Эшелон
комплексная безопасность

МОНИТОРИНГ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ В РАМКАХ СМИБ. ПРИМЕНЕНИЕ SIEM-СИСТЕМЫ «КОМРАД»

Александр Дорофеев, CISSP, CISA, CISM
Директор по развитию

СОДЕРЖАНИЕ

PDCA И СМИБ


Постоянное улучшение СМИБ
Заинтере-сованные стороны
Требования к СМИБ
Создание (PLAN)
Внедрение и управление (DO)
Мониторинг и анализ (CHECK)
Обеспечение и улучшение (ACT)
Заинтере-сованные стороны
Управляемая СМИБ

СТРУКТУРА ISO 27001

0 Введение

1 Область применения

2 Нормативные ссылки

3 Термины и определения

PLAN

- 4 Контекст организации
- 5 Лидерство
- 6 Планирование
- 7 Поддержка

DO

- 8 Операционная деятельность

CHECK

- 9 Оценка производительности

ACT

- 10 Улучшение

СТРУКТУРА ISO 27001 ПОДРОБНЕЕ

PLAN

4 Контекст организации

- Понятие контекста.
- Ожидания заинтересованных сторон.
- Область распространения СМИБ.

5 Лидерство

- Приверженность руководства.
- Политика ИБ.
- Роли, ответственность и полномочия.

6 Планирование

- Оценка риска и возможностей.
- Цели ИБ.

7 Поддержка

- Ресурсы.
- Компетенция.
- Осведомленность.
- Коммуникации.
- Документируемая информация.

DO

8 Операционная деятельность

- Планирование и контроль операций.
- Оценка рисков.
- Обработка рисков.

CHECK

9 Производительность и оценка

- Мониторинг, измерение, анализ и оценка.
- Внутренний аудит.
- Анализ со стороны руководства.

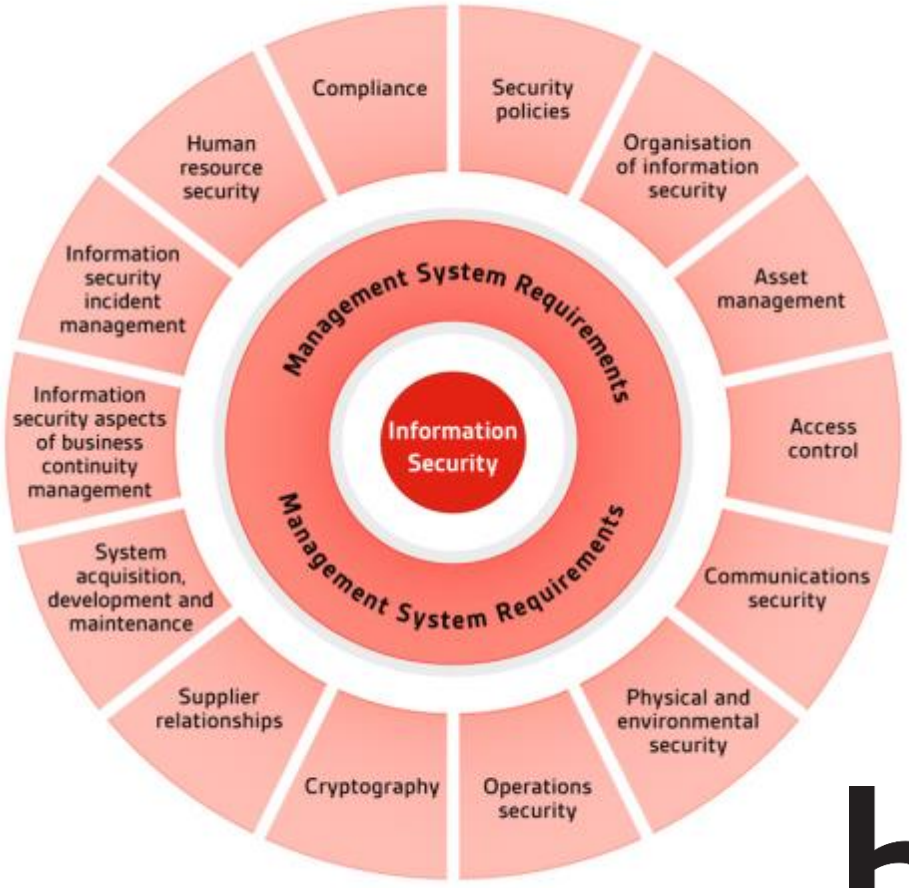
ACT

10 Улучшения

- Несоответствия и корректирующие действия.
- Постоянное улучшение.

ПРИЛОЖЕНИЕ А

- 14 доменов
- 114 средств управления



УПРАВЛЕНИЕ ИНЦИДЕНТАМИ ПО ISO 27001

A.16.1 Management of information security incidents and improvements

- A.16.1.1 Responsibilities and procedures
- A.16.1.2 Reporting information security events
- A.16.1.3 Reporting information security weakness
- A.16.1.4 Assessment of and decision on information security events
- A.16.1.5 Response to information security incidents
- A.16.1.6 Learning from information security incidents
- A.16.1.7 Collection of evidence

МОНИТОРИНГ СОБЫТИЙ ПО ISO 27001

A.12.4 Logging and monitoring

- A.12.4.1 Event logging
- A.12.4.2 Protection of log information
- A.12.4.3 Administrator and operator logs

Реализация требований мер ISO 27001 с помощью SIEM-системы «КОМРАД»

СОВРЕМЕННАЯ АТАКА = СПЕЦОПЕРАЦИЯ

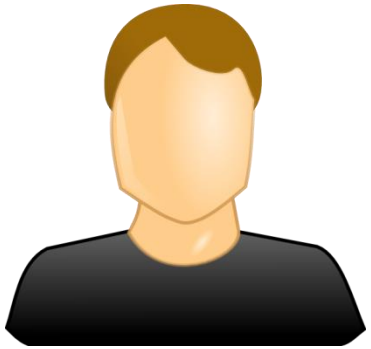
Как своевременно реагировать на таргетированные атаки?

НЕОБХОДИМО ОТСЛЕЖИВАТЬ МАССУ ПРИЗНАКОВ НАРУШЕНИЯ ИБ

Аутентификация: как успешная, так и неуспешная

Срабатывания антивирусного ПО

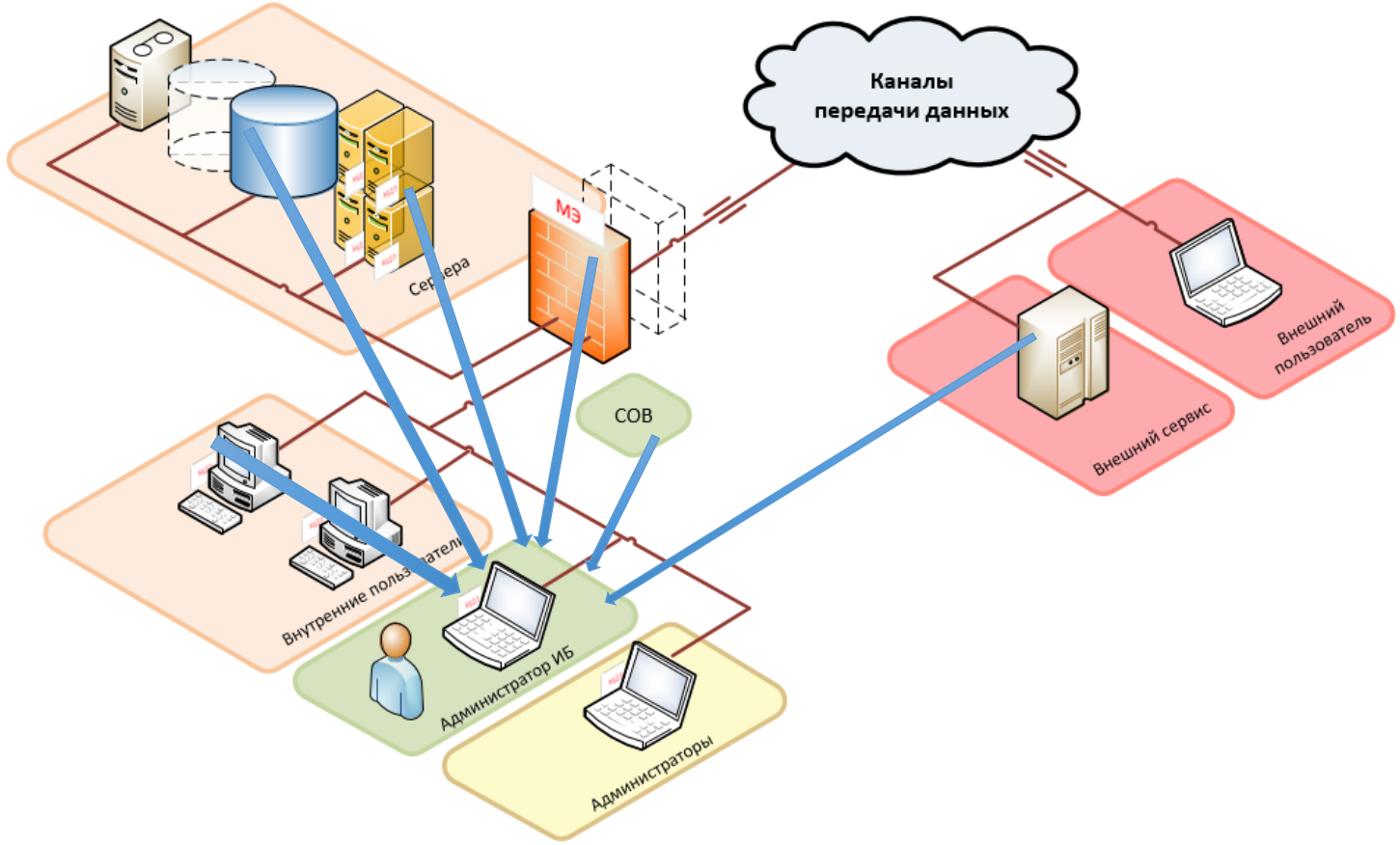
Подозрительные запросы к СУБД



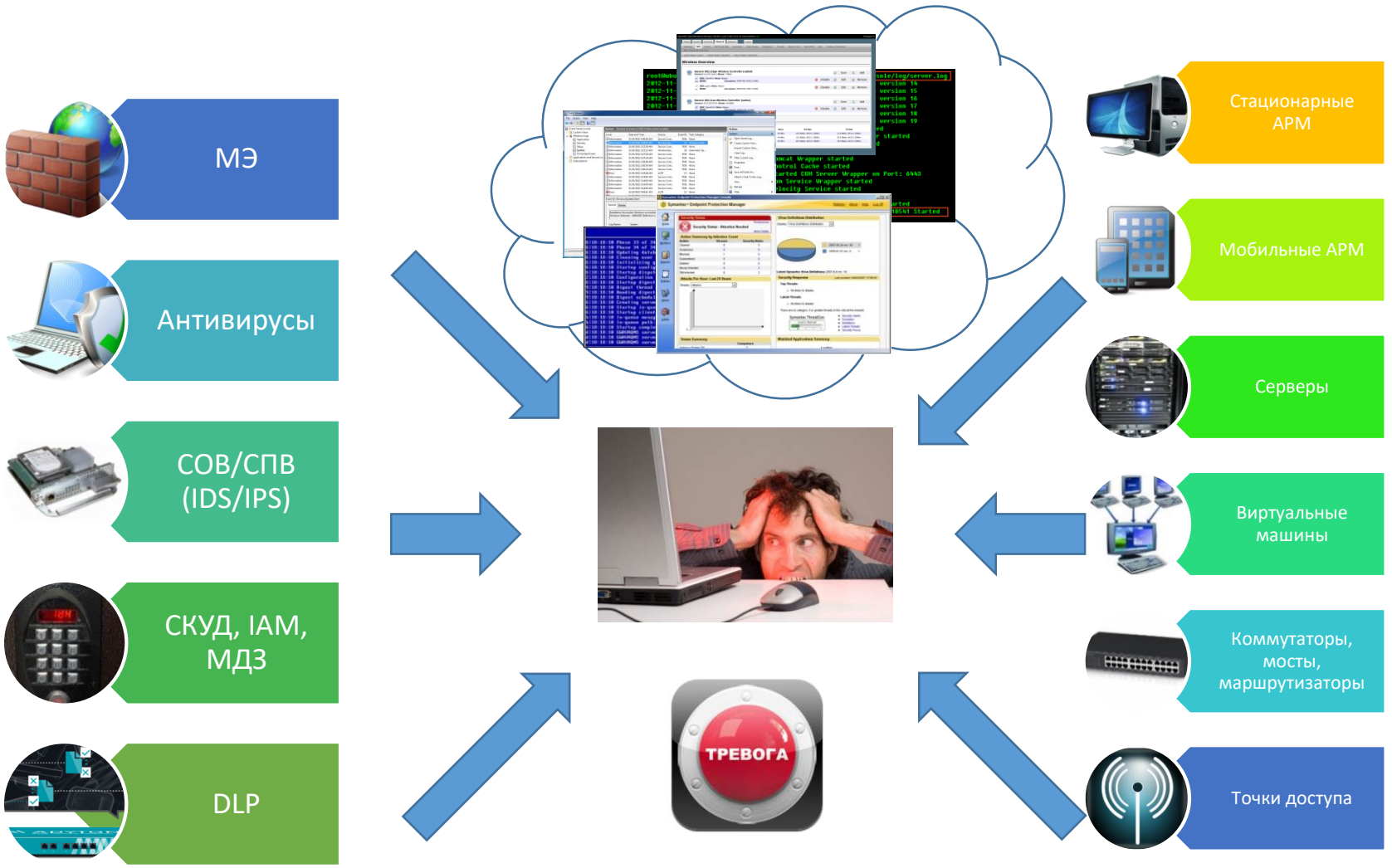
Нетипичное поведение пользователя в ОС

и т.д. и т.п.

ДЛЯ ЭТОГО НАДО ОСУЩЕСТВЛЯТЬ МОНИТОРИНГ ВСЕЙ ИНФРАСТРУКТУРЫ



РУЧНОЙ СБОР МОЖЕТ БЫТЬ ПРОБЛЕМАТИЧНЫМ



КОМРАД

гибкая и производительная система централизованного управления событиями информационной безопасности, совместимая с отечественными средствами защиты информации.

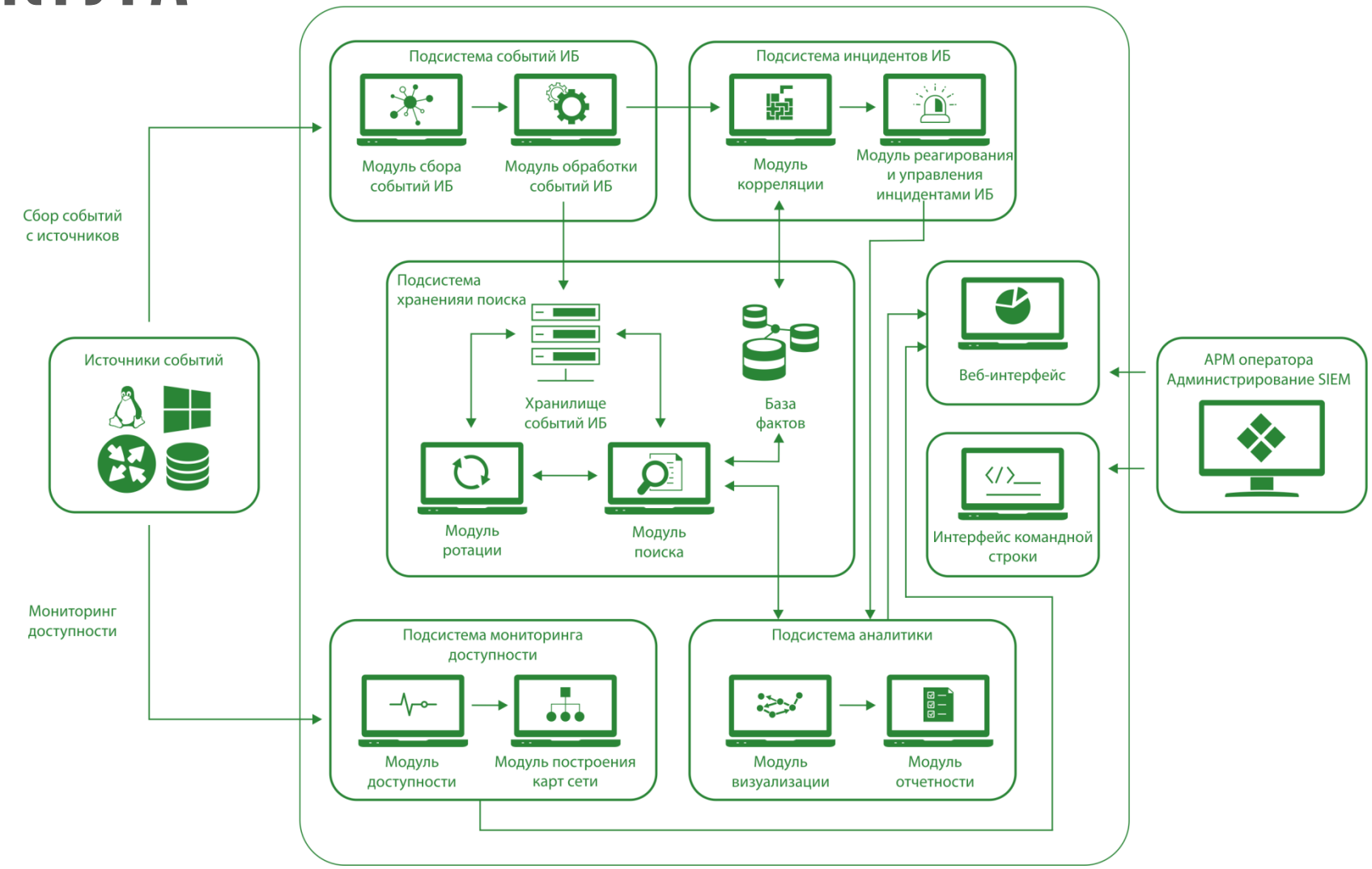
Сертификаты: ФСТЭК России №3498 Минобороны России №2315

ПРИНЦИП РАБОТЫ SIEM-СИСТЕМЫ

Оповещение
и учёт инцидентов

Аналитика

АРХИТЕКТУРА



КОМРАД: ОТЛИЧИТЕЛЬНЫЕ ВОЗМОЖНОСТИ

производительность:
до 20 000 EPS

универсальный
адаптер для любого
источника событий

широкий спектр
поддерживаемых
отечественных СЗИ

удобный
пользовательский
интерфейс

визуальный анализ
данных

оповещение об инциденте
любым способом: email, SMS…

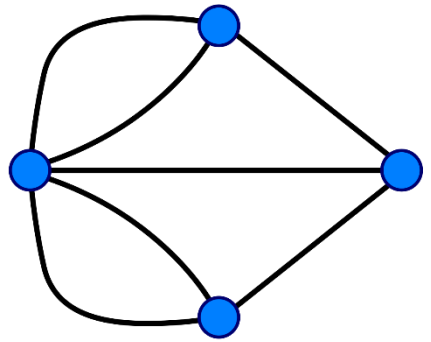
ПОДДЕРЖКА ОТЕЧЕСТВЕННЫХ СЗИ

- МЭ и СОВ «Рубикон»/«Рубикон-К»
- Сканер-ВС
- Astra Linux
- Kaspersky Security Center
- Форпост
- SecretNet 3.5-3.7 (сервер управления)
- БлокХост-Сеть
- vGate R2
- ViPNet Coordinator HW2000
- VIPNet IDS
- АССОИ «Матрица»
- …

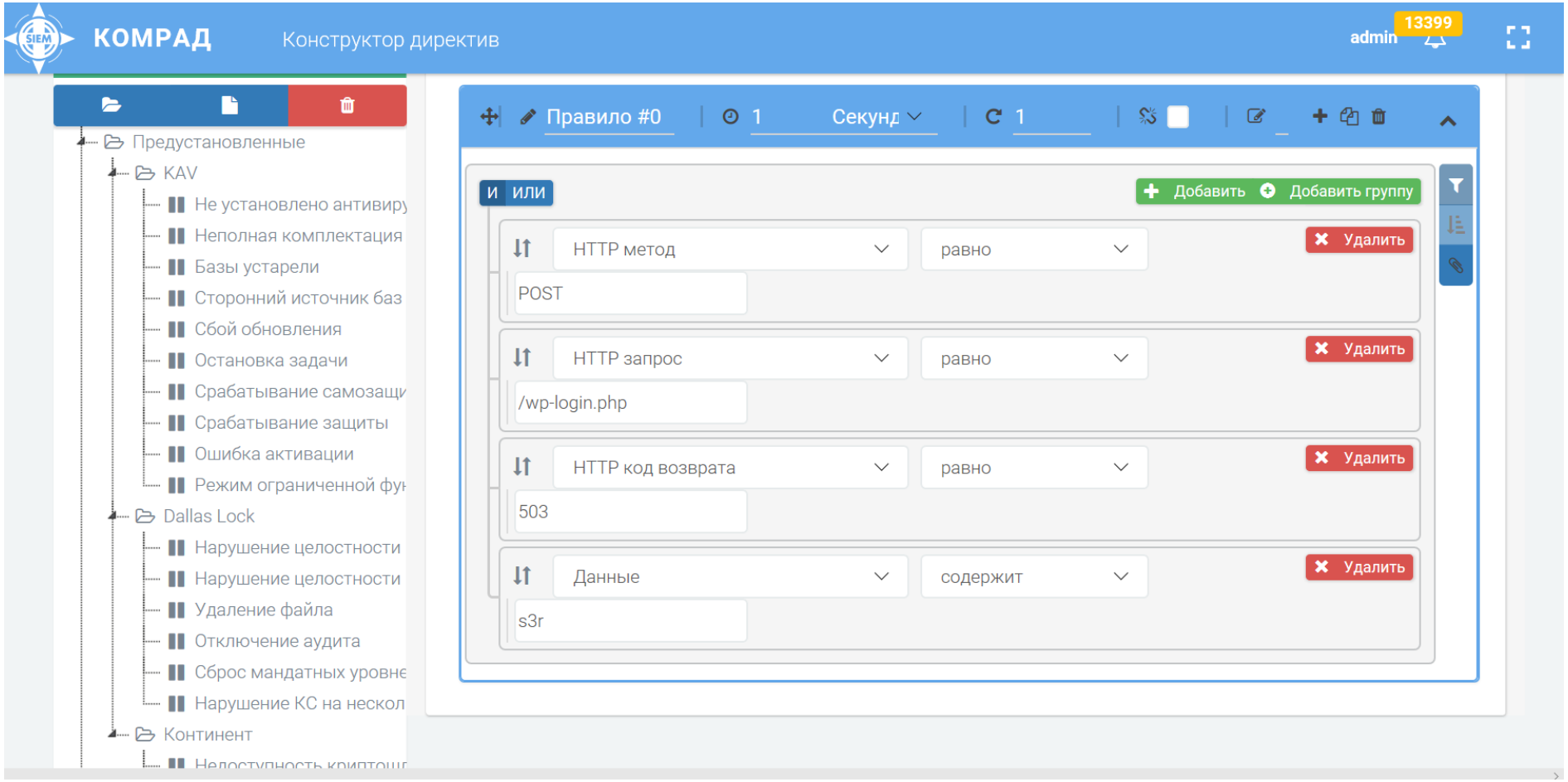
МЕТОДЫ КОРРЕЛЯЦИИ, ИСПОЛЬЗУЕМЫЕ В SIEM КОМРАД

- **Основанный на правилах (rule based)** — взаимосвязи между событиями определяются аналитиками в заранее заданных специфических правилах.

- **Основанный на графах (graph based)** — поиск зависимостей между системными компонентами в представлении ввиде графа.



СОЗДАНИЕ НОВОГО ПРАВИЛА КОРРЕЛЯЦИИ



ПОЛЯ ДЛЯ ФОРМИРОВАНИЯ ПРАВИЛ (1)

ID плагина
SID плагина
Протокол
IP источника
IP назначения
Порт источника
Порт назначения
Имя источника
Имя назначения
MAC источника
MAC назначения
Имя файла
Имя пользователя

АССОИ событие

Имя шлюза

Тип шлюза

Описание команды

Имя запроса

Имя сетевого интерфейса

Роль пользователя

Название фильтра

Направление трафика

Адрес шлюза

CEF значимость

CEF вендор

CEF продукт

CEF версия продукта

CEF ID события

CEF описание

CEF сообщение

WMI имя компьютера

WMI журнал

WMI сообщение

WMI тип (строка)

WMI категория (строка)

WMI имя источника

WMI тип события

WMI номер записи

WMI идентификатор

WMI категория

WMI код события

WMI причина ошибки

Домашняя директория

Команда

Действие

Терминал

Интерпретатор

ID пользователя

ID группы

Имя группы

Сообщение

Категория события

ПОЛЯ ДЛЯ ФОРМИРОВАНИЯ ПРАВИЛ (2)

Сервис
Уровень тревоги
ID правила
Файл журнала
Класс COB
Группа COB
Номер CVE
Адрес ссылки
Имя тэга
Тип атаки
Имя узла
CSSID шлюза
WMI идентификатор безопасности

Событие
KAV сообщение
Результат операции
Имя шлюза
ID группы правил
Длина пакета
Приоритет правила
Классификация
Приоритет
Причина
Время отклика
Статус запроса
Код иерархии

Тип MIME
Байт передано
Комментарий
Правило
Имя компьютера
Имя сервера
Параметр
Неверный пароль
ID сигнатуры
Версия IP
Доступ
Отправлено
Получено

Информация
Длина
Объект доступа
Права
Принтер
Документ
Количество копий
Количество страниц
Порт
Тип атаки

ПРАВИЛА КОРРЕЛЯЦИИ SIEM КОМРАД «ИЗ КОРОБКИ» (1)

1) Xmlrpc, обнаружение PingBack-атаки.
2) Обнаружение межсайтового скриптинга.
3) Обнаружение мутированных входных данных.
4) Обнаружение Sql-выражений из пользовательского ввода.
5) Обнаружение неавторизованного Remote Code Execution-Wordpress.
6) Обнаружение уязвимости Local file include.
7) Обнаружение неавторизованного Remote Code Execution-Ping.
8) Обнаружение сканера уязвимостей Openvas.
9) Обнаружение сканера уязвимостей w3af.
10) Обнаружение сканера уязвимостей Acunetix.
11) Обнаружение исходящей активности Tor-нодов.
12) Обнаружение входящей активности Tor-нодов.
13) Обнаружение неавторизованного Content Injection-Wordpress.
14) Обнаружение исходящей активности на файлобменник.

ПРАВИЛА КОРРЕЛЯЦИИ SIEM КОМРАД «ИЗ КОРОБКИ» (2)

15) Обнаружение исходящей активности к C&C серверам.
16) Обнаружение исходящей активности к IRC каналам.
17) Обнаружение использования анонимайзеров.
18) Обнаружение входящей активности Mirai botnet.
19) Обнаружение брутфорс атаки на wordpress.
20) Обнаружение входящей активности crawler-ботов.
21) Контроль учетных записей-эскалация привилегий, создание/удаление, смена пароля.
22) Обнаружение брутфорс атаки на Rdp.
23) Обнаружения уязвимости Rdp-MaxChannelids.
24) Обнаружение исходящей активности к соц.сетям(vk, twitter, facebook).
25) Обнаружение исходящей активности Skype.
26) Обнаружение входящей активности Tcp-Break, таких клиентов telnet, nc
27) Обнаружение исходящей активности Remote Access.
28) Обнаружение нового пользователя в OpenvVpn.
29) Обнаружение несоответствия сертификата в OpenVpn.
30) Обнаружение параллельного соединения с двух разных IP OpenVpn.
31) Контроль криптошлюза и обновления ключей Континента.
32) Нарушение целостности, удаление, отключение, контроль мандатных уровней DallasLock.
33) Полный контроль над KAV.

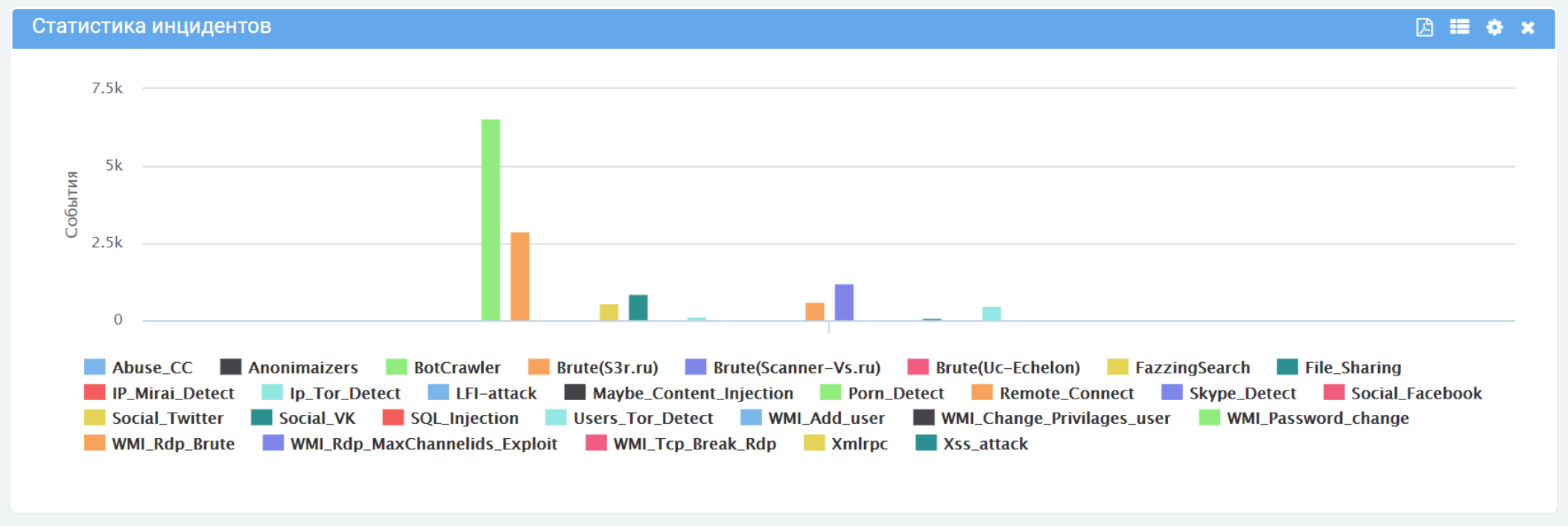
НАСТРОЙКА ПРАВИЛ КОРРЕЛЯЦИИ

Включаем сбор всего, что можем собрать с помощью SIEM-системы, и начинаем отфильтровывать лишнее.

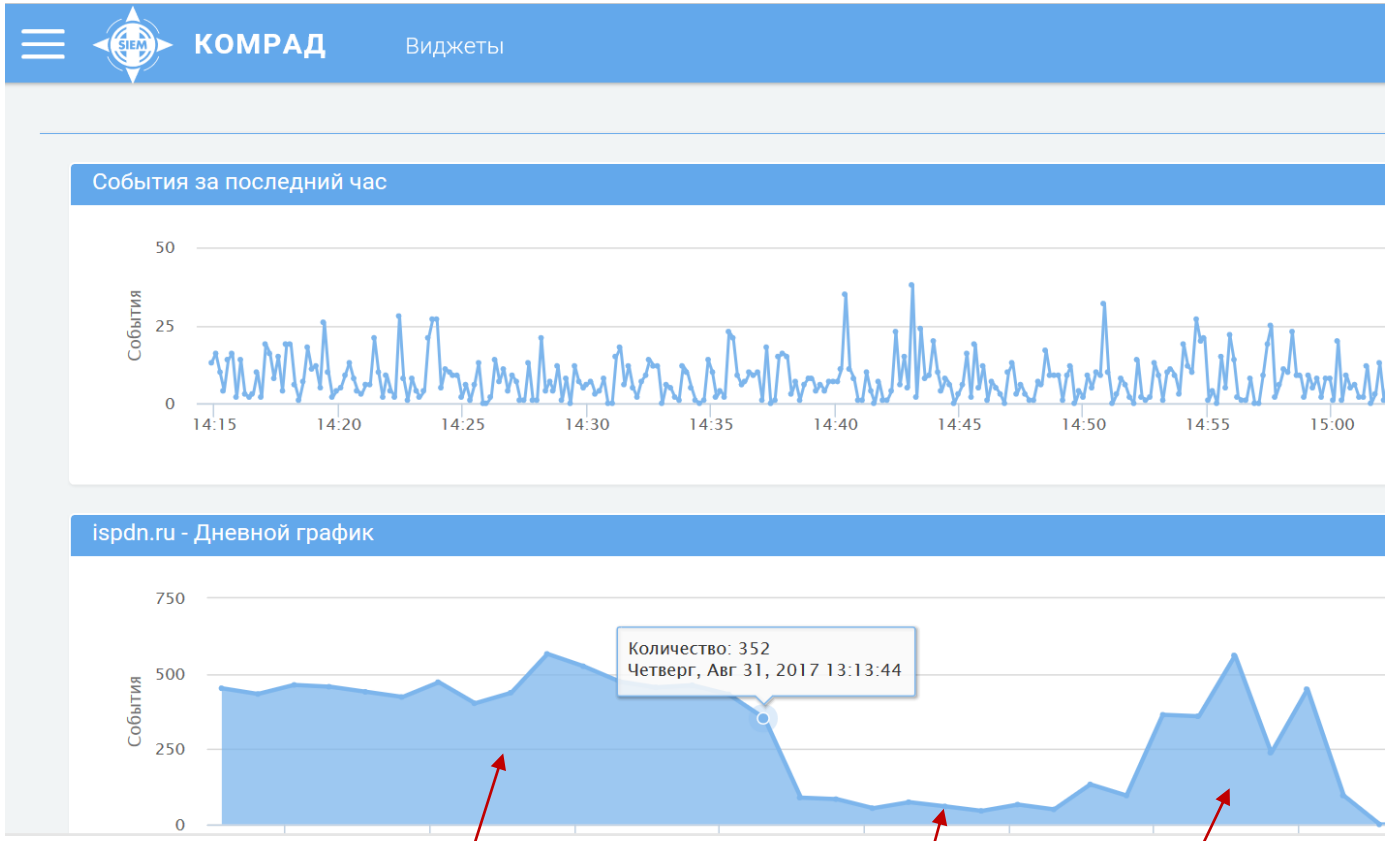
rule of thumb

ПРАКТИКА ПРИМЕНЕНИЯ SIEM-КОМРАД В ESOC

ВСЕ ИНЦИДЕНТЫ



АТАКИ БОТОВ НА ISPDN.RU

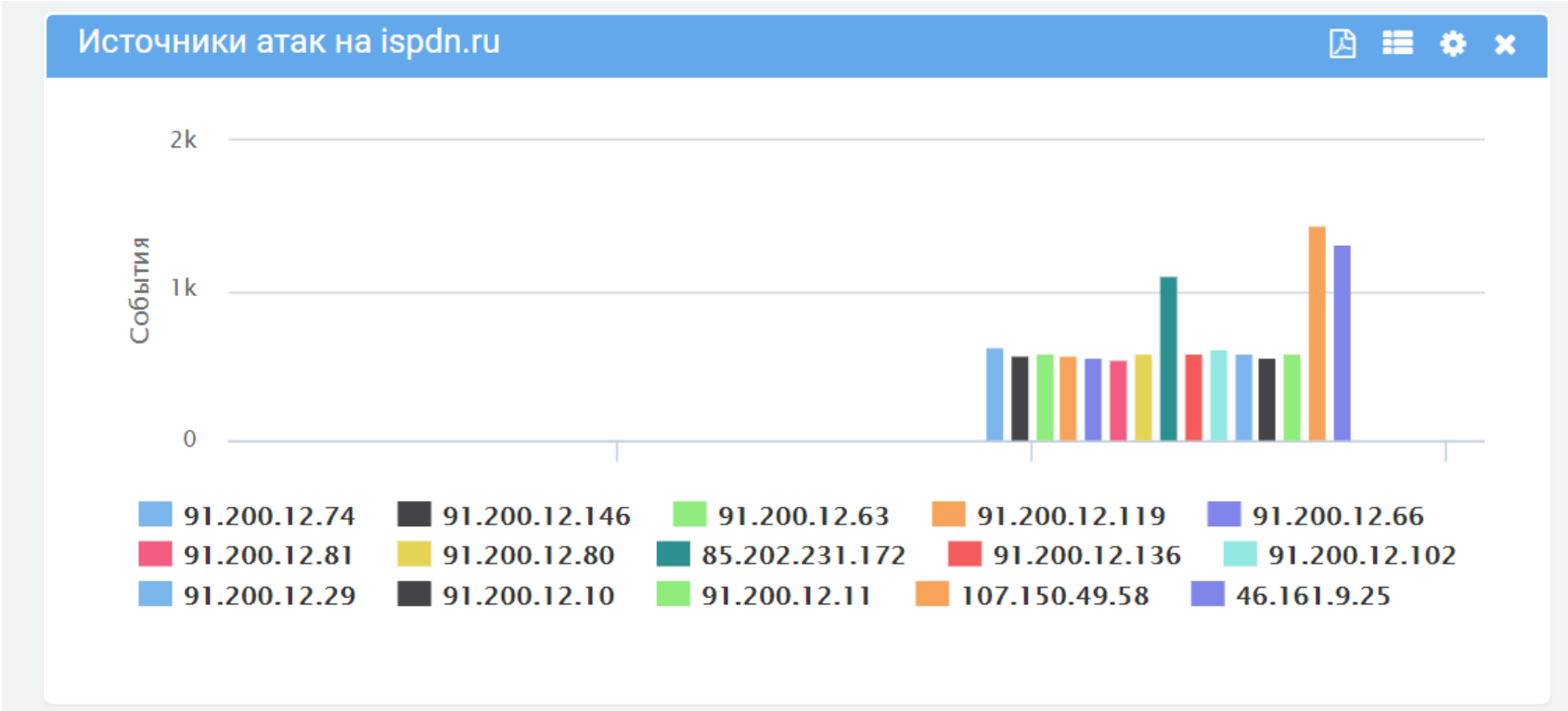


Атака

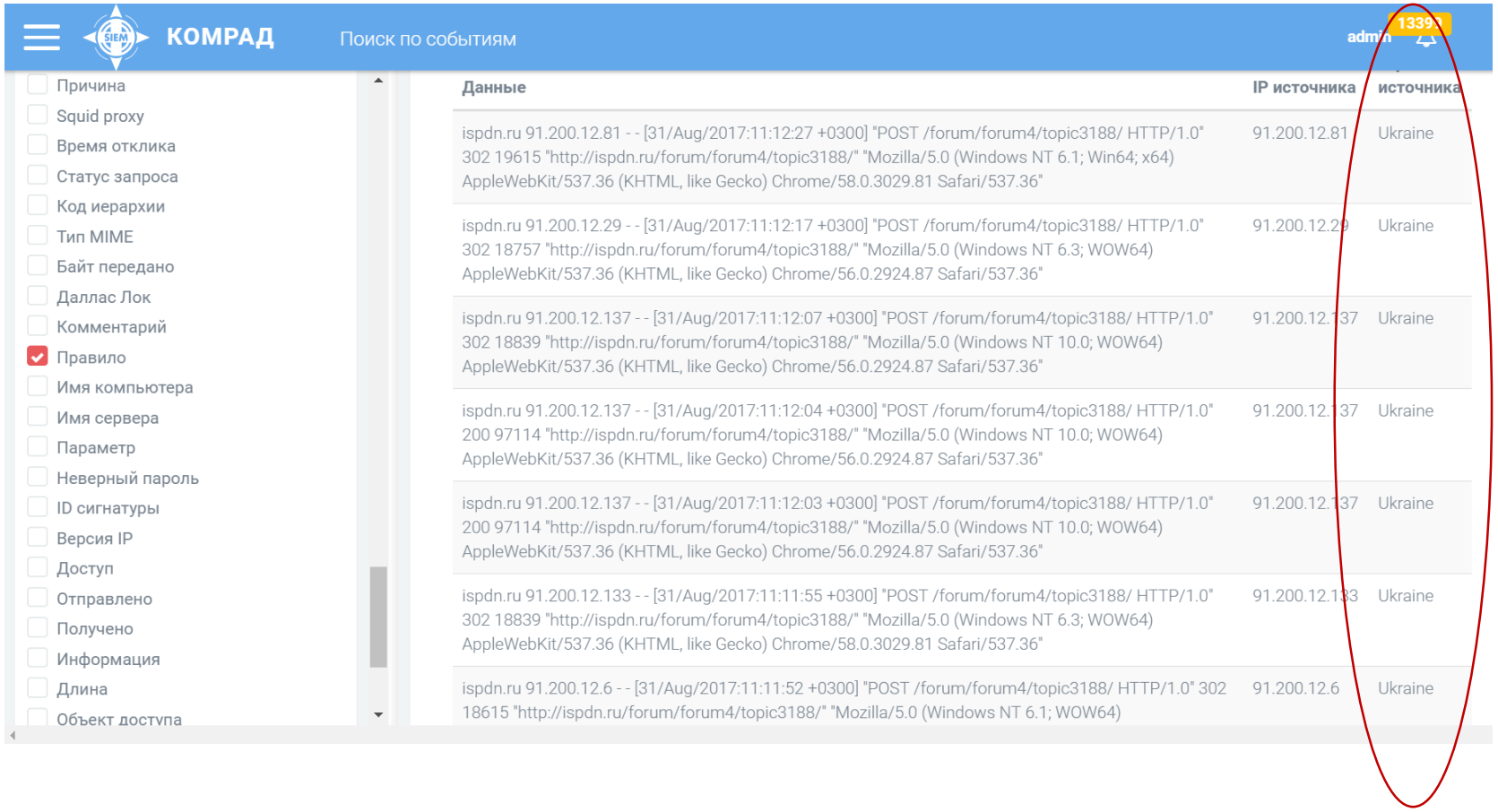
Блокировка ботов

Прорвался с нового адреса

ИСТОЧНИКИ АТАК: СОТНИ ЗАПРОСОВ В ДЕНЬ



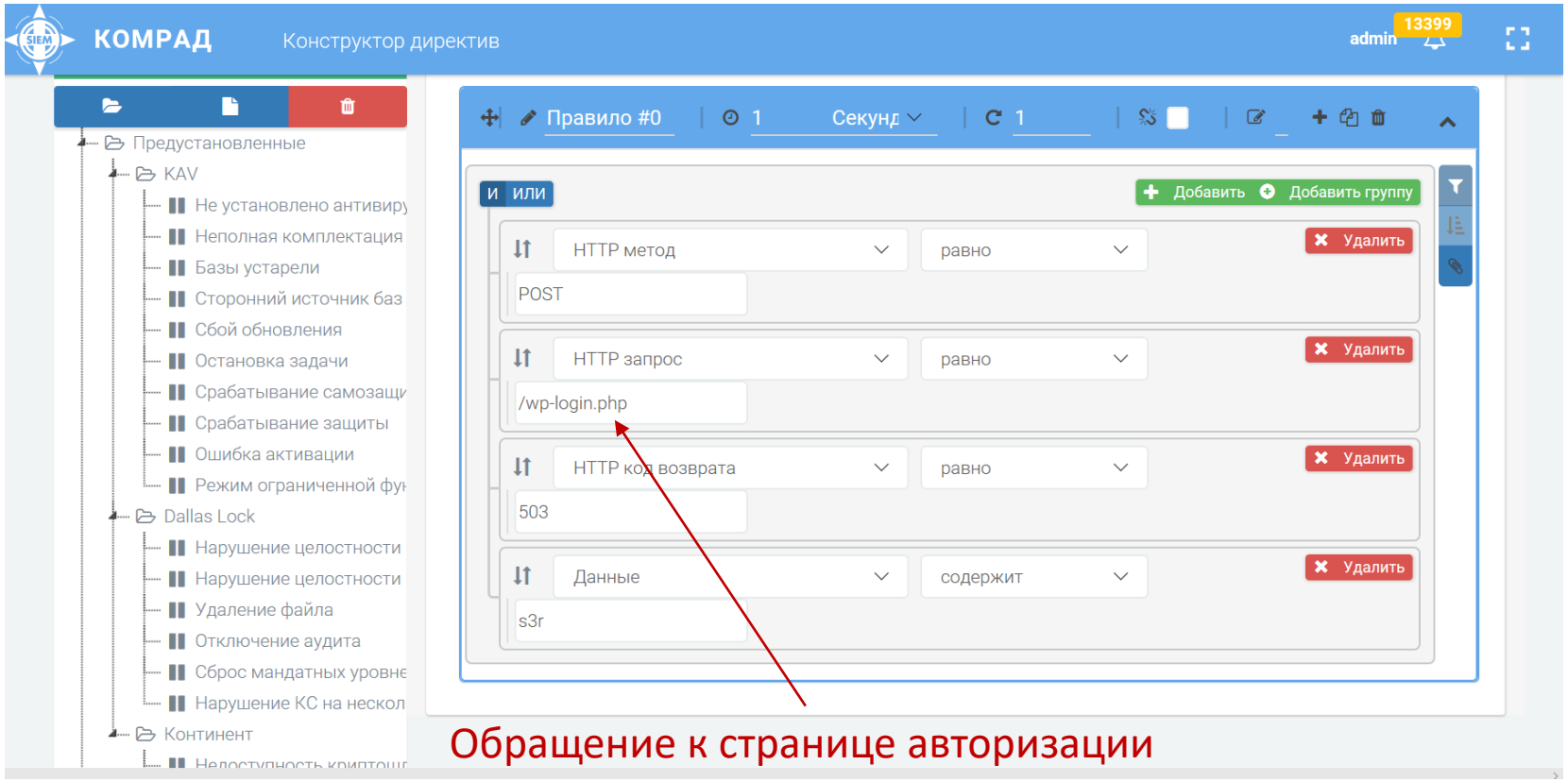
ГОСТИ ИЗ УКРАИНЫ



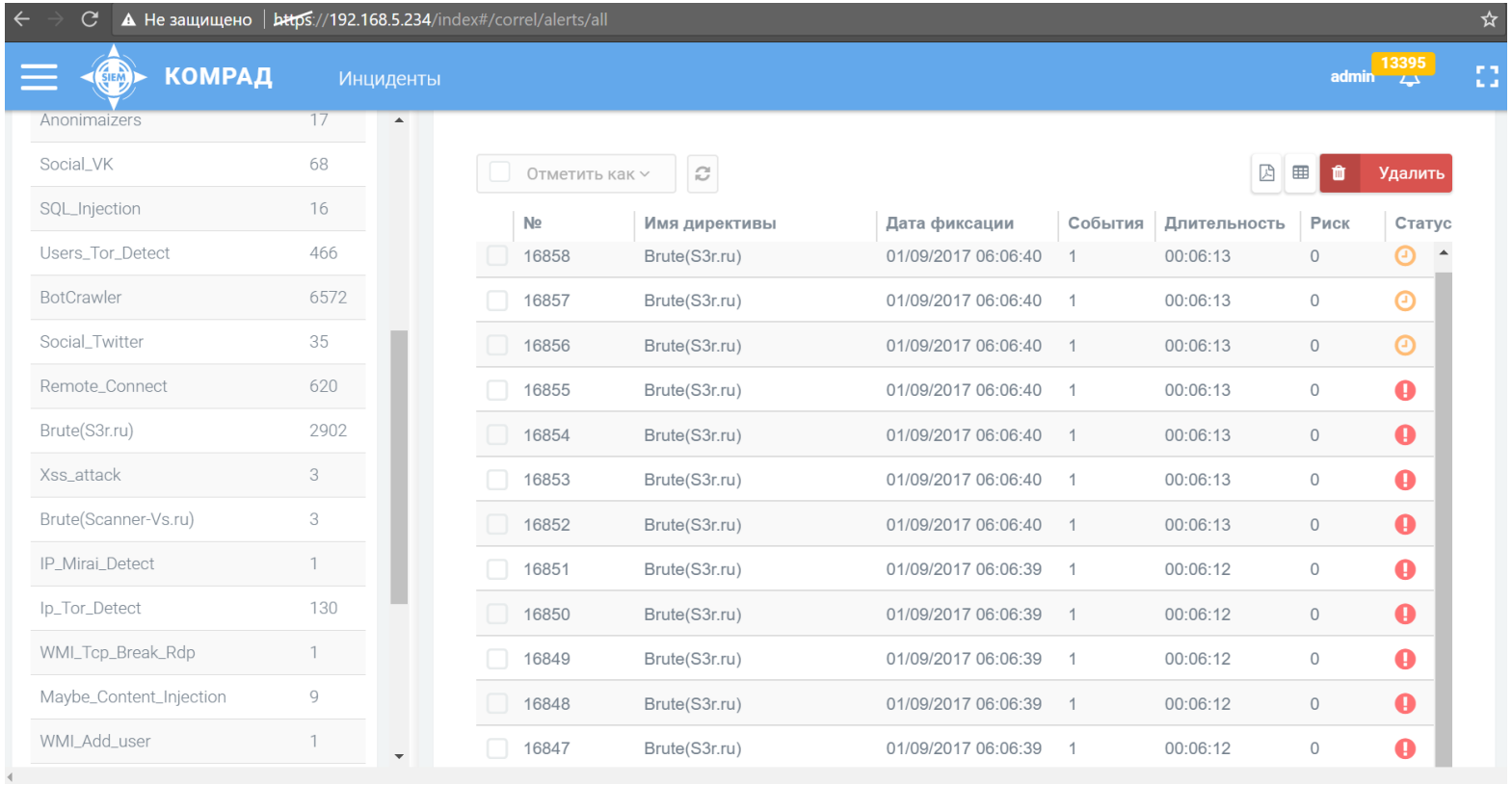
НАШ ОТВЕТ БОТАМ: БЛОКИРОВКА ГОСТЕЙ

```
 GNU nano 2.2.6                                    File: ispdn.ru/public_html/.htaccess

Options -Indexes
ErrorDocument 404 /404.php

#php_flag session.use_trans_sid off
php_value display_errors 0
#php_value allow_url_fopen 0

php_value max_execution_time 150
php_value memory_limit 256M
php_value upload_max_filesize 700M
php_value post_max_size 700M
php_value magic_quotes_gpc off


<IfModule mod_rewrite.c>
#  Options +FollowSymLinks
  RewriteEngine On
  RewriteCond %{REQUEST_FILENAME} !-f
  RewriteCond %{REQUEST_FILENAME} !-l
  RewriteCond %{REQUEST_FILENAME} !-d
  RewriteCond %{REQUEST_FILENAME} !/bitrix/urlrewrite.php$
  RewriteRule ^(.*)$ /bitrix/urlrewrite.php [L]
</IfModule>
AddDefaultCharset utf-8
AddType 'text/html; charset=utf-8' .html .htm .shtml


# блокируем доступ ботам - делал Крайников
Order Deny,Allow
Deny from 91.200.0.0/16
Deny from 46.161.9.25
```

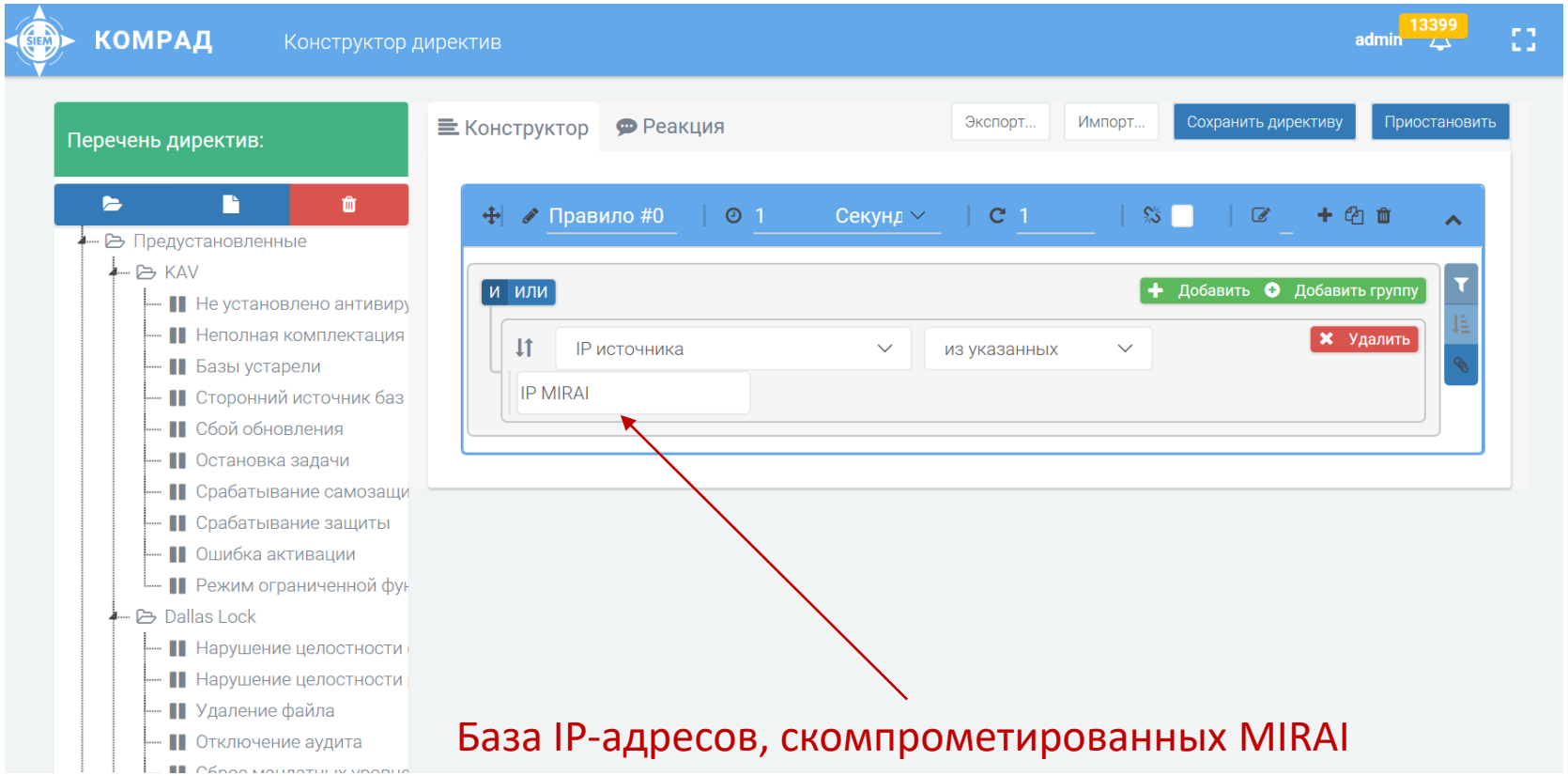
ВЫЯВЛЕНИЕ ПЕРЕБОРА ПАРОЛЕЙ



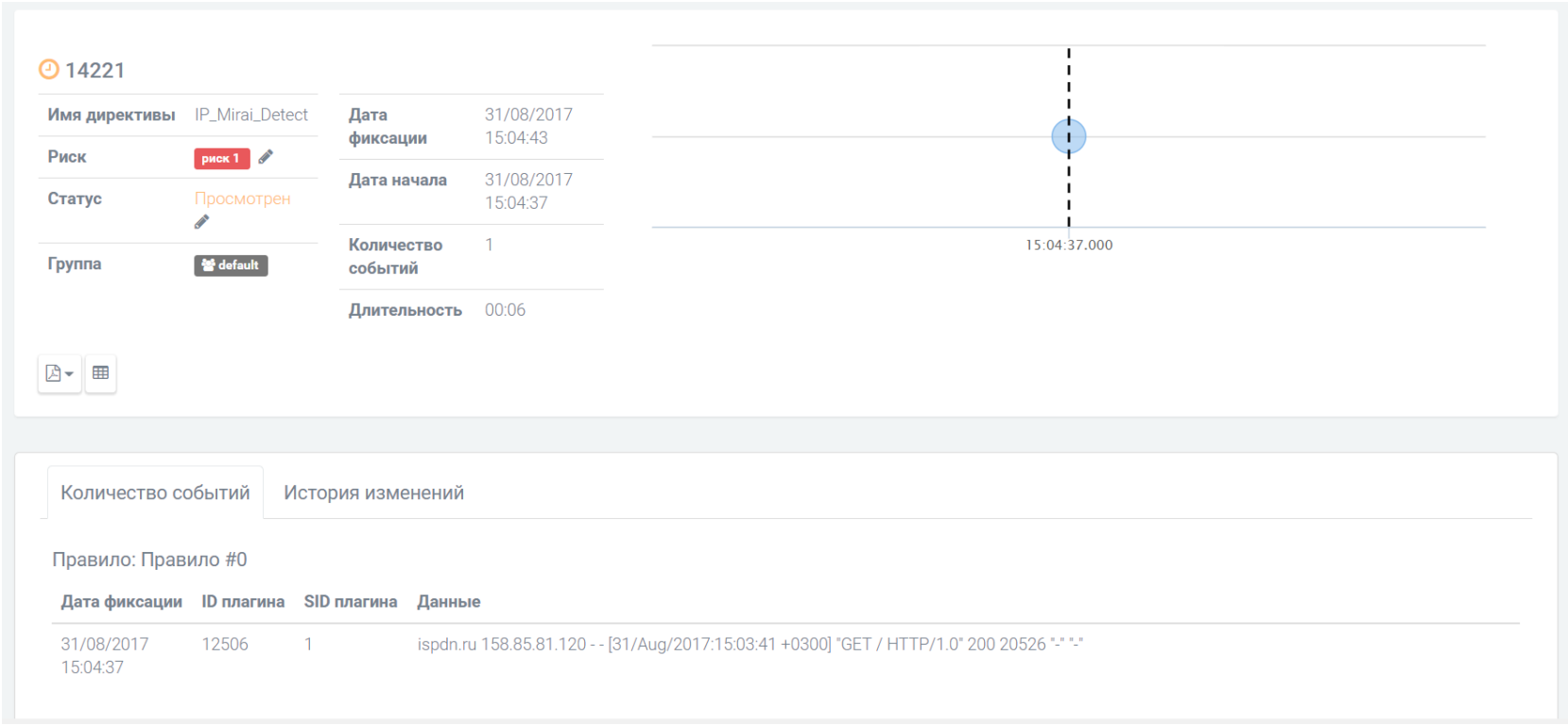
ВЫЯВЛЕННЫЙ ПОПЫТКИ ПОДБОРА ПАРОЛЕЙ К S3R.RU



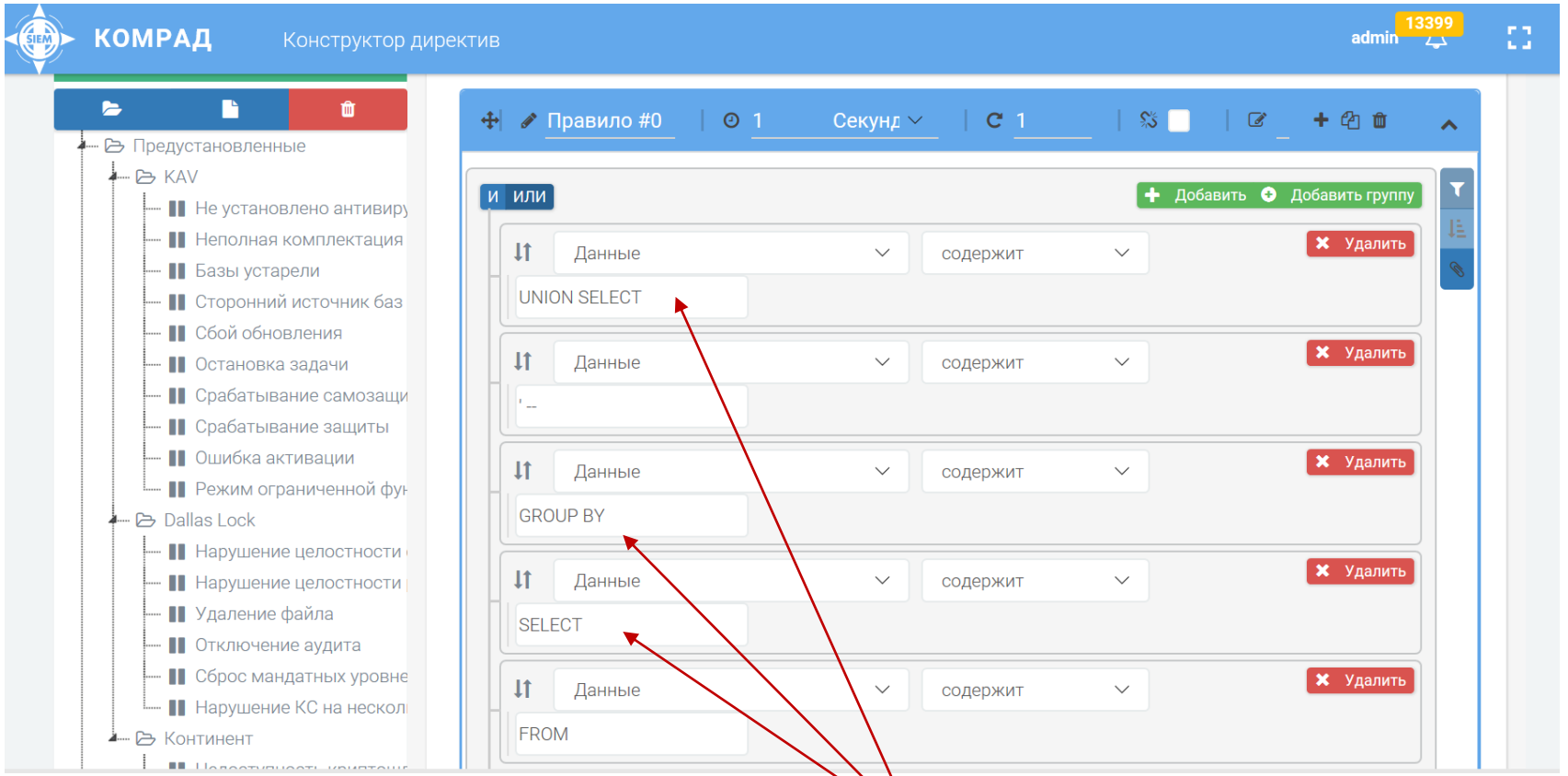
ВЫЯВЛЕНИЕ ПОПЫТКИ АТАКИ ОТ ЧЕРВЯ «MIRAI»



ЧЕРВЬ ПОПЫТАЛСЯ К НАМ ЗАЙТИ...

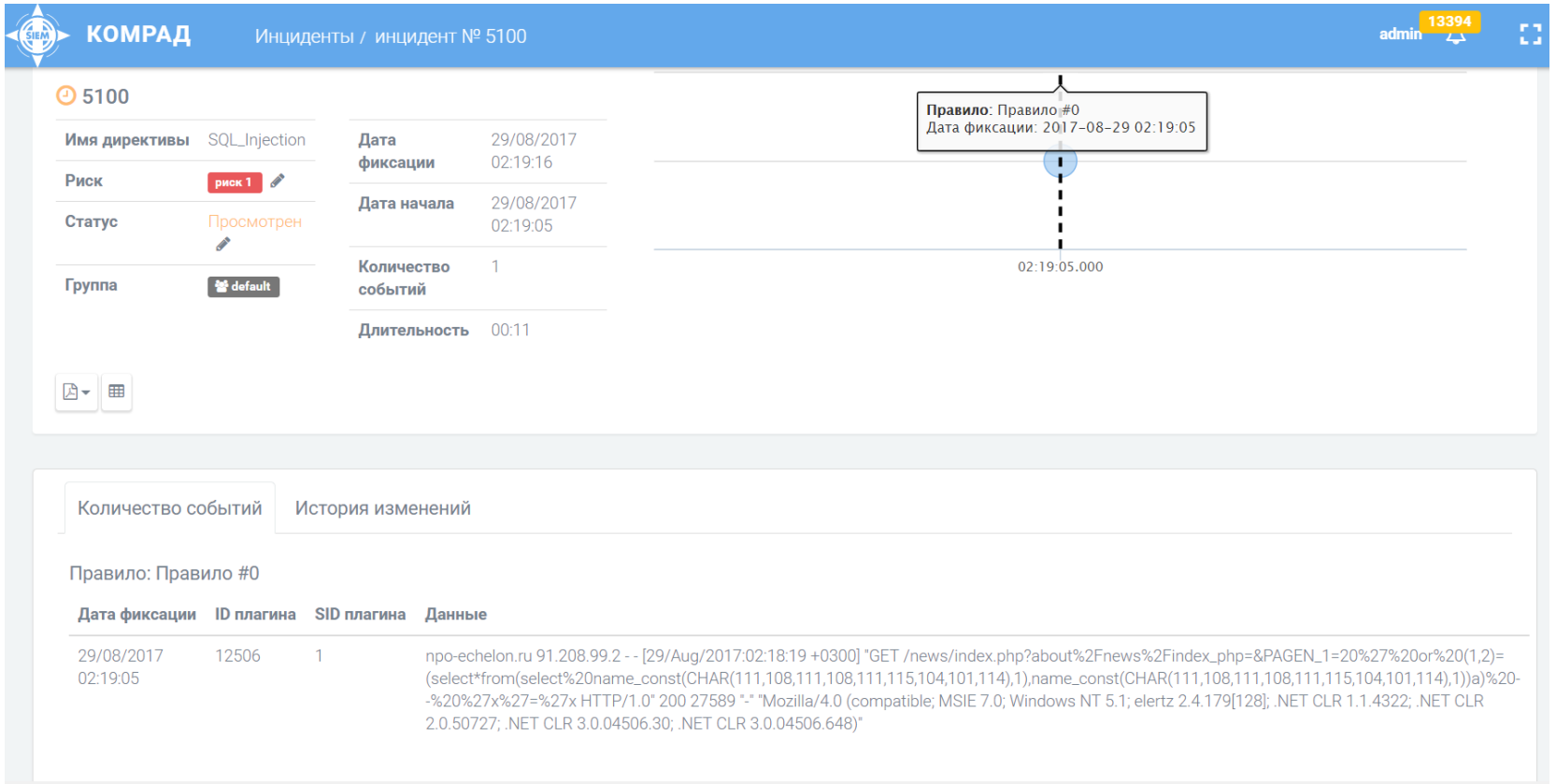


ВЫЯВЛЕНИЕ ПОПЫТОК SQL-ИНЪЕКЦИЙ

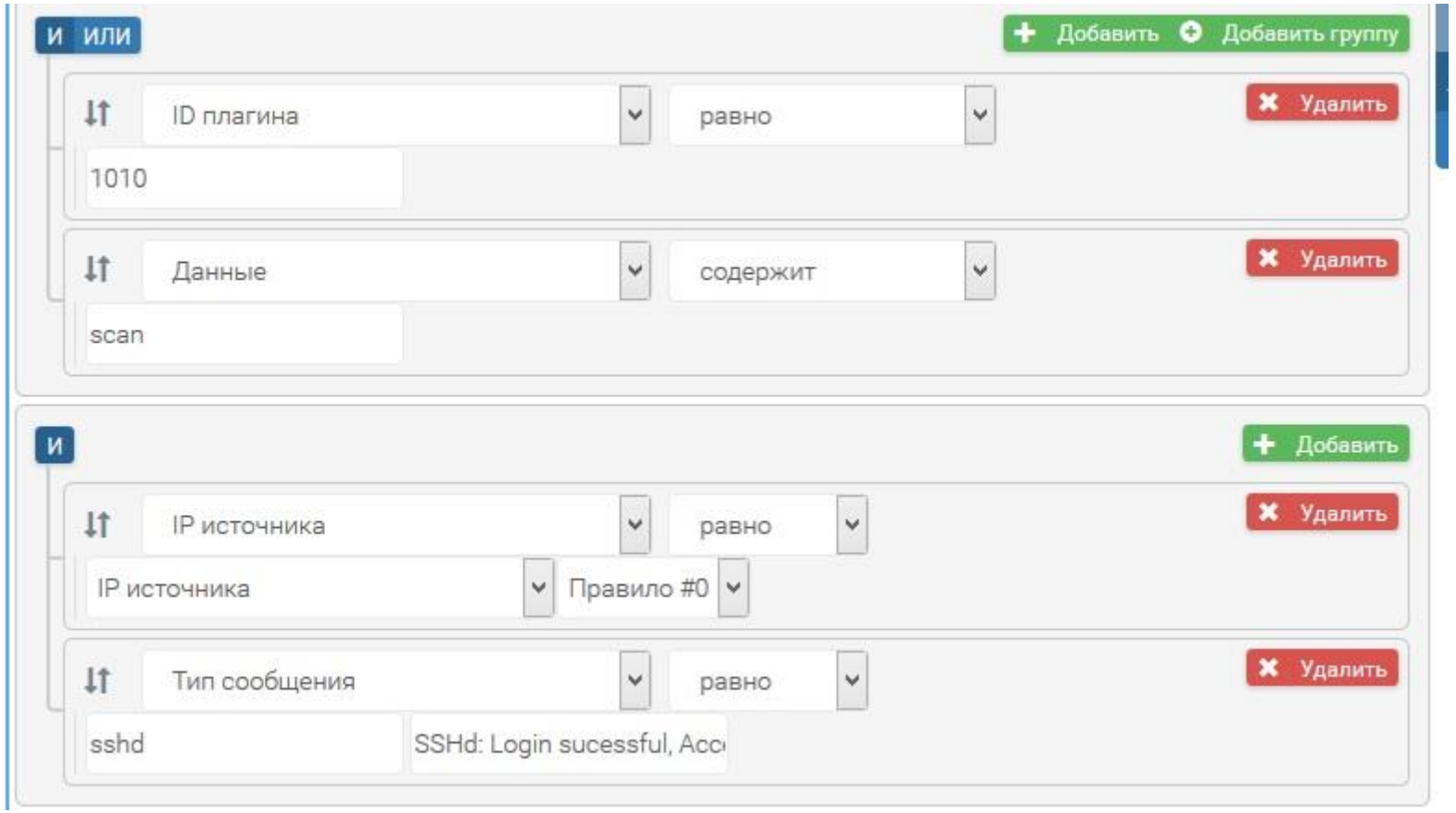


SQL-запросы в HTTP-трафике

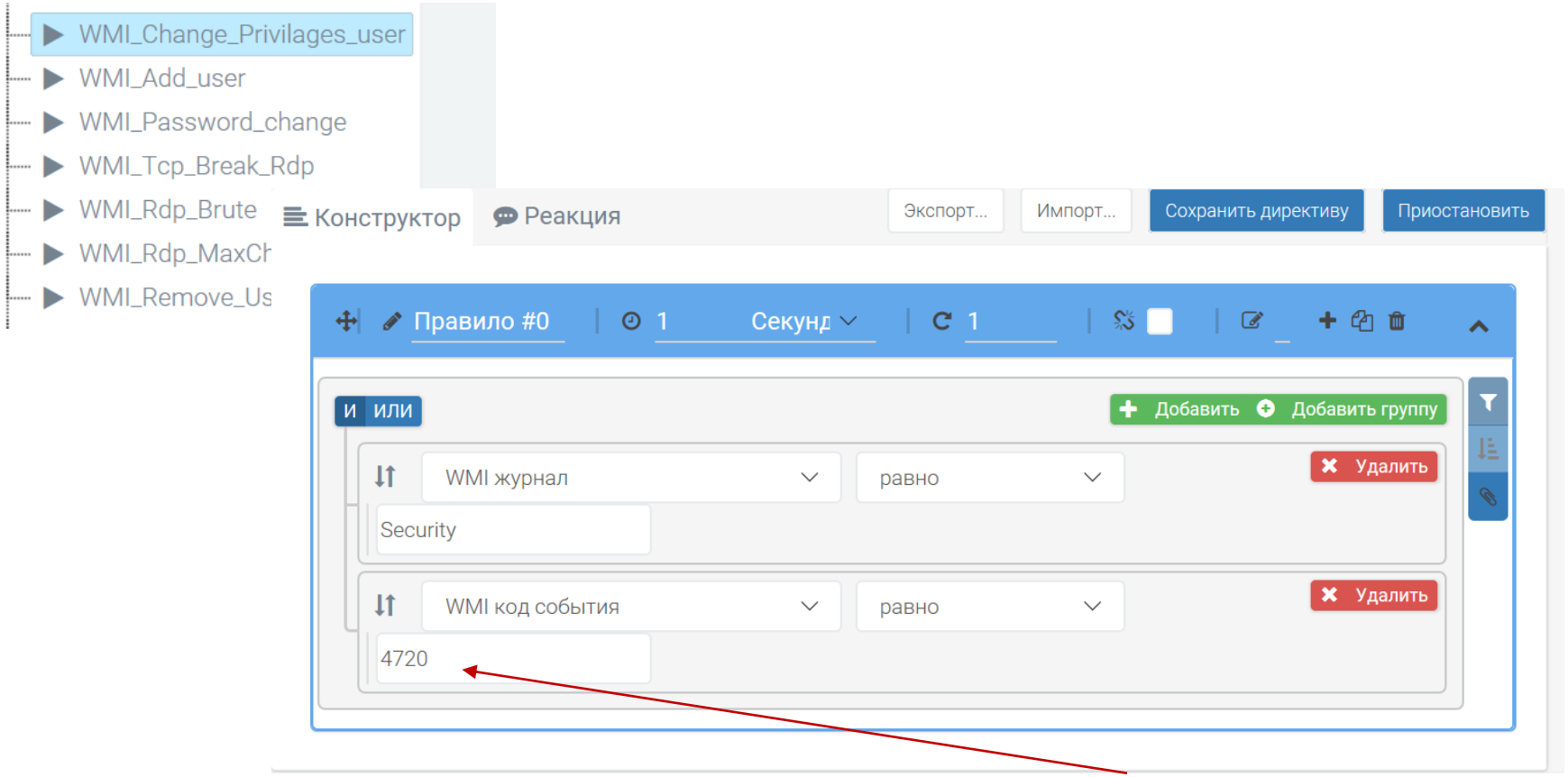
ПОПЫТКА SQL-ИНЪЕКЦИИ



РАЗВЕДКА И АВТОРИЗАЦИЯ



КОНТРОЛЬ МАНИПУЛЯЦИЙ С УЧЕТНЫМИ ЗАПИСЯМИ WINDOWS



СПАСИБО ЗА ВНИМАНИЕ!


Эшелон
комплексная безопасность