УДК 159.99

МЕТОДЫ И ПОДХОДЫ К ОЦЕНКЕ УЯЗВИМОСТЕЙ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ (CVSS, EPSS И ISO/IEC 27005)

И. О. ПЕТРОЧЕНКО, С. Г. САЕВИЧ
(Представлено: канд. пед. наук, доц. П. П. МАТЕЛЕНОК)

Развитие информационных технологий 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. Особую актуальность приобретают подходы, обеспечивающие системную и количественную оценку выявленных уязвимостей. Общепризнанными представителями таких подходов, методик, предназначенных для стандартизированной оценки степени критичности уязвимостей на основе множества факторов являются CVSS, EPSS И ISO/IEC 27005.

Отметим, что 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]. Угрозы обычно исходят из уязвимостей, которые приводят к нарушению безопасности в информационных системах. Уязвимость представляет собой особенности объекта информационной системы, которые могут вызвать нарушение безопасности информации. Эти особенности могут быть связаны с недостатками в функционировании системы, архитектурными особенностями, протоколами обмена, интерфейсами, используемым ПО, аппаратными платформами, а также условиями эксплуатации и размещения системы, а также с невнимательностью сотрудников. Уязвимость может возникать из-за ошибок в организации системы информационной безопасности, ошибок программирования, недостатков в проектировании системы, использования ненадежных паролей, вирусов и других факторов. Некоторые уязвимости известны только теоретически, в то время как другие активно используются и имеют соответствующие эксплойты. Источники угроз могут использовать эти уязвимости для нарушения безопасности информации с целью получения незаконной выгоды или нанесения ущерба владельцам, пользователям или собственникам информации. Устранение или значительное ослабление уязвимостей может значительно уменьшить возможности для реализации угроз безопасности информации [2].

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 уязвимости разделяются на объективные, субъективные и случайные уязвимости [3]. Объективные уязвимости возникают в результате особенностей конструкции и характеристик оборудования. Их полное устранение затруднено, но возможно снижение риска с помощью технических и инженерных методов.

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

CVSS предоставляет количественную шкалу от 0 до 10, где 0 означает отсутствие угрозы, а 10 – максимальную критичность уязвимости. Основное внимание уделяется оценке серьезности уязвимости с учетом воздействия на конфиденциальность, целостность и доступность информации. CVSS активно поддерживается международным сообществом FIRST [1].

EPSS использует шкалу от 0 до 1, отражающую вероятность эксплуатации уязвимости злоумышленниками в реальных условиях. Основывается на актуальных данных об угрозах, включая частоту атак и активность эксплойтов. Разработка EPSS ведется в рамках сообщества OpenDXL и групп по анализу уязвимостей.

В отличие от CVSS и EPSS, ISO/IEC 27005 не фиксирует конкретный диапазон оценок, поскольку представляет собой методологию комплексной оценки рисков, включающую как качественные, так

и количественные подходы. В рамках этого стандарта оцениваются риски с учетом вероятности возникновения угроз и их влияния на бизнес-процессы организации. Управление и развитие стандарта осуществляется международными организациями ISO и IEC.

Таблица 1. – Сравнительный анализ стандартов

	CVSS	EPSS	ISO/IEC 27005
Диапазон оценок	От 0 до 10: 0 – отсутствие угрозы, 10 – максимальная угроза	От 0 до 1: 0 – низкая вероятность эксплуатации, 1 – высокая	Не фиксирован: методология для качественной и количественной оценки рисков
Управление	Поддерживается FIRST (Forum of Incident Response and Security Teams)	Развивается OpenDXL и сообществом анализа уязвимостей	Регулируется ISO и IEC (Международные стандарты)
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

Использование этих аналитических моделей, в том числе CVSS, помогает не только в количественной оценке уязвимостей, но и в формировании более эффективных стратегий по минимизации рисков и защите информационных систем от потенциальных угроз. В результате анализа установлено, что уязвимости являются основой для возникновения угроз информационной безопасности. Их классификация на объективные, субъективные и случайные помогает точнее определять причины возникновения и способы устранения. Сравнение подходов CVSS, EPSS и ISO/IEC 27005 показало, что они дополняют друг друга: CVSS оценивает серьезность уязвимостей, EPSS – вероятность их эксплуатации, а ISO/IEC 27005 обеспечивает комплексное управление рисками.

Использование аналитических моделей позволяет повысить точность оценки уязвимостей и эффективно распределять ресурсы на их устранение. Комплексный подход к оценке рисков необходим для повышения уровня защищенности информационных систем.

Остановимся отдельно на CVSS. Common Vulnerability Scoring System – 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. Метрика – количественный показатель свойств.

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).

В таблицах 2 и 3 представлены обобщенные преимущества и недостатки системы CVSS при анализе защищенности информационных систем.

Таблица 2. – Преимущества CVSS в контексте оценки защищенности

Преимущество	Описание
Стандартизация	Обеспечивает универсальный подход к количественной оценке уязвимостей, упрощая взаимодействие между различными участниками процессов информационной безопасности
Широкое использование	Используется международными организациями, государственными структурами и коммерческими компаниями, став отраслевым стандартом
Удобство для автоматизации	Поддерживает интеграцию в автоматизированные системы управления уязвимостями за счет структуры вектора и расчетных моделей
Адаптивность	Позволяет адаптировать оценки к конкретной среде эксплуатации благодаря временным метрикам и метрикам среды

Таблица 3. – Недостатки CVSS в контексте оценки защищенности

Недостаток	Описание
Субъективность оценки	Несмотря на то, что CVSS предлагает стандартизированную методологию, некоторые метрики требуют оценки, основанной на экспертных суждениях. Это означает, что результаты могут зависеть от опыта и интерпретации специалистов, что приводит к определенной степени субъективности в итоговой оценке уязвимости
Ограниченная чувствительность к сложным атакам	CVSS в своей текущей форме не всегда может точно отразить сложные многоступенчатые атаки, которые могут включать взаимодействие нескольких уязвимостей или атакующих действий
Запаздывание обновлений	Так как CVSS обновляется не так часто, новые типы угроз и методов атак могут быть недостаточно учтены в оценках, что снижает ее актуальность
Ориентация на технические параметры	CVSS оценивает в первую очередь технические характеристики уязвимости, при этом не всегда учитывается ее воздействие на бизнес-процессы и организационные риски

Таким образом, несмотря на ряд ограничений, CVSS остается важным инструментом для количественной оценки уязвимостей в информационных системах. Понимание как преимуществ, так и недостатков этой системы позволяет более обоснованно подходить к ее использованию и, при необходимости, комбинировать с другими методами оценки рисков для более точных и комплексных результатов.

ЛИТЕРАТУРА

1. Марков, А. С. Систематика уязвимостей и дефектов безопасности программных ресурсов / А. С. Марков, А. А. Фадин // Защита информ ции. Инсайд. – 2013. – №3. – С. 56–61.
2. Информационная безопасность и анализ угроз. Безопасник [Электронный ресурс]. – Режим доступа: http://bezopasnik.org/article/21.html. – Дата доступа: 11.05.2025.
3. ISO/IEC 27005 [Электронный ресурс]. – Режим доступа: https://www.iso.org/ru/standard/80585.html. – Дата доступа: 09.04.2025.