УДК 004.056

С.П. Серёдкин, Д.А. Святковский

Иркутский государственный университет путей сообщения, г. Иркутск, Российская Федерация

УЯЗВИМОСТИ VS УГРОЗЫ: КЛЮЧЕВОЙ ФОКУС СОВРЕМЕННОЙ КИБЕРБЕЗОПАСНОСТИ

Аннотация. *Статья посвящена анализу основных составляющих защиты информационных систем, с акцентом на приоритетное управление уязвимостями по сравнению с реакцией на угрозы. Рассматриваются основные категории уязвимостей и угроз, а также аргументируется важность проактивного подхода, направленного на снижение рисков кибербезопасности и созданию устойчивой системы защиты.*
В статье рассматриваются современные подходы к обеспечению защиты информации, такие как автоматизация процессов, искусственный интеллект, DevSecOps и защита облачных систем. Отдельное внимание уделено вызовам, с которыми сталкиваются организации в условиях растущей сложности киберугроз, и предложены стратегии повышения эффективности управления уязвимостями. Материал предназначен для специалистов в области информационной безопасности, разработчиков и руководителей, заинтересованных в создании надежных и устойчивых информационных систем.

Ключевые слова: *уязвимости, угрозы, управление уязвимостями, кибербезопасность, DevSecOps, автоматизация.*

S.P. Seryodkin, D.A. Svyatkovsky

Irkutsk State Transport University, Irkutsk, the Russian Federation

VULNERABILITIES VS THREATS: THE KEY FOCUS OF MODERN CYBERSECURITY

Abstract. *The article is devoted to the analysis of the main components of information system protection, with an emphasis on priority vulnerability management in comparison with threat response. The main categories of vulnerabilities and threats are considered, and the importance of a proactive approach aimed at reducing cybersecurity risks and creating a sustainable protection system is argued. The article discusses modern approaches to information security, such as automation of processes, artificial intelligence, DevSecOps and protection of cloud systems. Special attention is paid to the challenges faced by organizations in the context of the growing complexity of cyber threats, and strategies for improving vulnerability management are proposed. The material is intended for information security specialists, developers and managers interested in creating reliable and sustainable information systems.*

Keywords: *vulnerabilities, threats, vulnerability management, cybersecurity, DevSecOps, automation.*

Введение

В современном цифровом мире, где информационные технологии обеспечивают функционирование практически всех сфер жизнедеятельности, кибербезопасность становится критически важной для обеспечения устойчивого функционирования, как государственных учреждений, так и бизнес сектора.

В центре внимания специалистов по кибербезопасности находятся два ключевых понятия: уязвимости и угрозы. Хотя обе категории играют значимую роль в процессах защиты информации, управление уязвимостями, по нашему мнению, оказывается более эффективным и приоритетным подходом по сравнению с реакцией на угрозы.

Так, в 2024 году было зарегистрировано рекордное количество уязвимостей, причем многие из них критически опасны. Аналитики отмечают, что атаки на основе недавно обнаруженных уязвимостей начинают проводиться уже через одну-две недели после их раскрытия, что оставляет компаниям минимальное время на реагирование. Доля уязвимостей в 2024

году остаётся высокой, что указывает на недостаточную эффективность текущих мер по их предотвращению [1, 2].

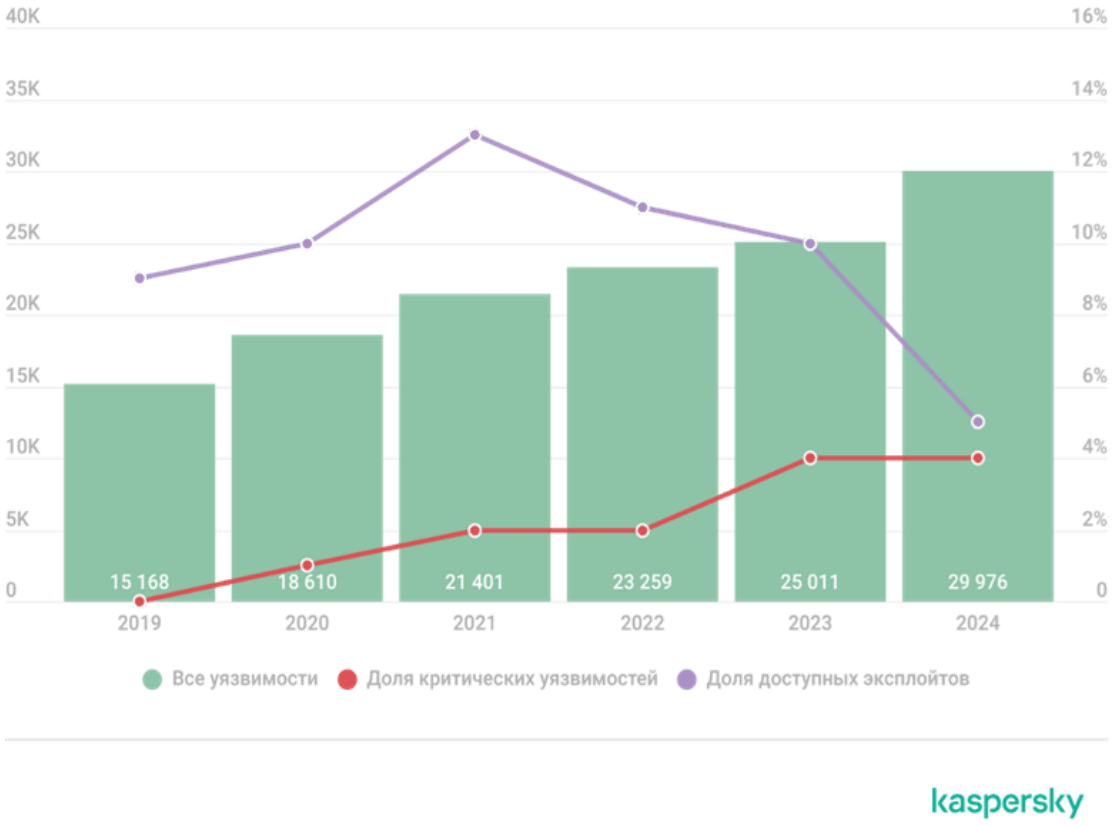

Рис. 1. Количество новых зарегистрированных уязвимостей

Цель данной статьи заключается в анализе подходов управления уязвимостями как инструментария в современных стратегиях кибербезопасности.

Понятие уязвимостей и угроз

Уязвимость представляет собой слабое место в системе, которое может быть использовано злоумышленником для проведения атаки. Уязвимости могут существовать на различных уровнях: программном обеспечении, аппаратном обеспечении, сетевых протоколах, человеческом факторе и в организационных процессах.

Угроза — это потенциальное событие, способное нанести ущерб системе или её компонентам. По природе источников, угрозы варьируются по своей природе и источникам, включая как внутренние, так и внешние факторы.

Приоритет управления уязвимостями

Управление уязвимостями предполагает выявление и устранение слабых мест до того, как они будут использованы злоумышленниками. Такой превентивный подход значительно снижает риск реализации атак. В отличие от этого, реакция на угрозы фокусируется на обнаружении и нейтрализации атак уже после их начала, что требует больше ресурсов и времени, а также может привести к значительным потерям [3].

Устранение уязвимостей напрямую уменьшает возможные точки атаки, делая систему менее привлекательной для злоумышленников. Это позволяет снизить общее количество потенциальных угроз, поскольку многие атаки основываются на эксплуатации известных уязвимостей. Управление уязвимостями служит фундаментом для обеспечения кибербезопасности, минимизируя необходимость в постоянной реакции на новые и возникающие угрозы.

В долгосрочной перспективе управление уязвимостями оказывается более экономически эффективным, чем реакция на угрозы. Исправление уязвимостей на ранних стадиях разработки или эксплуатации системы обходится значительно дешевле, чем устранение послед-

ствий успешных атак, включающих восстановление данных и прочие расходы. Инвестиции в управление уязвимостями позволяют организациям избежать значительного ущерба.

Систематическое управление уязвимостями способствует созданию многоуровневой системы защиты, в которой каждый уровень безопасности обеспечивает устранение потенциальных слабых мест. Такой подход обеспечивает более высокий уровень общей безопасности системы по сравнению с подходами, основанными исключительно на реагировании на угрозы.

Один из ярких примеров, когда уязвимость оказалась важнее самой угрозы, — атака ransomware WannaCry в 2017 году.

WannaCry распространялся по всему миру и нанёс ущерб на миллиарды долларов. Важнейшей особенностью этого инцидента было то, что сам вирус не был технологически сложным. Однако он использовал уязвимость SMBv1 (CVE-2017-0144), известную как EternalBlue, для проникновения и распространения внутри сетей [4].

Почему уязвимость оказалась важнее угрозы?

Незакрытая уязвимость сделала возможным масштаб атаки, EternalBlue была известна за несколько месяцев до начала атаки, а Microsoft выпустила патч (MS17-010) для её устранения. Однако многие организации проигнорировали обновление, что позволило WannaCry беспрепятственно распространяться.

Проактивное ликвидация уязвимости могло бы предотвратить атаки на компании, которые установили обновление вовремя, избежали последствий WannaCry. Угроза ransomware осталась нереализованной, так как её ключевой механизм — эксплуатация SMB — был устранён.

Реагирование на угрозы, особенно в случае крупных инцидентов, может быть дорогостоящим. Например, средняя стоимость утечки данных в 2023 году составила $4.45 млн. за инцидент [5]. Регулярное устранение уязвимостей обходится дешевле и минимизирует риски катастрофических последствий.

Современные тенденции в управлении уязвимостями

Автоматизация и искусственный интеллект.

С увеличением числа уязвимостей и сложностью угроз традиционные методы защиты оказываются недостаточно эффективными. Автоматизация процессов обнаружения и управления уязвимостями, а также использование искусственного интеллекта (ИИ) для анализа возникновения угроз, позволяет быстрее реагировать на инциденты и предугадывать потенциальные атаки. Однако, несмотря на развитие технологий, проактивное управление уязвимостями остается ключевым аспектом, на который следует обратить внимание [6].

Интеграция безопасности на этапы разработки (Development security operations).

Интеграция кибербезопасности в процесс разработки программного обеспечения с самого начала позволяет выявлять и устранять уязвимости на ранних стадиях. Данный подход способствует созданию более безопасных систем и снижает риски появления уязвимостей в конечном продукте, что в свою очередь уменьшает необходимость в последующей реакции на угрозы [7, 8].

Облачная безопасность.

С увеличением использования облачных сервисов возросла необходимость обеспечения безопасности данных, хранящихся в облаке. Управление уязвимостями и защита от угроз в облачной среде требует специальных подходов и инструментов, учитывающих особенности облачных архитектур. Обеспечение процесса устранения уязвимостей в облачных системах значительно снижает реализацию потенциальных угроз.

Повышение внимания к человеческому фактору.

Человеческий фактор продолжает оставаться одной из крупнейших источников угроз безопасности. Обучение сотрудников основам информационной безопасности и внедрение программ повышения осведомленности помогают минимизировать риски, связанные с ошибками и небрежностью пользователей. Управление уязвимостями включает также разра-

ботку процедур и политик, направленных на снижение человеческого фактора как источника угрозы.

Основные инструменты и технологии управления уязвимостями

Сканеры уязвимостей.

Сканеры уязвимостей автоматизируют процесс обнаружения слабых мест в системах. Они выполняют сканирование сети, приложений и систем на наличие известных уязвимостей, предоставляя детальные отчеты для их устранения. Использование сканеров позволяет систематически и регулярно проверять состояние безопасности, предотвращая эксплуатацию уязвимостей [9].

Платформы управления уязвимостями (Vulnerability management platforms).

Эти платформы объединяют функции обнаружения, анализа, приоритизации и устранения уязвимостей. Они помогают организациям систематизировать процесс управления уязвимостями и обеспечивать постоянное соблюдение стандартов безопасности. Такие платформы часто включают функции упорядочения уязвимостей, что позволяет фокусироваться на наиболее критичных проблемах [10].

Автоматизированные системы обновлений и патч-менеджмента.

Автоматизация процесса установки обновлений и патчей обеспечивает своевременное устранение уязвимостей, снижая окно возможностей для атакующих. Интеграция автоматизированных систем обновлений в процессы управления уязвимостями значительно повышает эффективность защиты.

Вызовы в управлении уязвимостями

Быстрое изменение ландшафта угроз.

Киберугрозы постоянно эволюционируют, выходят новые типы атак и эксплойтов. Специалистам по безопасности необходимо постоянно обновлять знания и инструменты для эффективной защиты. Однако проактивное управление уязвимостями позволяет адаптироваться к этим изменениям быстрее и эффективнее.

Недостаток квалифицированных специалистов.

Рынок труда в области кибербезопасности испытывает дефицит квалифицированных специалистов, что усложняет задачу обеспечения защиты организаций от современных угроз. Инвестиции в обучение и развитие персонала, а также использование автоматизированных инструментов, могут частично смягчить этот вызов.

Сложность интеграции разнообразных инструментов.

Многие организации используют множество различных инструментов и платформ для управления безопасностью, что может привести к проблемам интеграции и обмена информацией между ними. Разработка унифицированных систем управления уязвимостями помогает преодолеть эту сложность.

Баланс между безопасностью и удобством.

Обеспечение высокой степени безопасности иногда может противоречить удобству использования систем. Найти оптимальный баланс между этими аспектами является постоянным вызовом, но управление уязвимостями позволяет минимизировать компромиссы, обеспечивая необходимый уровень защиты без значительного снижения удобства.

Стратегии повышения эффективности управления уязвимостями

1. Проактивный подход к безопасности.

Организациям необходимо активно выявлять и устранять уязвимости до того, как они будут использованы злоумышленниками. Это включает регулярное проведение аудитов безопасности, пенетрационных тестов и непрерывного мониторинга систем на наличие новых уязвимостей.

2. Инвестиции в обучение и развитие персонала.

Повышение квалификации сотрудников и обучение их современным методам управления уязвимостями способствует укреплению общей безопасности организации. Создание

специализированных команд по управлению уязвимостями позволяет более эффективно реагировать на возникающие угрозы.

3. Разработка политик и процедур безопасности.

Наличие четких политик и процедур по управлению уязвимостями помогает стандартизировать процессы и повысить эффективность защиты. Такие политики должны охватывать все аспекты управления уязвимостями, от их обнаружения до устранения и мониторинга.

4. Использование многоуровневой защиты.

Комбинация различных методов и технологий защиты, таких как межсетевые экраны, системы обнаружения вторжений, шифрование данных и аутентификация, позволяет создать многоуровневую оборону против кибератак. Управление уязвимостями поддерживает этот многоуровневый подход, устраняя слабые места на каждом уровне.

Заключение

Хотя угрозы кибербезопасности остаются значимыми и требуют внимания, управление уязвимостями на наш взгляд выступает более эффективным и приоритетным подходом в современных стратегиях защиты информации. Устранение уязвимостей до момента их эксплуатации снижает риск реализации атак, способствует созданию устойчивых систем безопасности. В условиях постоянно меняющегося ландшафта киберугроз, проактивное и систематическое управление уязвимостями становится необходимым условием для обеспечения надежной и устойчивой защиты информационных систем.

Таким образом, представленный подход может быть реализована для обеспечения целей защиты информации на предприятиях и учреждениях и может быть полезен для специалистов по защите информации и студентов профильных специальностей.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Уязвимости операционных систем стали главной целью злоумышленников в 2024 году | Kaspersky / [Электронный ресурс] // kaspersky.ru : [сайт]. — URL: https://www.kaspersky.ru/about/press-releases/uyazvimosti-operacionnyh-sistem-stali-glavnoj-celyu-zloumyshlennikov-v-2024-godu (дата обращения: 08.03.2025);
2. А. И. Белоус, В. А. Солодуха. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения / А. И. Белоус, В. А. Солодуха. - Москва: Техносфера, 2021. - 481 с. : ил., цв. ил., табл.; 24 см. - (Мир электроники);
3. Менеджмент уязвимостей / [Электронный ресурс] // ptsecurity.com : [сайт]. — URL: https://www.ptsecurity.com/ru-ru/research/analytics/vulnerability-management-instructions-for-use/ (дата обращения: 16.12.2024);
4. WannaCry (WannaCrypt) – анализ вируса-шифровальщика и методов защиты / [Электронный ресурс] // anti-malware : [сайт]. — URL: https://www.anti-malware.ru/analytics/Threats_Analysis/WannaCry_WannaCrypt_private_matter (дата обращения: 16.12.2024);
5. Отчёт IBM: личная информация клиентов и сотрудников – главные жертвы утечек / [Электронный ресурс] // securitylab.ru : [сайт]. — URL: https://www.securitylab.ru/news/540308.php (дата обращения: 20.12.2024);
6. Искусственный интеллект и машинное обучение в кибербезопасности / [Электронный ресурс] // Kasperky : [сайт]. — URL: https://www.kaspersky.ru/resource-center/definitions/ai-cybersecurity (дата обращения: 16.12.2024);
7. Что такое DevSecOps? Определение и лучшие методики | Microsoft Security / [Электронный ресурс] // microsoft.com : [сайт]. — URL: https://www.microsoft.com/ru-ru/security/business/security-101/what-is-devsecops (дата обращения: 16.12.2024);
8. БДУ - Уязвимости / [Электронный ресурс] // bdu.fstec.ru : [сайт]. — URL: https://bdu.fstec.ru/vul (дата обращения: 16.12.2024);
9. Анализ ландшафта уязвимостей в первом квартале 2024 года | Securelist / [Электронный ресурс] // securelist.ru : [сайт]. — URL: https://securelist.ru/vulnerability-report-q1-2024/109484/ (дата обращения: 16.12.2024);

10. Обзор рынка систем управления уязвимостями (Vulnerability Management, VM) / [Электронный ресурс] // anti-malware : [сайт]. — URL: https://www.anti-malware.ru/analytics/Market_Analysis/Vulnerability-Management (дата обращения: 16.12.2024).

REFERENCES

1. A. I. Belous, V. A. Solodukha. *Fundamentals of Cybersecurity. Standards, Concepts, Methods, and Tools* / A. I. Belous, V. A. Solodukha. - Moscow: Technosphere, 2021. - 481 pages: illustrations, color illustrations, tables; 24 cm. - *(World of Electronics)*;

2. Operating system vulnerabilities have become the main target of hackers in 2024 | Kaspersky / [Electronic resource] // kaspersky.ru : [website]. — URL: https://www.kaspersky.ru/about/press-releases/uyazvimosti-operacionnyh-sistem-stali-glavnoj-celyu-zloumyshlennikov-v-2024-godu (accessed: 08.03.2025);

3. Vulnerability Management / [Electronic resource] // ptsecurity.com : [website]. — URL: https://www.ptsecurity.com/ru-ru/research/analytics/vulnerability-management-instructions-for-use/ (accessed: 16.12.2024);

4. WannaCry (WannaCrypt) – Ransomware Analysis and Protection Methods / [Electronic resource] // anti-malware : [website]. — URL: https://www.anti-malware.ru/analytics/Threats_Analysis/WannaCry_WannaCrypt_private_matter (accessed: 16.12.2024);

5. IBM Report: Personal Data of Clients and Employees as the Main Victims of Breaches / [Electronic resource] // securitylab.ru : [website]. — URL: https://www.securitylab.ru/news/540308.php (accessed: 20.12.2024);

6. Artificial Intelligence and Machine Learning in Cybersecurity / [Electronic resource] // Kaspersky : [website]. — URL: https://www.kaspersky.ru/resource-center/definitions/ai-cybersecurity (accessed: 16.12.2024);

7. What is DevSecOps? Definition and Best Practices | Microsoft Security / [Electronic resource] // microsoft.com : [website]. — URL: https://www.microsoft.com/ru-ru/security/business/security-101/what-is-devsecops (accessed: 16.12.2024);

8. BDU - Vulnerabilities / [Electronic resource] // bdu.fstec.ru : [website]. — URL: https://bdu.fstec.ru/vul (accessed: 16.12.2024);

9. Vulnerability Landscape Analysis for Q1 2024 | Securelist / [Electronic resource] // securelist.ru : [website]. — URL: https://securelist.ru/vulnerability-report-q1-2024/109484/ (accessed: 16.12.2024);

10. Overview of the Vulnerability Management Market (Vulnerability Management, VM) / [Electronic resource] // anti-malware : [website]. — URL: https://www.anti-malware.ru/analytics/Market_Analysis/Vulnerability-Management (accessed: 16.12.2024).

Информация об авторах

Серёдкин Сергей Петрович – к.э.н., доцент кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: Seredkin_SP@irgups.ru.

Святковский Дмитрий Александрович – студент магистратуры направления «Безопасность информационных систем и технологий», Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: lbcbvfcflbvf@mail.ru.

Information about the authors

Sergey Petrovich Seredkin – Ph.D. in Economics, Associate Professor of the Department of "Information Systems and Information Security", Irkutsk State Transport University, Irkutsk, e-mail: Seredkin_SP@irgups.ru.

Dmitry Alexandrovich Svyatkovsky – Master's student in "Information Systems and Technologies Security", Irkutsk State Transport University, Irkutsk, e-mail: lbcbvfcflbvf@mail.ru.