



**АКЦИОНЕРНОЕ ОБЩЕСТВО «ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ»
(АО «ПМ»)**

**БАЗА ДАННЫХ СИГНАТУРНЫХ ПРАВИЛ ОБНАРУЖЕНИЯ АТАК
AM RULES**

Эксплуатация базы данных сигнатурных правил обнаружения атак AM Rules
на примере ViPNet IDS NS 3.7

На 13 листах

Москва 2023

Аннотация

Настоящий документ является описывает эксплуатационные характеристики Базы данных сигнатурных правил обнаружения атак AM Rules (далее - БРП).

Содержание

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ	4
1 Общие сведения.....	5
2 Инструкция по первичной аутентификации в ViPNet IDS NS 3.7.....	6
3 Регистрация и характеристики Событий	8
4 Просмотр и поиск информации о Событиях	10

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

В настоящем документе применяют следующие сокращения:

АО «ПМ»	Акционерное общество «Перспективный мониторинг»
БРП	База данных сигнатурных правил обнаружения атак AM Rules
СЗИ	Средство защиты информации
ИБ	Информационная безопасность

1 Общие сведения

Основным направлением деятельности АО «ПМ» является оценка практической защищённости информационных систем, выявление их уязвимостей при помощи средств инструментального и ручного анализа, реагирование на инциденты безопасности, разработка Программного комплекса автоматизированного поиска, обработки и визуализации данных из открытых источников «Тардис» и Программного комплекса обучения методам обнаружения, анализа и устранения последствий компьютерных атак «Empire».

БРП предназначена для конфигурирования СЗИ для эффективного обнаружения компьютерных атак и других событий ИБ (далее - События). БРП предоставляет инструкции (далее - Правила), на основе которых СЗИ создают внутреннюю логику обнаружения, а также конфигурационные файлы. События могут быть просмотрены в интерфейсе СЗИ, экспортированы или автоматически отправлены на внешние обработчики.

2 Инструкция по первичной аутентификации в ViPNet IDS NS

3.7

Порядок подключения к веб-интерфейсу ViPNet IDS NS:

- запустить на терминале управления веб-браузер;
- в адресной строке веб-браузера ввести: `https://[Адрес]`, где [Адрес] - адрес доступа (IP-адрес или доменное имя) управляющего интерфейса ViPNet IDS NS;
- пройти аутентификацию в системе обнаружения вторжений ViPNet IDS NS 3.7 (Рисунок 1);

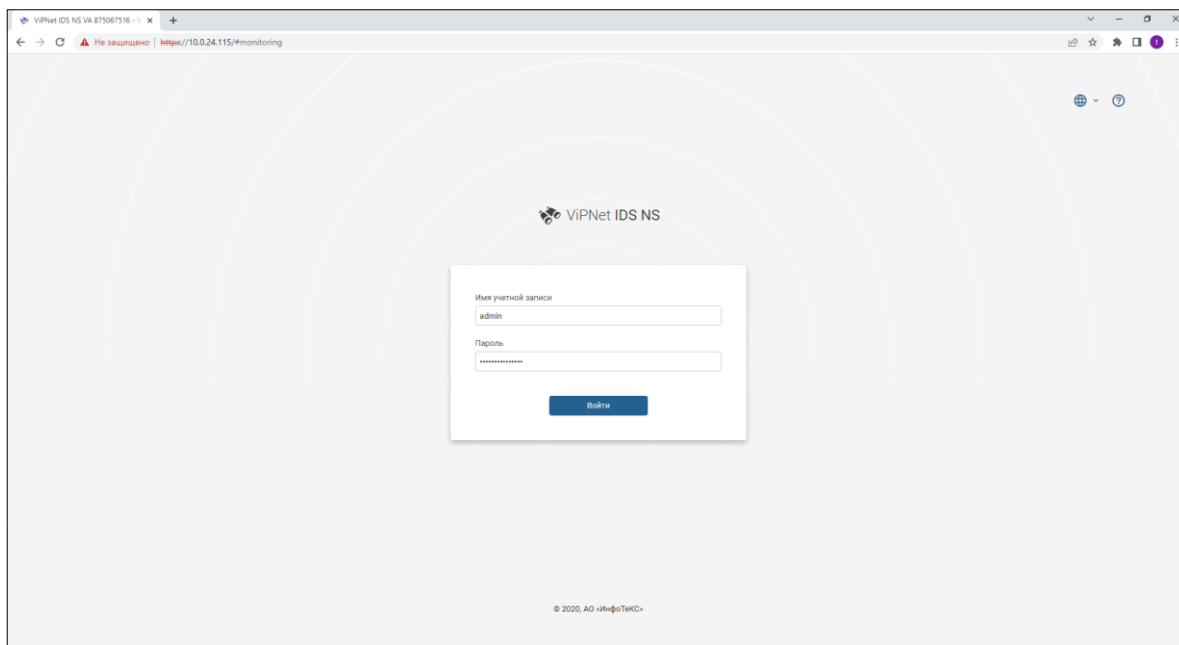
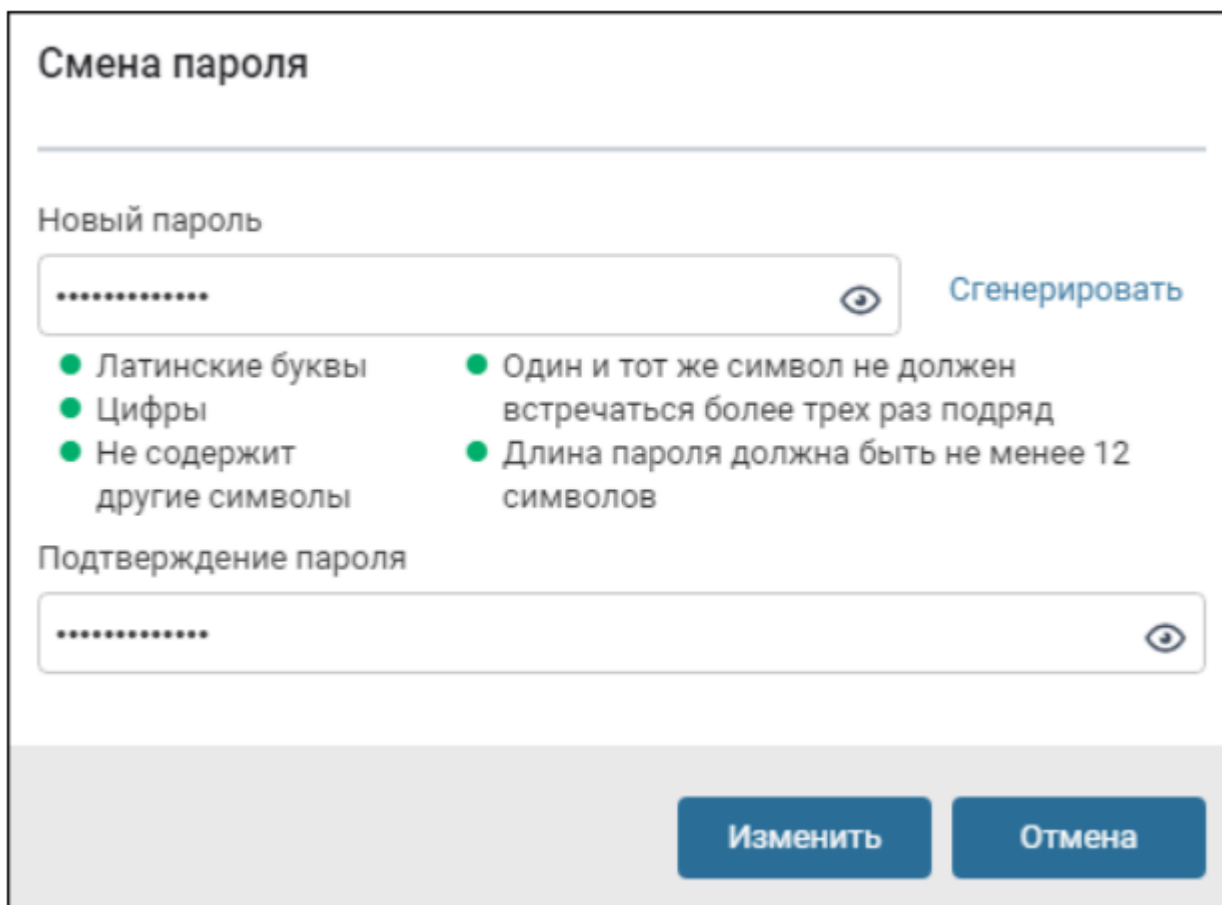


Рисунок 1 – Аутентификация в системе


- в соответствующих полях ввести имя и пароль учетной записи. При первом подключении к веб-интерфейсу для аутентификации ввести данные встроенной учетной записи главного администратора: имя по умолчанию - `admin`, пароль по умолчанию - `vipnet`;
- нажать «Войти»;
- при первом подключении к веб-интерфейсу после успешной авторизации сменить пароль встроенной учетной записи главного

администратора, заданный по умолчанию. Для этого в окне «Смена пароля» задать новый пароль самостоятельно или нажать «Сгенерировать» для выработки случайного пароля (Рисунок 2);




Смена пароля

Новый пароль

.....  Сгенерировать

- Латинские буквы
- Цифры
- Не содержит другие символы
- Один и тот же символ не должен встречаться более трех раз подряд
- Длина пароля должна быть не менее 12 символов

Подтверждение пароля

..... 

Изменить Отмена

Рисунок 2 – Смена пароля

– для подтверждения ввести новый пароль повторно и нажать «Изменить».

3 Регистрация и характеристики Событий

БРП эксплуатируются посредством использования их в соответствующих СЗИ, в данном случае ViPNet IDS NS 3.7, которое использует БРП в функционале обнаружения Событий.

События регистрируются в журнале событий ViPNet IDS NS. Запись о событии в журнале содержит сведения о вредоносном пакете или файле, а также сработавшем Правиле.

Характеристики События:

- дата и время регистрации с точностью до миллисекунды;
- уровень важности;
- количество однотипных Событий, агрегированных в единую запись;
- сведения о сработавшем Правиле: название, группа, класс, описание, текст и код;
- тип;
- сведения о сетевом пакете или файле:
 - а) протокол передачи данных транспортного уровня и прикладного уровня;
 - б) MAC-адреса, IP-адреса и порты источника и получателя (если применимо);
 - в) идентификатор виртуальной сети VLAN ID;
 - г) параметры HTTP-сессий:
 - 1) доменное имя ресурса, запрашиваемого клиентским приложением;
 - 2) информация о клиентском приложении, запросившем ресурс;
 - д) характеристики вредоносного файла:
 - 1) относительный URI;
 - 2) размер в байтах;


- 3) хэш-сумма, рассчитанная по алгоритму MD5;
- 4) категория, тип и его описание;
- дополнительные сведения из вспомогательных источников.

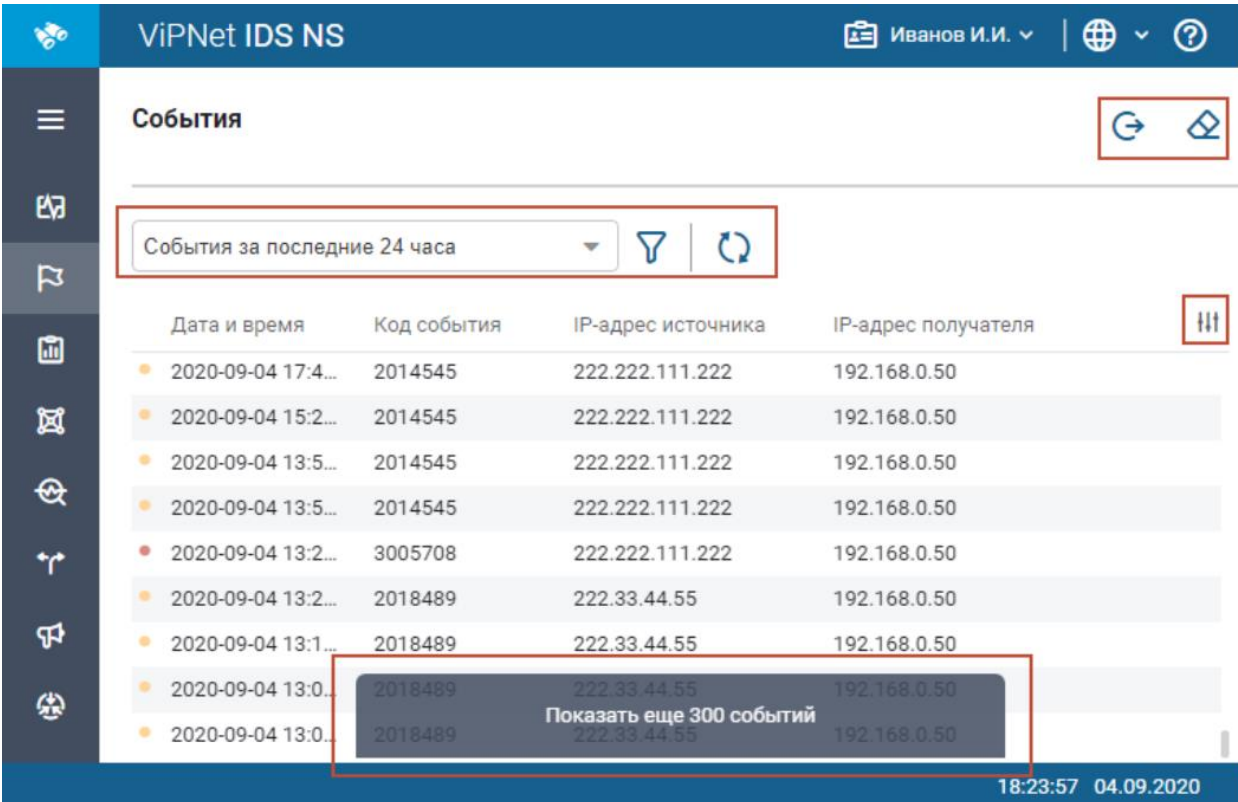
4 Просмотр и поиск информации о Событиях

Информация о зарегистрированных Событиях содержится в журнале событий. Журнал - это список записей о Событиях, представленный в веб-интерфейсе в табличном виде. Чтобы просмотреть информацию о Событии, необходимо найти его запись в списке.

Порядок просмотра записей о событиях:

- подключиться к веб-интерфейсу ViPNet IDS NS;
- на панели навигации перейти в раздел «Мониторинг - События».


По умолчанию в списке отображаются записи о Событиях, зарегистрированных за последние сутки. Первоначально в списке отображаются не более 300 записей. Для просмотра следующих 300 записей с помощью полосы прокрутки необходимо переместиться в конец списка и нажать «Показать еще 300 событий». Для обновления информации в списке на панели инструментов нажать значок  (Рисунок 3).



The screenshot displays the 'События' (Events) section of the ViPNet IDS NS interface. The header shows the user 'Иванов И.И.' and a refresh icon. The main area features a table with columns for 'Дата и время', 'Код события', 'IP-адрес источника', and 'IP-адрес получателя'. A red box highlights the 'Показать еще 300 событий' button at the bottom of the table.

Дата и время	Код события	IP-адрес источника	IP-адрес получателя
2020-09-04 17:4...	2014545	222.222.111.222	192.168.0.50
2020-09-04 15:2...	2014545	222.222.111.222	192.168.0.50
2020-09-04 13:5...	2014545	222.222.111.222	192.168.0.50
2020-09-04 13:5...	2014545	222.222.111.222	192.168.0.50
2020-09-04 13:2...	3005708	222.222.111.222	192.168.0.50
2020-09-04 13:2...	2018489	222.33.44.55	192.168.0.50
2020-09-04 13:1...	2018489	222.33.44.55	192.168.0.50
2020-09-04 13:0...	2018489	222.33.44.55	192.168.0.50
2020-09-04 13:0...	2018489	222.33.44.55	192.168.0.50

Рисунок 3 – Записи о событиях

Для удобства анализа информации в журнале событий есть возможность настройки видимости столбцов в таблице. Для этого необходимо нажать в последнем столбце заголовка таблицы значок  и с помощью флажков выбрать состав отображаемых столбцов.

Информация о событии распределена по следующим вкладкам карточки:

Событие - основные характеристики события (Рисунок 4).

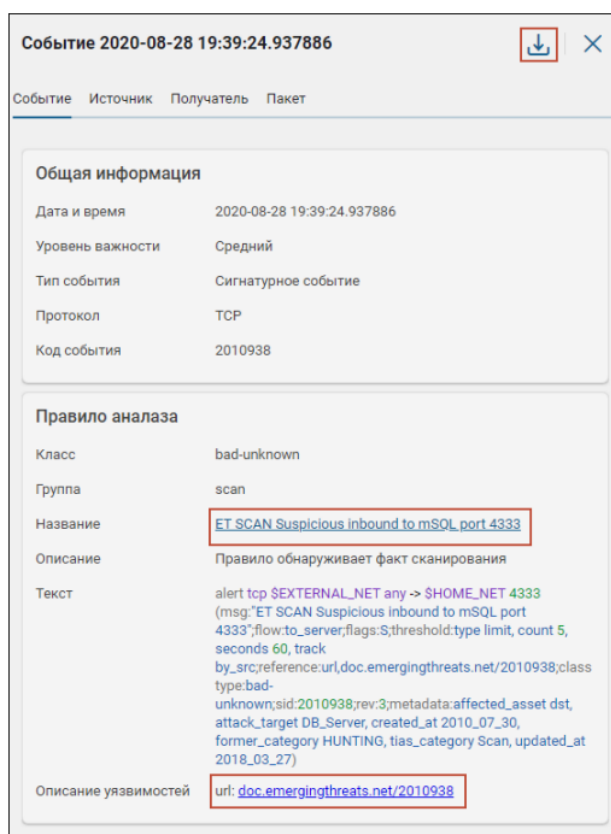


Рисунок 4 – Характеристики события

В группе «Правило анализа» расположены дополнительные инструменты для анализа события:

– быстрый переход к просмотру карточки сработавшего правила - нажатие на название правила. Данная возможность может быть полезна, например, при обнаружении ложных срабатываний правил, когда необходимо внести изменения в текст или отключить правило;

– ссылки на веб-ресурсы с описанием уязвимостей, связанных с обнаруженной угрозой.

Источник / Получатель - сведения об источнике/получателе вредоносного пакета или файла (Рисунок 5).

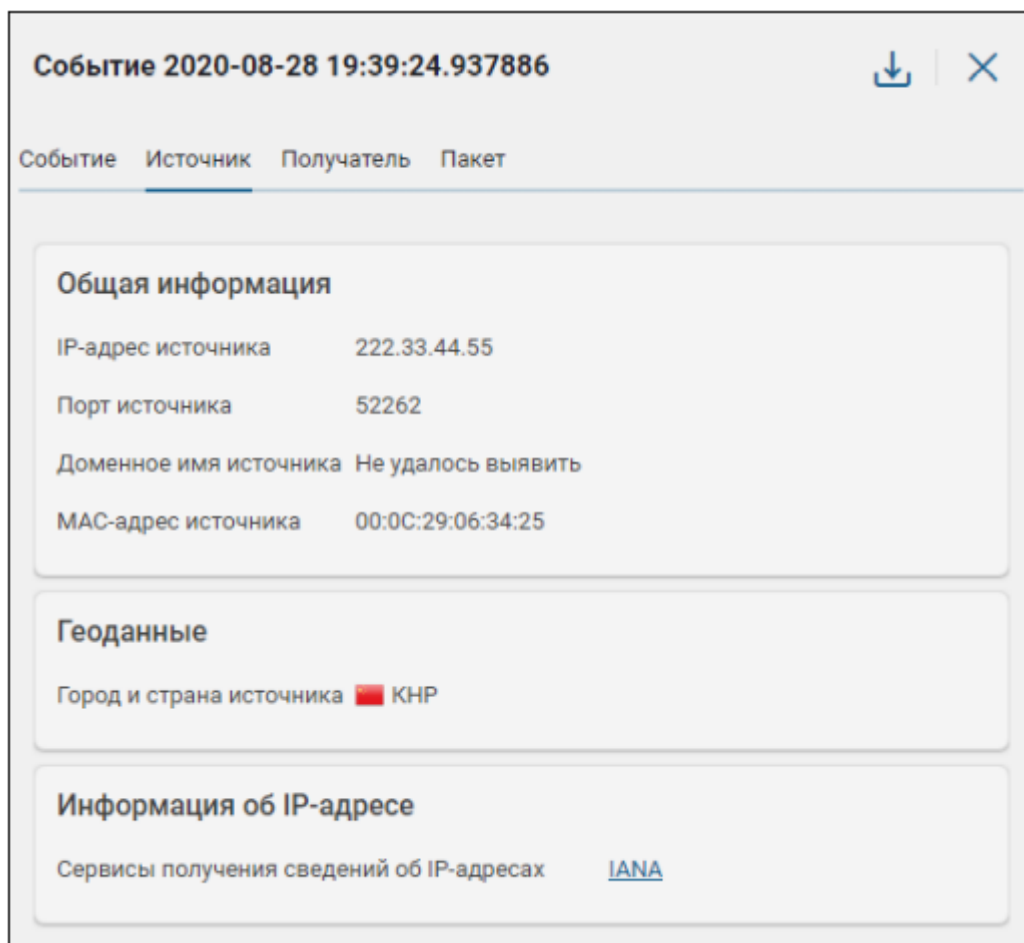


Рисунок 5 – Сведения об источнике

Пакет - содержание вредоносного пакета (Рисунок 6).

Событие 2020-09-11 01:32:25.7518 ↓ | ✕

Событие	Источник	Получатель	Пакет
Смещен...	Шестнадцатеричные данные	Данные в виде текста	
0000	00 50 56 2f 41 4f 00 0c 29 06 3...	.PV/AO..).4%..E.	
0010	FA 4f AC C5 40 00 40 06 7E 67 D...	ú0~A@.@. ~gPPoPÀ~	
0020	00 32 00 50 95 8c FC 73 54 ED 4...	.2.P•Eüs TíA",.€.	
0030	51 00 BD 63 00 00 01 01 08 0A 0...	Q.%c....(ü..	
0040	4D 07 3A 62 61 64 2D 75 6E 6B 6...	M.:bad-u nknown;s	
0050	69 64 3A 32 30 31 31 38 31 30 3...	id:20118 10;rev:1	
0060	29 0A 61 6C 65 72 74 20 74 63 7...).alert tcp \$HOM	
0070	45 5f 4E 45 54 20 61 6E 79 20 2...	E_NET an y -> \$EX	
0080	54 45 52 4E 41 4C 5f 4E 45 54 2...	TERNAL_N ET \$HTTP	
0090	5f 50 4f 52 54 53 20 28 6D 73 6...	_PORTS (msg:"ET	
00A0	44 45 4C 45 54 45 44 20 5A 65 7...	DELETED Zeus htt	
00B0	70 20 63 6C 69 65 6E 74 20 6C 6...	p client library	
00C0	20 64 65 74 65 63 74 65 64 22 3...	detecte d";flow:	
00D0	65 73 74 61 62 6C 69 73 68 65 6...	establis hed,to_s	

Рисунок 6 – Сведения о пакете