**УДК 005.3**

# ИСПОЛЬЗОВАНИЕ СИСТЕМЫ CVSS ДЛЯ ОЦЕНКИ УЯЗВИМОСТЕЙ И ПОВЫШЕНИЯ ЗАЩИЩЕННОСТИ WEB-РЕСУРСОВ НЕФТЕПЕРЕРАБАТЫВАЮЩИХ ПРЕДПРИЯТИЙ

***И. О. ПЕТРОЧЕНКО, А. Л. БЕКЕРОВА, канд. пед. наук, доц. А. П. МАТЕЛЕНОК***
*Полоцкий государственный университет имени Евфросинии Полоцкой, Новополоцк, Беларусь*

Современные информационные технологии непрерывно развиваются, что приводит к усложнению архитектуры информационных систем и увеличению числа потенциальных уязвимостей. На фоне роста количества кибератак, нацеленных на нарушение конфиденциальности, целостности и доступности информации, возрастает потребность в эффективных средствах анализа защищенности [1]. Поэтому к числу актуальных задач управления информатизацией на объектах транспортирования, хранения и распределения газа, нефти и нефтепродуктов относится разработка подходов, обеспечивающие системную и количественную оценку выявленных уязвимостей. Для обеспечения системного подхода к решению обозначенной проблемы необходимо написать программное обеспечение основанное на подходе позволяющую проводить системную и количественную оценку выявленных уязвимостей. Одним из таких подходов является Common Vulnerability Scoring System – широко распространенная методика, предназначенная для стандартизированной оценки степени критичности уязвимостей на основе множества факторов. **CVSS** – это стандарт для оценки критичности уязвимостей в информационных системах. С момента своего появления CVSS прошла несколько значительных изменений, адаптируясь к новым вызовам в области кибербезопасности.

Для понимания развития стандарта начнем с третьей версии – CVSS v3.1, которая стала широко применяться благодаря своей простоте и трехуровневой структуре оценки, изображенной на рисунке 1. Однако со временем выявились ограничения этой модели, и для более точной оценки в 2023 году была представлена новая версия – CVSS v4.0

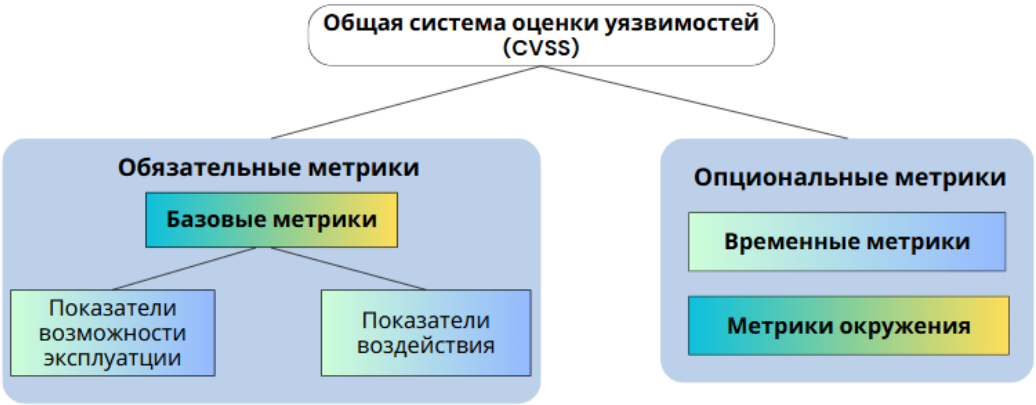


**Рисунок 1. – Метрики CVSS v3.1**

CVSS версии 3.1 использует трехуровневую структуру оценки, включающую следующие группы метрик: базовые (Base Metric Group), временные (Temporal Metric Group) и окружения (Environmental Metric Group).

Переходя к анализу базовых метрик, первой будет рассмотрена метрика «Вектор атаки (AV)». Она отражает степень удаленности потенциального злоумышленника от уязвимого компонента.

Чем менее ограничен доступ к целевой системе и чем дальше может находится атакующий для успешной эксплуатации уязвимости, тем выше уровень риска, что, в свою очередь, увеличивает итоговую оценку критичности. После определения возможной удаленности атакующего, при помощи вектора атаки, важным аспектом остается оценка сложности самой атаки, то есть тех условий, которые должны быть выполнены помимо воли злоумышленника. Эти параметры отражаются в следующей базовой метрике – «Сложность атаки (AC)».

Важной характеристикой, влияющей на успешность эксплуатации уязвимости, является уровень доступа, которым должен обладать злоумышленник до осуществления атаки. Этот параметр оценивается с помощью метрики «Требуемый уровень привилегий (PR)». Она показывает, насколько глубоко атакующий должен быть интегрирован в систему для проведения атаки: от полного отсутствия доступа до административных прав. Чем меньше требуемых привилегий, тем выше потенциальная опасность уязвимости, и, соответственно, выше итоговая оценка. Кроме технических характеристик уязвимости, важным фактором является необходимость участия пользователя в процессе атаки. Данный аспект отражается в метрике «Взаимодействие с пользователем (UI)». Она определяет, может ли злоумышленник выполнить атаку самостоятельно или требуется какое-либо действие со стороны другого пользователя, например, открытие вредоносного файла или установка программы. Отсутствие необходимости взаимодействия с пользователем увеличивает опасность уязвимости, а следовательно – и итоговую оценку. После рассмотрения необходимости участия пользователя в атаке, логично перейти к следующей важному параметру – «Область воздействия уязвимости (S)». Эта метрика отражает, ограничивается ли воздействие уязвимости рамками одного компонента или может распространяться на другие компоненты, находящиеся под управлением различных механизмов безопасности. Метрика «Влияние на конфиденциальность (C)» отражает степень нарушения конфиденциальности при успешной эксплуатации уязвимости. Необходимой метрикой группы воздействия является «Влияние на целостность (I)». Целостность информации означает ее достоверность, неизменность и защиту от несанкционированного изменения. Данная метрика оценивает последствия нарушения целостности в результате успешной атаки и, как и в случае с конфиденциальностью, оказывает влияние на итоговую оценку уязвимости. Наряду с конфиденциальностью и целостностью, третьей ключевой характеристикой, оцениваемой в рамках группы метрик воздействия, является «Влияние на доступность (A)». Доступность означает возможность своевременного и непрерывного доступа к информационным ресурсам системы. Данная метрика отражает последствия для доступности системы или ее компонентов в случае успешной атаки.

Оценка базовых метрик позволяет определить фундаментальную степень критичности уязвимости, исходя из ее технических характеристик. Однако на практике уровень угрозы, связанный с конкретной уязвимостью, может изменяться со временем под влиянием различных внешних факторов. Именно для учета таких изменений в системе CVSS предусмотрена группа временных метрик. Эти метрики учитывают три ключевых аспекта: степень проработанности и доступности эксплойта, наличие официального исправления, а также достоверность информации об уязвимости. Их использование не является обязательным, однако при задании значений временных метрик итоговая оценка становится более точной и реалистично отражает актуальный уровень риска на конкретный момент времени.

Разработанный программный продукт для оценки уязвимостей и повышения защищенности web-ресурсов нефтеперерабатывающих предприятий предоставляет набор функций, обеспечивающих пассивный аудит безопасности веб-приложений, анализ уязвимостей и удобное управление результатами. Ниже перечислены ключевые функции и их назначение:

1. Пассивное сканирование веб-сайта.

Функция scan_website(url) выполняет пассивный анализ веб-приложения путем сбора HTTP-заголовков, выявления используемых технологий (например, CMS или серверное ПО).

2. Расчет CVSS-оценок.

Функция calculate_cvss реализует алгоритм расчета CVSS v3.1, принимая метрики атаки, сложности, прав доступа и влияния, и отображает итоговую оценку риска с категорией в интерфейсе.

3. Поиск уязвимостей в базе NVD.

Функция get_cve_for_tech отправляет запрос к API NVD, используя ключевое слово, основанное на обнаруженной технологии, и возвращает список уязвимостей (CVE) с их идентификаторами и оценками критичности.

4. Проверка SSL/TLS-сертификатов.

Функция check_ssl анализирует SSL/TLS-сертификат веб-приложения, извлекая информацию о его валидности, дате истечения и издателе, что позволяет оценить безопасность сетевого соединения.

5. Анализ HTTP-заголовков.

Функция analyze_headers анализирует HTTP-заголовки, выявляя отсутствие защитных заголовков (например, CSP, HSTS) или наличие уязвимостей, таких как раскрытие информации о сервере.

CVSS Risk Evaluator, разработанный в рамках представленных материалов, ориентирован на пассивный сбор информации и последующий анализ рисков на основе стандарта CVSS. Программа использует открытые источники данных (веб-сайт и API базы NVD), но все вычисления выполняются локально, что обеспечивает автономность, приватность и гибкость оценки. Пользователь получает возможность вручную управлять метриками и просматривать историю сканирований.

## ЛИТЕРАТУРА

1. Саевич, С. Г. Сравнительная характеристика подходов мониторинга и управления компьютерными сетями / С. Г. Саевич, А. П. Мателенок // Наука – образованию, производству, экономике : Материалы 77-й Региональной научно-практической конференции преподавателей, научных сотрудников и аспирантов, Витебск, 28 февраля 2025 года. – Витебск: Витебский государственный университет им. П. М. Машерова, 2025. – С. 43–45. – EDN CLWTHI.