УДК [004.056+003.26] (075.8)

Студ. Г.В. Булгак
Науч. рук. проф. П.П. Урбанович
(Кафедра информационных систем и технологий, БГТУ)

WEB-ПРИЛОЖЕНИЕ УПРАВЛЕНИЯ СИСТЕМОЙ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Средства управления системой обнаружения вторжений (СОВ) играют важную роль в решении проблемы защиты информационных ресурсов [1].

Разработано web-приложение, которое позволяет объединить многие детали и упростить работу с СОВ. Программа разработана с целью помочь организациям (системным администраторам, специалистам по информационной безопасности и др.) контролировать систему обнаружения вторжений, а также следить за информационными событиями в сети.

Системы данного типа хранят информацию об активности в следующем виде [2]:

– временной штамп;

– тип события;

– тип протокола;

– сетевой адрес источника;

– сетевой адрес принимающей стороны.

Это минимальный набор информации. На самом деле могут быть и другие поля в зависимости от события.

Основные требования для данного вида средств включают: управление правилами, просмотр событий, управление конфигурацией системы обнаружения вторжений.

На данный момент таких продуктов существует немного. Есть простые системы, функционал которых позволяет только настраивать правила. Есть более сложные, которые позволяют, например, строить различные графики по событиям в сети, интегрироваться с системами для визуализации, осуществлять конфигурирование системы и так далее.

При выборе платформы учитывалась ее совместимость с операционной системой Windowsи простота её использования. Данным критериям отвечает платформа ASP.NET. Одно из главных преимуществ *ASP.NET* в сравнении с другими платформами создания веб приложений – это бесплатная доступность полноценных инструментов программирования. Ни одно бесплатное приложение для других

веб-технологий не сравниться с возможностями и удобством работы с инструментами для *ASP.NET*

Среди многочисленных доступных для работы языков был выбран C#.

Для создания актуального приложения необходимо ознакомиться с существующими аналогами управления СОВ. Это поможет понять, в каком функционале нуждаются пользователи, как он устроен, а также подметить их недостатки, чтобы не допустить их в своей работе. Основное различие между двумя популярными продуктами Suricata и Snort заключается в наличии у первого возможности использования графического процессора для вычислений в режиме системы обнаружения вторжений. Более того система Suricata [3] уже имеет достаточно большую базу правил и написана с использованием современных технологий. Она изначально рассчитана на многопоточность, в то время как Snort – продукт однопоточный. Для аутентификации и авторизации используется фреймворк Identity.

При реализации визуальной части использовался язык JavaScript. В качестве СУБД – MS SQL Server вкупе с Entity Framework, выступающим в роли ORM-инструмента для связи базы данных с платформой веб-приложения.

При выборе СУБД для разрабатываемого приложения рассматривались следующие характеристики MS SQL Server:

1. Надежность и безопасность.
2. Масштабируемость.
3. Производительность.
4. Инструменты управления.
5. Поддержка технологий XML, JSON.

В целом, MSSQL Server является надежным, масштабируемым и производительным решением для управления базами данных, которое предоставляет множество инструментов для управления и поддержки баз данных, а также поддержку многих технологий.

Разработанное приложение представляет собой web-сервер на ASP.NET, который работает на IIS и использует операционную систему WindowsServer 2019. Для начала работы с приложением необходимо пройти авторизацию. Всю информацию о пользователях хранит фреймворк Identity в базе данных MSSQLServer. Приложение предоставляет возможность работы с файлами системы обнаружения вторжений посредством интерфейса web-браузера GoogleChrome. На рис.1 приведена схема архитектура приложения.

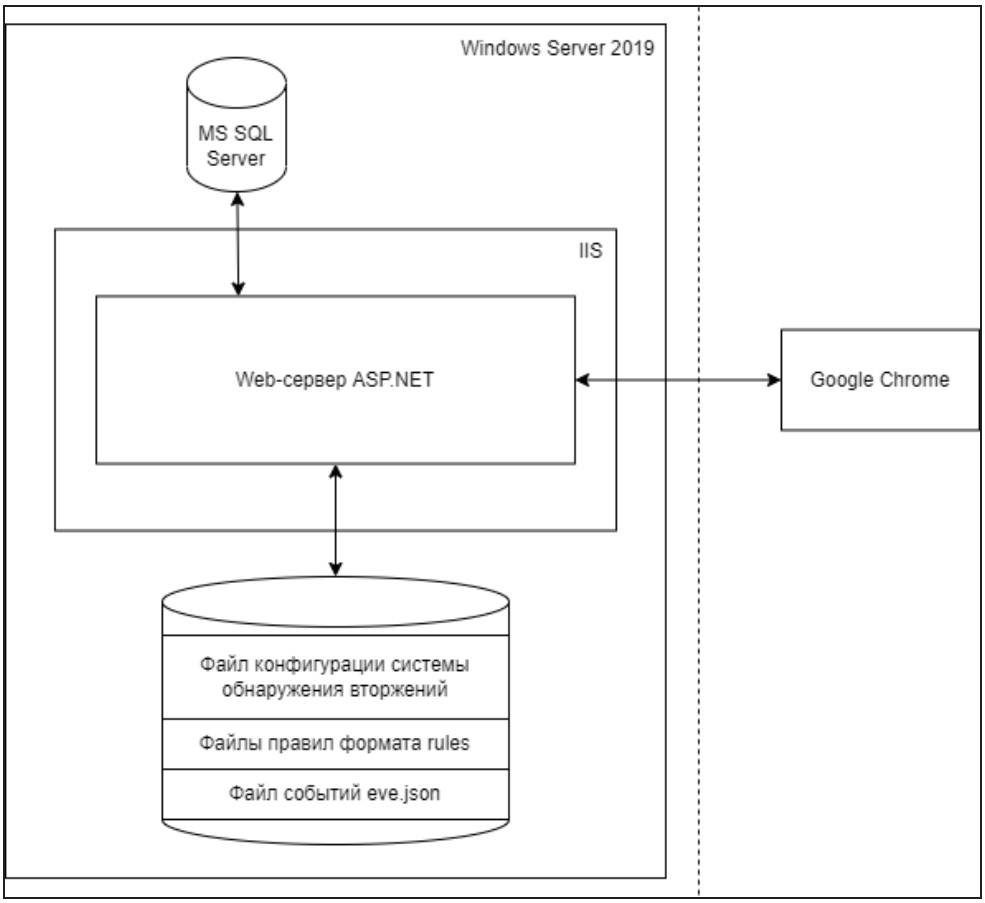

Рисунок 1 - Архитектуры приложения

Таким образом, разработанная система отвечает основным требованиям средств управления системой обнаружения вторжений. Она может использоваться для эффективного управления и помогать в защите инфраструктуры компании.

ЛИТЕРАТУРА

1. Урбанович, П. П. Защита информации: конспект-лекция, ч. 2 = Information Protection, Part 2: BASIC METHODS / П. П. Урбанович. – Минск: БГТУ, 2019. – 34 с. – на англ. яз.

2. Khraisat, A., Gondal, I., Vamplew, P. et al. Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecur 2, 20 (2019). https://doi.org/10.1186/s42400-019-0038-73.

3. Документация по Suricata [Электронный ресурс]. – Режим доступа: https://suricata.readthedocs.io/en/latest/ – Дата доступа: 25.03.2023.

4. Документация по Bootstrap [Электронный ресурс]. – Режим доступа: https://getbootstrap.com/docs/5.3/ Дата доступа:27.03.2023.