БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2024. – № 1 (112). – 52–73

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004 DOI: 10.17212/2782-2230-2024-1-52-73

ВОПРОСЫ ПРИМЕНЕНИЯ АЛГОРИТМОВ ПРИОРИТИЗАЦИИ УЯЗВИМОСТЕЙ ПРИ ОРГАНИЗАЦИИ ПРОЦЕССА VULNERABILITY MANAGEMENT*

А.Г. ПОДСЕВАЛОВ[1], М.И. КУДИНОВ[2]

[1] *630073, г. Новосибирск, пр. Карла Маркса 20, Новосибирский государственный технический университет, лаборант кафедры защиты информации. E-mail: podsevalov.2019@stud.nstu.ru*
[2] *630073, г. Новосибирск, пр. Карла Маркса 20, Новосибирский государственный технический университет, лаборант кафедры защиты информации. E-mail: m.kudinov.2019@stud.nstu.ru*

Целью настоящего научного исследования является анализ возможностей повышения уровня защиты организации от киберугроз путем применения алгоритмов приоритизации уязвимостей. Существуют различные подходы к созданию алгоритмов приоритизации уязвимостей, учитывающие множество метрик, например: потенциальное воздействие на информационную систему при эксплуатации уязвимости, сложность эксплуатации уязвимости, сложность устранения и т. д. Статья посвящена вопросам организации процесса управления уязвимостями, в частности различным способам (алгоритмам) их приоритизации для определения очередности устранения и рационального распределения человеческих ресурсов организации. Рассмотрены и проанализированы различные алгоритмы приоритизации уязвимостей, сделаны выводы об их достоинствах и недостатках. Предложен вариант алгоритма приоритизации уязвимостей, учитывающий наиболее важные метрики, а также рекомендации ФСТЭК России.

Ключевые слова: информационная безопасность, кибербезопасность, уязвимость, приоритизация, алгоритмы приоритизации, анализ угроз, уровень защищенности, риски, процесс управления уязвимостями, CVSS, ФСТЭК

* Статья получена 12 февраля 2024 г.

ВВЕДЕНИЕ

Уязвимости в информационных системах представляют собой слабые места или ошибки в программном обеспечении, которые могут быть использованы злоумышленниками для несанкционированного доступа, атаки или кражи конфиденциальных данных. Злоумышленники активно стремятся использовать неисправленные уязвимости в информационных системах, чтобы нанести ущерб государственным и частным организациям.

Вместе с тем в последнее время количество новых уязвимостей непрерывно растет: с 2022 по 2023 год среднемесячное количество общеизвестных уязвимостей (CVE) увеличилось на 13 % [1]. При этом организации испытывают нехватку персонала (ресурсов) службы безопасности.

Это привело к тому, что уязвимости сохраняются в информационных системах организаций в течение длительного времени, создавая значительное преимущество для злоумышленников.

Следовательно, для эффективного управления уязвимостями крайне важно применять подходы, обеспечивающие приоритизацию устранения выявленных уязвимостей. Это позволит в первую очередь исправлять наиболее критичные уязвимости безопасности, что сведет к минимуму вероятность проведения злоумышленниками кибератак.

1. ПРОЦЕСС УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ

Управление уязвимостями – это непрерывный, критически важный и сложный процесс, который позволяет организациям разработать процедуру выявления, оценки и устранения уязвимостей в защищаемых ИТ-активах.

Целью управления уязвимостями является снижение общей подверженности информационных систем организации рискам путем устранения как можно большего числа уязвимостей.

Процесс управления уязвимостями включает пять основных этапов (рисунок):

1) мониторинг уязвимостей и оценки их применимости;
2) оценка уязвимостей;
3) определение методов и приоритетов устранения уязвимостей;
4) устранение уязвимостей;
5) контроль устранения уязвимостей.

На этапе мониторинга уязвимостей и оценки их применимости осуществляется выявление уязвимостей на основании данных, получаемых из внешних и внутренних источников, и принятие решений по их последующей обработке.

На этапе оценки уязвимостей определяется уровень критичности уязвимостей применительно к информационным системам органа (организации).

На этапе определения методов и приоритетов устранения уязвимостей определяется приоритетность устранения уязвимостей и выбираются методы их устранения: обновление программного обеспечения и (или) применение компенсирующих мер защиты информации.

На этапе устранения уязвимостей принимаются меры, направленные на устранение или исключение возможности использования (эксплуатации) выявленных уязвимостей.

На этапе контроля устранения уязвимостей осуществляется сбор и обработка данных о процессе управления уязвимостями и его результатах, а также принятие решений по улучшению данного процесса.

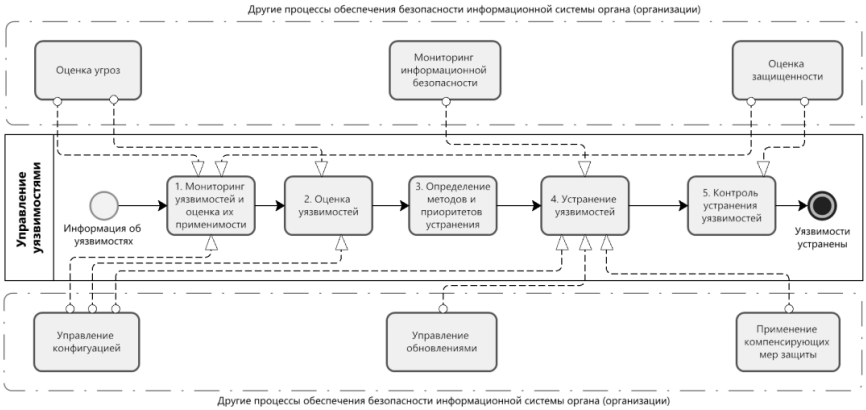

Схема процесса управления уязвимостями

Vulnerability management process diagram

1.1. ПОДХОДЫ К ПРИОРИТИЗАЦИИ УЯЗВИМОСТЕЙ

После проведения работ по мониторингу и оценке уязвимостей наступает процесс их приоритизации. Приоритизация уязвимостей – это процесс систематической оценки и ранжирования уязвимостей на основе их потенциального воздействия (или других показателей) для определения очередности устранения. Количество уязвимостей, выявленных в процессе сканирования ресурсов, может достигать десятков тысяч, а иногда и больше, из-за этого зачастую возникает проблема определения их приоритета.

Человеческие ресурсы всегда ограничены, вследствие этого практически невозможно устранить все найденные уязвимости. В первую очередь необходимо обращать внимание на те уязвимости, с помощью которых можно нанести наибольший ущерб организации. Главная задача на этапе приоритизации – определить наиболее критичные уязвимости для бизнес-процессов. Для организаций из разных сфер деятельности будут характерны свои уязвимости. Например, для компании, ведущей свою деятельность в области электронной коммерции, наиболее критичны веб-уязвимости, а для организации, занимающейся производством продукции, критичными будут уязвимости, дающие возможность вывести из строя производственное оборудование.

Отсутствие четкой системы приоритизации приводит к неправильному распределению ресурсов для устранения уязвимостей. Чтобы избежать подобных трудностей, специалистам по информационной безопасности необходимо четко понимать основные бизнес-процессы организации.

Эффективная приоритизация уязвимостей позволяет организациям рационально распределять свои ресурсы и сосредоточиться на снижении наиболее критических рисков для своих информационных систем и данных.

Существуют следующие основные подходы к приоритизации уязвимостей.

1. Потенциальное воздействие на информационную систему

Потенциальное воздействие на информационную систему – это ущерб, который проэксплуатированная уязвимость может оказать на информационные системы организации. Уязвимости обычно оцениваются на основе такой шкалы, как «Общая система оценки уязвимостей» (CVSS), которая учитывает сложность доступа, требования к аутентификации и влияние на конфиденциальность, целостность и доступность.

CVSS позволяет легко найти уязвимость, определить, какое программное обеспечение уязвимо, и найти соответствующие исправления.

Однако есть два основных недостатка CVSS:

- огромное количество уязвимостей помечено CVSS как «высокие» или «критические», хотя очень немногие из них когда-либо фактически использовались в реальных условиях;
- рейтинг CVSS не имеет никакого отношения к тому, насколько важны затронутые ИТ-активы, их тип, роль и выполняемые функции в информационной системе. Это может отвлечь внимание от защиты более важных ресурсов.

2. Сложность эксплуатации

Сложность эксплуатации (эксплуатируемость) выражается в повышении трудоемкости, с которой уязвимость может быть использована злоумышленником, и в наборе профессиональных навыков. Эти данные помогают сосредоточиться на тех уязвимостях, которые с наибольшей вероятностью станут объектом атаки злоумышленников.

3. Инфраструктурные показатели

Инфраструктурные (контекстные) показатели отражают факт взаимосвязи уязвимости с конкретной организационной средой, учитывая роль системы, данные, которые она обрабатывает, и ее важность для бизнес-операций. Уязвимость в критически важной системе будет иметь более высокий приоритет, чем уязвимость в менее критичной системе. Этот метод позволяет учитывать следующее:

- чувствительность активов, затронутых уязвимостью, и их важность для деятельности организации;
- уязвимости, которые могут оказать прямое влияние на непрерывность бизнеса (например, финансовые операции или конфиденциальные данные).

4. Использование средств защиты информации

Средства защиты информации (СЗИ) относятся к мерам безопасности и гарантиям, позволяющим смягчить или не допустить эксплуатацию уязвимости. Оценка уязвимостей в контексте использующихся СЗИ помогает эффективно распределять ресурсы.

Этот метод позволяет отдавать более высокий приоритет уязвимостям в тех системах, в которых отсутствует глубокоэшелонированная защита, плохие методы обеспечения безопасности или устаревшие конфигурации безопасности.

5. Разведка угроз (Threat Intelligence)

Включение анализа угроз в процесс определения приоритетов уязвимостей позволяет организациям выявлять уязвимости, которые активно используются в реальных условиях. Эта информация может помочь компаниям сосредоточить свои усилия на уязвимостях, которые представляют непосредственную угрозу, гарантируя эффективное распределение ресурсов для устранения наиболее серьезных рисков.

6. Сложность устранения

Оценка доступности исправлений расставляет приоритеты для тех уязвимостей, у которых исправления или меры по устранению недоступны или труднореализуемые.

7. Комбинация ключевых факторов

Чтобы эффективно расставить приоритеты в отношении рисков безопасности, важно найти баланс между этими ключевыми факторами. Слишком сильная зависимость от одного фактора (например, оценок CVSS) может привести к неполному представлению о риске, связанном с уязвимостью. Вместо этого можно рассмотреть все эти факторы вместе (или часть), чтобы получить полное представление о ландшафте рисков и соответствующим образом расставить приоритеты уязвимостей. Это позволит лучше подготовиться к эффективному распределению ресурсов и сосредоточить свое внимание на наиболее критических уязвимостях.

2. АЛГОРИТМЫ ПРИОРИТИЗАЦИИ УЯЗВИМОСТЕЙ

2.1. МЕТОДИКА ОЦЕНКИ КРИТИЧНОСТИ ФСТЭК РОССИИ

ФСТЭК России разработал и рекомендовал к применению методический документ «Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств».

Расчет критичности уязвимости в соответствии с методикой происходит по следующей формуле:

$$V = I_{\text{CVSS}} \cdot I_{\text{inf}\,r}, \tag{1}$$

Показатель I_{CVSS} определяется путем расчета базовых, временных и контекстных метрик применительно к конкретной информационной системе по методике (CVSS) 3.0 или 3.1.

Показатель $I_{\text{inf}\,r}$ характеризует влияние уязвимости программных, программно-аппаратных средств на функционирование информационной системы. Этот показатель рассчитывается по следующей формуле:

$$I_{\text{inf}\,r} = k \cdot K + l \cdot L + p \cdot P, \tag{2}$$

где K – показатель, характеризующий тип компонента информационной системы, подверженного уязвимости; L – показатель, характеризующий количество уязвимых компонентов информационной системы (автоматизированных рабочих мест, серверов, телекоммуникационного оборудования, средств защиты информации и других компонентов); P – показатель, характеризующий влияние уязвимого компонента на защищенность периметра информационной системы; k, l, p – весовые коэффициенты показателей.

Расчет весовых коэффициентов и оценок показателей, определяющих влияние уязвимости программных, программно-аппаратных средств на информационную систему, проводится в соответствии с табл. 1.

Таблица 1

Table 1

Оценки показателей

Indicator ratings

Показатель	Вес	Значение	Оценка	Итог ($k \cdot K_i$, $l \cdot Lj$, $p \cdot Pm$)
Тип компонента информационной системы, подверженного уязвимости (K)	0,4	Уязвимости подвержены компоненты информационной системы, обеспечивающие реализацию критических процессов (бизнес-процессов), функций, полномочий	1	0,4
		Уязвимости подвержены серверы	0,8	0,32
		Уязвимости подвержено телекоммуникационное оборудование, система управления сетью передачи данных	0,8	0,32
		Уязвимости подвержены автоматизированные рабочие места	0,5	0,2
		Уязвимости подвержены другие компоненты	0,5	0,2
Количество уязвимых компонентов информационной системы (автоматизированных рабочих мест, серверов, телекоммуникационного оборудования, средств защиты информации и других компонентов) (L)	0,2	Более 70 % компонентов от общего числа компонентов в информационной системе	1	0,2
		50…70 % компонентов от общего числа компонентов в информационной системе	0,8	0,16
		10…50 % компонентов от общего числа компонентов в информационной системе	0,6	0,12
		Менее 10 % компонентов от общего числа компонентов в информационной системе	0,5	0,10

Окончание табл. 1

End of the Tab. 1

Показатель	Вес	Значение	Оценка	Итог ($k \cdot K_i$, $l \cdot Lj$, $p \cdot Pm$)
Влияние на эффективность защиты периметра системы, сети (P)	0,4	Уязвимое программное, программно-аппаратное средство доступно из сети Интернет	1	0,4
		Уязвимое программное, программно-аппаратное средство недоступно из сети Интернет	0,5	0,2

В итоге полученная количественная оценка переводится в качественную в соответствии с табл. 2.

Таблица 2

Table 2

Перевод баллов в качественную оценку

Converting points into qualitative assessment

Суммарное количество баллов уязвимости	Оценка уровня критичности уязвимости
$7{,}0 \le V \le 10{,}0$	Критичный
$4{,}5 \le V < 7{,}0$	Высокий
$1{,}5 \le V < 4{,}5$	Средний
$V < 1{,}5$	Низкий

Методика в качестве варианта получения оценки I_{CVSS} предлагает применять калькулятор Банка данных угроз безопасности информации ФСТЭК России. Поэтому расчет показателя для большого числа уязвимостей является трудоемкой задачей, так как на данный момент нет инструментов для автоматизации расчета оценок по контекстному вектору CVSS.

2.2. МОДЕЛЬ КОНТЕКСТНО-ЗАВИСИМОЙ ПРИОРИТЕЗАЦИИ УЯЗВИМОСТЕЙ (CAVP)

Данная модель, во-первых, улучшает существующие метрики CVSS за счет включения временных характеристик уязвимостей. Во-вторых, обеспечивает пошаговый процесс определения приоритетов уязвимостей, который можно интегрировать в рабочий процесс управления рисками организации. Модель CAVP состоит из следующих этапов:

- создание и анализ базы данных CVE;
- сканирование уязвимостей;
- расчет контекстно-зависимой системы оценки уязвимостей (CAVSS);
- визуализация определения приоритетов уязвимостей.

Тремя категориями временных показателей CVSS являются зрелость кода эксплойта (ECM), уровень устранения (RL) и достоверность отчета (RC). В настоящее время не существует определенных показателей для этих временных метрик.

В разрабатываемой методике определен набор эвристических правил для определения различных значений временных метрик (табл. 3).

Таблица 3

Table 3

Значения временных меток

Timestamp values

Метрика	Значение метрики	Правило
Зрелость кода эксплойта (ECM)	Not Defined	Not used
	High	A CNA (Vendors and Projects) link & Vendor Advisory tag
	Functional	Third Party Advisory & ECM Value is NOT High
	Proof of Concept	(VDB Entry tag or US Government Resource tag or URL contains SecurityFocus or SecurityTracker or Exploit-Db)
	Unproven	Not satisfy any rules above (default)

Окончание табл. 3

End of the Tab. 3

Метрика	Значение метрики	Правило
Уровень исправления (RL)	Unavailable	Not used
	Official Fix	A CNA (Vendors and Projects) link and Patch tag
	Temporary Fix	Excluded
	Workaround	Patch tag OR Mitigation tag & RL Value is NOT Official Fix
	Not Defined	Not satisfy any rules above (default)
Доверие к отчету (RC)	Not Defined	Not used
	Confirmed	A CNA (Vendors and Projects) link and Patch tag
	Reasonable	VDB Entry tag Or Issue Tracking tag & RC value is NOT Confirmed
	Unknown	Not satisfy any rules below (default)

На основе определенных значений временных показателей можно рассчитать временную оценку на основе данных из базы данных CVE, используя следующее уравнение:

$$\mathrm{CAVSS}(T) = [B \cdot ECM \cdot RL \cdot RC]. \quad (3)$$

Затем общий балл CAVSS рассчитывается по формуле, приведенной ниже:

$$\mathrm{CAVSS}(0) = \mathrm{MIN}(B, T, E), \quad (4)$$

Как и CVSS, общий балл CAVSS затем делится на уровни критичности: критический, высокий, средний, низкий.

Благодаря применению модели CAVP только от 20 до 30 % известных CVE были приоритетными для дальнейшего расследования. Это позволило бы командам SOC лучше распределять ограниченные ресурсы для устранения уязвимостей с высоким риском.

2.3. НАСТУПАТЕЛЬНЫЙ ПОДХОД К ПРИОРИТИЗАЦИИ

Взяв за основу наступательную безопасность и выявив уязвимости, которые могут привести к взлому, данный подход предлагает три дополнительных показателя в дополнение к CVSS.

Weaponized Exploit (WX) – подсчет ссылок на эксплойты (ExploitDB, Metasploit и Github). Это неограниченное число, которое дает представление о том, насколько широко доступен эксплойт для данной уязвимости. Это также неявно сообщает организации, что доступ к эксплуатации становится проще по мере увеличения рейтинга

Utility – это полезный показатель для выявления как текущей, так и будущей угрозы (если она еще не использована). Измерение ведется по трем категориям: 0, 1 и 2. Например, уязвимости удаленного использования кода обычно очень привлекательны для злоумышленников.

Opportune – это мера, позволяющая упростить поиск уязвимостей, для которых может не потребоваться код эксплойта (например, обнаружение пароля по умолчанию). Мы разделяем подходящее время на две категории: 0 означает, что благоприятного момента нет, 1 означает, что подходящее время существует. Уязвимости с подходящей оценкой 1 – это те, которые не требуют какого-либо кода для использования, поэтому очень привлекательны для хакеров.

В итоге оценка учитывает как CVSS, так и новые метрики. Расчет производится по следующей формуле:

$$(\mathrm{CVSS} + \mathrm{WX})(\mathrm{utility} + 1)(\mathrm{opportune} + 1) \times$$

$$\times (\mathrm{EnvironmentalFactors}), \qquad (5)$$

Следовательно, учитывается вероятность возможности использования уязвимости, ее воздействие, нынешний и будущий ландшафт угроз. Методика также включает контекстные факторы для актива с учетом доступности из сети Интернет и критичности (с разными весами).

Таким образом, вместо использования категориального подхода для определения приоритетов или ограниченной формулы, предписанной CVSS, эта формула позволяет ранжировать уязвимости и сосредоточиться на наиболее важных в первую очередь.

2.4. СИСТЕМА РЕЙТИНГА И ОЦЕНКИ УЯЗВИМОСТИ (VRSS)

Система рейтинга и оценки уязвимостей (VRSS) использует качественный рейтинг и количественный балл для оценки уязвимостей. Для расчета оценки используются те же шесть показателей, что и в базовой группе CVSSv2.

Качественный рейтинг основан на трех показателях воздействия:

- влияние на конфиденциальность;
- влияние на целостность;
- влияние на доступность.

Каждому из этих трех показателей можно присвоить три разных значения («не влияет», «влияет частично» и «влияет»).

Уязвимость сначала качественно классифицируется на три уровня (высокий, средний и низкий) на основе оценки воздействия в диапазоне 6–9, 2–5 и 0–1 соответственно. Оценка воздействия присваивается на основе различных комбинаций воздействия на объекты.

Например, когда каждый из коэффициентов: К (конфиденциальность), Ц (целостность), Д (доступность) имеет полное влияние, присваивается оценка воздействия 9, а оценка воздействия 0 назначается при отсутствии влияния. Оценка возможности использования в диапазоне от 0 до 1 генерируется с использованием показателей:

- вектор доступа;
- сложность доступа;
- аутентификация.

Формула оценки эксплуатационной способности аналогична формуле CVSS. Веса этих метрик такие же, как и в CVSS v2. Окончательная оценка в диапазоне от 0 до 10 получается путем сложения оценки воздействия и оценки эксплуатационной способности:

$$\begin{gathered} \textit{Exploitability score} = 2 \cdot \textit{Access Vector} \cdot \textit{Access Complexity}, \\ \textit{Base score} = \textit{Exploitability score} + \textit{Impact Score}. \end{gathered} \tag{6}$$

VRSS использует стратегию доминирования воздействия для расчета баллов. Оценки, полученные с помощью VRSS, сильно смещены в сторону пока-

зателей воздействия. В VRSS оценка воздействия может принимать значения в диапазоне от 0 до 9, а оценка возможности использования варьируется только от 0 до 1.

3. ПРЕДЛАГАЕМЫЙ МЕТОД ПРИОРИТИЗАЦИИ УЯЗВИМОСТЕЙ

При изучении особенностей приоритизации уязвимостей предлагается алгоритм, дополняющий методику расчета критичности уязвимостей ФСТЭК. Для возможности автоматизации в формуле в качестве параметра I_{CVSS} учитывается базовая оценка CVSS 3.0 или 3.1. При этом в параметре $I_{\text{inf}\,r}$ добавляются коэффициенты Exploitation Activities и Exploit Availability, которые учитывают реальные факты использования уязвимостей и публичную доступность эксплойта. Эта информация может быть получена из открытых источников, например: AttackerKB, CISA KEV, Metasploit, Vulners.com, EPSS.

Также к инфраструктурным показателям помимо типа компонента информационной системы добавляется показатель Asset priority, который дифференцирует активы по степени влияния на бизнес-процессы защищаемой организации и измеряется по шкале от 1 до 10. Это позволит избежать ситуации, когда два одинаковых по типу актива имеют одинаковые веса, хотя имеют разную критичность в рамках информационной системы организации.

Формула для оценки уязвимостей может быть сформулирована как взвешенная комбинация различных факторов и может выглядеть следующим образом:

$$\text{Score} = I_{\text{CVSS}} \cdot I_{\text{inf}\,r}, \tag{7}$$

$$I_{\text{inf}\,r} = K1 * COUNT(IP) + K2 * Asset\ \ priority + K3 * Asset\ type +$$

$$+ K4 * Perimetr\ type + K5 * Exploitation\ \ Activities + K6 * Exploit\ \ Availability. \tag{8}$$

Весовые коэффициенты $K1$ – $K6$ позволяют настраивать важность каждого из параметров в оценке критичности уязвимости и в сумме должны равняться единице^

- $K1 = 0.2$,
- $K2 = 0.2$,
- $K3 = 0.2$,
- $K4 = 0.2$,

- $K5 = 0.1$,
- $K6 = 0.1$.

Выражение (8) может быть адаптировано в соответствии с конкретными требованиями защищаемой организации. Важно также учесть, что весовые коэффициенты $K1 – K6$ могут быть подобраны в результате обсуждений с заинтересованными сторонами и экспертами в области информационной безопасности.

ЗАКЛЮЧЕНИЕ

Подводя итог, можно сделать вывод о ключевой важности эффективного процесса управления уязвимостями и стратегии их приоритизации для обеспечения безопасности информационных ресурсов.

Внедрение алгоритмов приоритизации уязвимостей предоставляет возможность оптимизации ресурсов, уменьшения времени устранения уязвимостей и повышения общей безопасности. Однако выбор правильных алгоритмов и параметров для оценки критичности требует тщательного анализа контекста организации, учета особенностей среды и внутренних потребностей.

В результате исследования был предложен вариант алгоритма приоритизации уязвимостей, дополняющий методику расчета критичности уязвимостей ФСТЭК. Добавление параметров Exploitation Activities и Exploit Availability позволит учитывать факты использования уязвимостей в реальном времени и публичную доступность эксплойта, что даст более полную картину о ландшафте угроз по каждой уязвимости.

Параметр Asset priority позволит дифференцировать активы по степени влияния на бизнес-процессы защищаемой организации. Это поможет сосредоточиться на уязвимостях, находящихся на наиболее критичных активах, и даст возможность оптимизировать распределение ресурсов.

СПИСОК ЛИТЕРАТУРЫ

1. *Seaberg A.* 1,900 new cyber vulnerabilities each month in 2023, Says Coalition // Independent Agent magazine. – 2023, 22 February. – URL: https://www.iamagazine.com/markets/1-900-new-cyber-vulnerabilities-each-month-in-2023-says-coalition (accessed: 11.03.2024).

2. Руководство по организации процесса управления уязвимостями в органе (организации). Методический документ / ФСТЭК России. – URL: https://fstec.ru/files/1096/---17--2023-/2011/---17--2023-.pdf (дата обращения: 11.03.2024).

3. Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств / ФСТЭК России. – URL: https://fstec.ru/files/992/---28--2022-804/1722/---28--2022-.pdf (дата обращения: 11.03.2024).

4. *Баринов А.Е., Скурлаев С.В., Соколова А.Н.* Методика оценки рисков, вызванных уязвимостями в программном обеспечении автоматизированных систем управления технологическими процессами // Вестник УрФО. Безопасность в информационной сфере. – 2017. – № 3 (25). – С. 34–42. – URL: https://www.elibrary.ru/item.asp?id=30770418 (дата обращения: 11.03.2024).

5. *Нурдинов Р.А.* Определение вероятности нарушения критических свойств информационного актива на основе CVSS метрик уязвимостей // Современные проблемы науки и образования. – 2014. – № 3. – С. 70. – URL: https://www.elibrary.ru/item.asp?id=22527869 (дата обращения: 11.03.2024).

6. *Котенко И.В., Двойникова А.Е.* Система оценки рисков CVSS и ее использование для анализа защищенности компьютерных систем // Защита информации. Инсайд. – 2017. – № 5 (41). – С. 54–60. – URL: https://www.elibrary.ru/item.asp?id=23099118 (дата обращения: 12.03.2024).

7. *Краснов А.Е., Мосолов А.С., Феоктистова Н.А.* Оценивание устойчивости критических информационных инфраструктур к угрозам информационной безопасности // Безопасность информационных технологий. – 2021. – Т. 28, № 1. – С. 106–120. – DOI: 10.26583/bit.2021.1.09.

8. *Кисилева Т.В., Маслова Е.В.* Процесс управления информационными рисками на основе их анализа // Системы управления и информационные технологии. – 2011. – № 2-1 (44). – С. 129–133. – URL: https://www.elibrary.ru/item.asp?id=16537297 (дата обращения: 12.03.2024).

9. *Риберг Г., Малмквист К., Щербакова А.* Многоуровневый подход к оценке безопасности программных средств // Вопросы кибербезопасности. – 2014. – № 1 (2). – С. 36–39. – URL: https://www.elibrary.ru/item.asp?id=21288719 (дата обращения: 12.03.2024).

10. Оценка применимости методики CVSS для риск-анализа защищаемых систем / А.С. Пахомова, Д.Н. Рахманин, Л.В. Паринова, Ю.К. Язов // Информация и безопасность. – 2017. – Т. 20, № 1. – С. 129–132. – URL: https://www.elibrary.ru/item.asp?id=29315860 (дата обращения: 12.03.2024).

11. *Бобов М.Н., Горячко Д.Г.* Оценка рисков информационной безопасности с использованием стандарта CVSS 3.0 // Комплексная защита информации: материалы XXII научно-практической конференции. – Новополоцк, 2017. – С. 19–22. – URL: https://www.elibrary.ru/item.asp?id=32718090 (дата обращения: 12.03.2024).

12. *Doynikova E., Kotenko I.* CVSS-based probabilistic risk assessment for cyber situational awareness and countermeasure selection // Proceedings – 2017 25th Euromicro International Conference on Parallel, Distributed and Net-

work-Based Processing (PDP). – St. Petersburg, 2017. – P. 346–353. DOI: 10.1109/PDP.2017.44.

13. *Павлов Д.В., Рахматулин К.Е.* CVSS. Контекстные метрики безопасности // Применение современных информационных технологий в служебно-боевой деятельности: сборник статей межвузовской научно-практической конференции. – Пермь, 2022. – С. 123–132. – URL: https://www.elibrary.ru/item.asp?id=50033413 (дата обращения: 12.03.2024).

14. *Давлатов Ш.Р., Кучинский П.В.* Анализ защищенности веб-ресурсов на основе метрики CVSS // Информатика. – 2020. – Т. 17, № 3. – С. 72–77. – DOI: 10.37661/1816-0301-2020-17-3-72-77.

15. Quantitative model of attacks on distribution automation systems based on CVSS and attack trees / E. Li, C. Kang, F. Chang, L. He, M. Hu, X. Li // Information (Switzerland). – 2019. – Vol. 10 (8). – P. 251. – DOI: 10.3390/info10080251.

16. *Мельников А.В., Чирков В.Е.* Алгоритм оценки относительного уровня опасности совместной эксплуатации уязвимостей информационной безопасности на основе CVSS // Вестник Воронежского института МВД России. – 2019. – № 1. – С. 37–44. – URL: https://www.elibrary.ru/item.asp?id=37164655 (дата обращения: 12.03.2024).

17. *Столярова Н.Я., Золотухина Е.Б.* Классификация программного приложения с помощью инструментальных методов обработки информации согласно метрике уязвимостей CVSS v2.0 // Colloquium-Journal. – 2019. – № 11-1 (35). – С. 136–142. – URL: https://www.elibrary.ru/item.asp?id=38304274 (дата обращения: 12.03.2024).

18. CVSS metric-based analysis, classification and assessment of computer network threats and vulnerabilities / V.R. Kebande, I. Kigwana, H.S. Venter, R.D. Wario, N.M. Karie // 2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD). – IEEE, 2018. – P. 8465420. – DOI: 10.1109/ICABCD.2018.8465420.

19. System for estimation CVSS severity metrics of vulnerability based on text mining technology / A. Nikonov, A. Vulfin, V. Vasilyev, A. Kirillova, V. Mikhailov // Proceedings of ITNT 2021 – 7th IEEE International Conference on Information Technology and Nanotechnology. – IEEE, 2021. – DOI: 10.1109/ITNT52450.2021.9649232.

20. Cybersecurity risk assessment based on cognitive attack vector modeling with CVSS score / A. Nikonov, A. Vulfin, V. Vasilyev, A. Kirillova // Proceedings of ITNT 2021 – 7th IEEE International Conference on Information Technology and Nanotechnology. – IEEE, 2021. – DOI: 10.1109/ITNT52450.2021.9649191.

21. *Wu Ch., Wen T., Zhang Yu.* A revised CVSS-based system to improve the dispersion of vulnerability risk scores // Science China Information Sciences. – 2018. – Vol. 62 (3). – P. 39102. – DOI: 10.1007/s11432-017-9445-4.

22. *Figueroa-Lorenzo S., Añorga J., Arrizabalaga S.* A survey of IIoT protocols: a measure of vulnerability risk analysis based on CVSS // ACM Computing Surveys. – 2020. – Vol. 53 (2). – P. 3381038. – DOI: 10.1145/3381038.

23. *Majid M.A., Ariffi K.A.Z.* Success factors for cyber security operation center (SOC) establishment // Proceedings of the 1st International Conference on Informatics, Engineering, Science and Technology, INCITEST 2019, 18 July 2019. – Bandung, Indonesia, 2019. – DOI: 10.4108/eai.18-7-2019.2287841.

24. A human capital model for mitigating security analyst burnout / S. Sundaramurthy, X. Ou, A.G. Bardas, J. Case, M. Wesch, J. Mchugh, S.R. Rajagopalan // SOUPS 2015. Proceedings of the Eleventh Symposium on Usable Privacy and Security. – Ottava, Canada, 2015. – P. 347–359.

25. *Onwubiko C.* Cyber security operations centre: Security monitoring for protecting business and supporting cyber defense strategy // 2015 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), London, UK. – IEEE, 2015. – P. 1–10. – DOI: 10.1109/CyberSA.2015.7166125.

26. *Andrade R.O., Yoo S.G.* Cognitive security: a comprehensive study of cognitive science in cybersecurity // Journal of Information Security and Applications. – 2019. – Vol. 48. – P. 102352. – DOI: 10.1016/j.jisa.2019.06.008.

27. *Ahmed R.K.A.* Overview of security metrics // Software Engineering. – 2016. – Vol. 4 (4). – P. 59–64. – DOI: 10.11648/j.se.20160404.11.

28. *Houngbo P.J., Hounsou J.T.* Measuring information security: understanding and selecting appropriate metrics // International Journal of Computer Science and Security. – 2015. – Vol. 9 (2). – P. 108–120.

Подсевалов Артем Георгиевич, лаборант кафедры защиты информации Новосибирского государственного технического университета. Основное направление научных исследований – кибербезопасность, управление уязвимостями, алгоритмы приоритизации. E-mail: podsevalov.2019@stud.nstu.ru

Кудинов Михаил Игоревич, лаборант кафедры защиты информации Новосибирского государственного технического университета. Основное направление научных исследований – кибербезопасность, управление уязвимостями, алгоритмы приоритизации. E-mail: m.kudinov.2019@stud.nstu.ru

DOI: 10.17212/2782-2230-2024-1-52-73

Issues of using vulnerability prioritization algorithms when organizing the vulnerability management process*

A.G. Podsevalov[1], M.I. Kudinov[2]

[1] *Novosibirsk State Technical University, 20 Karl Marx Avenue, Novosibirsk, 630073, Russian Federation, laboratory assistant of the Information Security Department. E-mail: podsevalov.2019@stud.nstu.ru*
[2] *Novosibirsk State Technical University, 20 Karl Marx Avenue, Novosibirsk, 630073, Russian Federation, laboratory assistant of the Information Security Department. E-mail: m.kudinov.2019@stud.nstu.ru*

The purpose of this scientific research is to analyze the possibilities of increasing the level of protection of an organization's defense against cyber threats by applying vulnerability prioritization algorithms. There are various approaches to creating vulnerability prioritization algorithms that take into account many metrics. For example, the potential impact on the information system when exploiting the vulnerability, the complexity of exploiting the vulnerability, the difficulty of eliminating it, etc. This article is devoted to the issues of organizing the process of managing vulnerabilities, in particular, various methods (algorithms) of their prioritization to determine the priority of elimination and the rational distribution of human resources of the organization. Various algorithms for prioritizing vulnerabilities were reviewed and analyzed, and conclusions were drawn about their advantages and disadvantages. In conclusion, the work proposes a version of the vulnerability prioritization algorithm that takes into account the most important metrics, as well as the recommendations of the FSTEC of Russia.

Keywords: information security, cybersecurity, vulnerability, prioritization, prioritization algorithms, threat analysis, security level, risks, vulnerability management process, CVSS, FSTEC

REFERENCES

1. Seaberg A. 1,900 new cyber vulnerabilities each month in 2023, Says Coalition. *Independent Agent magazine*, 2023, 22 February. Available at: https://www.iamagazine.com/markets/1-900-new-cyber-vulnerabilities-each-month-in-2023-says-coalition (accessed 11.03.2024).

2. FSTEC of Russia. *Rukovodstvo po organizatsii protsessa upravleniya uyazvimostyami v organe (organizatsii). Metodicheskii dokument* [Guidelines for organizing the process of vulnerability management in an agency (organization)]. Available at: https://fstec.ru/files/1096/---17--2023-/2011/---17--2023-.pdf (accessed 11.03.2024).

* *Received 12 February 2024.*

3. FSTEC of Russia. *Metodika otsenki urovnya kritichnosti uyazvimostei programmnykh, programmno-apparatnykh sredstv* [Methodology for assessing the level of criticality of software, firmware and hardware vulnerabilities]. Available at: https://fstec.ru/files/992/---28--2022-804/1722/---28--2022-.pdf (accessed 11.03.2024).

4. Barinov A.E., Skurlaev S.V., Sokolov A.N. Metodika otsenki riskov, vyzvannykh uyazvimostyami v programmnom obespechenii avtomatizirovannykh sistem upravleniya tekhnologicheskimi protsessami [Method for risk assessment caused by vulnerabilities in ICS software]. *Vestnik UrFO. Bezopasnost' v informatsionnoi sfere = Journal of the Ural Federal District. Information security*, 2017, no. 3 (25), pp. 34–42. Available at: https://www.elibrary.ru/item.asp?id=30770418 (accessed 11.03.2024).

5. Nurdinov R.A. Opredelenie veroyatnosti narusheniya kriticheskikh svoistv in-formatsionnogo aktiva na osnove CVSS metrik uyazvimostei [Determining the probability of violation of critical properties of an information asset based on CVSS vulnerability metrics]. *Sovremennye problemy nauki i obrazovaniya = Modern problems of science and education*, 2019, no. 3, p. 70. Available at: https://www.elibrary.ru/item.asp?id=22527869 (accessed 11.03.2024).

6. Kotenko I.V., Dvoinikova A.E. Sistema otsenki riskov CVSS i ee ispol'zovanie dlya analiza zashchishchennosti komp'yuternykh sistem [CVSS risk assessment system and its use for analyzing the security of computer systems]. *Zashchita informatsii. Insaid*, 2017, no. 5 (41). pp. 54–60. (In Russian). Available at: https://www.elibrary.ru/item.asp?id=23099118 (accessed 12.03.2024).

7. Krasnov A.E., Mosolov A.S., Feoktistova N.A. Otsenivanie ustoichivosti kriticheskikh informatsionnykh infrastruktur k ugrozam informatsionnoi bezopasnosti [Assessing the resilience of critical information infrastructures to information security threats]. *Bezopasnost' informatsionnykh tekhnologii = IT Security*, 2021, vol. 28, no. 1, pp. 106–120. – DOI: 10.26583/bit.2021.1.09.

8. Kisileva T.V., Maslova E.V. Protsess upravleniya informatsionnymi riskami na osnove ikh analiza [Administrative process by the information risks on the basis of their analysis]. *Sistemy upravleniya i informatsionnye tekhnologii = Automation and Remote Control*, 2011, no. 2-1 (44), pp. 129–133. (In Russian). Available at: https://www.elibrary.ru/item.asp?id=16537297 (accessed 12.03.2024).

9. Reber G., Malmquist K., Shcherbakov A. Mapping the application security terrain. *Voprosy kiberbezopasnosti = Issues of cybersecurity*, 2014, no. 1 (2), pp. 36–39. Available at: https://www.elibrary.ru/item.asp?id=21288719 (accessed 12.03.2024).

10. Pakhomova A.S., Rahmanin D.N., Parinova L.V., Yazov Yu.K. Otsenka primenimosti metodiki CVSS dlya risk-analiza zashchishchaemykh sistem [Usability assesment of CVSS version 2 vulnerability ckoring to risk-analysis of trusted

systems]. *Informatsiya i bezopasnost' = Information & Security*, 2017, vol. 20, no. 1, pp. 129–132. Available at: https://www.elibrary.ru/item.asp?id=29315860 (accessed 12.03.2024).

11. Bobov M.N., Goryachko D.G. [Information security risk assessment using the CVSS 3.0 standard]. *Kompleksnaya zashchita informatsii* [Comprehensive information protection]. Materials of the XXII scientific and practical conference, Polotsk, 2017, pp. 19–22. (In Russian). Available at: https://www.elibrary.ru/item.asp?id=32718090 (accessed 12.03.2024).

12. Doynikova E., Kotenko I. CVSS-based probabilistic risk assessment for cyber situational awareness and countermeasure selection. *Proceedings – 2017 25th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP)*, St. Petersburg, 2017, pp. 346–353. DOI: 10.1109/PDP.2017.44.

13. Pavlov D.V., Rahmatulin K.E. [CVSS. Contextual security metrics]. *Primenenie sovremennykh informatsionnykh tekhnologii v sluzhebno-boevoi deyatel'nosti* [Application of modern information technologies in service and combat activities], Perm, 2022, pp. 123–132. (In Russian). Available at: https://www.elibrary.ru/item.asp?id=50033413 (accessed 12.03.2024).

14. Davlatov Sh.R., Kuchinsky P.V. Analiz zashchishchennosti veb-resursov na osnove metriki CVSS [Web resource security analysis based on CVSS metrics]. *Informatika = Informatics*, 2020, vol. 17, no. 3, pp. 72–77. DOI: 10.37661/1816-0301-2020-17-3-72-77.

15. Li E., Kang C., Chang F., He L., Hu M., Li X. Quantitative model of attacks on distribution automation systems based on CVSS and attack trees. *Information* (Switzerland), 2019, vol. 10 (8), p. 251. DOI: 10.3390/info10080251.

16. Melnikov A.V., Chirkov V.E. Algoritm otsenki otnositel'nogo urovnya opasnosti sov-mestnoi ekspluatatsii uyazvimostei informatsionnoi bezopasnosti na osnove CVSS [Algorithm for assessing the relative level of danger of joint operation of information security vulnerabilities based on CVSS]. *Vestnik Voronezhskogo instituta MVD Rossii = Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia*, 2019, no. 1, pp. 37–44. Available at: https://www.elibrary.ru/item.asp?id=37164655 (accessed 12.03.2024).

17. Stolyarova N.Ya., Zolotukhina E.B. Klassifikatsiya programmnogo prilozheniya s pomo-shch'yu instrumental'nykh metodov obrabotki informatsii soglasno metrike uyazvimostei CVSS v2.0 [Classification of the software application with the help of instrumental methods of processing information according to the CVSS v2.0 vertification metric]. *Colloquium-Journal*, 2019, no. 11-1 (35), pp. 136–142. (In Russian). Available at: https://www.elibrary.ru/item.asp?id=38304274 (accessed 12.03.2024).

18. Kebande V.R., Kigwana I., Venter H.S., Wario R.D., Karie N.M. CVSS metric-based analysis, classification and assessment of computer network threats

and vulnerabilities. *2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD)*. IEEE, 2018, p. 8465420. DOI: 10.1109/ICABCD.2018.8465420.

19. Nikonov A., Vulfin A., Vasilyev V., Kirillova A., Mikhailov V. System for estimating CVSS severity metrics of vulnerability based on text mining technology. *Proceedings of ITNT – 7th IEEE International Conference on Information Technology and Nanotechnology*. IEEE, 2021. DOI: 10.1109/ITNT52450.2021.9649232.

20. Nikonov A., Vulfin A., Vasilyev V., Kirillova A. Cybersecurity risk assessment based on attack cognitive vector modeling with CVSS score. *Proceedings of ITNT – 7th IEEE International Conference on Information Technology and Nanotechnology*. IEEE, 2021. DOI: 10.1109/ITNT52450.2021.9649191.

21. Wu Ch., Wen T., Zhang Yu. A revised CVSS-based system to improve the dispersion of vulnerability risk scores. *Science China Information Sciences*, 2018, vol. 62 (3), p. 39102. DOI: 10.1007/s11432-017-9445-4.

22. Figueroa-Lorenzo S., Añorga J., Arrizabalaga S. A survey of IIoT protocols: a measure of vulnerability risk analysis based on CVSS. *ACM Computing Surveys*, 2020, vol. 53 (2), p. 3381038. DOI: 10.1145/3381038.

23. Majid M.A., Ariffi K.A.Z. Success factors for cyber security operation center (SOC) establishment. *Proceedings of the 1st International Conference on Informatics, Engineering, Science and Technology, INCITEST 2019*, 18 July 2019, Bandung, Indonesia. DOI: 10.4108/eai.18-7-2019.2287841.

24. Sundaramurthy S.C., Bardas A.G., Case J., Ou X., Wesch M., McHugh J., Rajagopalan S.R. A human capital model for mitigating security analyst burnout. *SOUPS 2015. Proceedings of the Eleventh Symposium on Usable Privacy and Security*, Ottava, Canada, 2015, pp. 347–359.

25. Onwubiko C. Cyber security operations centre: Security monitoring for protecting business and supporting cyber defense strategy. *2015 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, London, UK, 2015, pp. 1–10. DOI: 10.1109/CyberSA.2015.7166125.

26. Andrade R.O., Yoo S.G. Cognitive security: a comprehensive study of cognitive science in cybersecurity. *Journal of Information Security and Applications*, 2019, vol. 48, p. 102352. DOI: 10.1016/j.jisa.2019.06.008.

27. Ahmed R.K.A. Overview of security metrics. *Software Engineering*, 2016, vol. 4 (4), pp. 59–64. DOI: 10.11648/j.se.20160404.11.

28. Houngbo P.J., Hounsou J.T. Measuring information security: understanding and selecting appropriate metrics. *International Journal of Computer Science and Security*, 2015, vol. 9 (2), pp. 108–120.

Для цитирования:

Подсевалов А.Г., *Кудинов М.И.* Вопросы применения алгоритмов приоритизации уязвимостей при организации процесса vulnerability management // Безопасность цифровых технологий. – 2024. – № 1 (112). – С. 52–73. – DOI: 10.17212/2782-2230-2024-1-52-73.

For citation:

Podsevalov A.G., Kudinov M.I. Voprosy primeneniya algoritmov prioritizatsii uyazvimostei pri organizatsii protsessa vulnerability management [Issues of using vulnerability prioritization algorithms when organizing the vulnerability management process]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2024, no. 1 (112), pp. 52–73. DOI: 10.17212/2782-2230-2024-1-52-73.