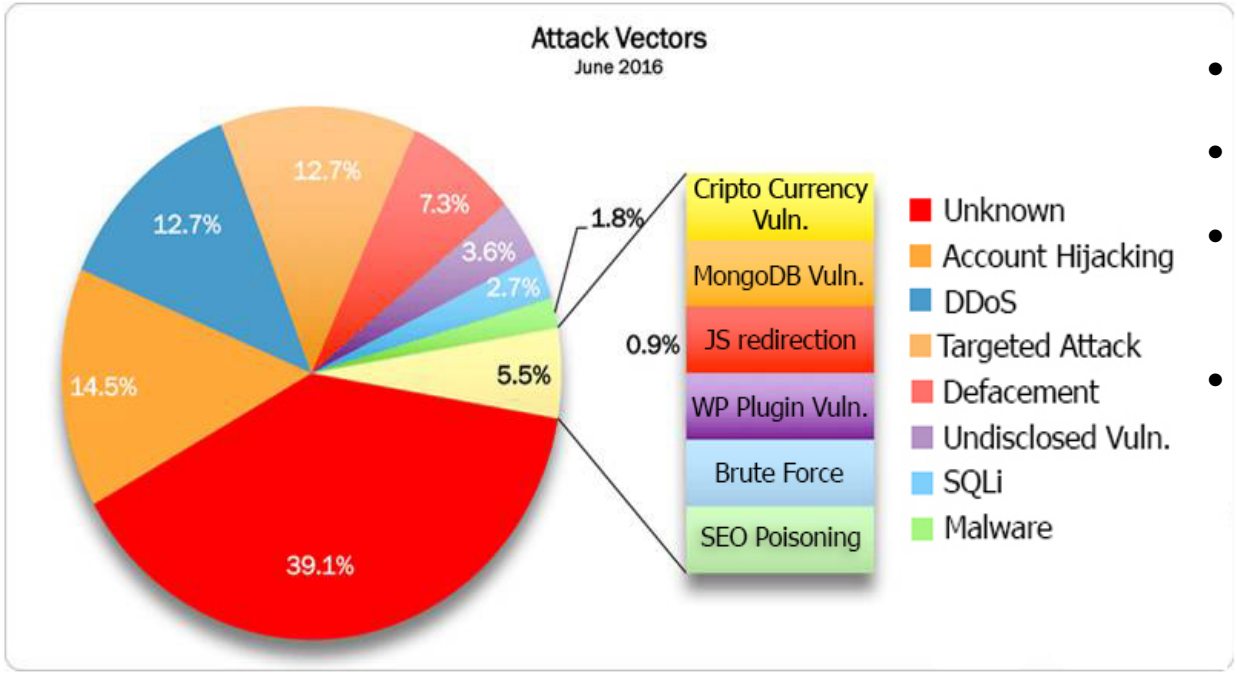
ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

# Доверие к БРП — необходимое условие безопасности КИИ

Владимир Клименко

Генеральный директор ЗАО «Перспективный мониторинг»

# Состояние кибератак в мире



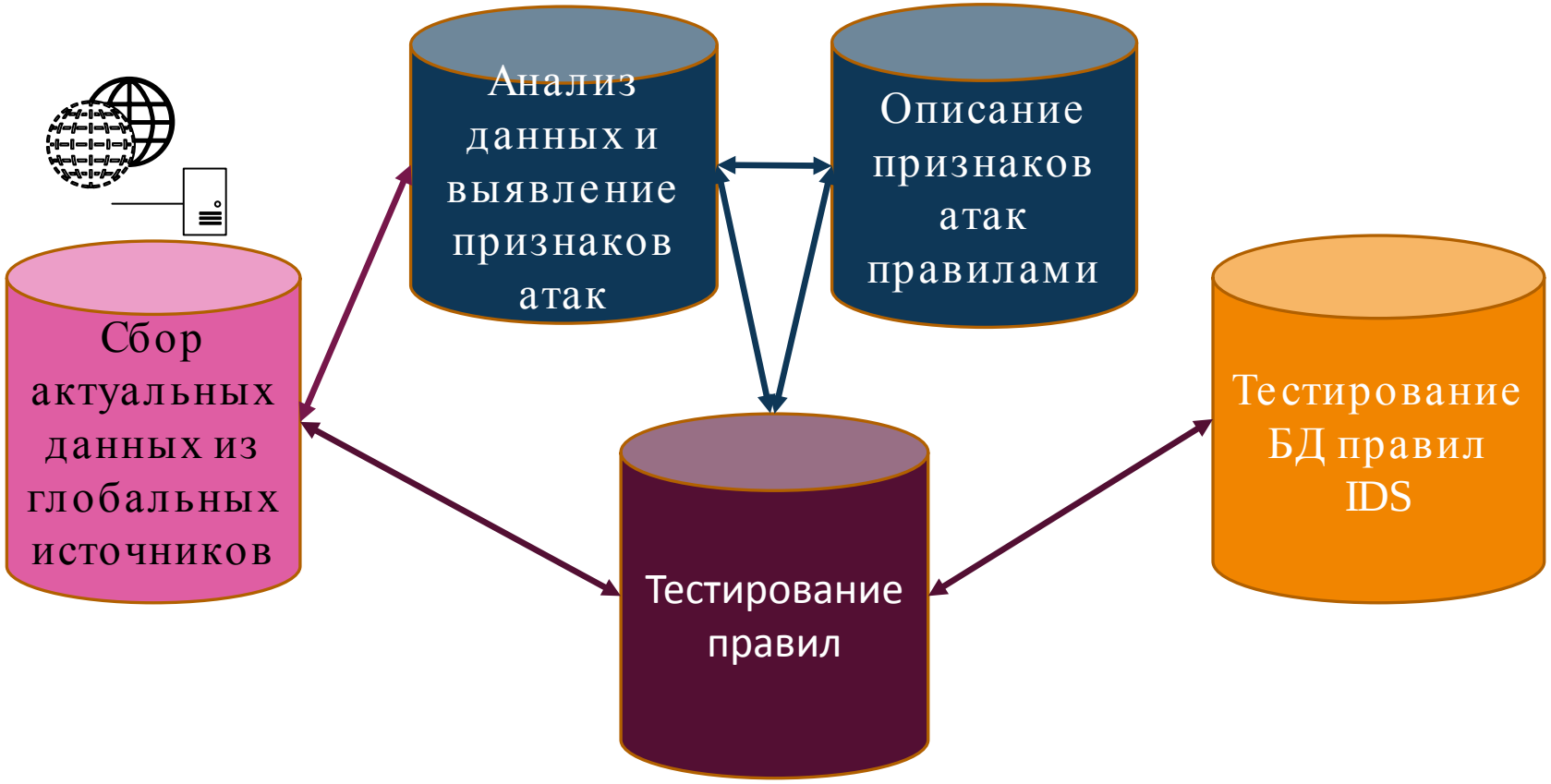

## Итоги 2017 года

- **6,8 млн руб**. в день хищения в России, GiB, 2017
- **531**— атаки на Банки РФ за год, ФинСЕРТ, 2017
- **4,17** млрд руб. — годовой ущерб от кибератак в России, GiB, 2017
- **42%** российских компаний хотя бы один раз за последний год теряли важную информацию из-за взлома или утечек данных, ЛК, 2017

# Способы выявления атак

| Сигнатурный метод | Метод выявления аномалий |
| --- | --- |
| Основан на экспертизе аналитиков | Обнаружение отклонений от пороговых значений |
| Описание атаки последовательностью признаков | Оценка параметров сетевого трафика на основе правил |
| + точность определения атак<br>- выявление только известных атак | + выявление неизвестных атак<br>- большое количество ложных срабатываний |

# Как делают правила IDS



# Поставщики сигнатур

**«Перспективный мониторинг» в составе ГК «ИнфоТеКС», Россия**

AM (платные, в продукте ViPNet IDS)

**SourceFire (с 2013 г. в составе Cisco Systems), США**

VRT community (условно бесплатные) — лицензии GNU GPL 2.0

VRT community (условно бесплатные) — VRT Certified Rules License (от подразделения «Vulnerability Research Team», сейчас «Talos Group»)

**Emerging Threats (с 2014 г. в составе Proofpoint), США**

ET Open (условно бесплатные) — лицензии GNU GPL 2.0, BSD License

ET Pro (платные) — лицензии ET Pro, GNU GPL 2.0, BSD License

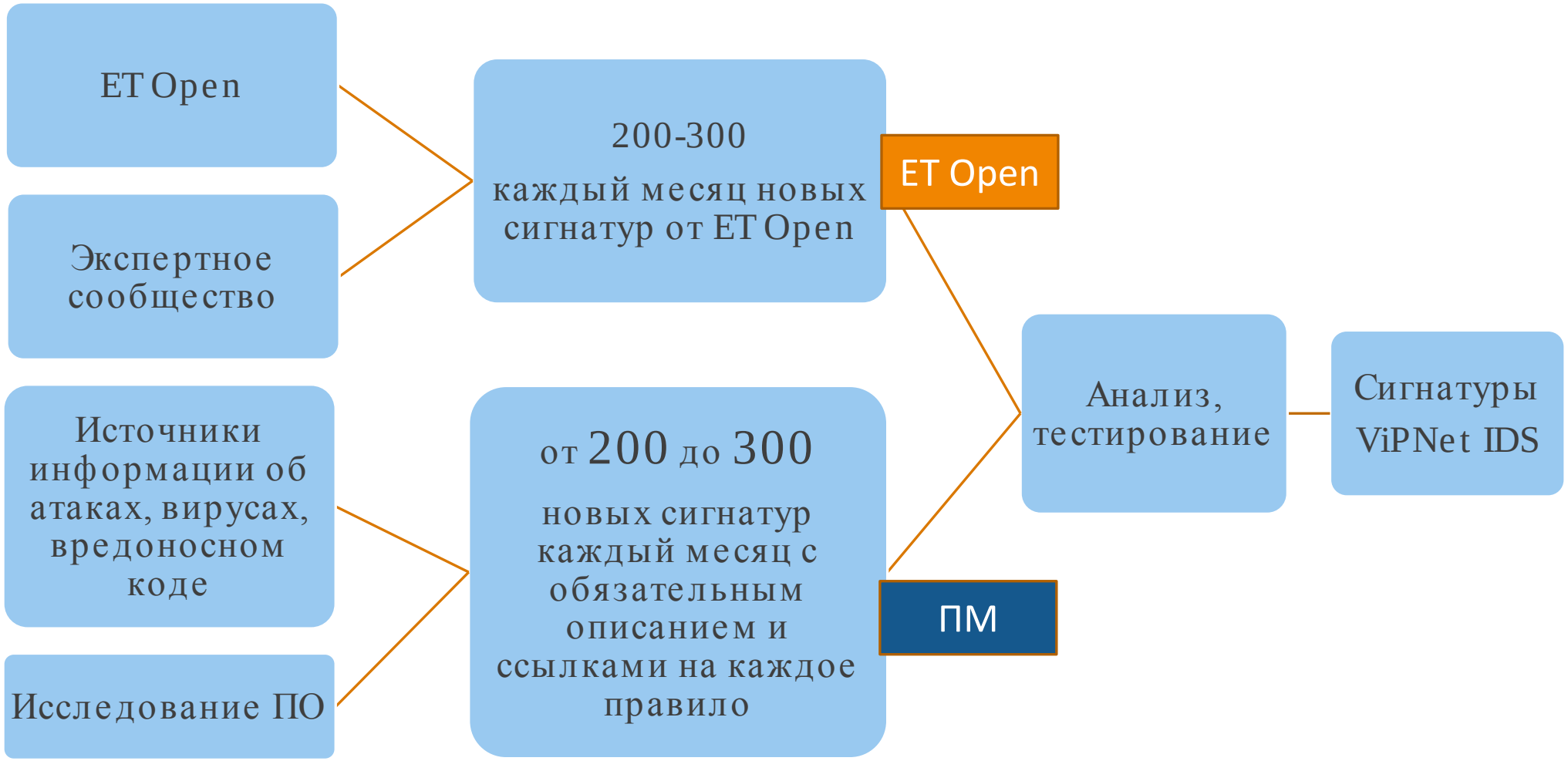
**Idappcom, Великобритания**

Idappcom (платные)

# Риски использования сторонних сигнатур

- Получение сигнатур с ошибками
- Отсутствие или исчезновение сигнатур на конкретные уязвимости
- Отсутствие учёта Российской специфики
- Смена политики лицензирования и/или продаж сигнатур: (смена собственника, поглощение компаний, сотрудничество со спецслужбами, санкции,… )

# Разработка сигнатур



# Российская база — AM Rules

РОССИЙСКАЯ ФЕДЕРАЦИЯ

**СВИДЕТЕЛЬСТВО**

о государственной регистрации базы данных

№ 2016620316

«База данных сигнатурных правил обнаружения атак AM Rules»

Правообладатель: *Закрытое акционерное общество «Перспективный мониторинг» (RU)*

Авторы: *Головенков Евгений Владимирович (RU), Богданов Роман Сергеевич (RU), Минаков Андрей Геннадьевич (RU)*

Заявка № 2015621242
Дата поступления 09 октября 2015 г.
Дата государственной регистрации в Реестре баз данных *03 марта 2016 г.*

*Руководитель Федеральной службы по интеллектуальной собственности*

*Г.П. Ивлиев*

Образец трафика Dridex

Правила AM Rules выявили вредоносный скрипт

AM TROJAN W97M.Downloader VB Obfuscated Script Download

AM POLICY

AM TROJAN

AM TROJAN Possible Dridex EXE

Правила остальных разработчиков

ET POLICY EXE

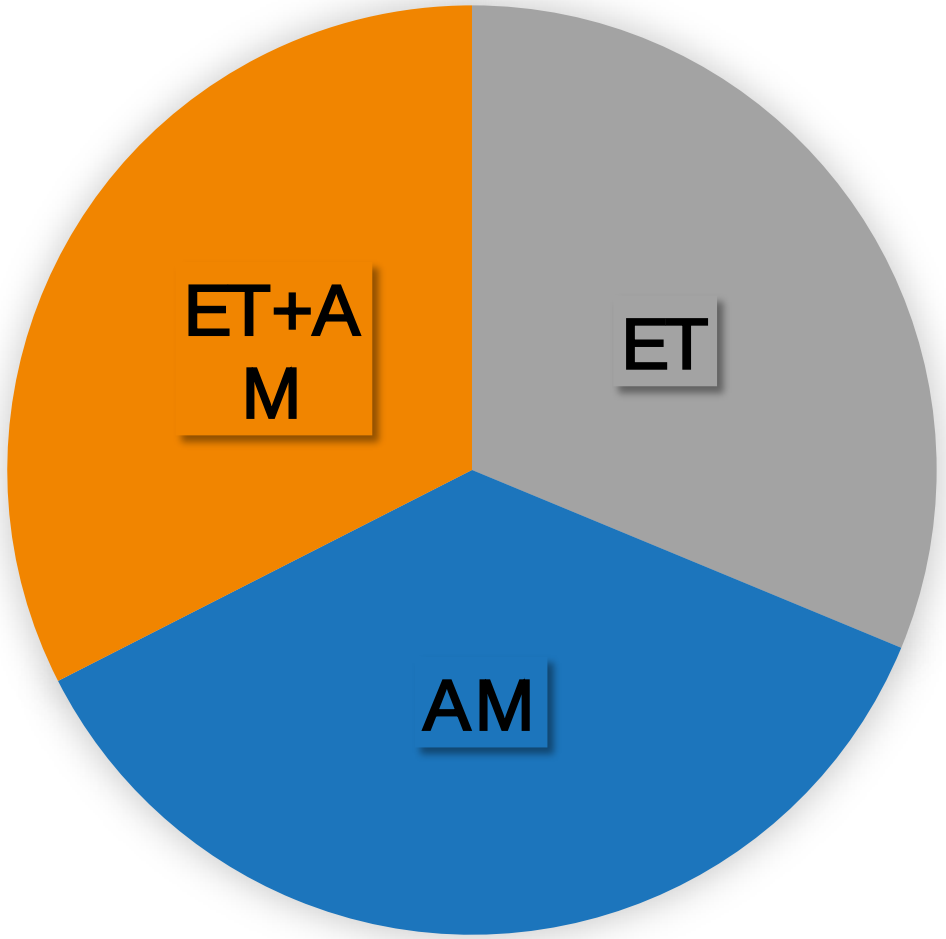
ET INFO SUSPICIOUS

ET TROJAN Gozi Checkin

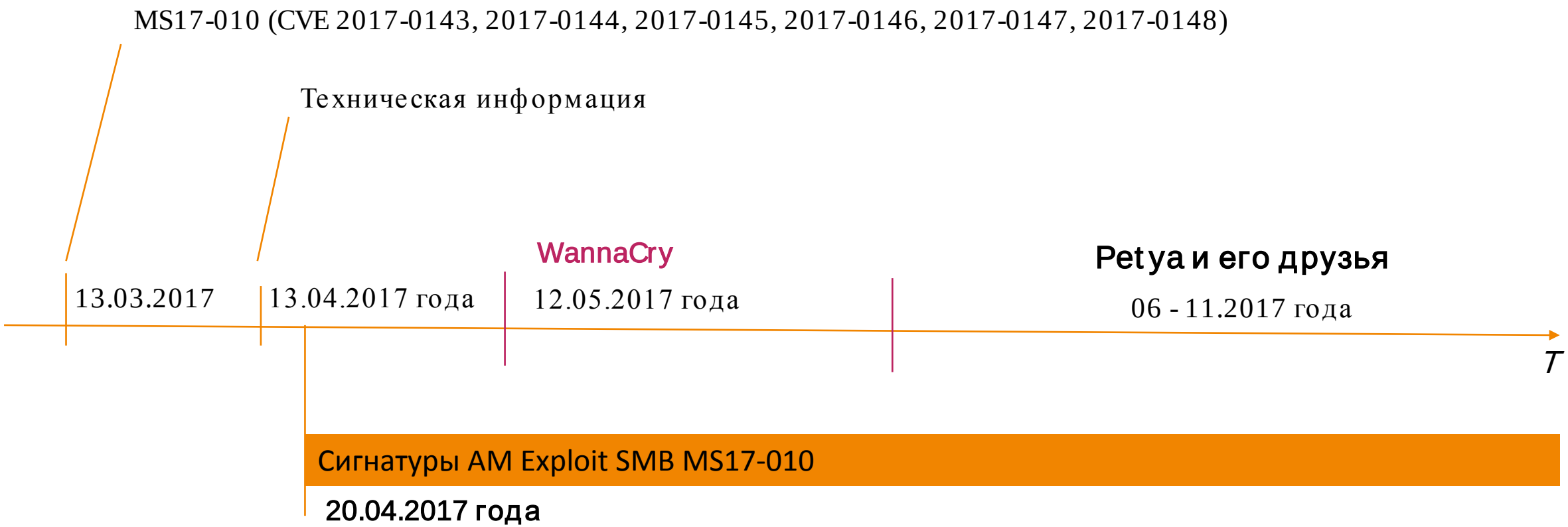
# Преимущества AM Rules

- Проведение тестирования на срабатывание
- Возможность оперативного обновления БРП
- Актуальность
- Учет отечественной специфики
- Описание на двух языках (русский и английский)

# Без AM Rules вы не видите 40% инцидентов



# Применение базы знаний



# Спасибо за внимание!


## Владимир Клименко

Генеральный директор

компании «Перспективный мониторинг»

amonitoring.ru