

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

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

Инструкция по установке баз данных сигнатур правил обнаружения атак  
AM Rules на примере ViPNet IDS NS 3.7

На 22 листах

Москва 2023

## **Аннотация**

Настоящий документ является инструкцией по установке Базы данных сигнатурных правил обнаружения атак AM Rules (далее - БРП).

БРП существуют во множестве вариантов в зависимости от системы защиты информации (далее - СЗИ), для которой они предназначены. Данная инструкция описывает процесс ручной установки БРП на систему обнаружения вторжений ViPNet IDS NS 3.7. Установка на другие системы линейки ViPNet IDS NS производится в аналогичном порядке.

## СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ .....	4
1 Общие сведения.....	5
2 Инструкция по развертыванию ViPNet IDS NS 3.7 VA.....	6
2.1 Инструкция по развертыванию виртуальной машины ViPNet IDS NS 3.7 VA .....	6
2.2 Инструкция по первичной аутентификации в ViPNet IDS NS 3.7 VA .....	10
2.3 Инструкция по установке и активации лицензии .....	13
3 Инструкция по установке БРП .....	20
4 Инструкция по установке AM Ruleset Analyzer.....	22

## ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

В настоящем документе применяют следующие сокращения:

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

## **1 Общие сведения**

Основным направлением деятельности АО «ПМ» является оценка практической защищенности 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 создает внутреннюю логику обнаружения, а также конфигурационные файлы. События могут быть просмотрены в интерфейсе СЗИ, экспортированы или автоматически отправлены на внешние обработчики.

## **2 Инструкция по развертыванию ViPNet IDS NS 3.7 VA**

Порядок подготовки ViPNet IDS NS VA:

- установить компьютер, предназначенный для установки платформы виртуализации;
- подключить компьютер к сети переменного тока напряжением 220 В;
- подключить выбранный сетевой интерфейс компьютера коммутационным кабелем к сетевому оборудованию сегмента локальной сети;
- установить на компьютер одну из поддерживаемых платформ виртуализации, в соответствии с документацией производителя;
- если ViPNet IDS NS VA предназначен для анализа трафика в физической сети, подключить выбранный сетевой интерфейс компьютера с установленной платформой виртуализации коммутационным кабелем к сетевому адаптеру устройства дублирования трафика;
- подготовить на платформе виртуализации виртуальную машину ViPNet IDS NS VA (см. подраздел 2.1);
- активировать лицензию для ViPNet IDS NS VA;
- установить Базу решающих правил.

### **2.1 Инструкция по развертыванию виртуальной машины ViPNet IDS NS 3.7 VA**

На платформах виртуализации Oracle VM VirtualBox, VMware Workstation Pro и VMware vSphere ESXi виртуальная машина ViPNet IDS NS VA импортируется из образа ПО ViPNet IDS NS в формате OVA. Описание развертывания виртуальной машины ViPNet IDS NS VA приведено на примере аппаратной платформы виртуализации VMware vSphere ESXi. Предполагается, что в сети уже развернут сервер VMware vCenter Server, а к нему настроено подключение клиента vSphere Client.

Для развертывания потребуется файл с образом ПО ViPNet IDS NS в формате OVA - ids-ns-va-3.7.0-[Номер сборки].ova из комплекта поставки.

Порядок развертывания образа ViPNet IDS NS VA и настройки интерфейсов захвата трафика:

- запустить клиент vSphere Client и подключиться к серверу VMware vCenter Server;
- в главном окне vSphere Client в меню «File» выбрать Deploy OVF Template и следовать указаниям мастера (Рисунок 1);

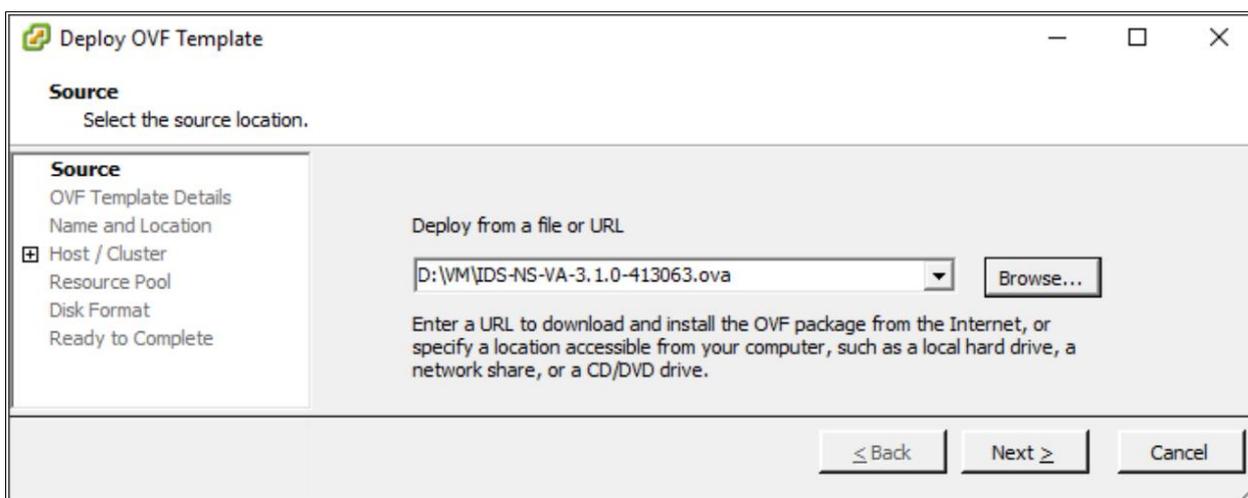


Рисунок 1 – Выбор файла с образом виртуальной машины

- на шаге «Source» нажать «Browse», выбрать файл формата OVA с образом виртуальной машины ViPNet IDS NS VA;
- на шаге «OVF Template Details» ознакомиться с параметрами виртуальной машины;
- на шаге «Name and Location» в поле «Name» указать имя виртуальной машины, выбрать каталог ее расположения;
- на шаге «Resource Pool» выбрать пул ресурсов, который определяет объем оперативной памяти и процессор, предоставляемый для виртуальной машины;

– на шаге «Storage» указать раздел или твердотельный накопитель из выбранного пула ресурсов, на котором будут храниться файлы виртуальной машины (Рисунок 2);

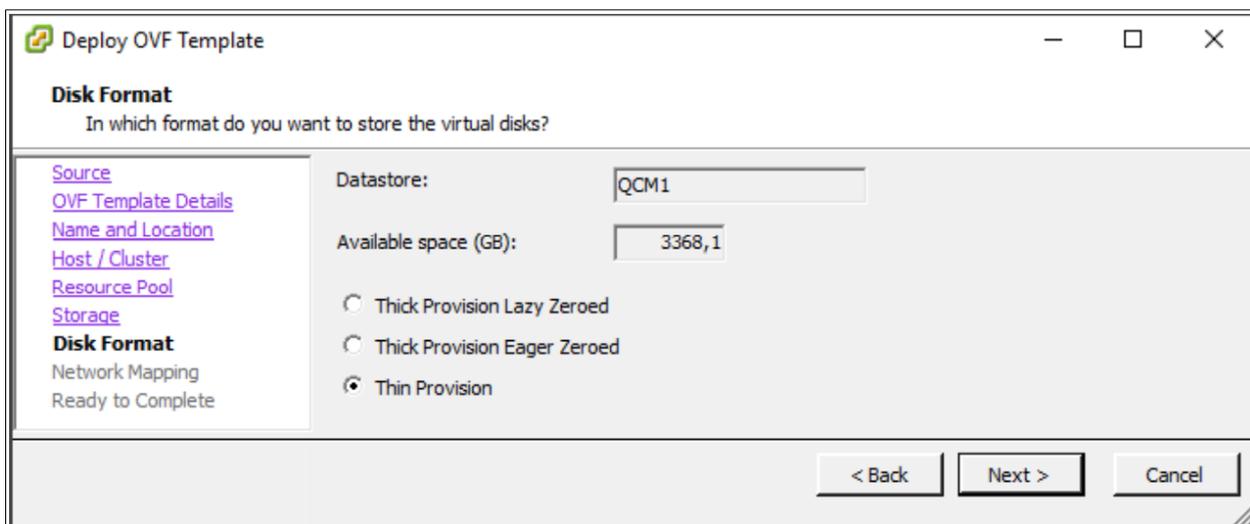


Рисунок 2 – Выбор типа жесткого диска

- на шаге «Disk Format» выбрать тип жесткого диска «Thin Provision»;
- на шаге «Network Mapping» выбрать имя сети подключения с типом Bridged для управляющего сетевого интерфейса;
- на шаге «Ready to Complete» проверить настройки виртуальной машины и нажать «Finish»;
- дождаться завершения процесса развертывания виртуальной машины.

Чтобы настроить сетевой интерфейс виртуальной машины для захвата трафика из виртуальной сети: в настройках виртуальной машины для одного или нескольких (в зависимости от количества виртуальных сетей) сетевых адаптеров, назначенных в качестве интерфейсов захвата, выбрать в качестве сети подключения существующую виртуальную сеть.

Для этого:

- на панели навигации вызвать контекстное меню созданной виртуальной машины и выбрать «Edit Settings»;

- в окне «Virtual Machine Properties» на вкладке «Hardware» выбрать сетевой адаптер, назначенный для захвата трафика, а в списке «Network Connection» выбрать имя виртуальной сети (Рисунок 3).

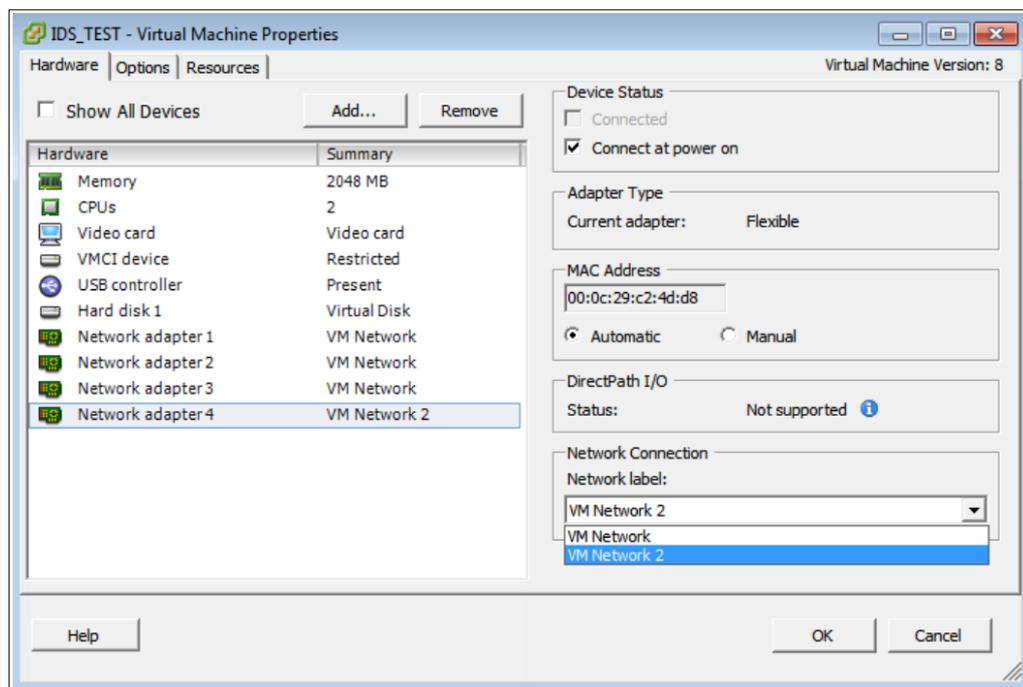


Рисунок 3 – Подключение интерфейса захвата виртуальной машины к виртуальной сети

В свойствах виртуального коммутатора для каждой виртуальной сети, трафик которой необходимо анализировать, включить режим, позволяющий принимать все пакеты, независимо от того, кому они предназначены.

Для этого:

- перейти на вкладку «Configuration»;
- выбрать виртуальный коммутатор и нажать «Properties» (Рисунок 4);
- в окне Properties перейти на вкладку «Security» и в списке «Promiscuous Mode» выбрать «Accept» (Рисунок 5).

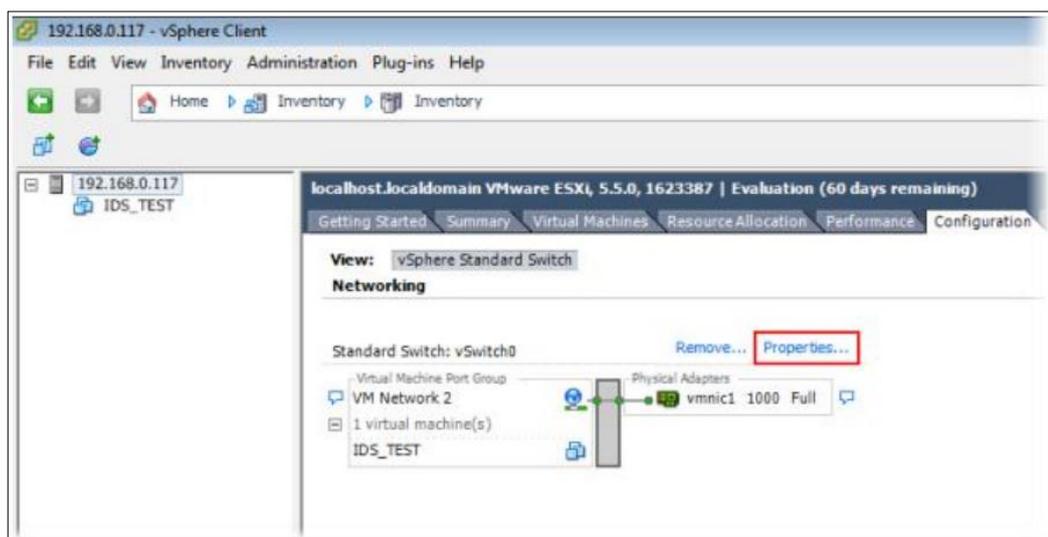


Рисунок 4 – Просмотр свойств созданного виртуального коммутатора

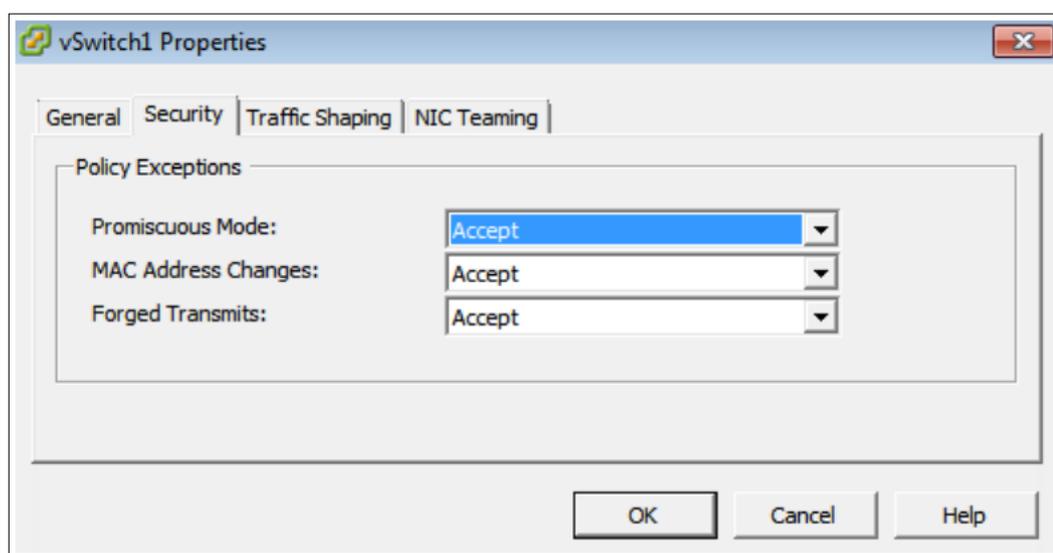


Рисунок 5 – Включение режима Promiscuous mode

## 2.2 Инструкция по первичной аутентификации в ViPNet IDS NS

### 3.7 VA

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 6);

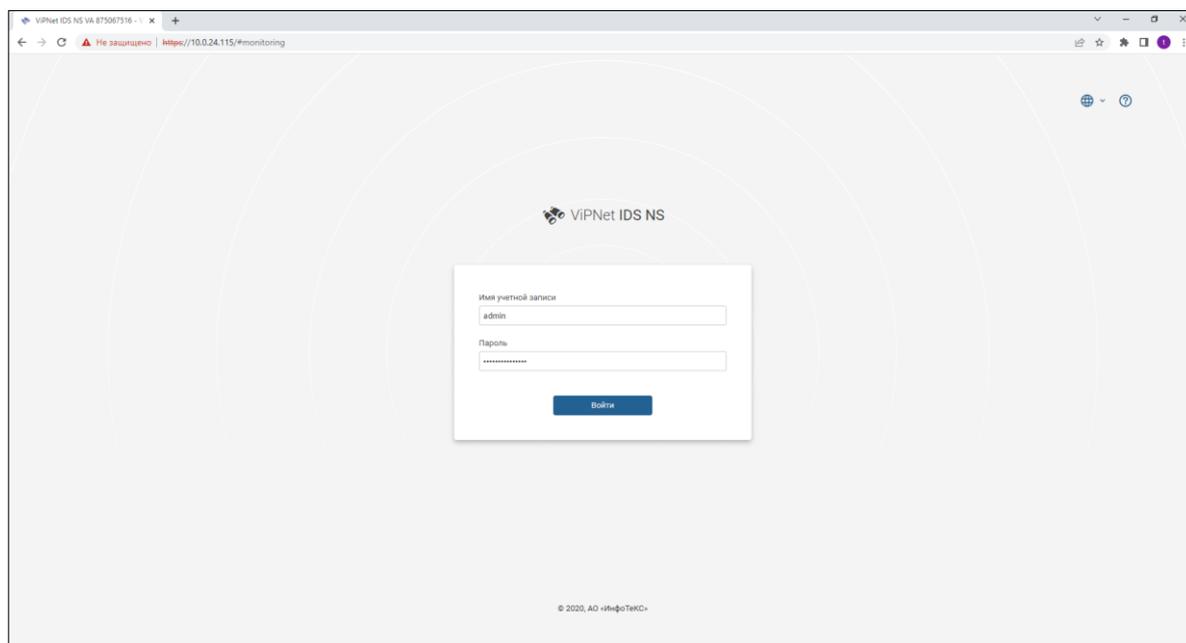


Рисунок 6 – Аутентификация в системе

– 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. Для подтверждения ввести новый пароль повторно и нажать Изменить (Рисунок 7).

## 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 7 – Смена пароля

## 2.3 Инструкция по установке и активации лицензии

В боковом разделе «Инфопанель» выбрать пункт «О программе» (Рисунок 8).

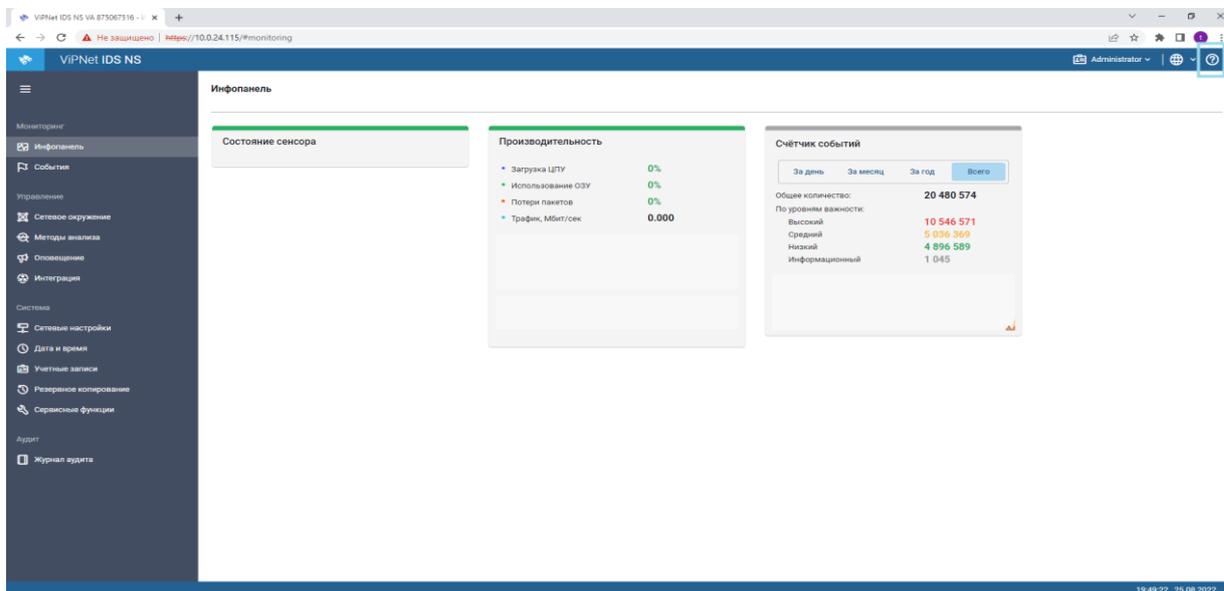


Рисунок 8 – Установка и активация лицензии

В открывшемся окне выбрать пункт «Установить лицензию» (Рисунок 9).

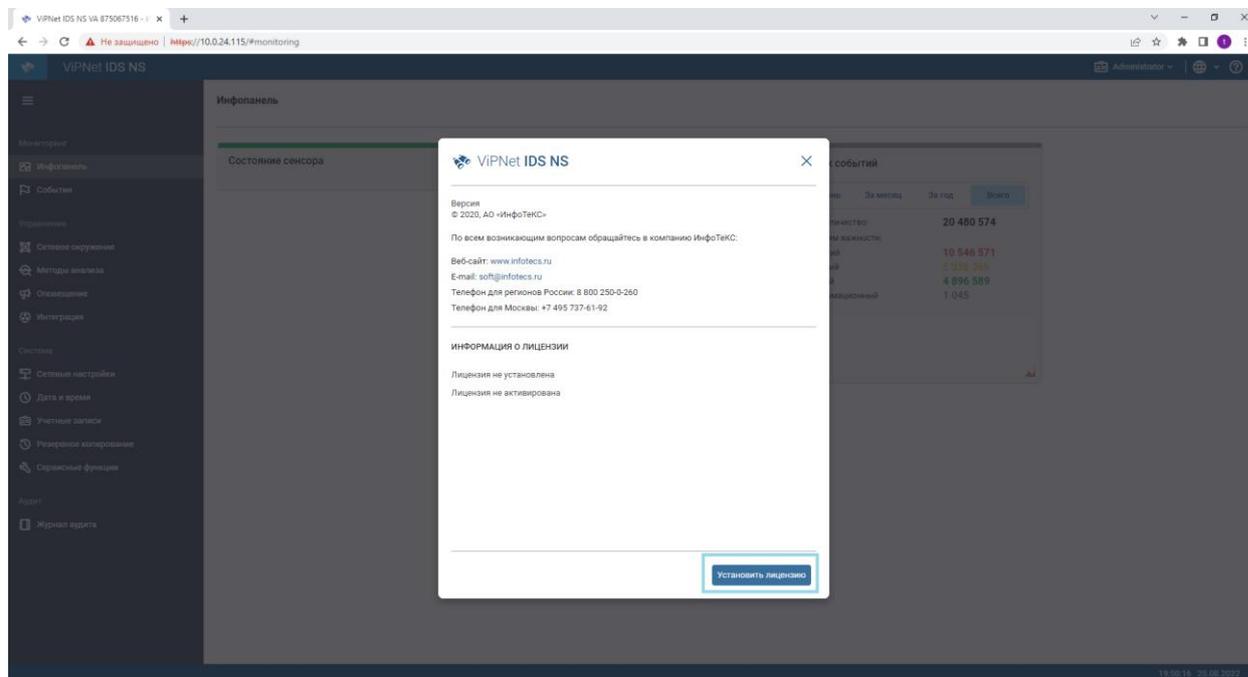


Рисунок 9 – Установка и активация лицензии

В диалоговом окне «Загрузка файла» нажать на иконку папки, чтобы выбрать файл лицензии (Рисунок 10).

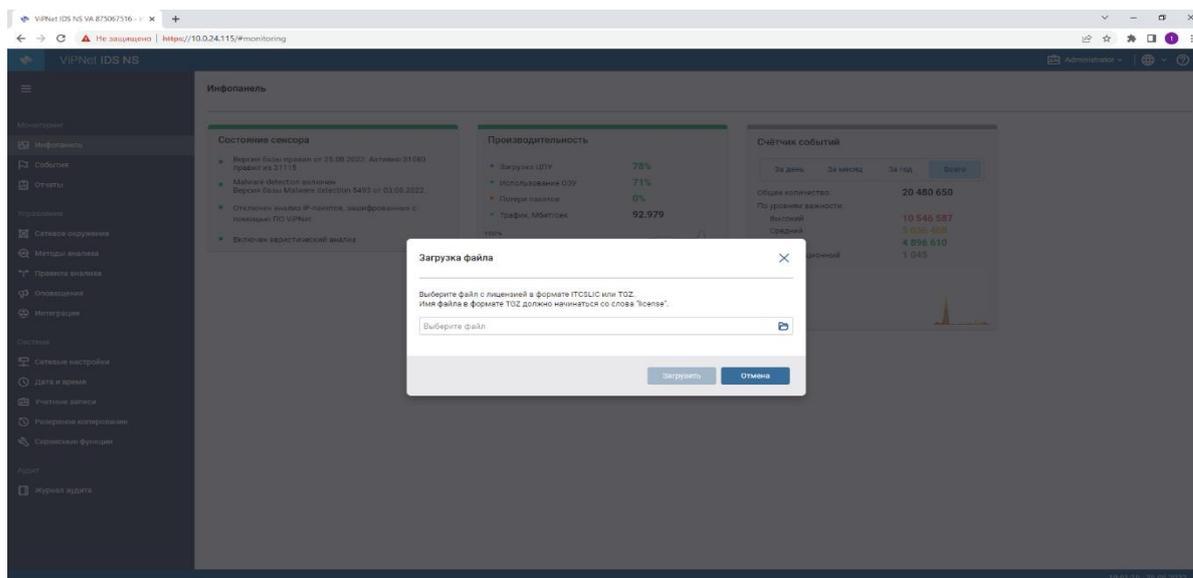


Рисунок 10 – Установка и активация лицензии

Далее с помощью диалогового окна операционной системы загрузить файл лицензии (Рисунок 11).

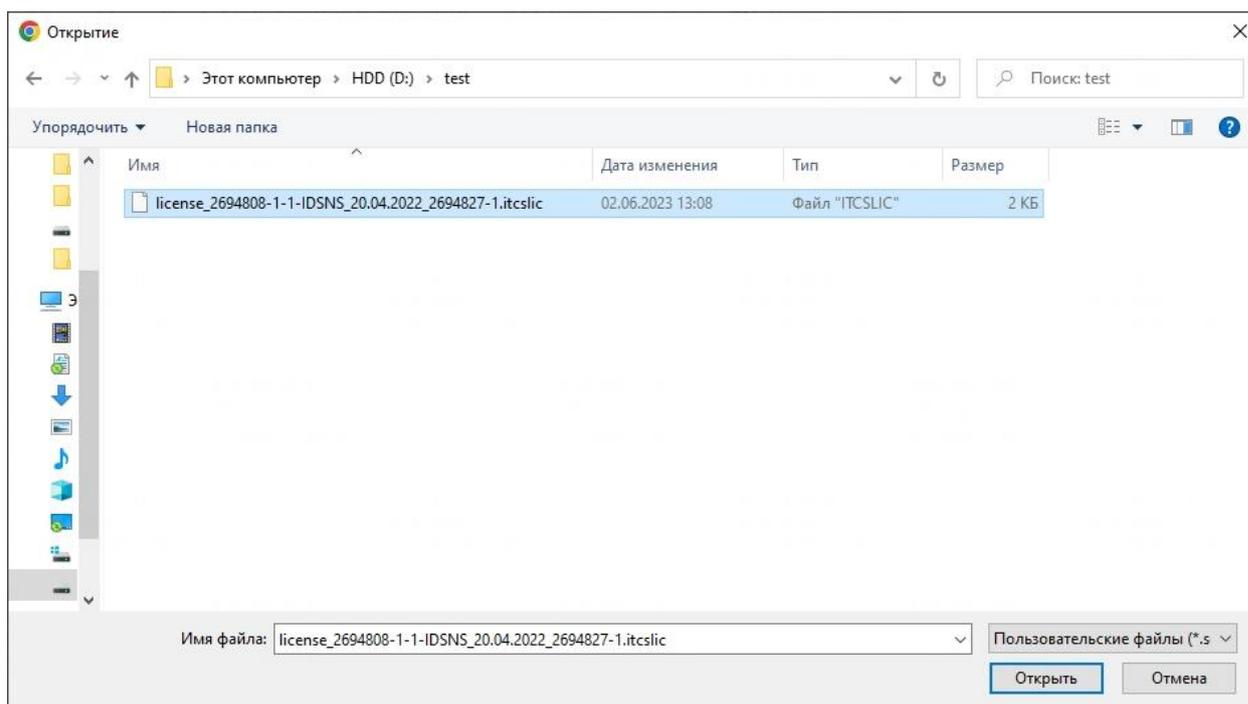


Рисунок 11 – Выбор файла лицензии

После чего в боковом разделе «Инфопанель» в блоке «Состояние сенсора» нажать «Активировать» (Рисунок 12).

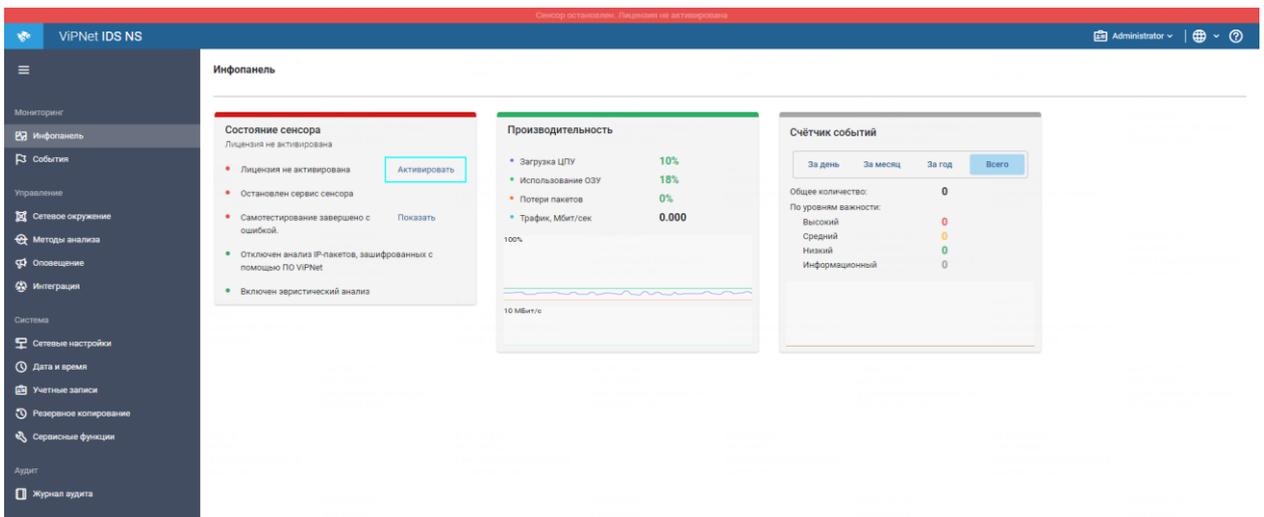


Рисунок 12 – Окно инфопанели с кнопкой «Активировать»

После нажатия кнопки «Активировать» пользователю будет предложено ознакомиться и принять лицензионное соглашение (Рисунок 13).

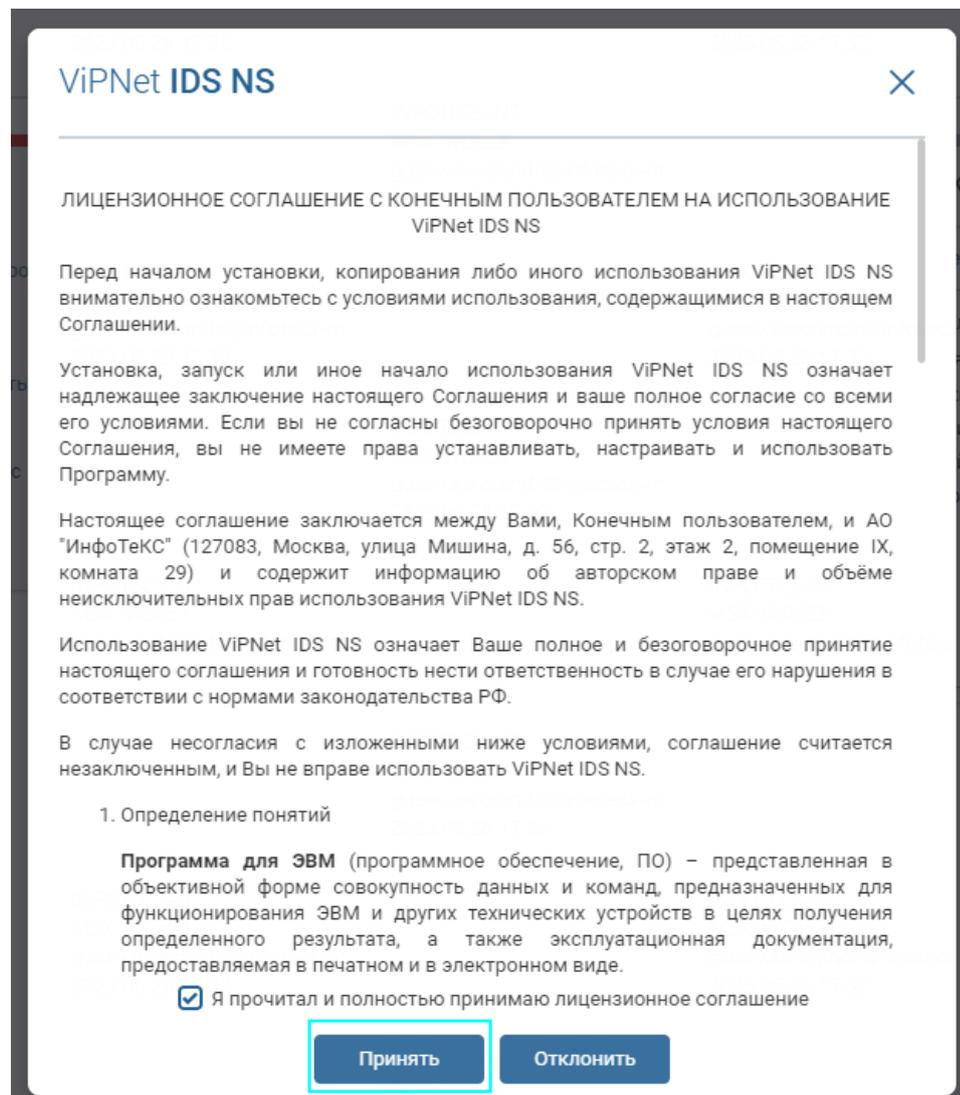


Рисунок 13– Лицензионное соглашение с конечным пользователем

В случае, если ViPNet IDS NS развёрнут без доступа в Интернет, а у терминала управления доступ в Интернет настроен, активация возможна по электронной почте. Для этого необходимо выбрать «Запросить активацию по e-mail» в окне активации лицензии (Рисунок 14).

Активация лицензии ViPNet IDS NS

Чтобы получить доступ к функционалу ViPNet IDS NS, необходимо активировать лицензию. Активация подтверждает подлинность продукта ViPNet IDS NS на компьютере и тот факт, что он не установлен на большем числе компьютеров по сравнению с тем, которое разрешено условиями лицензионного соглашения.

Активируйте лицензию через Интернет, если компьютер имеет доступ к сети. Если доступ в Интернет ограничен, вы можете воспользоваться возможностью активации лицензии по E-mail. В ответном письме вы получите код активации, который нужно ввести в поле ниже.

Активировать через Интернет    **Запросить активацию по E-mail**    Сформировать текст запроса

Ключ продукта    8XQ8-8GMN-WWG9-XG68

Код компьютера    4H342W4-5B5384K-53SZVNM-7YZQN5X-5GS42PL

Код активации        Активировать лицензию

Закрыть

Рисунок 14 – Запросить активацию по E-mail

Далее автоматически откроется выбранное в ОС приложение для работы с электронной почтой (Рисунок 15).

The image shows a Microsoft Outlook message template window. On the left, there is a button labeled "Отправить" (Send) with a paper plane icon. To its right are four buttons: "От" (From), "Кому..." (To...), "Копия..." (Cc...), and "СК..." (Subject). The "Кому..." field contains the text "offlinereg2: WORLD off-line Registration". The "Тема" (Subject) field contains "Регистрация VIPNet". Below these fields is a large text area containing the following text:

Данное письмо сформировано автоматически. Для успешной активации его необходимо отправить по адресу [reg@infotecs.biz](mailto:reg@infotecs.biz).  
Не изменяйте это письмо.

Локализация: RUS  
Пользователь:  
Организация:  
Продукт: ViPNet IDS NS  
Версия: 1  
Серийный номер: 8XQ8- -WWG9-XG68  
Код компьютера: 4H342W4-5B5384K- -7YZQN5X-5GS42PL  
Checksum: 4WWWW8E-729ZPMF-443GDVG

Рисунок 15 – Окно шаблона сообщения Microsoft Outlook

Код активации из ответного сообщения необходимо ввести в поле «код активации» и нажать «Активировать лицензию».

В случае наличия доступа к Интернету необходимо выбрать «Активировать через Интернет» (Рисунок 16).



---

Версия 3.7.0-582985  
Аппаратная платформа: ViPNet IDS NS VA  
Имя сенсора: ViPNet IDS NS VA 251530290  
© 2020, АО «ИнфоТекС»

По всем возникающим вопросам обращайтесь в компанию ИнфоТекС:

Веб-сайт: [www.infotecs.ru](http://www.infotecs.ru)

E-mail: [soft@infotecs.ru](mailto:soft@infotecs.ru)

Телефон для регионов России: 8 800 250-0-260

Телефон для Москвы: +7 495 737-61-92

---

#### ИНФОРМАЦИЯ О ЛИЦЕНЗИИ

Идентификатор лицензии	3203978/1/1-IDSNS
Срок действия лицензии	до 20.04.2024
Подписка на обновление правил обнаружения	до 20.04.2024
Подписка на обновление базы Malware detection	до 20.04.2024

> [ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ](#)

Рисунок 17 – Информация о продукте с активированной лицензией

### 3 Инструкция по установке БРП

В боковом списке перейти в раздел «Правила анализа», далее в меню «Настройка» выбрать пункт «Обновить базу правил» (Рисунок 18).

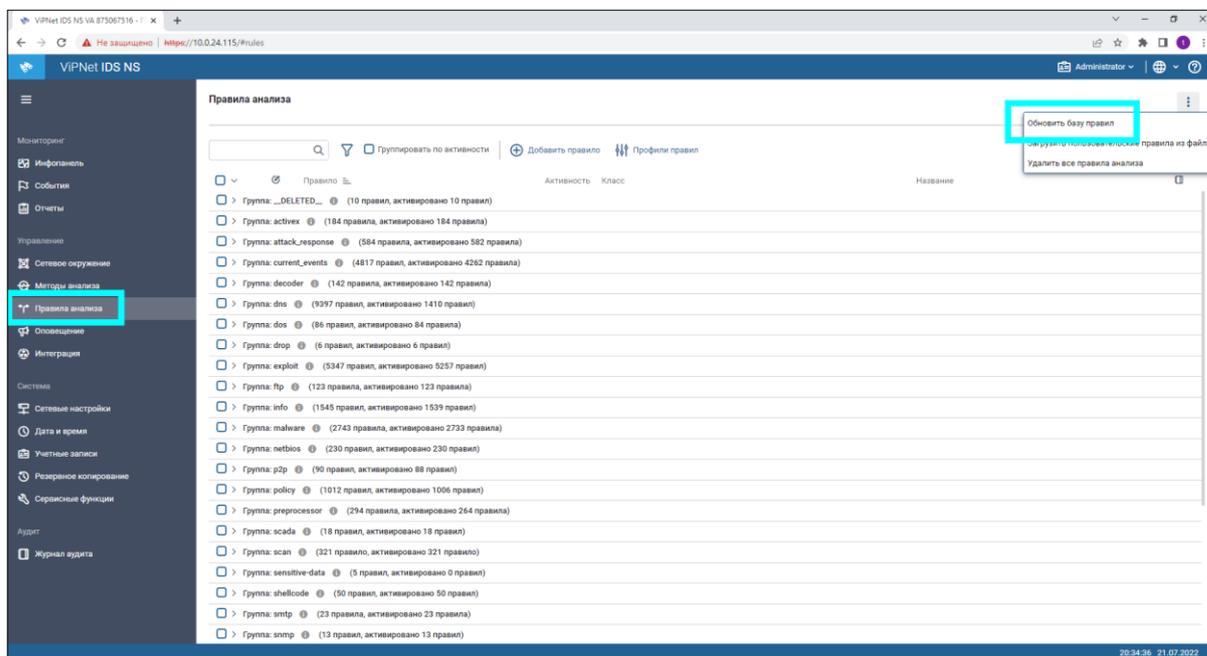


Рисунок 18 – Обновление баз правил

В диалоговом окне «Загрузка файла» нажать на иконку папки, чтобы выбрать файл обновления БРП (Рисунок 19).

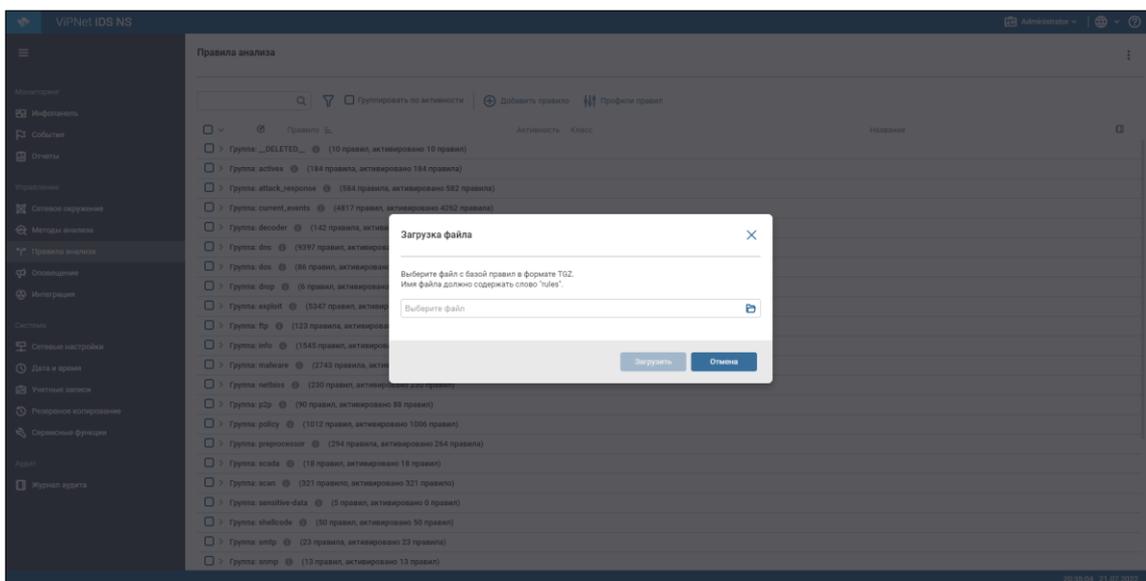


Рисунок 19 – Обновление баз правил

С помощью диалогового окна операционной системы (на примере представлено окно Microsoft Windows 10) загрузить файл (Рисунок 20).

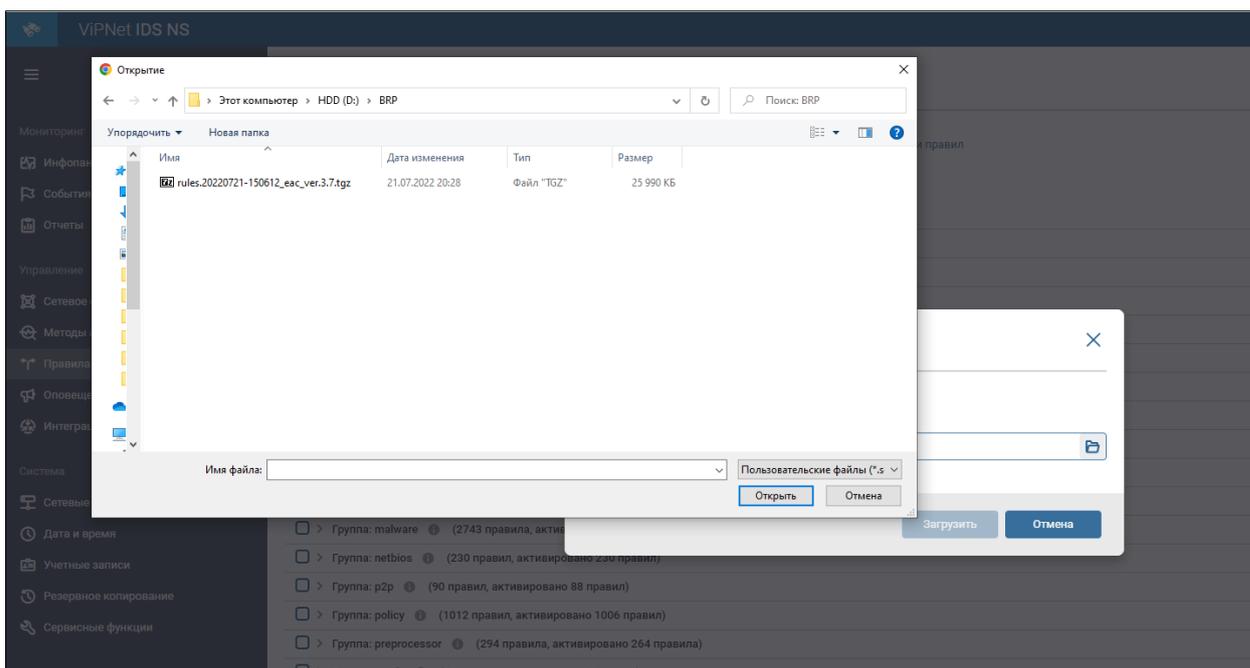


Рисунок 20 – Обновление баз правил

#### **4 Инструкция по установке AM Ruleset Analyzer**

AM Ruleset Analyzer не требует установки (является портативным ПО).