

ОСОБЕННОСТИ И ПРЕИМУЩЕСТВА СИСТЕМ МОДЕЛИРОВАНИЯ АТАК И ВЗЛОМОВ

С.А. Евдокимова¹, Т.П. Новикова²

¹ФГБОУ ВО «Воронежский государственный университет инженерных
технологий»

²Санкт-Петербургский государственный лесотехнический университет
имени С.М. Кирова (СПбГЛТУ)

Аннотация. Работа посвящена симуляторам кибератак злоумышленников на корпоративные компьютерные системы и рассматривает их функции, особенности архитектуры и процесса использования. В качестве преимуществ данных систем отмечается раннее обнаружение уязвимостей, автоматизация моделирования атак и оценка показателей эффективности обеспечения безопасности.

Ключевые слова: симуляция взлома и атак, моделирование атак, угрозы безопасности, уязвимости, оценка безопасности.

FEATURES AND ADVANTAGES OF ATTACK AND HACKING SIMULATION SYSTEMS

S.A. Evdokimova¹, T.P. Novikova²

¹Voronezh State University of Engineering Technologies

²St. Petersburg State Forest Technical University named after S.M. Kirov

Abstract. The paper is devoted to simulations of cyber-attacks by intruders on corporate computer systems and examines their functions, architecture features and the use process. The advantages of these systems include early detection of vulnerabilities, automation of attack modeling, and evaluation of security performance indicators.

Keywords: simulation of hacking and attacks, attack modeling, security threats, vulnerabilities, security assessment.

Уязвимости в компьютерных системах могут возникать из-за некорректных конфигураций средств защиты, слабых паролей, устаревшего программного обеспечения, отсутствия шифрования при передаче чувствительной информации и других причин [1-3]. Растущее число приложений, которые используют облачные сервисы и устройства Интернета вещей, создает новые проблемы безопасности [4-6]. Организации часто не проводят регулярную оценку безопасности, что приводит к успешным взломам и хакерским атакам. Злоумышленники постоянно разрабатывают новые изощренные методы атак, делая традиционные средства защиты недостаточными.

Организации в основном полагаются на сочетание проверок соответствия требованиям, оценок уязвимостей и периодическое тестирование на проникновение для оценки уровня безопасности. Эти методы эффективны, но проводятся на определенный момент времени и дают ограниченное представление о том, как работают средства контроля безопасности в реальных условиях атаки. Средства аудита безопасности направлены на соблюдение политики, сканирование и поиск уязвимостей выявляет слабые места без оценки возможности их использования или защитных мер. Тесты на проникновение являются более надежным методом, но они ограничены масштабом, временем и затратами, они не могут проводиться достаточно часто для получения реального состояния системы защиты корпоративной среды.

Поэтому для моделирования и обнаружения угроз в режиме реального времени следует использовать динамические подходы.

Симуляция взлома и атак (Breach and Attack Simulation) – процесс моделирования кибератак и попыток взлома с целью оценки эффективности систем обеспечения безопасности организации и возможности реагирования на инциденты [7]. Данный подход включает создание реалистичных сценариев атак и их выполнение в контролируемой среде для выявления уязвимостей, слабых мест и потенциальных пробелов безопасности внутри информационной системы и корпоративной компьютерной сети.

Процесс BAS включает следующие этапы:

- планирование – определение объема и целей симуляции, включая системы (приложения) и сети для тестирования, конкретные сценарии атак, которые будут смоделированы;
- проектирование симуляции – создание реалистичных сценариев атак (фишинг, повышение привилегий, несанкционированный доступ и т.д.) на основе известных угроз и специфики деятельности организации;

- проведение симуляции вручную или с помощью автоматизированного средства;
- анализ результата симуляции – включает просмотр журналов, мониторинг поведения системы и оценку эффективности существующих средств контроля безопасности и процедур реагирования на инциденты;
- формирование отчета.

Отличие BAS от этичного взлома и тестирования на проникновения состоит в использовании специализированных платформ симуляции и моделирования взломов и атак. Платформы BAS предназначены для постоянной имитации враждебного поведения в корпоративной компьютерной системе с целью проверки эффективности средств контроля безопасности. BAS автоматизированно воспроизводит известные тактики и приемы злоумышленников, чтобы оценить, могут ли существующие средства защиты предотвратить, обнаружить или смягчить их действие.

Архитектура платформы BAS состоит из взаимодействующих функциональных уровней, которые в совокупности обеспечивают непрерывное моделирование, наблюдение и оценку [8]. Первый уровень – уровень моделирования атак, который отвечает за выполнение действий злоумышленников в корпоративной среде. Второй уровень – уровень взаимодействия с управлением и наблюдения, который отражает реакцию механизмов безопасности на имитируемые атаки. Он включает в себя средства защиты конечных точек, средства сетевого контроля, системы идентификации и управления доступом, шлюзы безопасности электронной почты, системы обнаружения вторжений и платформы аналитики безопасности. Третий уровень – уровень анализа показателей, который объединяет исходные результаты моделирования в интерпретируемые показатели эффективности. Четвертый уровень включает интеграцию с рабочими процессами обеспечения безопасности и процессом принятия решений.

В настоящее время кроме платформ для моделирования BAS существуют фреймворки для эмуляции атак и попыток взломов злоумышленников [8, 9]. Они выявляют уязвимости и противодействуют действиям злоумышленников, используя элементы геймификации. К таким средствам можно отнести:

- Kaspersky Interactive Protection Simulation – представляет собой виртуальную платформу обучения навыкам кибербезопасности в виде стратегической командной игры, демонстрируя, как кибербезопасность связана с эффективностью бизнеса;

- Интерактивный симулятор от «Лаборатории Касперского» - симулятор программ-вымогателей;
- CyberBattleSim – симулятор построен на основе искусственного интеллекта и предназначен для понимания действий хакеров;
- Infection Monkey – это BAS с открытым исходным кодом, проверяет устойчивость сети;
- BAS AttackIQ – выполняет автоматическую проверку безопасности путем моделирования реальных киберугроз;
- Автоматизированный стимулятор атак ХМ Cyber – гибридная платформа BAS;
- Симулятор для реальной практики в расследовании кибератак Standoff Cyberbones и другие.

В пользу виртуального симулятора, построенного под обучение и геймификацию, выступают многие авторы, отмечая, что геймификация позволяет сохранять вовлеченность в течение длительного интервала времени и делает процесс обучения интересным [8-10]. В работе [9] авторы предлагают вариант программной реализации симулятора киберугроз, интерфейс которого состоит из интерактивных офисных помещений, в которые расположены компьютерная и офисная техника, элементы коммуникаций. Путем перемещения по комнатам пользователь взаимодействует с внутренними объектами и решает отдельные практические задачи.

Авторы в [11] применяли для моделирования взломов и атак платформу на основе искусственного интеллекта, объединяющую алгоритмы машинного обучения и автоматизации моделирования атак, анализ уязвимостей и предоставление информации о безопасности в режиме реального времени. Система BAS, управляемая искусственным интеллектом, обеспечивала непрерывную оценку безопасности, снизились ложные срабатывания и время реагирования на инциденты. Работа системы моделирования взломов и атак на основе искусственного интеллекта начинается со сбора данных, которые затем подвергаются обработке и нормализации для обеспечения согласованности и точности. Прогнозирование траектории атаки с помощью нейронной сети определяют потенциальные маршруты атаки, затем выполняется обнаружение уязвимостей, которые интегрируются в аналитику угроз для автоматизированного построения стратегии реагирования.

Проведенные исследования показали преимущества BAS на основе искусственного интеллекта над традиционными методами тестирования на проникновение, так как повысилась точность обнаружения угроз, киберустойчивость всей компьютерной системы, недостатки были устранены автоматически [11].

К преимуществам BAS можно отнести:

- выявление уязвимостей до того, как ими воспользуются злоумышленники;
- моделирование реальных сценариев атак обеспечивает более точную оценку средств контроля безопасности исследуемой системы и возможностей реагирования на инциденты по сравнению с традиционными методами оценки уязвимостей;
- повышается готовность к реагированию на инциденты, выявляются пробелы в процедурах обеспечения безопасности;
- устранение уязвимостей на более ранних этапах их возникновения может потенциально снизить финансовый ущерб и потерю репутации.

Таким образом, подход автоматизированного моделирования взломов и атак является эффективным механизмом непрерывной проверки средств контроля безопасности компьютерной системы организации.

Список литературы

1. Малышев, Д.А. Архитектура защищенного веб-приложения для управления программными проектами / Д.А. Малышев, С.А. Евдокимова // Проблемы и перспективы моделирования систем и процессов : материалы Всероссийской научно-практической конференции. – Воронеж, 2025. – С. 280-286.
2. Сумин, В.И. Разработка подхода формирования структуры принятия управленческих решений сотрудниками сложных организационных систем специального назначения / В.И. Сумин, А.С. Дубровин, А.С. Кравченко // Моделирование систем и процессов. – 2025. – Т. 18, № 3. – С. 99-106.
3. Выбор критерия оптимальности при принятии управленческих решений в сложных технических системах / А.В. Скрыпников [и др.] // Моделирование систем и процессов. – 2024. – Т. 17, № 1. – С. 120-128.
4. Евдокимова, С. А. Уязвимости информационной безопасности систем компьютерного зрения / С. А. Евдокимова // Информационные технологии. Физика и математика : материалы 90-й научно-технической конференции профессорско-преподавательского состава, научных сотрудников и аспирантов (с международным участием). – Минск, 2026. – С. 49-53.

5. Dosunmu, A.A. Security orchestration and automation models for accelerating incident detection and response / A.A. Dosunmu, P.O. Ogundele // Computer Science & IT Research Journal. – 2025. – Vol. 6(11). – Pp. 878-894. – DOI: 10.51594/csitrj.v6i11.2163.

6. Высоцкая, И. А. Обоснование информационно-интеллектуальной поддержки принципов действия технических систем / И. А. Высоцкая // Моделирование систем и процессов. – 2024. – Т. 17, № 1. – С. 19-26.

7. Dosunmu, A. Breach and Attack Simulation Frameworks for Continuous Validation of Enterprise Security Controls / A. Dosunmu, P.O. Ogundele // International Journal of Scientific Research in Computer Science Engineering and Information Technology. – 2024. – Vol. 10(3). – Pp. 1100-1119.

8. Обоснование необходимости разработки симулятора киберугроз для решения образовательных задач / В.Л. Акапьев, Р.А. Дунаев, Е.Г. Ковалева, А.В. Борисенко // Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России. – 2025. – № 4. – С. 117-130.

9. Акапьев, В. Л. Разработка программируемого симулятора киберугроз с элементами геймификации / В. Л. Акапьев, Р. А. Дунаев, А. В. Борисенко // Вестник Адыгейского государственного университета. Серия: Естественно-математические и технические науки. – 2025. – № 4 (371). – С. 38-50.

10. Оптимизация информационно-телекоммуникационных систем с использованием нейронных сетей: повышение эффективности и безопасности / А. В. Скрыпников [и др.] // Вестник Воронежского института ФСИИ России. – 2024. – № 4. – С. 135-139.

11. Ethical hacking and penetration testing: strengthening cyberdefense with ai-driven breach and attack simulation / C. Ubagaram [et al.] // International Journal of Information technology & Computer Engineering. – 2023. – Vol. 11, Is. 1. – Pp. 230-236.

References

1. Malyshev, D.A. Architecture secure web application for software project management / D.A. Malyshev, S.A. Evdokimova // Problems and prospects of modeling systems and processes. Materials of the All-Russian scientific and practical conference. – Voronezh, 2025. – Pp. 280-286.

2. Sumin, V.I. Development of an approach to forming the structure of managerial decision-making by employees of complex special-purpose organizational sys-

tems / V.I. Sumin, A.S. Dubrovin, A.S. Kravchenko // Modeling of systems and processes. – 2025. – Vol. 18, No. 3. – Pp. 99-106.

3. Selection of the optimality criterion in making managerial decisions in complex technical systems / A.V. Skrypnikov [et al.] // Modeling of systems and processes. – 2024. – Vol. 17, No. 1. – Pp. 120-128.

4. Evdokimova, S.A. Vulnerabilities of information security of computer vision systems / S.A. Evdokimova // Information technologies. Physics and mathematics. Materials of the 90th Scientific and Technical conference of faculty, researchers and graduate students (with international participation). – Minsk, 2026. – Pp. 49-53.

5. Dosunmu, A.A. Security orchestration and automation models for accelerating incident detection and response / A.A. Dosunmu, P.O. Ogundele // Computer Science & IT Research Journal. – 2025. – Vol. 6(11). – Pp. 878-894. – DOI: 10.51594/csitrj.v6i11.2163.

6. Vysotskaya, I.A. Substantiation of information and intellectual support for the principles of operation of technical systems / I.A. Vysotskaya // Modeling of systems and processes. - 2024. – Vol. 17, No. 1. – Pp. 19-26.

7. Dosunmu, A. Breach and Attack Simulation Frameworks for Continuous Validation of Enterprise Security Controls / A. Dosunmu, P.O. Ogundele // International Journal of Scientific Research in Computer Science Engineering and Information Technology. – 2024. – Vol. 10(3). – Pp. 1100-1119.

8. Substantiation of the need to develop a cyber threat simulator for solving educational problems / V.L. Akapyev, R.A. Dunaev, E.G. Kovaleva, A.V. Borisenko // Bulletin of the Saint Petersburg University of the State Fire Service of the Ministry of Emergency Situations of Russia. 2025. No. 4. pp. 117-130.

9. Akapyev, V.L. Development of a programmable simulator of cyber threats with gamification elements / V.L. Akapyev, R.A. Dunaev, A.V. Borisenko // Bulletin of the Adygea State University. Series: Natural-mathematical and technical sciences. – 2025. – № 4 (371). – Pp. 38-50.

10. Optimization of information and telecommunication systems using neural networks: improving efficiency and security / A.V. Skrypnikov [et al.] // Bulletin of the Voronezh Institute of the Federal Penitentiary Service of Russia. – 2024. – No. 4. – Pp. 135-139.

11. Ethical hacking and penetration testing: strengthening cyberdefense with ai-driven breach and attack simulation / C. Ubagaram [et al.] // International Journal of Information technology & Computer Engineering. – 2023. – Vol. 11, Is. 1. – Pp. 230-236.