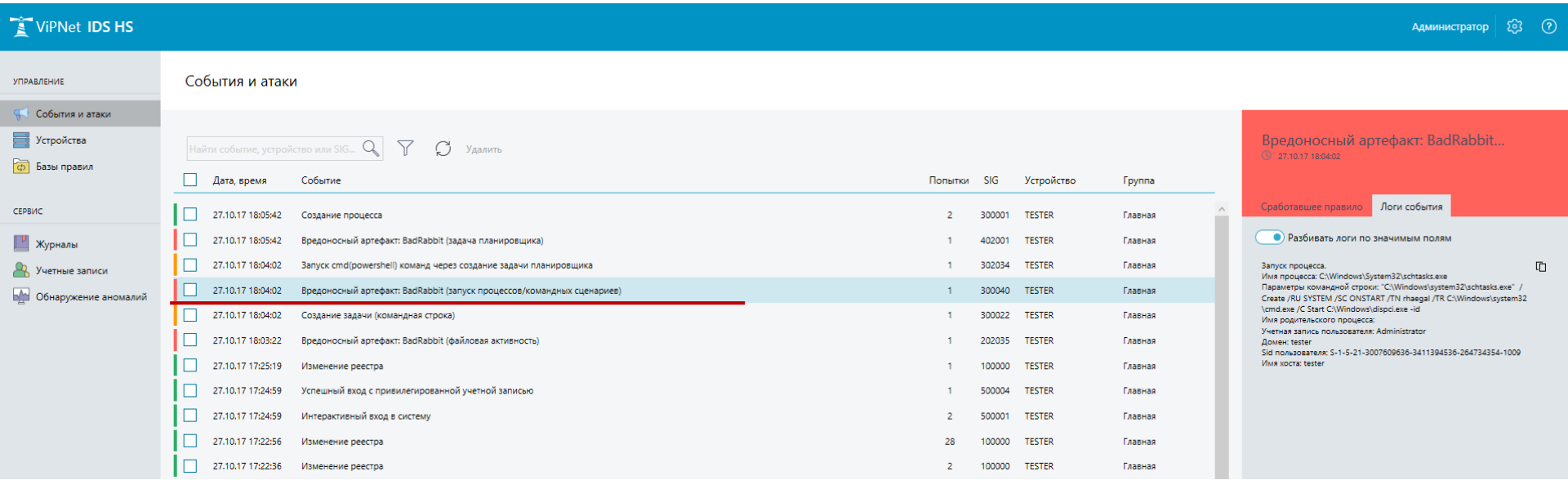
Подробная информация о событии

Рекомендации по дальнейшим действиям

# BadRabbit - detected

24.10.2017 в пик активности шифровальщика BadRabbit произошли срабатывания сигнатур на ViPNet IDS HS:

- Запуск потенциально опасного ПО: mimikatz (sid: 121003)
- Вредоносный артефакт: mimikatz components (sid: 121117)
- mimikatz activity: попытка извлечения данных учетных записей (sid: 180000)
- mimikatz activity: попытка проведения pass-the-hash атаки (sid: 180001)
- mimikatz activity: попытка повышения привилегий (sid: 180002)



# Перспективы развития

- 09.11.2017 вышла версия 1.2:
  - Интеграция с Active Directory и ViPNet-сетями
  - Поддержка syslog (формат CEF) и snmp
  - Интеграция с ViPNet TIAS
  - Возможность управления продуктом из консоли ViPNet IDS MC
  - Детализация событий и рекомендации
  - Поддержка AstraLinux 1.5 и Debian
- Версия будет передана на инспекционный контроль. (при купленной первой версии – обновление будет бесплатным)

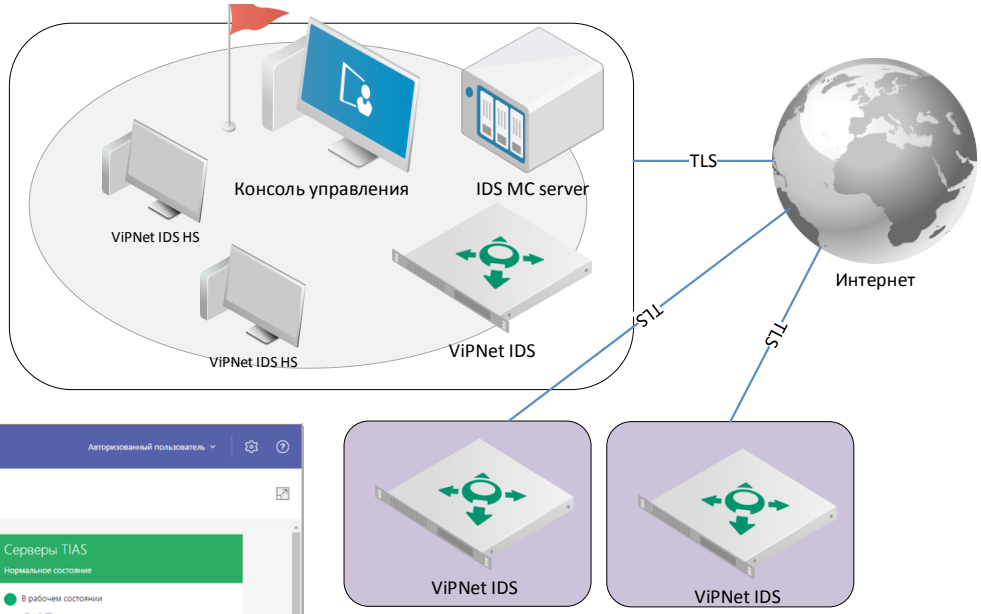
infotecs

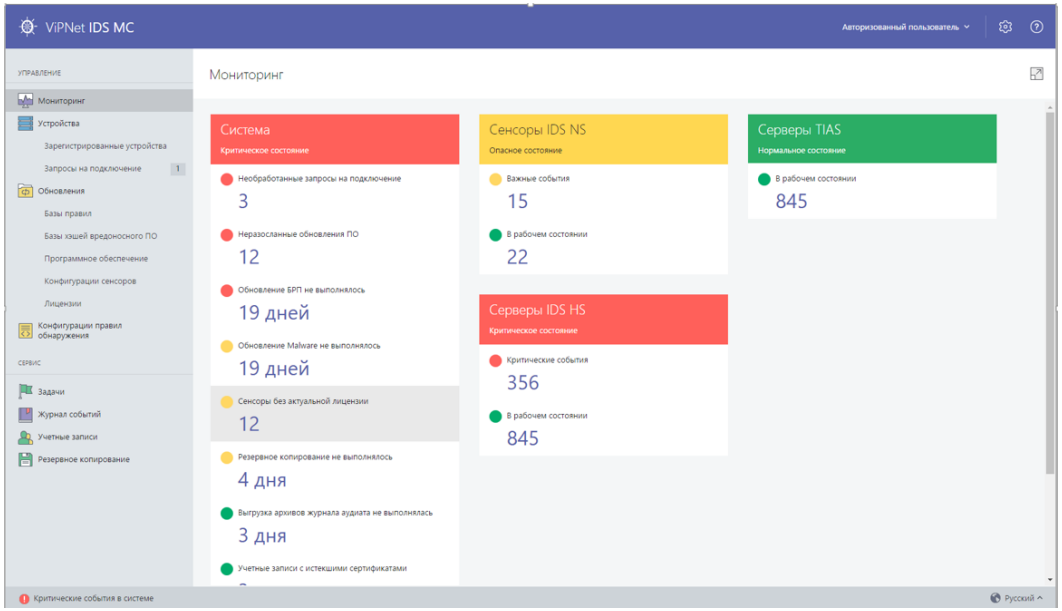
# Комплексное решение компании ИнфоТеКС для обнаружения и устранения угроз и вторжений.

# Интеграция с IDS MC

Единая консоль управления системами обнаружения вторжений:

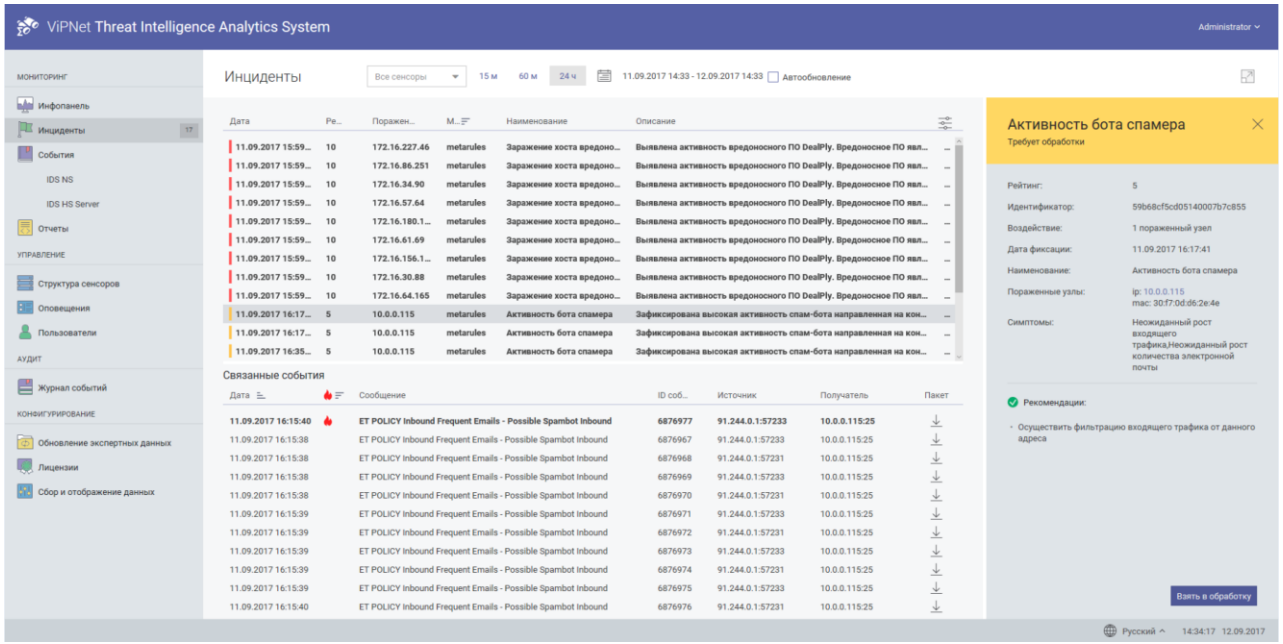
- ViPNet IDS NS
- ViPNet IDS HS



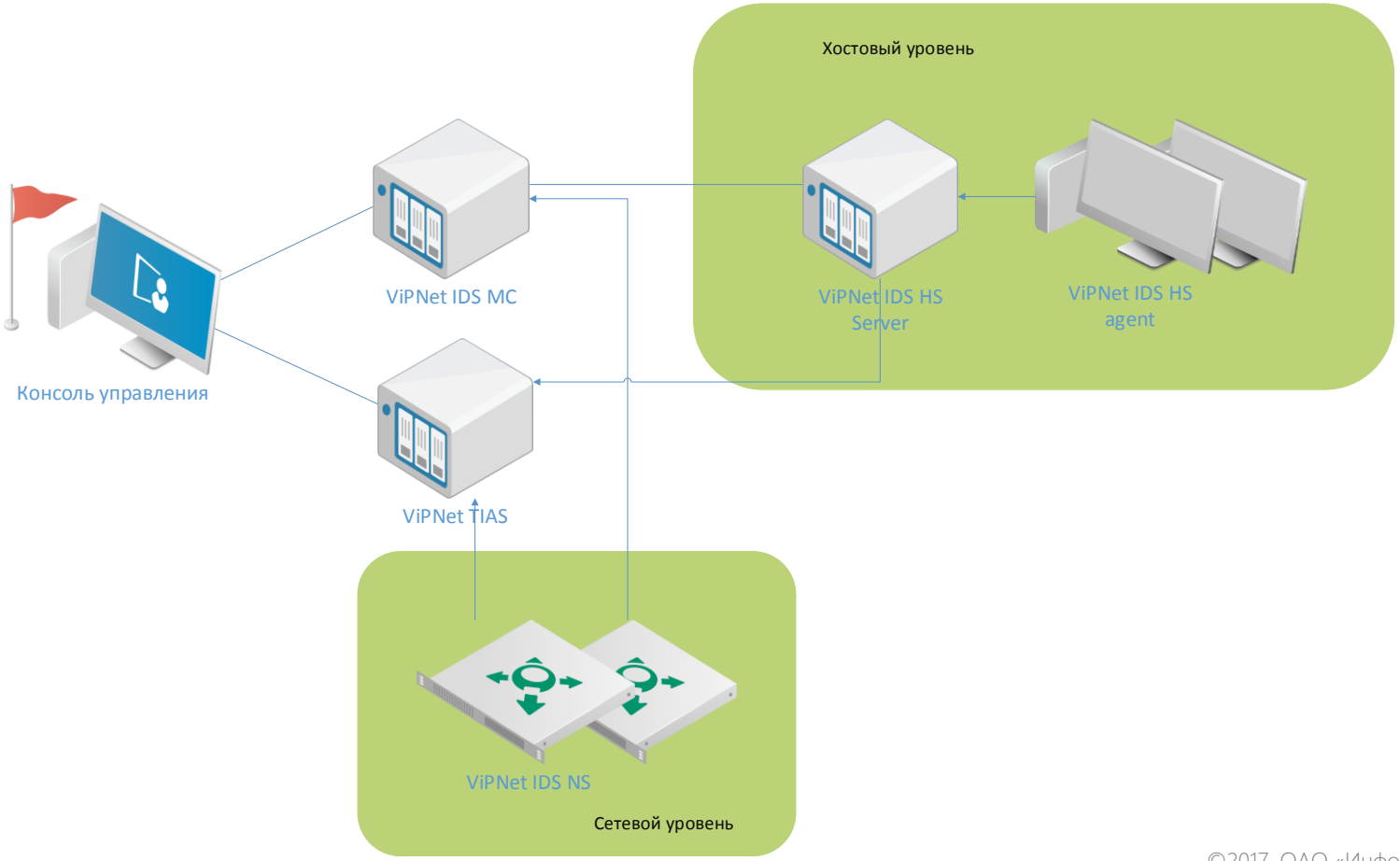



# Интеграция с TIAS

- Возможность передачи событий от IDS HS в TIAS для выявления инцидентов и построения цепочек событий безопасности, которые привели к инциденту



# ITDP:
# Intrusion&Threats – Detection&Prevention




Спасибо!