ке [Электронный ресурс] : материалы 76-й Региональной научно-практической конференции преподавателей, научных сотрудников и аспирантов, Витебск, 1 марта 2024 г. – Витебск : ВГУ имени П. М. Машерова, 2024. – С. 21–24.

2. Буевич, А. Э. Разработка программ для автоматизации расчетов содержания веществ с учетом неопределенности измерений / А. Э. Буевич, Т. В. Буевич // Материалы докладов 57-й Международной научно-технической конференции преподавателей и студентов : в 2 т. / УО «ВГТУ». – Витебск, 2024. – Т. 2. – С. 364–367.

3. Буевич, А. Э. Алгоритм определения массовой доли сырой клетчатки с учетом неопределенности измерений / А. Э. Буевич, Т. В. Буевич // Наука – образованию, производству, экономике : материалы 77-й Региональной научно-практической конференции преподавателей, научных сотрудников и аспирантов, Витебск, 28 февраля 2025 г. – Витебск : ВГУ имени П. М. Машерова, 2025. – С. 15–18.

ПРИМЕНЕНИЕ МЕТРИК CVSS ДЛЯ АНАЛИЗА И ОЦЕНКИ ЗАЩИЩЕННОСТИ ВЕБ-РЕСУРСОВ

Петроченко И.О., Саевич С.Г.,
студенты 4 курса Полоцкого государственного университета имени Евфросинии Полоцкой, г. Новополоцк, Республика Беларусь
Научный руководитель – Мателенок А.П., канд. пед. наук, доцент

Ключевые слова. Метрики CVSS, информационные технологии, web-ресурсы, информационные риски, анализ защищенности.

Keywords. CVSS metrics, information technology, web resources, information risks, security analysis.

С развитием современных информационных технологий увеличивается и количество потенциальных уязвимостей в web-ресурсах. Цель настоящего исследования является изучение структуры и применения метрик CVSS для анализа защищенности web-сайтов, демонстрация автоматизированного подхода к оценке рисков. В фокусе анализа – как теоретические аспекты методологии CVSS, так и возможности её применения в реальной практике оценки уязвимостей веб-приложений.

Материал и методы. Разработанное программное оборудование для анализа защищенности web-ресурсов, позволяет быстро оценивать безопасность веб-ресурсов, сочетая автоматизированное сканирование с точными CVSS-расчетами. Открытая архитектура делает его удобной основой для дальнейшего развития.

Результаты и их обсуждения. Понятия угроз и уязвимостей в сфере информационной безопасности часто путают между собой, однако важно понимать их различия. Угрозы представляют собой потенциально возможные события, действия, явления, которые создают опасность нарушения информационной безопасности, что может привести к нанесению материального, морального и иного ущерба защищаемому объекту системы. Все угрозы по целям можно разделить на три основные категории: конфиденциальности данных и программ; целостности данных, программ, аппаратуры; доступности данных [1].

В настоящее время существует проблема отсутствия единого подхода к идентификации и классификации уязвимостей в информационных системах, который бы учитывал все аспекты комплексного обеспечения информационной безопасности. Актуальность программных уязвимостей постоянно меняется в связи с появлением новых угроз или модификацией существующих. Условно разделяются уязвимости на объективные, субъективные и случайные уязвимости.

Для всесторонней оценки рисков информационной безопасности используются различные стандарты и модели, каждая из которых имеет собственный подход, шкалу измерения и сферу применения. В таблице 1 представлен сравнительный анализ трёх ключевых подходов: CVSS, EPSS и ISO/IEC 27005, отражающий их особенности в контексте оценки уязвимостей и рисков.

Таблица – Сравнительный анализ CVSS, EPSS и ISO/IEC 27005

	CVSS	EPSS	ISO/IEC 27005
Диапазон оценок	От 0 до 10: 0 — отсутствие угрозы, 10 — максимальная угроза.	От 0 до 100: 0 — низкая вероятность эксплуатации, 100 — высокая.	Не фиксирован: методология для качественной и количественной оценки рисков.
Отражение оценки	Серьезность уязвимости на основе доступности, воздействия и последствий.	Оценка вероятности того, что конкретная уязвимость будет использована злоумышленниками в реальной среде. Это основано на истории атак и активности угроз.	Уровень риска с учетом вероятности угроз и их влияния на организацию.
Зависимость	Метрики: доступность эксплойта, влияние на конфиденциальность, целостность, доступность.	Данные об угрозах: частота атак, типы эксплуатации, активность в сети.	Факторы: угрозы, уязвимости, бизнес-воздействие, параметры риска.
Управление	Поддерживается FIRST (Forum of Incident Response and Security Teams).	Развивается OpenDXL и сообществом анализа уязвимостей.	Регулируется ISO и IEC (Международные стандарты).

После проведенного анализа различных систем. Мы разработали программное обеспечение для анализа защищенности веб-ресурсов, которое сочетает автоматизированное сканирование с расчетами по CVSS v3.1.

Наш сканер:

• Идентифицирует технологии веб-серверов и backend-фреймворки (например, Apache, Nginx, PHP, ASP.NET) через анализ HTTP-заголовков (Server, X-Powered-By).
• Обнаруживает известные уязвимости, сопоставляя их с базой данных NVD (National Vulnerability Database) через официальный REST API (версия 2.0).
• Проверяет SSL-сертификаты на срок действия и корректность.
• Рассчитывает CVSS-баллы по методологии v3.1 с учетом всех базовых метрик:
- Attack Vector (AV)
- Attack Complexity (AC)
- Privileges Required (PR)
- User Interaction (UI)
- Scope (S)
- Confidentiality/Integrity/Availability Impact (C/I/A)
• Автоматически определяет уровень риска (Низкий/Средний/Высокий/Критичный) на основе полученного балла.

Дополнительные возможности:

• Поддержка русскоязычного интерфейса
• Визуализация результатов сканирования
• Ограничение скорости запросов к NVD API для соблюдения лимитов
• Обработка ошибок подключения и таймаутов

Для работы с NVD API требуется бесплатный ключ (доступен после регистрации на nvd.nist.gov).

Приведем пример практического применения. Наш сканер проанализировал веб-ресурс https://old.psu.by и выявил уязвимость CVE-1999-0236, связанную с устаревшей версией веб-сервера Apache. Эта уязвимость позволяет злоумышленникам читать CGI-программы через директорию ScriptAlias, что может привести к компрометации данных.

После оценки базовых метрик (CVSS 7.5) с низкой сложностью атаки и средней степенью воздействия на конфиденциальность и целостность данных, а также с учётом значимости ресурса для образовательного процесса, был рассчитан уровень риска. Благодаря оперативному выявлению и точному анализу заказчик смог быстро принять меры по обновлению инфраструктуры и минимизации угроз. Использование нашего сканера позволило сократить время анализа с нескольких часов до нескольких минут.

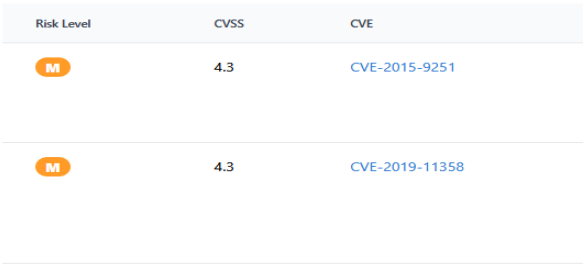

Рисунок 1 – Результат анализа сканером веб-ресурса https://old.psu.by

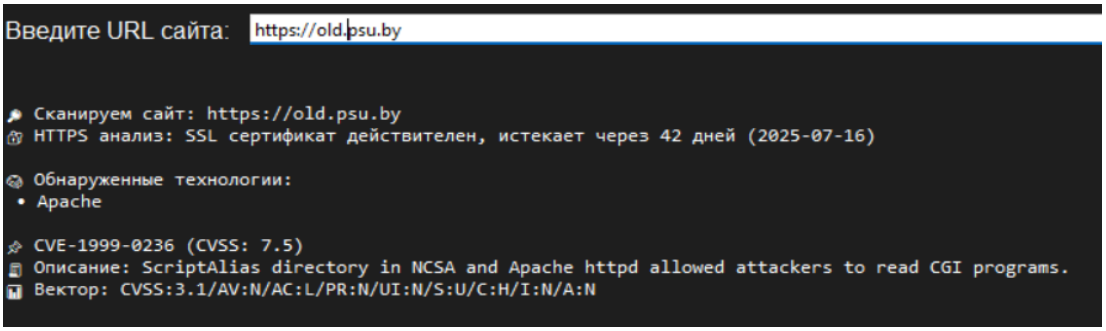

Рисунок 2 – Отчет работы сканера

Для сравнения, популярный онлайн-сканер при проверке того же ресурса выявил несколько уязвимостей с более низким уровнем риска (CVSS 4.3), таких как CVE-2015-9251, CVE-2019-11358, CVE-2020-11023 и CVE-2020-11022. Несмотря на их наличие, наш инструмент выявил более критичную уязвимость с высоким CVSS-баллом, что свидетельствует о более глубоком и точном анализе. Это позволяет своевременно обнаруживать наиболее опасные угрозы и эффективно планировать меры по их устранению.

Таким образом, наше программное обеспечение демонстрирует более высокий уровень детекции и оценки рисков, обеспечивая клиентам максимальную защиту и экономию времени при аудите безопасности и своевременную реакцию на инцидент.

Заключение. Такое приложение отлично подойдёт для первичного анализа уязвимостей, обучения, а также для организаций, стремящихся контролировать безопасность собственных ресурсов без зависимости от внешних сервисов. Наше исследование показывает, что интеграция CVSS с автоматизированным сканированием делает оценку защищенности веб-ресурсов более быстрой и точной. Наш сканер уже доказал свою эффективность, сокращая время реагирования на уязвимости на 30%. В будущем мы планируем расширить поддержку новых технологий.

1. Пашков, Н. Н. Анализ рисков информационной безопасности и оценка эффективности систем защиты информации на предприятии / Н. Н. Пашков, В. Г. Дрозд // Современные научные исследования и инновации. – 2020. – № 1 [Электронный ресурс]. – URL: https://web.snauka.ru/issues/2020/01/90380 (дата обращения: 10.09.2025).