DOI 10.36622/1682-7813.2024.27.4.006
УДК 621.372.004

ОЦЕНКА КРИТИЧНОСТИ УЯЗВИМОСТЕЙ С ИСПОЛЬЗОВАНИЕМ ДАННЫХ МНОЖЕСТВА РИСК-КАЛЬКУЛЯТОРОВ

А.А. Остапенко, В.П. Шелякин, Е.С. Короткова, А.С. Кривошеин, Д.А. Мальцева, П.А. Меркулов, Н.Д. Никитин, М.О. Титаренко

Статья посвящена исследованию методов оценки критичности уязвимостей в автоматизированных информационных системах (АИС) и телекоммуникационных сетях (ТКС) с использованием множества риск-калькуляторов. Рассматриваются существующие подходы к анализу критичности уязвимостей, такие как CVSS, SSVC, EPSS, VISS, OWASP Risk Rating Calculator, BVSS и HVSS. Проведен сравнительный анализ их метрик и алгоритмов, выявлены преимущества и ограничения каждого из калькуляторов. Научно-техническая задача исследования заключалась в разработке аналитических выражений для расчёта критичности уязвимостей. Полученные результаты могут быть полезны для повышения эффективности управления киберрисками и оптимизации процессов обеспечения информационной безопасности.

Ключевые слова: риск-калькулятор, CVSS, SSVC, EPSS, VISS, OWASP, BVSS, HVSS, уязвимость, критичность, кибератака.

Введение

В условиях современного цифрового развития кибератаки представляют собой одну из наиболее серьезных угроз как для юридических, так и физических лиц. С ростом объемов обрабатываемой информации предприятия становятся все более уязвимыми к таким атакам. В ответ на этот вызов появляются разнообразные инструменты и методы для оценки уязвимостей и защиты информационных систем, среди которых выделяются калькуляторы критичности уязвимостей, помогающий определить степень риска и соответствующие меры безопасности [1-12].

Однако множество существующих калькуляторов часто подвергаются критике за недостаточную объективность, поскольку их оценки зависят от разноплановых моделей и алгоритмов, которые не всегда учитывают всю сложность проектной ситуации.

Объектом исследования данной статьи являются киберугрозы и процессы эксплуатации уязвимостей в автоматизированных информационных системах (АИС) и телекоммуникационных сетях (ТКС). Предмет исследования включает методы и инструменты для оценки критичности, в частности с использованием множества калькуляторов критичности.

Цель работы заключается в комплексной оценке критичности уязвимостей. Научно-техническая задача данной работы состоит в анализе существующих подходов к расчёту критичности и разработке аналитических выражений, позволяющих оценивать её с использованием данных множества калькуляторов.

Анализ особенностей известных риск-калькуляторов

В контексте обеспечения кибербезопасности оценка уровня опасности уязвимостей стала одной из ключевых задач для организаций, стремящихся защитить свои информационные системы и данные. С учетом роста числа киберугроз и их сложности, предприятиям необходимо использовать эффективные инструменты и методики для выявления, анализа и оценки критичности уязвимостей. В этом контексте существует множество ресурсов и стандартов, и в данной статье будут рассмотрены и проанализированы следующие из них: CVSS (Common Vulnerability Scoring System) версии 3.1 и 4.0

[1,4-5], SSVC (Structured Shielding/Defense/Analysis of Vulnerability Exposure) [2], EPSS (Exploit Prediction Scoring System) [3], VISS (Vulnerability Impact Scoring System) [6,7], OWASP Risk Assessment Calculator [11], BVSS calculator (blockchain vulnerability scoring system) [8], Healthcare Vulnerability Scoring System (HVSS) Version 1.0 Calculator[9,10], Red Hat [12].

1. CVSS (Common Vulnerability Scoring System) версии 3.1 – механизм документирования и оценки основных технических аспектов уязвимостей, обнаруженных в различных типах программно-аппаратного обеспечения. Система генерирует числовые индикаторы, которые определяют уровень опасности конкретной уязвимости. Основные метрики системы охватывают внутренние параметры уязвимости, которые остаются неизменными на протяжении времени и в различных пользовательских условиях. К ним относятся:

- вектор атаки (качественная оценка (далее-КО) – Сетевой (N), Смежная сеть (A), Локальный (L), Физический (P));
- сложность атаки (КО – Высокая (H), Низкая (L));
- уровень привилегий (КО – Высокий (H), Низкий (L), Не требуется (N));
- взаимодействие с пользователем (КО – Требуется (R), Не требуется (N));
- влияние на другие компоненты системы (КО– Не оказывает (U), Оказывает (C));
- влияние на конфиденциальность, целостность и доступность (КО – Не оказывает (N), Низкое (L), Высокое (H)).

Группа временных метрик системы отражает характеристики уязвимости, которые изменяются со временем и не зависят от условий использования. Например, наличие удобного набора эксплойтов может повысить оценку CVSS, в то время как выпуск официального патча может привести к её снижению. В частности, временные метрики включают:

- доступность средств эксплуатации (КО – Не определено (X), Высокая (H), Есть сценарий (F), Есть PoC-код (P), Теоретическая (U));
- доступность средств устранения (КО – Не определено (X), Недоступно (U), Рекомендации (W), Временное (T), Официальное (O));
- степень доверия к информации об уязвимости (КО – Не определено (X), Подтверждена (C), Достоверные отчеты (R), Отчеты (U)).

Группа контекстуальных (экологических) метрик включает характеристики уязвимости, важные и специфичные для определенной пользовательской среды. К ним относятся факторы, такие как наличие средств безопасности, способных смягчить последствия успешной атаки, а также относительная значимость уязвимой системы в общей технологической инфраструктуре. В частности, контекстуальные метрики включают:

- требования к конфиденциальности, целостности и доступности (КО – Не определено (X), Низкие (L), Средние (M), Высокие (H));
- вектор атаки (корр.), сложность атаки (корр.), уровень привилегий (корр.), взаимодействие с пользователем (корр.), влияние на другие компоненты системы (корр.), влияние на целостность (корр.), конфиденциальность (корр.) и доступность (корр.) – КО данных метрик такие же, как в базовой и временной группе показателей.

В версии 4.0 системы оценки уязвимостей CVSS (Common Vulnerability Scoring System) были добавлены новые метрики, связанные с облачными технологиями, мобильными устройствами и Интернетом вещей (IoT). Также была обновлена методология расчета оценок CVSS для повышения их точности и адаптивности. CVSS 4.0 классифицирован на три категории метрик: базовые, временные и контекстные. Базовые метрики оценивают серьезность уязвимости, игнорируя специфические контексты или условия, и включают в себя:

1) вектор атаки,
2) сложность атаки,
3) требуемые привилегии,
4) влияние на конфиденциальность целостность и доступность.

Временные метрики используются для определения степени серьезности уязвимости, принимая во внимание период, который прошел с момента её выявления или публикации, и включают:

1) эксплуатируемость,
2) уровень оповещения.

Экологические метрики анализируют степень серьезности уязвимости, принимая во внимание специфические контексты или обстоятельства:

1) влияние на безопасность,
2) влияние на целостность,
3) влияние на доступность.

Значения метрик служат для вычисления оценки CVSS, которая варьируется от 0 до 10, где 0 указывает на отсутствие значительной угрозы, а 10 обозначает крайне серьезную угрозу. Уровни рейтинга в CVSS 4.0 устанавливаются на основе значений базовых, временных и экологических метрик. Более высокие значения этих метрик приводят к увеличению оценки CVSS и соответствующего уровня рейтинга. Всего выделяют 4 уровня:

1. Низкий (Low): 0.1-3.9.
2. Средний (Medium): 4.0-6.9.
3. Высокий (High): 7.0-8.9.
4. Критический (Critical): 9.0-10.0.

CVSS-калькулятор пользуется большой популярностью, он лежит в основе многих калькуляторов (HVSS, EPSS и др.) и широко применяется, так как он стандартизирован, универсален и его оценки позволяют сравнивать уязвимости между собой и определять приоритеты.

Система оценки общей уязвимости (CVSS) не совсем корректно используется для приоритизации уязвимостей и оценки рисков, ибо ее алгоритм не имеет обоснования. Это приводит к субъективности выводов и делает систему неадекватной. Определения атак «Сеть» и «Локальный» нечеткие и противоречивые. Критерии сложности атаки слабо структурированы и не отражают реальную степень риска. Концепция Scope запутывает оценки. Удаленные уязвимости не могут иметь оценку ниже 5,0, что создает искажения. Использование CVSSv2 и CVSSv3 приводит к «инфляции» оценок, увеличивая нагрузку на администраторов.

2. SSVC (Structured Shielding/ Defense/Analysis of Vulnerability Exposure) – это методология для оценки и приоритизации уязвимостей, ориентированная на специфические потребности различных заинтересованных сторон (например, ИТ-администраторов, разработчиков, менеджеров). В отличие от CVSS (Common Vulnerability Scoring System), который присваивает числовые баллы уязвимостям. SSVC направлен на рекомендации по конкретным действиям и позволяет организациям быстрее принимать осмысленные решения о том, как реагировать на уязвимости, опираясь на контекст и приоритеты бизнеса.

Основное отличие механизма SSVC от CVSS заключается в том, что SSVC представляет собой дерево решений вместо числового уравнения. На каждом уровне дерева (например, эксплуатация, автоматизация) представлены альтернативные уровни переменной, а на листьях указаны три возможные реакции на уязвимость: отслеживать, участвовать или действовать.

Однако SSVC имеет более простую модель причинно-следственных связей, чем CVSS, что может быть её недостатком. Ранее критиковали CVSS за ее недостаточную детализацию, ибо SSVC упрощает восемь переменных CVSS до четырех. Например, три переменные CVSS (Конфиденциальность, Целостность и Доступность) можно объединить в одну переменную SSVC — Mission & Well-Being.

Дерево CISA SSVC определяет решения Track, Track *, Attend и Act на основе пяти значений:

1. Статус эксплуатации.
2. Автоматизация эксплуатации.
3. Техническое воздействие.
4. Распространенность миссии.
5. Влияние на общественное благосостояние.

CISA использует собственную модель дерева решений SSVC для приоритизации соответствующих уязвимостей по четырем возможным решениям:

Track: Уязвимость не требует немедленных действий. Организация будет мониторить ситуацию и пересматривать

статус при появлении новой информации. CISA рекомендует устранять такие уязвимости в установленные сроки обновления.

Track *: Данная уязвимость имеет характеристики, требующие внимательного наблюдения. CISA советует устранить ее в стандартные сроки обновления.

Attend: Уязвимость требует внимания руководства организации. Необходимы действия, такие как запрос информации или помощь, а также публикация уведомления как внутри, так и снаружи организации. CISA рекомендует устранение уязвимостей Attend раньше стандартных сроков обновления.

Act: Уязвимость требует немедленного внимания со стороны руководства и высших должностных лиц. Действия включают запрос информации, помощь и публикацию уведомлений внутри и вокруг организации.

Так как SSVC не имеет строгих формул, важно использовать экспертные мнения и данные о конкретной среде для определения значений вышеуказанных метрик.

SSVC набирает популярность, особенно среди организаций, которые работают с высокими требованиями к безопасности, такими как государственные структуры и крупные компании, ориентированные на минимизацию рисков и оперативное управление уязвимостями. Причины популярности таковы:

1. Адаптивность под нужды организации: SSVC предлагает рекомендации, адаптированные к специфическим требованиям и ролям пользователей;
2. Упрощение принятия решений: методика помогает быстрее находить приоритеты и действовать без долгих расчетов;
3. Удобство для разных заинтересованных сторон: инструмент подходит для всех уровней организации: от ИТ-специалистов до руководства.

Как и у любого метода, у SSVC есть свои ограничения:

1. Отсутствие числовой оценки: для некоторых организаций это может быть неудобным, так как не дает единой метрики для сравнения, как в CVSS.
2. Сложности адаптации: для организаций с традиционными подходами переход на SSVC может потребовать адаптации и индивидуальной настройки для разных ролей и процессов.
3. Неоднозначность категорий: решения, такие как "наблюдать" или "ожидать", могут показаться слишком обобщенными, особенно для менее опытных специалистов.

SSVC предлагает более гибкий и контекстно-ориентированный подход, чем CVSS, и позволяет принять решение на основе специфических условий и ролей. Этот метод особенно эффективен для организаций с высокими требованиями к безопасности и индивидуальным управлением рисками, но требует времени на адаптацию и обучения специалистов для его полной эффективности.

3. EPSS (Exploit Prediction Scoring System) представляет новый подход к оценке уязвимостей, отличающийся от большинства систем. Вместо перехода от причины к оценке, EPSS использует обратный метод, основываясь на фактических результатах. В отличие от CVSS и SSVC, EPSS не включает номинальные компоненты, а его эффективность обусловлена качеством данных.

EPSS основывается на статистических моделях, которые используют данные об уязвимостях, связанных с ними событиях и факторах риска. Основное внимание уделяется байесовским моделям вероятности, анализа взаимосвязей между уязвимостями и данными о нападениях. Принцип работы включает в себя следующее.

1. Сбор данных: EPSS анализирует множество параметров уязвимостей, таких как тип уязвимости, связанные CVE (Common Vulnerabilities and Exposures) коды, а также внешние данные – отчёты о случаях эксплуатации и активности угроз.

2. Обработка факторов риска: система использует факторы, связанные с эксплойтами, такие как наличие уязвимостей в открытых источниках, информация о патчах, и данные об активности злоумышленников. Важными метриками также являются сложность эксплуатации и степень потенциального ущерба.

3. Моделирование и предсказание: EPSS оценивает вероятность того, что уязвимость

будет использована в течение определённого времени (как правило, 30 дней), и выдаёт оценку на основе вероятностных моделей. В EPSS шкала измерения колеблется от 0 до 1.

Пять основных факторов, влияющих на результаты EPSS таковы:

1) уязвимый код,
2) запись в базе данных Exploit,
3) количество ссылок в Национальной базе данных уязвимостей,
4) поставщик – есть ли Microsoft среди них,
5) наличие эксплойта в Metasploit.

Важно отметить, что EPSS не предлагает четкой причинно-следственной модели. Например, указание на Microsoft может означать популярность ПО, медленное обновление клиентами или слабую безопасность.

Произвольные границы в оценке могут привести к различиям в обработке схожих уязвимостей. Например, при пороге 0,5 уязвимости с вероятностями 0,499 и 0,501 будут оцениваться одинаково, что может привести к потере информации.

Многие организации используют EPSS в сочетании с системой CVSS (Common Vulnerability Scoring System) для лучшей оценки уязвимостей и принятия решений о внедрении патчей или других защитных мер.

Несмотря на полезность EPSS, у системы есть и недостатки:

1. Ограниченность данных: EPSS полагается на доступные данные об уязвимостях и случаях их эксплуатации, что может ограничивать её точность для менее известных уязвимостей.

2. Не учёт особенностей инфраструктуры: EPSS не принимает во внимание уникальные черты IT-инфраструктуры отдельной организации, включая специфические сетевые конфигурации, что может привести к снижению точности оценки в контексте конкретных условий.

3. Вероятностный подход: модель EPSS оценивает только вероятность эксплуатации, а не её потенциальные последствия, поэтому решение, основанное только на её оценке, может быть недостаточно комплексным.

4. Ограниченная интеграция с другими инструментами: хотя EPSS активно внедряется, её интеграция с популярными инструментами безопасности и платформами пока развита слабо.

4. VISS (Vulnerability Impact Scoring System**)** - это система для оценки последствий эксплуатации уязвимостей, ориентированная на анализ и классификацию уязвимостей с целью оценки уровня риска и потенциального ущерба от их эксплуатации. Она представляет собой альтернативу более известной CVSS (Common Vulnerability Scoring System), но акцентируется на оценке влияния уязвимости на конкретные системы и инфраструктуры.

VISS нализирует тринадцать аспектов воздействия уязвимостей, сгруппированных по категориям, связанным с платформой, инфраструктурой и данными. Это позволяет получить оценку воздействия, которая варьируется от 0 до 100. Эта оценка может быть скорректирована с помощью метрики компенсирующих мер, которые учитывают существующие меры безопасности и их влияние на уязвимость. Итоговая оценка представлена в виде векторной строки – сжатого текстового представления показателей и их значений, используемых для расчета. Как и в CVSS, каждому значению метрики соответствует определенное десятичное значение, что позволяет стандартизировать и облегчить понимание уровня риска, связанного с конкретной уязвимостью, и способствует более эффективному управлению безопасностью:

1. Влияние на PLI – платформу. Этот показатель позволяет пользователю указать тип вычислительной платформы, затронутой уязвимостью безопасности, независимо от того, где была обнаружена уязвимость.

2. Влияние ICI – платформы на конфиденциальность. Эта метрика позволяет пользователю указать влияние на конфиденциальность платформы в результате успешной эксплуатации обнаруженной уязвимости.

3. III – Влияние на целостность платформы. Эта метрика позволяет пользователю оценить влияние на целостность платформы в результате успешной эксплуатации обнаруженной уязвимости.

4. Влияние доступности платформы IAI. Эта метрика позволяет пользователю оценить влияние на доступность платформы в результате успешной эксплуатации обнаруженной уязвимости.

5. ITN – аренда инфраструктуры. Эта метрика позволяет пользователю определить, в какой инфраструктуре была обнаружена уязвимость. Значения этой метрики учитываются только при наличии определенного уровня воздействия на платформу.

6. STN – аренда программного обеспечения. Эта метрика позволяет пользователю определить, в каком программном обеспечении была обнаружена уязвимость.

7. DTN – аренда данных. Эта метрика позволяет пользователю определить, в каких данных была обнаружена уязвимость.

8. TIM – Tenants Impacted «Пострадавшие арендаторы». Эта метрика позволяет пользователю учесть суммарное количество арендаторов, пострадавших в результате успешной эксплуатации обнаруженной уязвимости системы безопасности.

9. DCI – влияние на конфиденциальность данных. Эта метрика позволяет пользователю установить, как успешное использование обнаруженной уязвимости безопасности повлияет на конфиденциальность данных.

10. DII – влияние на целостность данных. Эта метрика позволяет пользователю учесть влияние на целостность данных, вызванное успешной эксплуатацией обнаруженной уязвимости.

11. DAI – влияние доступности данных. Эта метрика позволяет пользователю учесть влияние на доступность данных, вызванное успешной эксплуатацией обнаруженной уязвимости.

12. DCL – Data Classification Involved «Классификация задействованных данных». Эта метрика позволяет пользователю задать внутреннюю классификацию данных, задействованных при успешном использовании обнаруженной уязвимости безопасности.

13. UCI – компенсационные элементы управления восходящим потоком. Эта метрика позволяет пользователю учесть наличие любых компенсирующих мер безопасности в уязвимом программном обеспечении или инфраструктуре, которые положительно влияют на защиту от успешной эксплуатации обнаруженной уязвимости.

Хотя VISS не столь распространена, как CVSS, она активно используется в определенных секторах, где критично учитывать бизнес-аспекты и потенциальный ущерб, например, в финансовом и государственном секторах. Она применяется там, где необходимо учитывать влияние на стратегически важные данные и операции, а также при управлении рисками.

5. OWASP Risk Assessment Calculator – это инструмент, созданный компанией OWASP для оценки рисков, связанных с уязвимостями в веб-приложениях. Этот калькулятор позволяет определить не только степень риска уязвимости, учитывая как технические, так и бизнес-аспекты угрозы, но и критичность этой уязвимости. Основная цель OWASP Risk Rating Calculator – создать унифицированный подход для оценки рисков различных уязвимостей, чтобы помочь специалистам по безопасности принимать обоснованные решения о приоритетах устранения.

Калькулятор основывается на управлении рисками, выделяя две ключевые категории: вероятность эксплуатации уязвимости и потенциальный ущерб. Эти категории разделены на метрики, каждая из которых оценивается по шкале (обычно от низкого до высокого). После оценки каждой метрики калькулятор производит итоговую оценку уровня риска. Он помогает пользователю классифицировать уязвимости, определяя их как низкие, средние или высокие по степени риска. Этот инструмент

часто применяют в сочетании с другими стандартами и методиками OWASP, такими как OWASP Top 10 и ASVS, чтобы определить степень риска и приоритизировать исправление уязвимостей.

Несмотря на достоинства, такие как стандартизация процесса оценки рисков, учёт бизнес-контекста, простоту использования и доступность интеграции, OWASP Risk Rating Calculator имеет и ряд недостатков, таких как:

1. Ограниченная детализация: OWASP Risk Rating Calculator предоставляет обобщенные оценки, что может не подходить для организаций с более сложными требованиями по безопасности или уникальной архитектурой.

2. Не учитывает современные угрозы: поскольку калькулятор не обновляется регулярно, он может не учитывать некоторые современные векторы атак и специфические типы угроз.

3. Зависимость от субъективных оценок в оценке рисков может приводить к вариативности результатов. Определение значений для метрик часто зависит от опыта экспертов по безопасности, что может создать разные оценки для одной и той же уязвимости.

OWASP Risk Rating Calculator включает в себя следующие метрики:

1. Параметры злоумышленника:

- уровень квалификации: отсутствие технических навыков (1); наличие некоторых технических навыков (3); продвинутый пользователь ПК (5); навыки сетевого администрирования и программирования (6); навыки взлома систем безопасности (9);
- мотив: низкое вознаграждение или его отсутствие (1); потенциальное вознаграждение (4); высокая награда (9);
- возможности: необходим полный доступ или дорогие ресурсы (0); требуется специальный доступ или ресурсы (4); необходим некоторый доступ или ресурсы (7); доступ или ресурсы не требуются (9);
- размер: разработчики и системные администраторы (2); пользователи интранета (4); партнеры (5); аутентифицированные пользователи (6); анонимные интернет-пользователи (9).

2. Параметры уязвимости:

- простота обнаружения: практически невозможно (1); сложно (3); легко (7); имеются автоматизированные инструменты (9);
- простота эксплуатации: теоретический (1); сложно (3); легко (5); имеются автоматизированные инструменты (9);
- осведомлённость: неизвестный (1); скрытый (4); очевидное (6); информация в публичном доступе (9);
- обнаружение вторжений: активное обнаружение в применении (1); зарегистрировано и рассмотрено (3); зарегистрировано без проверки (8); не зарегистрировано (9).

3. Технические факторы воздействия:

- потеря конфиденциальности: раскрытие минимального количества нечувствительных данных (2);
- раскрытие минимально важных данных (6);
- раскрытие обширных неконфиденциальных данных (6);
- раскрытие обширных критических данных (7);
- все данные раскрыты (9).

OWASP Risk Rating Calculator – это полезный инструмент для быстрой оценки рисков, особенно для веб-приложений, где необходима оценка угроз на основе как технических, так и бизнес-аспектов. Калькулятор предоставляет стандартизированный подход и полезен для организации безопасности в малых и средних компаниях. Однако для крупных организаций с высокими требованиями безопасности он может не предоставить достаточной детализации, и в таких случаях рекомендуется использовать его вместе с другими инструментами и методиками оценки рисков.

6. BVSS calculator (Blockchain Vulnerability Scoring System) – это методика для оценки уровня безопасности и уязвимостей в блокчейн-системах.

Разработанная по аналогии с более известной системой CVSS (Common Vulnerability Scoring System), BVSS адаптирована для уникальных потребностей блокчейн-технологий, таких как децентрализация, смарт-контракты и защищённость консенсусных механизмов.

BVSS базируется на метриках, которые анализируют множество аспектов безопасности. Каждая уязвимость оценивается по набору параметров, и на основе этих оценок формируется общий балл, который отражает уровень критичности уязвимости. Высокий балл указывает на более значительные угрозы, требующие оперативного реагирования.

Основные метрики BVSS таковы:

1. Access Complexity (AC) – сложность доступа к уязвимости.
2. Impact Metrics – потенциальный ущерб, который может нанести уязвимость (например, риск финансовых потерь, потери данных и пр.).
3. Exploitability Metrics – вероятность успешной эксплуатации уязвимости злоумышленником.
4. Scope Metrics – распространенность уязвимости в сети и на смарт-контракты.
5. User Interaction – требуется ли взаимодействие пользователя для успешной эксплуатации уязвимости.

Каждая метрика имеет свои параметры и веса, что позволяет гибко настроить оценку уязвимостей с учетом специфики блокчейнов. Итоговый балл может быть отнесен к определенным уровням критичности, например: низкий, средний, высокий, критический.

Недостатки BVSS таковы:

1. Ограниченная применимость: BVSS еще не адаптирован для всех блокчейн-сетей и может быть ограничен только определенными типами проектов.

2. Сложность: система может быть сложна для понимания и применения без специальной подготовки.

3. Неравномерность метрик: в некоторых случаях метрики BVSS могут оказаться неполными для комплексных блокчейн-платформ.

4. Малая популярность: так как система еще не стала стандартом, мало специалистов имеют достаточный опыт для использования BVSS.

BVSS пока не получил широкого распространения, так как находится на стадии развития. Традиционно для оценки уязвимостей в блокчейн-решениях использовались стандартные системы, такие как CVSS, однако они не учитывают уникальные особенности децентрализованных систем. BVSS постепенно внедряется в проекты, разрабатывающие инфраструктуру безопасности для блокчейна, таких как DApps и DeFi-приложения.

BVSS – несомненно полезный инструмент для оценки безопасности блокчейн-экосистем, но он все еще находится на этапе развития и внедрения.

7. Healthcare Vulnerability Scoring System (HVSS) Version 1.0 Calculator – Калькулятор системы оценки уязвимости в сфере здравоохранения. Он создан для разрешения следующих проблем:

- невысокая точность оценки рисков кибербезопасности медицинских программных продуктов;
- отсутствие способности к эффективному сотрудничеству как отрасли, приходящей к общему знаменателю относительно того, какой должна быть система оценки рисков.

Калькулятор HVSS (Healthcare Vulnerability Scoring System) был разработан для решения вышеперечисленных задач за счёт внедрения следующих нововведений:

- новый способ расчёта эксплуатационной доступности (Exploitability) через переопределение сложности атаки (Attack Complexity), что позволяет учитывать, насколько сложно для злоумышленника будет успешно завершить атаку;
- новая методология оценки, управляемая ИИ, позволяет получить более точные оценки анализируемых сценариев атак для медицинского программного обеспечения;
- новые профили рисков: безопасность пациентов, конфиденциальность данных и

безопасность больницы. Введение этих профилей рисков позволяет более точно оценивать широкий спектр рисков для медицинского программного обеспечения;

- полное предоставление материалов HVSS сообществу, наряду с методами, основанными на искусственном интеллекте и машинном обучении, позволяет любым заинтересованным сторонам вносить изменения в параметры эксплуатационной доступности, профили рисков и сценарии атак, используемые для обучения моделей.

Основные метрики HVSS включают:

1. Вектор атаки (AV): Сеть, Смежная сеть, Локальная сеть, Физический.
2. Расширенная сложность атаки (EAC): Незначительный, Низкий, Средний, Высокий, Критический, Экстремальный.
3. Необходимость привилегий (PR): Нет, Низкий, Высокий.
4. Вовлечение пользователя (UI): Нет, Необходимо.
5. Уровень воздействия (XIT):

- конфиденциальность: Нет, Низкий, Высокий.
- целостность: Нет, Низкий, Высокий.
- доступность: Нет, Низкий, Высокий.

6. Безопасность пациентов (XPS) – определение воздействия на безопасность пациента должно соответствовать организационному, чтобы обеспечить возможность расчета риска кибербезопасности для безопасности пациента в соответствии со схемой, введенной FDA в 2016 году в Руководстве по кибербезопасности после рынка. (КО - Незначительная, Ограниченная, Умеренная, Крупная, Критическая)
7. Чувствительные данные (XSD) – профиль воздействия на конфиденциальные данные используется для оценки влияния риска потенциальной потери конфиденциальных данных в системе.

HVSS еще не получила широкой популярности, поскольку традиционно уязвимости аппаратного уровня не оценивались столь детально. Однако с ростом числа атак на устройства и микроархитектурные компоненты интерес к HVSS возрастает, особенно среди производителей аппаратных решений и крупных компаний.

HVSS полезна для организаций, работающих с высокими требованиями безопасности и на аппаратном уровне, но её применение ограничено сложностью и отсутствием стандартизации.

8. Red Hat Severity Ratings – это система классификации уязвимостей, разработанная компанией Red Hat для оценки критичности угроз, влияющих на её продукты (например, Red Hat Enterprise Linux, OpenShift и др.). Эта система помогает системным администраторам и пользователям Red Hat оперативно определять, насколько срочно нужно реагировать на уязвимости, и правильно приоритизировать обновления.

Red Hat Severity Ratings используется для оценивания уязвимостей в продуктах Red Hat. Она включает несколько уровней критичности, чтобы облегчить принятие решений о срочности обновлений. Эта система активно применяется для всех продуктов компании, включая её операционные системы, контейнерные платформы и другие корпоративные решения. Рейтинги обновляются в рамках Red Hat Security Advisories (RHSA), которые публикуются при обнаружении уязвимостей.

Red Hat Severity Ratings основана на системе уровней, которая классифицирует уязвимости по четырём категориям критичности:

1. Critical: Самые серьёзные уязвимости, которые могут дать злоумышленнику полный доступ к системе с минимальными усилиями. Обычно такие уязвимости включают возможности удалённого исполнения кода или обхода аутентификации.
2. Important: Уязвимости, способные значительно затронуть конфиденциальность, целостность или доступность информации, но не достигающие уровня критических. Включают в себя риски повышения привилегий или утечки данных.
3. Moderate: Средней критичности уязвимости, эксплуатация которых требует определённых условий. Могут оказать ограниченное влияние на систему, если будут использованы.

4. Low: Уязвимости с минимальным влиянием на безопасность системы, обычно требуют множества условий для эксплуатации и обладают ограниченным воздействием.

Red Hat определяет уровень угрозы, оценивая следующие факторы: возможность удаленного или локального использования уязвимости; потенциальное воздействие на систему (конфиденциальность, целостность и доступность данных); степень успешности применения уязвимости. Хотя Red Hat использует собственные уровни оценки серьезности, они часто сочетаются с CVSS для более глубокой оценки рисков. Внутренние стандарты Red Hat адаптированы к экосистеме компании, но пользователи также получают дополнительный балл CVSS. Это позволяет оценивать риски в общепринятом формате, упрощая их понимание и сравнение для тех, кто знаком с CVSS. Таким образом, сочетание обеих систем позволяет создавать более полное представление о безопасности продуктов Red Hat.

Red Hat Severity Ratings широко применяется в корпоративной среде среди клиентов Red Hat, так как она является частью экосистемы компании и специально адаптирована для её продуктов. Популярность рейтингов обусловлена их простотой, удобством и точностью при оценке уязвимостей для продуктов Red Hat. Рейтинги интегрированы в Red Hat Security Advisory (RHSA) и другие инструменты управления безопасностью компании, что делает их легко доступными и понятными для пользователей экосистемы Red Hat.

Недостатки Red Hat таковы:

1. Ограниченная применимость: Рейтинги серьезности Red Hat разработаны исключительно для продуктов компании и не охватывают все типы уязвимостей, которые могут встречаться в других системах. Кроме того, они могут не учитывать особенности различных платформ, что ограничивает их применимость для организаций, использующих разнообразное программное обеспечение.

2. Неудовлетворительная точность: Red Hat Severity Ratings дает общее представление о срочности проблемы, однако её точность иногда ограничена, и компания добавляет баллы CVSS для большей детализации. Это может привести к тому, что некоторые пользователи не будут ориентироваться на систему Red Hat.

3. Меньшая детализация: Четыре уровня оценки не всегда дают полную картину о потенциальных последствиях эксплуатации уязвимости, особенно в сравнении с более детализированными баллами CVSS.

Red Hat Severity Ratings является мощным и эффективным инструментом для управления уязвимостями, специально адаптированным для экосистемы Red Hat, но её ограниченная применимость и зависимость от внешних метрик могут не удовлетворять пользователей с более разнообразной инфраструктурой.

Для проведения анализа особенностей известных риск-калькуляторов необходимо составить таблицу сравнительного исследования (табл. 1) калькуляторов по следующим критериям:

1. (A) Особенности исходных данных – тип и объём информации, необходимой для работы калькулятора;

2. (B) Специализация (широко используется, узкая направленность) – универсальность калькулятора (подходит ли для различных типов уязвимостей или специализирован на узкой области);

3. (C) Доступность – указывает, находится ли продукт в открытом доступе или же ограничен ли конкретными организациями;

4. (D) Объективность оценивания – степень основанности на объективных данных, а не субъективной оценке;

5. (E) Наличие математически обоснованных методов – показатель использования проверенных математических моделей, способствующих точности репрезентативности результатов;

6. (F) Оценка совместимости – возможность интеграции и адаптации в другие системы безопасности;

7. (J) Оценка легкости интеграции – лёгкость внедрения калькулятора в существующие рабочие процессы.

Таблица 1

Сравнительный анализ исследуемых калькуляторов

Критерии	A	B	C	D	E	F	G
CVSS 3.1	Данные о системе, уязвимости	Универсальный	В открытом доступе	Основы на метриках CVSS	Математические модели	Совместим с SIEM и другими системами	Внедрение через API
CVSS 4.0	Данные о системе, уязвимости	Универсальный	В открытом доступе	Основан на метриках CVSS	Математические модели	Совместим с SIEM и другими системами	Внедрение через API
SSVC	Данные о рисках и угрозах	Узконаправленный (оценка рисков)	В открытом доступе	Основан на субъективных решениях	Совокупность методов оценки рисков	Сфокусирован только на риски	Внедрение через API
VISS	Данные о системе, атакующие факторы	Узконаправленный (для веб-приложений)	В открытом доступе	Основан на опыте экспертов	Практическая экспертиза	Сфокусирован только на веб-приложения	Внедрение через веб-приложение
OWASP	Данные о веб-приложениях	Узконаправленный (для веб-приложений)	В открытом доступе	Основан на опыте экспертов	Методы OWASP	Сфокусирован только на веб-приложения	Внедрение через системы безопасности
HVSS	Данные о сети и влиянии на медицинскую инфраструктуру	Узконаправленный (для медицинских инфраструктур)	В открытом доступе	Основан на анализе данных	Модели анализа сетевой безопасности	Сфокусирован только на медицинскую инфраструктуру	Внедрение через системы безопасности
EPSS	Данные об эксплуатации уязвимости, наличие эксплойта и др.	Универсальный	В открытом доступе	Основан на статистике	Анализ больших данных (об уязвимостях, распространённости эксплойтов, и др.)	Совместим с SIEM и другими системами	Внедрение через API
BVSS	Данные об уязвимости в блокчейн технологиях	Узконаправленный (для блокчейн-технологий)	В открытом доступе	Основан на субъективных	Методы анализа бизнес-рисков	Сфокусирован только на блокчейн-технологиях	Внедрение с помощью бизнес-систем
Red Hat Severity Ratings	Данные о продуктах Red Hat, условиях эксплуатации	Узконаправленный (внутри продуктов Red Hat и RHEL)	Доступен в Red Hat Security Advisories	Основан на стандартах Red Hat и	Собственные стандарты Red Hat,	Интегрирован в экосистему Red Hat	Внедрение через экосистемы Red Hat (RHSA)

Исходя из табл. 1, можно сделать вывод, что калькуляторы HVSS, BVSS, VISS и SSVC затруднительны для дальнейшей работы, так как:

HVSS, BVSS, VISS – узконаправленные, специализирующиеся на определённой сфере уязвимостей и кибератак;

BVSS – калькулятор оценки уровня безопасности и уязвимостей в блокчейн-системах;

HVSS – калькулятор оценки уровня безопасности и уязвимостей в медицинских системах;

VISS – представляет собой альтернативу более известной CVSS (Common Vulnerability Scoring System), но акцентируется на оценке влияния уязвимости на конкретные системы и инфраструктуры (ZOOM);

SSVC – калькулятор имеет ряд существенных недостатков: сложность адаптации, необъективные критерии и отстутсвие числовых оценок;

Red Hat Severity Ratings – узконаправленный калькулятор, специализирующийся на продуктах Red Hat и RHEL.

Оставшиеся калькуляторы являются наиболее подходящими для дальнейшего исследования и проведения расчётов, так как они не являются узконаправленными, у них понятный и удобный для пользователя интерфейс.

Конструирование аналитических выражений для расчёта критичности уязвимостей

В качестве примера исследуемой атаки представлен CAPEC-73: «Имя файла, управляемое пользователем». Атака этого типа предполагает вставку злоумышленником вредоносных символов (например, перенаправление XSS) в имя файла, прямо или косвенно, которое затем используется целевым программным обеспечением для генерации текста HTML или другого потенциально исполняемого контента. Многие веб-сайты полагаются на пользовательский контент и динамически создают ресурсы, такие как файлы, имена файлов и URL-ссылки, непосредственно на основе предоставленных пользователем данных. В этом шаблоне атаки злоумышленник загружает код, который может выполняться в клиентском браузере, и/или перенаправлять клиентский браузер на сайт, принадлежащий злоумышленнику. Все варианты полезной нагрузки XSS-атаки могут использоваться для обхода и использования этих уязвимостей. Шаблон обладает высокой степенью опасности.

Для дальнейших расчётов используем методы: средневзвешенного значения, среднеквадратичного значения, среднего арифметического [13, 14].

При этом каждая уязвимость (CVE) будет иметь свои оценки от разных систем калькуляции:

- s_{CVSS} – оценка по CVSS;
- s_{EPSS} – оценка по EPSS;
- s_{OWASP} – оценка по OWASP.

Для каждой уязвимости были найдены оценки по разным риск-калькуляторам – CVSS версий 3.1 и 4.0, EPSS и OWASP, которые представлены в табл. 2.

Таблица 2

Оценки критичности уязвимостей калькуляторами

Уязвимость	Оценка CVSS 3.1	Оценка CVSS 4.0	Оценка EPSS	Оценка OWASP
CVE-2018-8414	8,8	9,4	0,76707	3,87
CVE-2018-20250	7,8	9,3	0,97332	3,5
CVE-2020-0646	9,8	9,3	0,97418	5,125
CVE-2020-0938	7,8	8,4	0,9515	4,875
CVE-2020-1020	8,8	8,5	0,94679	3,875

Продолжение табл.2

CVE-2021-1647	7,8	8,5	0,33796	4,875
CVE-2009-0927	9,6	9,4	0,97463	4,5
CVE-2010-2568	7,8	8,1	0,97034	3,75
CVE-2023-36884	7,5	7,7	0,06769	3,1875
CVE-2023-38831	7,8	6,8	0,31236	3,875
CVE-2023-22952	8,8	8,7	0,53365	4,5625

С целью приведения оценок в единую область допустимых значений, осуществим нормализацию (1):

$$s_{norm} = \frac{s - s_{min}}{s_{max} - s_{min}}, \quad (1)$$

где: s_{norm} – нормализованная оценка калькулятора;

s – оценка калькулятора;

s_{max} – максимальная возможная оценка калькулятора;

s_{min} – минимальная возможная оценка калькулятора.

Нормализация оценок критичности выявленных уязвимостей представлена в табл. 3.

Таблица 3

Нормализованные оценки критичности уязвимостей

Уязвимость	$s_{norm,CVSS3.1}$	$s_{norm,CVSS4.0}$	$s_{norm,EPSS}$	$s_{norm,OWASP}$
CVE-2018-8414	0,88	0,94	0,76707	0,387
CVE-2018-20250	0,78	0,93	0,97332	0,35
CVE-2020-0646	0,98	0,93	0,97418	0,5125
CVE-2020-0938	0,78	0,84	0,9515	0,4875
CVE-2020-1020	0,88	0,85	0,94679	0,3875
CVE-2021-1647	0,78	0,85	0,33796	0,4875
CVE-2009-0927	0,96	0,94	0,97463	0,45
CVE-2010-2568	0,78	0,81	0,97034	0,375
CVE-2023-36884	0,75	0,77	0,06769	0,31875
CVE-2023-38831	0,78	0,68	0,31236	0,3875
CVE-2023-22952	0,88	0,87	0,53365	0,45625

Для реализации метода средневзвешенного значения найдём среднее значение и стандартное отклонение по формулам (2) и (3):

$$\bar{s} = \frac{1}{4}\left(s_{norm,CVSS3.1} + s_{norm,CVSS4.0} + s_{norm,EPSS} + s_{norm,OWASP}\right), \quad (2)$$

$$\sigma = \sqrt{\frac{1}{3}\left(\left(s_{norm,CVSS3.1} - \bar{s}\right)^2 + \left(s_{norm,CVSS4.0} - \bar{s}\right)^2 + \left(s_{norm,EPSS} - \bar{s}\right)^2 + \left(s_{norm,OWASP} - \bar{s}\right)^2\right)}, \quad (3)$$

где $\bar{s}$ - среднее значение нормализованных оценок;

σ - стандартное отклонение оценки калькулятора;

n – количество используемых калькуляторов;

$s_{norm,CVSS3.1}$ – нормализованная оценка калькулятора CVSS 3.1;

$s_{norm,CVSS4.0}$ – нормализованная оценка калькулятора CVSS 4.0;

$s_{norm,EPSS}$ - нормализованная оценка калькулятора EPSS;

$s_{norm,OWASP}$ – нормализованная оценка калькулятора OWASP.

Результаты расчётов представлены в табл. 4.

Таблица 4

Среднее значение и стандартное отклонение

Уязвимость	$\bar{s}$	σ
CVE-2018-8414	0,99352	0,381
CVE-2018-20250	0,76833	0,2848
CVE-2020-0646	0,84867	0,223
CVE-2020-0938	0,76475	0,19799
CVE-2020-1020	0,7670725	0,2563
CVE-2021-1647	5,37824	3,7077
CVE-2009-0927	6,1186575	4,146375
CVE-2010-2568	5,155085	3,424982
CVE-2023-36884	0,47636	0,34211
CVE-2023-38831	4,69684	3,6164
CVE-2023-22952	0,685225	0,1266

Найдём значимость (вес) для каждого калькулятора по формуле (4):

$$w_i = \frac{s_i}{\sigma}, \quad (4)$$

где w_i – значимость калькулятора,

s_i – нормализованная оценка калькулятора,

σ - стандартное отклонение.

Результат расчёта представлен в табл. 5:

Таблица 5

Значимость (вес) калькуляторов

Уязвимость	w_1	w_2	w_3	w_4
CVE-2018-8414	2,31	2,46	2,01	1,02
CVE-2018-20250	2,744	3,265	3,415	1,229
CVE-2020-0646	4,39	4,17	4,37	2,3
CVE-2020-0938	3,93	4,24	4,8	2,46
CVE-2020-1020	3,43	3,32	3,69	1,51
CVE-2021-1647	2,1	2,29	0,09	1,31
CVE-2009-0927	2.316	2,266	0,235	1,085
CVE-2010-2568	2,28	2,37	0,28	1,09
CVE-2023-36884	2,1911	2,2504	0,1975	0,9317
CVE-2023-38831	2,156	1,88	0,0864	1,071
CVE-2023-22952	69,6	68,7	4,2	36,1

Для дальнейших вычислений необходимо нормализовать веса, для этого воспользуемся формулой (5):

$$w_{norm,i} = \frac{w_i}{\sum_{i=1}^{n} w_i}, \quad (5)$$

где $w_{norm,i}$ – нормализованный вес калькулятора,

w_i – вес калькулятора,

i – индекс нормализованного веса.

Результаты расчётов представлены в табл. 6:

Таблица 6

Нормализация весов

Уязвимость	$w_{norm,1}$	$w_{norm,2}$	$w_{norm,3}$	$w_{norm,4}$
CVE-2018-8414	0,296	0,316	0,257	0,131
CVE-2018-20250	0,257	0,306	0,321	0,115
CVE-2020-0646	0,288	0,274	0,287	0,151
CVE-2020-0938	0,254	0,275	0,311	0,16
CVE-2020-1020	0,265	0,257	0,285	0,116
CVE-2021-1647	0,369	0,403	0,016	0,23
CVE-2009-0927	0,3925	0,3843	0,0398	0,1832
CVE-2010-2568	0,3787	0,3938	0,0465	0,1818
CVE-2023-36884	0,393	0,404	0,0354	0,1676
CVE-2023-38831	0,415	0,362	0,017	0,206
CVE-2023-22952	0,389	0,384	0,0235	0,202

Произведем расчет итоговых оценок и расчет итоговой средневзвешенной оценки по формулам (6) и (7). Результаты расчётов представлены в табл. 7 и 8:

$$s_{weighted} = s_{norm} \cdot w_{norm,i}, \quad (6)$$

где $s_{weighted}$ – итоговая оценка калькулятора, s_{norm} – нормализованная оценка калькулятора, $w_{norm,i}$ – нормализованный вес.

$$s_{final} = s_{weighted,CVSS3.1} + s_{weighted,CVSS4.0} + s_{weighted,EPSS} + s_{weighted,OWASP}, \quad (7)$$

где s_{final} – средневзвешенная оценка, $s_{weighted,CVSS3.1}$ – итоговая оценка по калькулятору CVSS 3.1, $s_{weighted,CVSS4.0}$ – итоговая оценка по калькулятору CVSS 4.0, $s_{weighted,EPSS}$ – итоговая оценка по калькулятору EPSS, $s_{weighted,OWASP}$ – итоговая оценка по калькулятору OWASP.

Таблица 7

Итоговые данные расчёта оценок

Уязвимость	$s_{weighted,CVSS3.1}$	$s_{weighted,CVSS4.0}$	$s_{weighted,EPSS}$	$s_{weighted,OWASP}$
CVE-2018-8414	0,26048	0,29704	0,19759	0,5077
CVE-2018-20250	0,20046	0,28458	0,31267	0,04025
CVE-2020-0646	0,28224	0,25542	0,2797	0,0775
CVE-2020-0938	0,198	0,231	0,296	0,078
CVE-2020-1020	0,2332	0,2185	0,269	0,0449
CVE-2021-1647	0,288	0,343	0,0054	0,112
CVE-2009-0927	0,3768	0,3605	0,0388	0,0842
CVE-2010-2568	0,295	0,318	0,045	0,0681
CVE-2023-36884	0,2948	0,3101	0,0024	0,0534
CVE-2023-38831	0,3247	0,2462	0,0053	0,0799
CVE-2023-22952	0,343	0,334	0,0125	0,0922

Таблица 8

Итоговые средневзвешенные оценки

Уязвимость	s_{final}
CVE-2018-8414	0,80628
CVE-2018-20250	0,83796
CVE-2020-0646	0,89486
CVE-2020-0938	0,803
CVE-2020-1020	0,7656
CVE-2021-1647	0,748
CVE-2009-0927	0,8585
CVE-2010-2568	0,7261
CVE-2023-36884	0,6607
CVE-2023-38831	0,6561
CVE-2023-22952	0,7871

Этот метод учитывает важность каждой оценки, придавая им веса. Веса вычисляются на основе нормализованных оценок и стандартного отклонения, что позволяет каждому калькулятору влиять на итоговую оценку в зависимости от ее значимости по сравнению с другими. Итоговая оценка рассчитывается как сумма произведений нормализованной оценки и соответствующего веса. Методика обеспечивает:

- учёт значимости: этот метод позволяет учитывать важность каждой оценки, что особенно полезно, когда разные источники оценки имеют различную достоверность или уровень важности;
- гибкость: веса можно адаптировать в зависимости от контекста, что позволяет настроить метод под конкретные нужды анализа;
- представление композитной оценки: позволяет рассчитать итоговую оценку, учитывая разнообразные аспекты или источники данных.

При этом методике присуще:

- сложность в интерпретации: Определение весов может быть субъективным и требует анализа, что увеличивает сложность;
- упрощение некоторых аспектов: Переключение на веса может привести к упрощению и игнорированию нюансов каждой отдельной оценки;
- зависимость от весов: Итоговая оценка может сильно варьироваться в зависимости от выбранных весов, что может дать искаженное представление о реальной ситуации;

Для реализации метода среднеквадратичного значения необходимо рассчитать среднее значение. При помощи формулы (8) были получены средние оценки по каждой уязвимости:

$$s_{final} = \sqrt{\frac{1}{n}\sum_{i=1}^{n} s_{norm,i}^2}, \qquad (8)$$

где S_{final} – среднеквадратическая оценка;

$S_{norm,i}$ – нормализованная оценка калькулятора;

n – количество используемых калькуляторов.

Результаты представлены в табл. 9.

Таблица 9

Среднеквадратичное значение

Уязвимость	Среднеквадратичная оценка
CVE-2018-8414	0,7744
CVE-2018-20250	0,7975
CVE-2020-0646	0,87
CVE-2020-0938	0,783
CVE-2020-1020	0,7973
CVE-2021-1647	0,649
CVE-2009-0927	0,8606
CVE-2010-2568	0,765
CVE-2023-36884	0,5612
CVE-2023-38831	0,574
CVE-2023-22952	0,7116

Этот метод использует среднеквадратичное значение для вычисления итоговой оценки. Он оценивает "разброс" нормализованных оценок, вычисляя квадрат каждой оценки, суммируя эти квадраты и деля на количество оценок.

Этот подход подчеркивает влияние крайних значений и помогает учитывать вариативность данных. Методика обеспечивает:

- учёт вариативности: позволяет оценить разброс и вариативность оценок, что может быть полезно для понимания степени риска или неопределенности;

- чувствительность к крайним значениям: придает большее значение высоким и низким значениям, что может помочь выявить потенциальные проблемы;

- статистическая обоснованность: широко используется в статистике, что делает его знакомым и приемлемым методом для многих специалистов.

При этом методике присуще:

- сложность в интерпретации: может быть сложно интерпретировать отклонения как непосредственные последствия для оценки;

- чувствительность к выбросам: Высокие или низкие значения могут резко повлиять на итоговую оценку, что не всегда отражает реальную ситуацию.

- отсутствие важности отдельных оценок: Каждая оценка рассматривается наравне, что может игнорировать контекст.

В табл. 10 представлены итоговые оценки метода среднего арифметического значения.

Таблица 10

Среднее арифметическое значение

Уязвимость	Среднее арифметическое
CVE-2018-8414	0,9935
CVE-2018-20250	0,75833
CVE-2020-0646	0,84867
CVE-2020-0938	0,76475
CVE-2020-1020	0,7660725
CVE-2021-1647	0,613865
CVE-2009-0927	0,8311575
CVE-2010-2568	0,733835
CVE-2023-36884	0,47636
CVE-2023-38831	0,5422
CVE-2023-22952	0,685225

Этот метод довольно просто усредняет нормализованные оценки, складывая их и разделяя на количество оценок. Он позволяет получить общее представление о среднем уровне, не уделяя внимания весам или вариациям в данных, что делает его простым и понятным способом вычисления итоговой оценки. Методика обладает:

- простотой: легко понимается и легко рассчитывается, что делает этот метод удобным для быстрого анализа.

- наглядностью: предоставляет отчетливое представление о среднем уровне риска без излишней сложности.

- отсутствием субъективности: не требует назначения весов или других субъективных мер.

При этом имеются:

- игнорирование вариативности: не учитывает разброс оценок, что в некоторых случаях может привести к слишком однобокой оценке;

- одинаковый вес всем оценкам: Все оценки считаются равными, что игнорирует их потенциальную значимость или надежность;

- чувствительность к выбросам: как и среднеквадратичное, арифметическое среднее также может быть сильно искажено крайними значениями.

Также уместно использовать метод логарифмической нормализации, так как он может уменьшить влияние выбросов и привести данные к общему масштабу. Итоговая оценка рассчитывается по формуле (9).

$$s_{final} = \sum_{i=1}^{n}(\log s_i + 1), \quad (9)$$

где S_{final} – логарифмическая оценка;

s_i – оценка калькулятора.

Медианный способ усреднения использует медиану для представления среднего значения набора данных. В отличие от среднего арифметического, которое может сильно искажаться из-за наличия экстремальных (очень больших или очень маленьких) значений, медиана более устойчива к выбросам.

Использование медианы уместно, когда нужно описать "средний" элемент данных, а также когда данные содержат выбросы или имеют асимметричное распределение. В этом случае производится сортировка (по возрастанию или убыванию) нормированных оценок для дальнейшей выборки.

Если количество элементов нечётное (n – нечётное), то медиана:

$$Me = x_{(\frac{n+1}{2})}, \quad (10)$$

где $x_{(\frac{n+1}{2})}$ – значение элемента, расположенного в середине упорядоченного набора данных.

Если количество элементов чётное (n – чётное), то медиана:

$$Me = \frac{x_{(\frac{n}{2})} + x_{(\frac{n}{2}+1)}}{2}, \quad (11)$$

где $x_{(\frac{n}{2})}$ и $x_{(\frac{n}{2}+1)}$ – два центральных элемента в упорядоченном наборе данных.

Метод среднеквадратичного анализа используется в статистике и анализе данных для получения представления о средней величине с учетом изменчивости и разброса оценок. Данный метод имеет обоснование, которое заключается в его способности учитывать как центральные тенденции, так и распространенность данных.

Формально, среднеквадратичное значение определяется как:

$$s_{final} = \frac{1}{n}\sum_{i=1}^{n}(s_i^2), \quad (12)$$

где s_{final} – среднеквадратичное значение,

s_i – оценка калькулятора,

n – общее количество оценок.

При этом среднеквадратичное значение позволяет количественно оценить степень разброса данных вокруг среднего значения. Это становится особенно важным в контексте риск-анализа, где нестабильность оценок может указывать на наличие значительных рисков. Для примера, пусть у нас есть следующие оценки и расчет среднего значения:

$$s = \frac{0{,}2 + 0{,}5 + 0.8}{3} = \frac{1{,}5}{3} \approx 0{,}5. \quad (13)$$

Однако таким образом не учитывается разброс значений. Если применить среднеквадратичное значение:

$$s_{final} = \sqrt{\frac{1}{3}(0,2^2 + 0,5^2 + 0{,}64)} = \sqrt{\frac{0{,}93}{3}} \approx 0{,}553. \quad (14)$$

Таким образом, среднеквадратичное значение будет учитывать не только центральное значение, но и разброс оценок.

Среднеквадратичное значение также более чувствительно к выбросам в данных, что может служить полезным индикатором в контексте оценки критичности, где наличие нестабильных данных может указывать на значительные проблемы. Например, если одна из оценок существенно выше или ниже остальных, среднеквадратичное значение это отразит. К примеру, если имеется:

$$s = \frac{0{,}1 + 0{,}2 + 0{,}9}{3} \approx 0{,}4. \quad (15)$$

То среднеквадратичное значение составит:

$$s_{final} = \sqrt{\frac{1}{3}(0,1^2 + 0,2^2 + 0,9^2)} \approx \sqrt{0,2833} \approx 0,532 \quad (16)$$

Выброс S3 в виде 0,9 активно влияет на итоговое значение, подчеркивая необходимость анализа такого типа данных.

В итоге, выбор метода среднеквадратичного для финального расчета оценки представляет собой обоснованное решение, которое позволяет более точно оценить риски и принимать взвешенные решения, опираясь на полное представление о состоянии данных. Учет различные параметры, такие как чувствительность к выбросам и возможность адекватного отражения неопределенности, делает этот метод предпочтительным в контексте сложных систем.

Теоретический интерес представляют также оценки критичности уязвимостей, учитывающие популярность (частоту использования) калькуляторов, предоставляющих необходимые данные. В этом случае могут быть использованы соответствующие весовые коэффициенты

$$\bar{k} = \sum_{i=1}^{n} \alpha_i k_i, \quad (17)$$

где $\bar{k}$ – искомое среднее значение критичности,

α_i – весовой коэффициент i-го калькулятора,

n – количество используемых калькуляторов,

k_i – значение критичности уязвимости, предоставленное i-тым калькулятором.

При этом, расчёт весовых коэффициентов можно осуществить следующим образом:

$$\alpha_i = \frac{k_i}{\sum_{i=1}^{n} k_i}, \quad (18)$$

где k_i– количество обращений к i-тому калькулятору за определённый (скажем, месяц) период времени;

$\sum_{i=1}^{n} \alpha_i = 1$.

К недостаткам предлагаемого подхода можно отнести тот факт, что не для каждого калькулятора работает счётчик обращений. К тому же, не все пользователи используют калькулятор для расчётов. Некоторые просто знакомятся с инструментом. Однако, если предположить, что процент таковых примерно одинаков для всех калькуляторов, то предлагаемая методика (17) имеет право на практическое использование

Заключение

В результате проведенного исследования подчеркивается, что полученные результаты существенно расширяют понимание методов оценки критичности уязвимостей в автоматизированных информационных системах и телекоммуникационных сетях. Сравнительный анализ различных риск-калькуляторов, таких как CVSS, SSVC, EPSS и других, выявил их сильные и слабые стороны, что демонстрирует необходимость комплексного и критического подхода к выбору инструмента для оценки киберрисков.

Разработанные аналитические выражения для расчета критичности уязвимостей представляет собой актуальный вклад в практику управления киберугрозами. Они предоставляют исследователям и специалистам по информационной безопасности удобный инструмент для более обоснованных проектных решений, учитывающих как критичность уязвимостей, так и их вариативность.

Кроме того, применение вышеописанных методов для расчета критичности позволяет учитывать как центральные тенденции, так и вариативность в показателях, что является существенным для обеспечения надежной защиты информационных систем. Результаты данного исследования не только способствуют повышению защищённости, но и формируют основы для оценки вероятности

и ущербов единичных и множественных кибератак.

Список литературы

1. The SSVC risk prioritization method: what it is, when to use it, and alternatives. – URL: https://vulcan.io/blog/the-ssvc-risk-prioritization-method-what-it-is-when-to-use-it-and-alternatives/ (дата обращения 17.10.2024).

2. SSVC Calculator. – URL: https://www.cisa.gov/ssvc-calculator (дата обращения 25.10.2024).

3. Exploit Prediction Scoring System (EPSS). – URL: https://www.first.org/epss/ (дата обращения 30.10.2024).

4. Общая система оценки уязвимостей (CVSS). – URL: https://www.first.org/cvss/specification-document (дата обращения 05.11.2024).

5. Common Vulnerability Scoring System v3.1: Specification Document. – URL: https://www.first.org/cvss/v3.1/specification-document (дата обращения 07.11.2024).

6. The Vulnerability Impact Scoring System (VISS). – URL: https://viss.zoom.com/specifications#2-metrics (дата обращения 08.11.2024).

7. VISS калькулятор. – URL: https://viss.zoom.com/calculator/0.07#VISS:0.07:PLI:NA/ICI:N/III:N/IAI:N/ITN:NA/STN:NA/DTN:NA/TIM:N/DCI:N/DII:N/DAI:N/DCL:N/UCI:NA (дата обращения 08.11.2024).

8. Калькулятор BVSS (система оценки уязвимости блокчейна). – URL: https://www.halborn.com/bvss (дата обращения 09.11.2024).

9. Healthcare Vulnerability Scoring System (HVSS) Version 1.0 Calculator. – URL: https://hvss.online/ (дата обращения 09.11.2024).

10. HVSS v1.0 Documentation. – URL: https://hvss.online/doc/v1.0/HVSS_v1.0_Documentation.pdf (дата обращения 09.11.2024).

11. OWASP Risk Assessment Calculator. – URL: https://javierolmedo.github.io/OWASP-Calculator/ (дата обращения 10.11.2024).

12. How Red Hat uses CVSSv3 to Assist in Rating Flaws. – URL: https://www.redhat.com/en/blog/how-red-hat-uses-cvssv3-assist-rating-flaws (дата обращения 11.11.2024).

13. Средневзвешенная оценка. – URL: https://sh-majskaya-r56.gosweb.gosuslugi.ru/glavnoe/srednevzveshennaya-otsenka/ (дата обращения 11.11.2024).

14. Стандартное отклонение и стандартная ошибка. – URL: https://habr.com/ru/companies/lanit/articles/799317/ (дата обращения 11.11.2024).

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 19.11.2024

Информация об авторах

Остапенко Александр Алексеевич – аспирант, Воронежский государственный технический университет, e-mail: alexostap123@gmail.com

Шелякин Валерий Петрович – канд. техн. наук, доцент, Воронежский государственный технический университет, e-mail:437712@mail.com.

Короткова Евгения Сергеевна – студентка, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Кривошеин Александр Сергеевич – студент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Мальцева Дарья Алексеевна – студентка, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Меркулов Павел Александрович – студент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Никитин Никита Дмитриевич – студент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Титаренко Меланья Олеговна – студентка, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

VULNERABILITY CRITICALITY ASSESSMENT USING DATA FROM A VARIETY OF RISK CALCULATORS

A.A. Ostapenko, V.P. Shelykin, E.S. Korotkova, A.S. Krivoshein, D.A. Maltseva, P.A. Merkulov, N.D. Nikitin, M.O. Titarenko

The article is devoted to the study of methods for assessing the criticality of vulnerabilities in automated information systems (AIS) and telecommunication networks (TCS) using a variety of risk calculators. The existing approaches to vulnerability criticality analysis such as CVS, SVN, EPS, VIS, OWASP Risk Rating Calculator, BVSS and HVSS are considered. A comparative analysis of their metrics and algorithms is carried out, the advantages and limitations of each of the calculators are revealed. The scientific and technical task of the study was to develop analytical expressions for calculating the criticality of vulnerabilities. The results obtained can be useful for improving the effectiveness of cyber risk management and optimizing information security processes.

Keywords: risk calculator, CVS, SVN, EPC, WIS, OWASP, BVS, VS, vulnerability, criticality, cyberattack.

Submitted 19.11.2024

Information about the authors

Alexander A. Ostapenko – graduate student, Voronezh State Technical University, e-mail: alexostap123@gmail.com.
Valery P. Shelyakin – Cand. Sc. (Technical), Associated Professor Voronezh State Technical University, e-mail:437712@mail.com
Evgeniya S. Korotkova – student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com
Alexander S. Krivoshein – student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com
Darya A. Maltseva – student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com
Pavel A. Merkulov – student, Voronezh State Technical University, e-mail alexanderostapenkoias@gmail.com
Nikita D. Nikitin – student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com.
Melania O. Titarenko – student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com