ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

АКЦИОНЕРНОЕ ОБЩЕСТВО «ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ»

(АО «ПМ»)

БАЗА ДАННЫХ СИГНАТУРНЫХ ПРАВИЛ ОБНАРУЖЕНИЯ АТАК AM RULES

Эксплуатация прикладного ПО AM Ruleset Analyzer

На 8 листах

Москва 2023

Аннотация

Настоящий документ описывает эксплуатационные характеристики прикладного программного обеспечения AM Ruleset Analyzer.

Содержание

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

В настоящем документе применяют следующие сокращения:

АО «ПМ»	Акционерное общество «Перспективный мониторинг»
БРП	База данных сигнатурных правил обнаружения атак AM Rules

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 «Ampire».

Программное обеспечение AM Ruleset Analyzer предназначено для визуализации характеристик состава БРП, таких как, например, категории правил, их количество, распределение по профилям защиты.

2 Работа с AM Ruleset Analyzer

Порядок работы с AM Ruleset Analyzer:

– запустить исполняемый файл «AM Ruleset Analyzer.exe»;

– нажать на кнопку «Выберите БРП» (Рисунок 1);

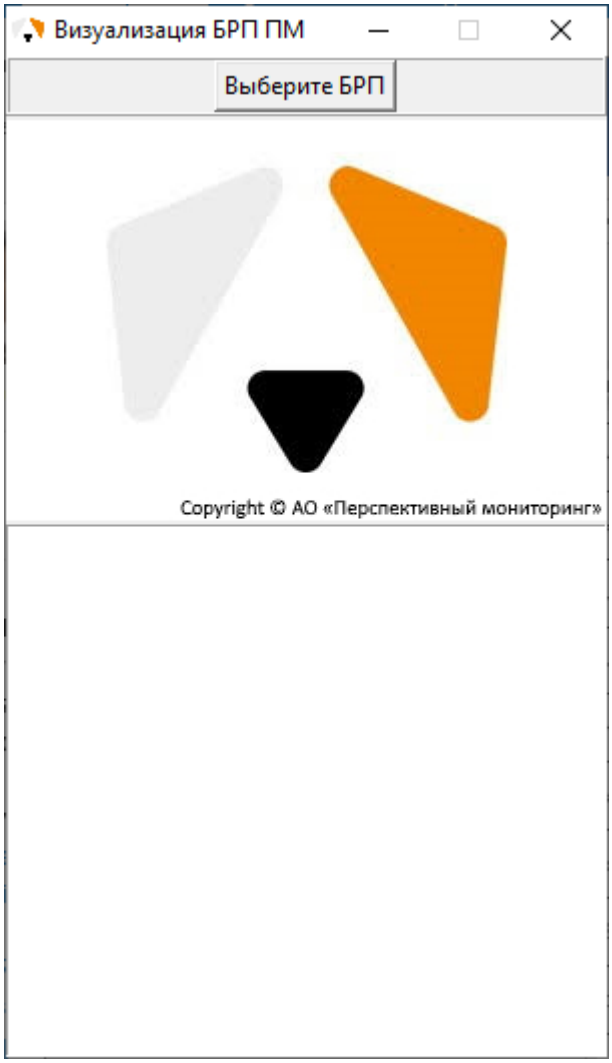

Рисунок 1 – Интерфейс визуализатора

– в диалоговом окне выбрать БРП, для которой необходимо сформировать отчет (Рисунок 2);

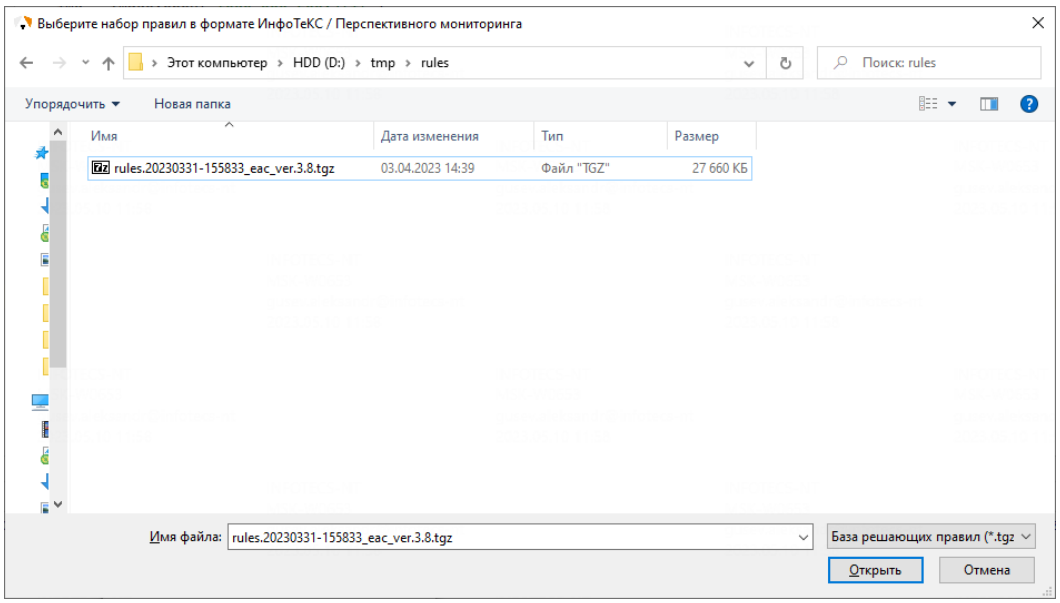

Рисунок 2 – Диалоговое окно выбора БРП

– секция прогресса информирует пользователя о текущем состоянии составления отчета. Отчет будет сохранен в той же директории, что и БРП. Также визуализатор автоматически осуществит попытку открытия итогового pdf-файла в прикладном ПО, которое выбрано в настройках операционной системы (Рисунок 3);

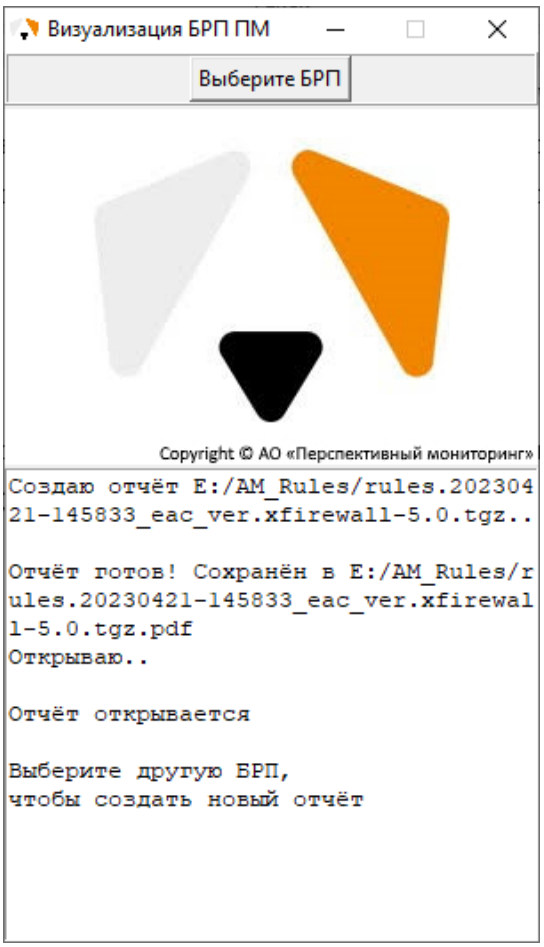

Рисунок 3 – Интерфейс визуализатора

– при необходимости пользователь может построить новый отчет без перезапуска ПО.