ОРИГИНАЛЬНАЯ СТАТЬЯ

DOI: 10.26794/3030-7097-2026-2-1-35-44
УДК 004.56(045)

Обзор инструментов для тестирования на проникновение: сравнение функционала и удобства использования

А.И. Любимов, С.А. Резниченко
Финансовый университет при Правительстве Российской Федерации, Москва, Российская Федерация

АННОТАЦИЯ

В статье представлен детальный анализ ключевых инструментов пентестинга (Metasploit, Core Impact, Immunity Canvas, Security Forest и др.), востребованных в сфере информационной безопасности. **Цель исследования** — сравнивать функциональность, удобство использования и специфику перечисленных решений, чтобы помочь специалистам выбрать оптимальный инструмент в зависимости от задач, бюджета и уровня квалификации. В работе раскрыта суть и значимость тестирования на проникновение (пентестинга) в контексте современной кибербезопасности; систематизированы этапы проведения пентеста (сбор информации, выявление уязвимостей, планирование атак, анализ результатов); приведены сравнительные характеристики инструментов в виде таблиц (поддерживаемые ОС, лицензии, интерфейсы, стоимость, языки программирования, особенности обновлений и отчетности); визуализированы процессы работы инструментов с помощью UML-диаграмм; затронуты этические и правовые аспекты применения пентестинга. **Основные выводы:** пентестинг — не разовая мера, а неотъемлемый элемент жизненного цикла системы безопасности, требующий регулярного применения; не существует универсального инструмента: автоматизированные сканеры (например, Nmap, Nessus) эффективны для первичного выявления уязвимостей, а фреймворки эксплуатации (Metasploit, Core Impact) — для подтверждения серьезности уязвимостей и демонстрации реального ущерба; коммерческие продукты предлагают глубину анализа и автоматизацию за высокую стоимость, а решения с открытым исходным кодом — гибкость при большей требовательности к квалификации специалиста; наилучшая результативность достигается при комбинировании автоматизированных и ручных методов проверки; решающий фактор успеха — квалификация и аналитическое мышление специалиста, действующего в правовых и этических рамках. Статья полезна специалистам по информационной безопасности, а также тем, кто изучает методы защиты данных и тестирования на проникновение.

Ключевые слова: тестирование на проникновение; пентестинг; информационная безопасность; уязвимость; инструменты тестирования; кибербезопасность; защита данных; хакерские атаки; безопасность сети; системы проникновения

Для цитирования: **Любимов А.И., Резниченко С.А. Обзор инструментов для тестирования на проникновение: сравнение функционала и удобства использования.** ***Цифровые решения и технологии искусственного интеллекта.*** **2026;2(1):35-44. DOI: 10.26794/3030-7097-2026-2-1-35-44**

ORIGINAL PAPER

Overview of Penetration Testing Tools: Comparison of Functionality and Ease of Use

A.I. Lyubimov, S.A. Reznichenko
Financial University under the Government of the Russian Federation, Moscow, Russian Federation

ABSTRACT

This study provides a detailed analysis of penetration testing tools such as Metasploit, Core Impact, Immunity Canvas, and Security Forest. It compares their functionality, usability, and role in identifying vulnerabilities in information systems. The main focus is on the features of each tool, their strengths and weaknesses, and their areas of application. Penetration testing is an important element of a comprehensive approach to cybersecurity, allowing vulnerabilities to be identified at all stages of the information system lifecycle. The paper examines the stages of penetration testing, including information gathering, vulnerability identification, attack planning, and results analysis. Particular attention is paid to automated tools, which greatly simplify the testing process but require competent use. The article also discusses the ethical and legal aspects of penetration testing, emphasizing the need to comply with legislation and professional ethics. The article will be useful for information security specialists, as well as anyone interested in modern data protection methods. The paper emphasizes that the choice of tool depends on specific tasks and context, and that successful pentesting requires not only technical skills, but also a deep understanding of information protection processes.

Keywords: penetration testing; pentesting; information security; vulnerability; testing tools; cybersecurity; data protection; hacker attacks; network security; intrusion systems

For citation: **Lyubimov A.I., Reznichenko S.A. Overview of penetration testing tools: Comparison of functionality and ease of use. *Digital solutions and artificial intelligence technologies*. 2026;2(1):35-44. DOI: 10.26794/3030-7097-2026-2-1-35-44**

ВВЕДЕНИЕ

Современный мир стремительно трансформируется, углубляясь в эпоху цифровых технологий, в которой огромное количество данных ежедневно создается, обрабатывается и хранится. С этой беспрецедентной цифровизацией возрастает и необходимость защищать наши данные от угроз, которые становятся сложнее, изощреннее и, увы, все более распространенными. Вопрос кибербезопасности сегодня поднят на совершенно новый уровень и требует не просто базовых мер предосторожности, а системного подхода с применением продвинутых методов и технологий.

Когда мы размышляем о защите информации, мы чаще всего обращаем внимание на обычные средства безопасности, такие как антивирусы, брандмауэры или сложные пароли. Однако все эти инструменты — всего лишь один из уровней многослойной системы обороны. Гораздо важнее выявить потенциальные слабые места самой структуры сети или программного обеспечения еще до того, как злонамеренные хакеры смогут воспользоваться ими. Именно здесь на помощь приходят методы тестирования на проникновение, или, как их называют профессионалы, пентесты. Это процесс, который представляет собой своего рода «управляемую атаку», проводимую с целью выявления уязвимостей системы безопасности.

Почему это приобретает столь высокую значимость? Потому что нельзя защитить то, что ты не знаешь, как атаковать. Любая система, остающаяся неизученной, становится идеальной мишенью для злоумышленников. Они постоянно совершенствуют свои стратегии, находят лазейки, используют уязвимости и эксплуатируют ошибки кода. Без тестирования на проникновение компания рискует потерять не только данные, но и доверие клиентов, средства и репутацию.

Этот процесс помогает организациям понять степень риска, которому они подвергаются, и в последующем принять соответствующие меры. Однако важно понимать, что пентест — это не единоличное решение всех проблем. Это лишь элемент целого набора тактик, который должен работать в связке с другими средствами безопасности. Это подобно тренировочному полигону: чем больше вы знаете о своих слабых местах, тем эффективнее сможете отразить реальную атаку.

На сегодняшний день рынок изобилует инструментами для тестирования на проникновение, которые способны решать самые разнообразные задачи — от анализа корпоративных сетей до оценки защищенности веб-приложений. В статье мы рассмотрим основные продукты, которые давно зарекомендовали себя как надежные союзники профессионалов в области кибербезопасности. Каждый из этих инструментов играет уникальную роль, дополняя общий комплекс мер по обеспечению защиты.

Одной из основных задач тестирования на проникновение является выявление уязвимостей до того, как это сделает злоумышленник, и их быстрое устранение. Злоумышленники используют различные автоматизированные программные средства и проводят сетевые атаки, чтобы получить доступ к системам.

Благодаря тестированию на проникновение менеджеры могут получить представление о том, насколько защищена их сеть с точки зрения злоумышленника. Целью тестирования на проникновение является поиск методов обхода сетевых уязвимостей и их устранение до того, как хакер обнаружит их и воспользуется ими.

Во-вторых, даже зная о рисках, пользователи и сетевые администраторы могут нуждаться в отчете о тестировании на проникновение. С его помощью они способны убедить руководство в необходимости финансирования устранения проблем.

В-третьих, для подтверждения того, что наши сети настроены надежно, может быть проведено тестирование на проникновение. Отчет о тестировании на проникновение помогает проверить эффективность работы сотрудников службы безопасности нашей организации. Этот тест не повышает безопасность системы или сети; вместо этого он выявляет различия между предполагаемой и фактической реализацией.

В-четвертых, это помогает компаниям соблюдать законодательные требования, установленные правительством для ведения бизнеса.

Наконец, тестирование на проникновение используется для оценки новой технологии. Новая технология должна быть оценена перед запуском в производство. Тестирование на проникновение является простым и доступным инструментом, поскольку ни одна новая технология не может считаться полностью надежной без предварительной проверки.

ЭТАПЫ И ИНСТРУМЕНТЫ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ

Тестирование на проникновение, или пентест, представляет собой процесс оценки защищенности компьютерных систем и сетей путем имитации атак, потенциально возможных на данном объекте. В век цифровой трансформации и увеличивающегося числа кибератак такой подход становится не просто значимым инструментом в арсенале специалистов по безопасности, а необходимостью. Однако успешное проведение подобных тестов невозможно без специализированных инструментов, которые предоставляют средства для анализа, эксплуатации уязвимостей и разработки отчетов. В этой статье мы проведем обзор наиболее популярных инструментов для пентестинга, их функциональности, а также рассмотрим аспекты их использования.

Определенный набор входных данных, процедур и результатов называется методологией. Она дает нам инструкции о том, как перейти от входных данных к выходным.

На первом этапе мы выбираем, какая система, сеть или онлайн-приложение будут подвергнуты тестированию на проникновение.

Профиль злоумышленника, который будет использовать тестировщик, и продолжительность теста — это два аспекта, которые определяют масштаб теста.

Сбор информации — это следующий шаг. Как следует из названия, он предоставляет тестировщику информацию о различных целевых сетях. Наша цель — собрать как можно больше информации о нашей целевой сети, доступной для широкой публики. Для диагностики сети мы применяем такие инструменты, как ping, traceroute и ipconfig.

Выявление уязвимостей — это третий шаг [3]. Его основная цель — обнаружение слабых мест в целевой системе или сети, которые могут быть использованы злоумышленниками. Для этого применяются как стандартные процедуры, так и автоматизированные средства.

Тестировщик может вручную выявить распространенные ошибки настройки и дефекты в целевой сети или хосте с помощью ручного обнаружения уязвимостей. Сканеры уязвимостей — это коммерческие и бесплатные инструменты, доступные в рамках автоматизированной процедуры. Они позволяют проверить программное обеспечение целевой сети на наличие слабых мест. Такие сканеры выявляют уязвимости, потенциально пригодные для взлома наших систем и сетей.

Эти автоматизированные программы могут только выявлять уязвимости; тестирование на проникновение — это не то, что они могут сделать.

На четвертом этапе — анализе информации и планировании атаки — собираются данные, полученные на предыдущих этапах. Специалист по тестированию на проникновение может спланировать нападение на объект с помощью этой технической и общедоступной информации. Специалист по тестированию также определяет, какой объект нуждается в дальнейшем изучении.

Существует две составляющие нападения и проникновения [4]. Атака и проникновение составляют первую фазу. Следует попытаться использовать слабые места, выявленные в процессе анализа уязвимостей.

Самый распространённый способ, который применяют многие сканеры для сопоставления IP-адреса с сетевым хостом,— это ICMP-эхо-запрос (ping). Такие инструменты, как Nessus, могут задействовать пакеты TCP или UDP, чтобы определить активность хоста.

Опираясь на этот механизм, мы используем средства эксплуатации [5] для подтверждения наличия уязвимости. На рынке представлено большое число решений — как коммерческих, так и с открытым исходным кодом. Специалисты по тестированию на проникновение и злоумышленники зачастую применяют идентичный инструментарий. Перечисленные средства эксплуатации — лишь небольшая часть доступного арсенала. Большинство инструментов этой категории рассчитаны на однократное применение.

Как видно из *табл. 1*, инструменты первичного сканирования образуют класс доступного и специализированного ПО. Их ключевые различия лежат в плоскости поддерживаемых ОС и наличия узкоспециализированных функций (например, анализ логов в Unicornscan), что определяет выбор тестировщика в зависимости от конкретного сценария разведки.

В 2003 г. HD Moore разработал платформу Metasploit с открытым исходным кодом [6]. С ее помощью можно проводить исследования эксплойтов, тестирование на проникновение, создание сигнатур IDS, а также исследования и разработку уязвимостей.

Перед использованием эксплойта пользователь выбирает полезную нагрузку. Он может воспользоваться целевой удаленной службой. Ее можно использовать в сочетании со сценарием Meterpreter для управления программами, запускающими бэкдор. Платформа Metasploit отлично подходит для создания сценариев и проведения тестов на проникновение, предоставляя инструменты безопасности и эксплойты.

Представленная на *рис. 1* диаграмма иллюстрирует модульную архитектуру Metasploit, где

Таблица 1 / Table 1

Инструменты для сканирования и обнаружения уязвимостей / Tools for Scanning and Detecting Vulnerabilities

Название	Назначение	ОС	Лицензия
Nmap	Сканирование сети, сканирование портов	Linux, Windows	Бесплатно
SuperScan	Обнаружение открытых TCP/UDP портов	Linux, Windows	Бесплатно
Hping	Сканирование портов, удаленное определение ОС	Windows	Бесплатно
AngryIP	Сканирование TCP, Открытие хостов	Windows	Бесплатно
Unicornscan	Сканер TCP/UDP портов, Анализ логов PCAP	Unix/Linux	Бесплатно
Advanced Port Scanner	Сканирование портов TCP, Многопоточность	Windows	Бесплатно

Источник / Source: составлено авторами / Compiled by the authors.

Рис. 1 / Fig. 1. **UML — диаграмма, показывающая процесс работы Metasploit / Is a UML Diagram Showing the Metasploit Process**

Источник / Source: составлено авторами / Compiled by the authors.

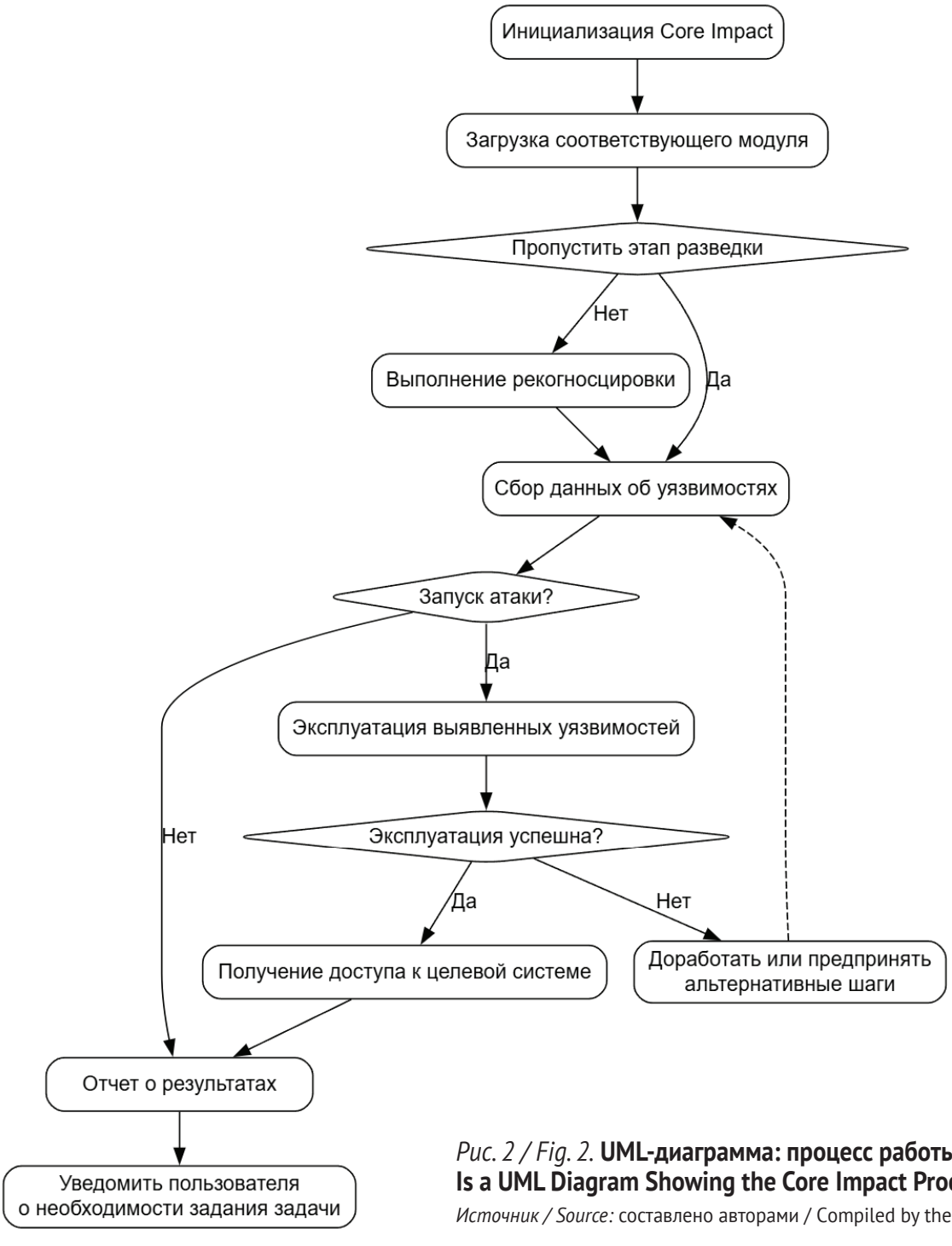

Рис. 2 / Fig. 2. **UML-диаграмма: процесс работы Core Impact / Is a UML Diagram Showing the Core Impact Process**

Источник / Source: составлено авторами / Compiled by the authors.

процесс эксплуатации реализован как последовательность строго детерминированных этапов. Такая структура обеспечивает гибкость при выборе вектора атаки и объясняет широкую распространенность фреймворка в качестве базового инструмента для идентификации уязвимостей.

Для платформы Metasploit доступны как база команд, так и графический интерфейс пользователя. Ее версия с графическим интерфейсом называется Armitage.

Core Impact — это коммерческая платформа компании Core Security Technologies [2]. С помощью Core Impact Pro можно оценить степень безопасности и методы многовекторного тестирования для сетевых, онлайн-, мобильных и беспроводных сред.

Схема работы Core Impact (*рис. 2*) демонстрирует интегрированный подход, при котором этапы сканирования, эксплуатации и постэксплуатации объединены в единый автоматизированный контур. Это позволяет не только обнаруживать уязвимости, но и моделировать цепочки атак, оценивая реальный ущерб для информационной инфраструктуры.

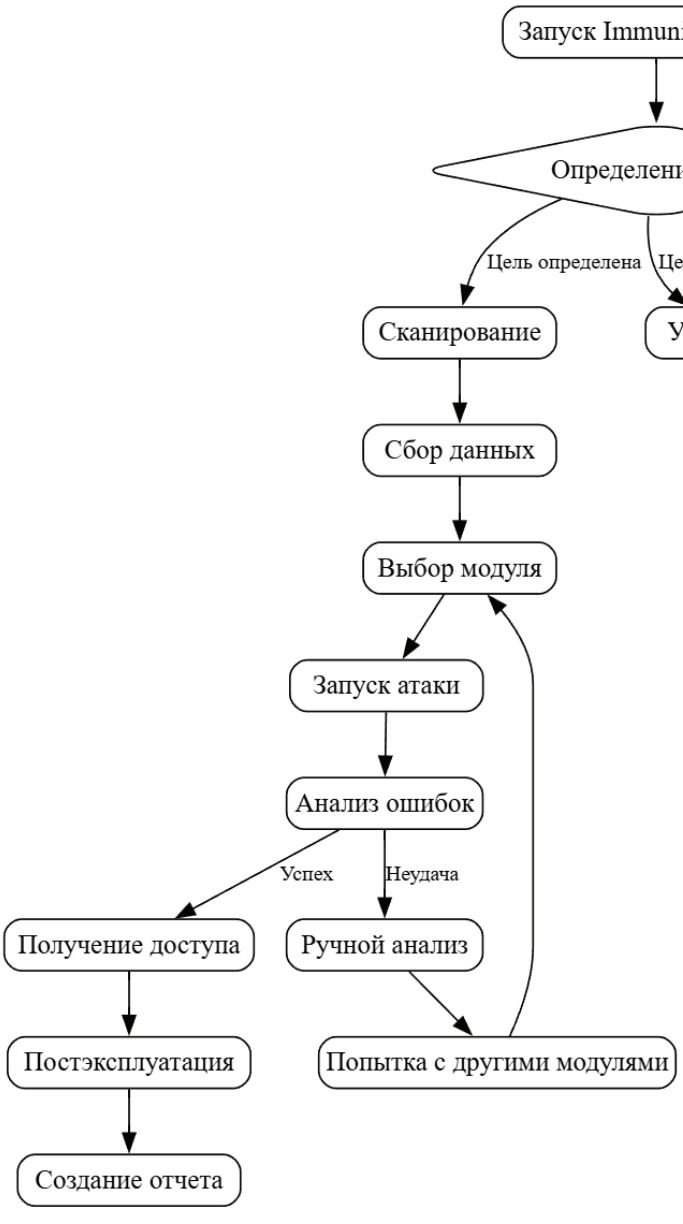

Рис. 3 / Fig. 3. **UML — диаграмма, показывающая процесс работы Immunity Canvas / Is a UML Diagram Showing the Immunity Canvas Process**

Источник / Source: составлено авторами / Compiled by the authors.

Архитектура фреймворка, показанная на диаграмме, оптимизирована для точного применения специфичных атакующих модулей, что позиционирует его как решение для целевых проверок устойчивости систем к сложным векторам атак.

ImmunitySec разработала коммерческий инструмент для устранения уязвимостей — Canvas. Последняя версия Immunity Canvas — 6,45. Он предназначен не для тестирования на проникновение, а, скорее всего, для тестирования безопасности и разработки эксплойтов. Canvas предлагает среду MOS-защиты, которая облегчает быстрое обнаружение уязвимостей. Компания может проверить конкретное представление о состоянии своей безопасности с помощью Immunity Canvas (*рис. 3*).

Платформа Security Forest Exploitation Framework — в ней также есть инструменты с открытым исходным кодом, которые могут быть использованы тестировщиками на проникновение. Этот фреймворк использует набор кода эксплойта, известный как «Дерево эксплойтов». Его интерфейс позволяет тестировщику запускать код эксплойта через веб-браузер (*рис. 4*). Он поддерживает полный исходный код, а иногда даже включает эксплойты нулевого дня.

Сравнительные характеристики, описанные в *табл. 2*, позволяют увидеть различия фреймворков по критериям функциональной насыщенности и целевой аудитории.

Наблюдается прямая корреляция между стоимостью решения и уровнем его автоматизации, в то время как open-source-альтернативы сохраняют преимущество в гибкости и доступности для кастомизации.

Для тестирования на проникновение доступно гораздо больше платформ, чем упомянуто выше. W3af — одна из них. По сути, это платформа для атак и аудита веб-приложений.

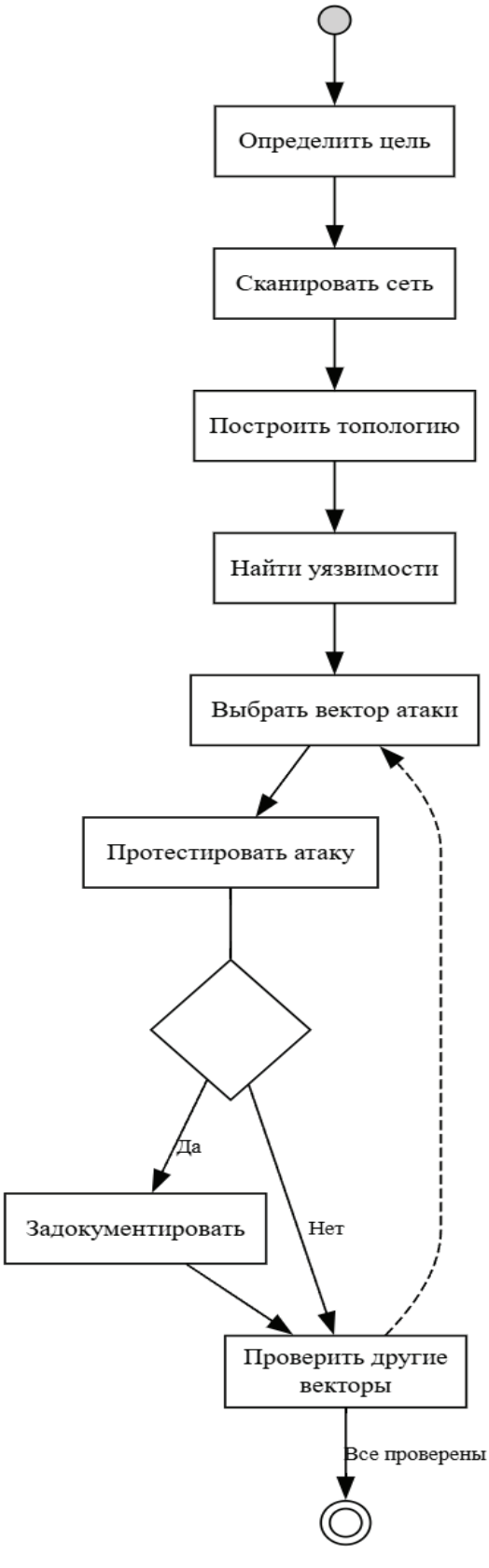

Рис. 4 / Fig. 4. **UML — диаграмма, показывающая процесс работы Security Forest / Is a UML Diagram Showing the Security Forest Process**

Источник / Source: составлено авторами / Compiled by the authors.

Ее можно применять для обнаружения уязвимостей в онлайн-приложениях и использования их слабых мест.

Большинство компаний и частных лиц сегодня работают с продуктами Microsoft, которые подвержены хорошо продуманным уязвимостям. Таким образом, защита данных и информации в настоящее время является наиболее сложной задачей.

Оценка сетевой безопасности или уязвимостей может быть в какой-то степени полезной, но она не обязательно показывает, как далеко могут зайти хакеры, чтобы воспользоваться уязвимостью. Хотя тестировщики на проникновение искренне пытаются в какой-то степени воспроизвести реальную атаку, они часто компрометируют систему, находя недостатки, которые можно эффективно использовать.

Хакеры и злоумышленники часто добиваются успеха в своих целях, поскольку им нужно найти лишь одну уязвимость, чтобы воспользоваться ею,— в то время как тестировщикам на проникновение может потребоваться обнаружить все уязвимости в сети. Учитывая, что тестирование на проникновение часто проводится в течение определенного периода времени, это сложный процесс.

Используемые в настоящее время платформы тестирования на проникновение недостаточно адаптированы для применения к различным типам систем или сетей. Ручные тесты, которые часто проводятся на таких платформах, как правило, представляют собой длительные и сложные процессы.

Из всего этого можно сделать вывод, что тест на проникновение сам по себе не повышает безопасность компьютера или сети.

Для устранения уязвимостей, обнаруженных в ходе теста на проникновение, необходимы определенные действия.

Тестирование на проникновение может быть использовано для эффективной и успешной киберзащиты.

ВЫВОДЫ

Проведенное исследование позволило сформулировать ряд ключевых выводов, основанных на сравнительном анализе инструментов и методологии тестирования на проникновение.

Пентестинг — систематическая необходимость. Тестирование на проникновение не является разовой мерой, а представляет собой неотъемлемый элемент жизненного цикла системы безопасности. Его необходимо регулярно применять при внедрении новых систем; после значительных обновлений инфраструктуры; для соблюдения нор-

Таблица 2 / Table 2

**Сравнительная таблица инструментов эксплуатации уязвимостей /
Comparative Table of Vulnerability Exploitation Tools**

Feature	Metasploit	Core Impact	Immunity Canvas	Security Forest
Количество эксплойтов	1467 эксплойтов	155 эксплойтов	800 эксплойтов	Огромное количество предустановленных эксплойтов
Интерфейс	Графический (GUI) и командная строка (CLI)	Графический (GUI)	Графический (GUI) и командная строка (CLI)	Графический (GUI) с ограниченными функциями
Платформа и установка	Независимая	Windows	Независимая	Windows
Стоимость	Бесплатно с ограничениями	2,5 млн руб. за одно рабочее место	300 тыс. руб. за 10 рабочих мест	Бесплатно
Язык программирования	Ruby, C	Python	Python	C, Python, Perl (для эксплойтов)
Обновления	Анонсируются на публичном сайте	Регулярные обновления доступны	Ежемесячные обновления	Периодические обновления
Выявление начальных хостов	Не поддерживается	Поддерживается	Не поддерживается	Не поддерживается
Функции отчетности	Бесплатно доступен, легко настраивается	Полностью автоматизирован, предлагает больше всего эксплойтов, профессиональный, но самый дорогой	Меньше эксплойтов, ниже стоимость, низкий уровень влияния	Предварительно скомпилированные и проиндексированные эксплойты

Источник / Source: составлено авторами / Compiled by the authors.

мативных требований; для независимой оценки эффективности защитных мер.

Отсутствие универсального инструмента. На рынке нет единого решения, покрывающего все потребности пентестинга. Различные инструменты дополняют друг друга: автоматизированные сканеры (Nmap, Nessus) эффективны для первичного выявления уязвимостей; фреймворки эксплуатации (Metasploit, Core Impact) необходимы для подтверждения серьезности уязвимостей и демонстрации потенциального ущерба.

Выбор между коммерческими и open-source решениями. Существует четкая дихотомия подходов: коммерческие продукты (например, Core Impact) обеспечивают глубокую автоматизацию и комплексный анализ, но имеют высокую стоимость; решения с открытым исходным кодом (например, Metasploit) предлагают гибкость и бесплатность, однако требуют от специалиста более высокой квалификации.

Оптимальная стратегия — комбинированный подход. Наибольшая эффективность достигается при интеграции: автоматизированных методов (быстрое сканирование, первичное выявление уязвимостей); ручных методов (глубокая проверка, подтверждение критичности уязвимостей).

Строгая этапность процесса. Пентестинг представляет собой последовательность четко определенных шагов: разведка и сбор информации; сканирование и выявление уязвимостей; эксплуатация уязвимостей для получения доступа; анализ полученных данных; составление отчета с рекомендациями по устранению недостатков.

Ключевая роль специалиста. Несмотря на развитие инструментов, решающим фактором успеха остается: квалификация тестировщика; его аналитическое мышление; способность действовать в правовых и этических рамках.

Пентестинг как инструмент повышения киберустойчивости. Грамотно проведенное тестирование на проникновение позволяет: выявить реальные уязвимости до их использования злоумышленниками; оценить реальный уровень защищенности инфраструктуры; обосновать необходимость инвестиций в безопасность; повысить общую киберустойчивость организации.

Таким образом, пентестинг — это не просто техническая процедура, а стратегический элемент системы информационной безопасности, требующий комплексного подхода, квалифицированных специалистов и регулярного применения.

СПИСОК ИСТОЧНИКОВ

1. Чуб В.С. Аудит безопасности информационной системы с использованием тестов на проникновение. *Молодой исследователь Дона.* 2018;6(15):88-90. URL: https://www.elibrary.ru/ywbgdj
2. Дворянкин О.А. Osint, Pentest и нетсталкинг — информационные технологии интернета. *Национальная ассоциация ученых.* 2022;84(2):6-13. URL: https://www.elibrary.ru/lqlpwz
3. Казыханов А.А., Байрушин Ф.Т. Pentest как основа обеспечения безопаности на средних и крупных предприятиях. *Символ науки.* 2016;10-2(22):50-51. URL: https://www.elibrary.ru/ wxdfbp
4. Аверьянов В.С., Карцан И.Н. К вопросу выявления уязвимостей IPS/IDS систем. *Актуальные проблемы авиации и космонавтики.* 2020;2:191-197. URL: https://www.elibrary.ru/rhmmin
5. Алиева Е.М.К., Ширинова Ш.З.К. Актуальность атак с использованием SQL-инъекций. *In The World Of Science and Education.* 2025;3:163-167. DOI: 10.24412/3007-8946-2025-152-163-167
6. Шкрадюк А.Д. Оценка безопасности информационных систем с помощью тестирования на проникновение. *Умная цифровая экономика*. 2022:4(2):18-30. URL: https://www.elibrary.ru/tshjtt
7. Симбирцев Д.В., Жуков В.Г. Разработка автоматизированной системы анализа защищенности веб-ресурсов. *Актуальные проблемы авиации и космонавтики.* 2011;7:430. URL: https://www.elibrary.ru/taozxn
8. Конев А.А., Паюсова Т.И. Большие языковые модели в информационной безопасности и тестировании на проникновение: систематический обзор возможностей применения. *Научно-технический журнал информационных технологий, механики и оптики.* 2025;1:41-52. DOI: 10.17586/2226-1494-2025-25-1-42-52
9. Мордвинова А.Ю., Нуриев С.А. Исследование уязвимостей и угроз безопасности стандарта IEEE 802.11. *Современные инновации, системы и технологии.* 2023;3:117-131. DOI: 10.47813/2782-2818-2023-3-3-0117-0131
10. Гыльджова А., Пирлиев К., Ходжамбердиев С., Худайберенов Р. Анализ безопасности ALT LINUX с применением LYNIS в качестве опорной модели для проверки защищенности. *Символ науки.* 2024;4-2-2:71-74. URL: https://www.elibrary.ru/bywpju
11. Серов С.А., Серов С.С., Петрова И.В. Metasploit Framework как средство эксплуатации уязвимых серверов. *Форум молодых ученых.* 2021;5:1307-1313. URL: https://www.elibrary.ru/honvex
12. Дедов Д.О. Защита SSH-порта с использованием имитации уязвимостей Honeypot. *Молодой исследователь Дона*. 2023;8-6(45):16-21. URL: https://www.elibrary.ru/hhlcno
13. Чемеркин Ю.С. Безопасность публичных сред облачных вычислений в условиях функциональной неопределенности. *T-Comm: телекоммуникации и транспорт*. 2014;6:56-60. URL: https://media-publisher.ru/en/content-6-2014/
14. Hahanova I.V. Method of Pentest Synthesis and Vulnerability Detection. *Радиоэлектроника и информатика*. 2012;4:68-73.
15. Samarov X.Q., Salimov Z.I.O., Qosimov I.S. Kiberxavfsizlikga oid fanlarga laboratoriya mashg‘ulotlarini bajarish uchun platformani yaratishning dolzarbligi. *In The World Of Science and Education.* 2025;15. URL: https://irc-els.com/docs/СБОРНИК%20МНЖ%2015%20ФЕВРАЛЯ%202025%20ТЕХНИЧЕСКИЕ%20НАУКИ.pdf.

REFERENCES

1. Chub V.S. Information system security audit using penetration tests. *A young researcher of the Don*. 2018;6(15):88-90. URL: https://www.elibrary.ru/ywbgdj (In Russ.).
2. Dvoryankin O.A. Osint, Pentest and netstalking — information technologies of the Internet. *National Association of Scientists.* 2022;84(2):6-13. URL: https://www.elibrary.ru/lqlpwz (In Russ.).
3. Kazykhanov A.A., Bayrushin F.T. Pentest as a basis for ensuring security in medium and large enterprises. *A symbol of Science*. 2016;10-2(22):50-51. URL: https://www.elibrary.ru/ wxdfbp (In Russ.).
4. Averyanov V.S., Kartsan I.N. On the issue of identifying vulnerabilities in IPS/IDS systems. *Actual Problems of Aviation and Cosmonautics.* 2020;2:191-197. URL: https://www.elibrary.ru/rhmmin (In Russ.).
5. Alieva E.M.K., Shirinova S.Z.K. The relevance of attacks using SQL injections. *In The World Of Science and Education.* 2025;3:163-167. (In Russ.). DOI: 10.24412/3007-8946-2025-152-163-167
6. Shkradyuk A.D. Information system security assessment using penetration testing. *Smart Digital Economy.* 2022:4(2):18-30. URL: https://www.elibrary.ru/tshjtt (In Russ.).
7. Simbirtsev D.V., Zhukov V.G. Development of an automated system for analyzing the security of web resources. *Actual Problems of Aviation and Cosmonautics*. 2011;7:430. URL: https://www.elibrary.ru/taozxn (In Russ.).

8. Konev A.A., Payusova T.I. Large language models in information security and penetration testing: a systematic review of application possibilities. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics.* 2025;1:41-52. (In Russ.). DOI: 10.17586/2226-1494-2025-25-1-42-52
9. Mordvinova A.Yu., Nuriev S.A. Investigation of vulnerabilities and security threats of the IEEE 802.11 standard. *Modern Innovations, Systems and Technologies*. 2023;3:117-131. (In Russ.). DOI: 10.47813/2782-2818-2023-3-3-0117-0131
10. Gylydzhova A., Pirliev K., Khodjamberdiev S., Khudaiberenov R. ALT LINUX security analysis using LYNIS as a reference model for security verification. *A Symbol of Science.* 2024;4-2-2:71-74. URL: https://www.elibrary.ru/bywpju (In Russ.).
11. Serov S.A., Serov S.S., Petrova I.V. Metasploit Framework as a means of exploiting vulnerable servers. *Forum of Young Scientists.* 2021;5:1307-1313. URL: https://www.elibrary.ru/honvex (In Russ.).
12. Dedov D.O. SSH port protection using imitation of Honeypot vulnerabilities. *A Young Researcher of the Don.* 2023;8-6(45):16-21. URL: https://www.elibrary.ru/hhlcno (In Russ.).
13. Chemerkin Yu.S. Security of public cloud computing environments in conditions of functional uncertainty. *T-Comm: Telecommunications and Transport*. 2014;6:56-60. URL: https://media-publisher.ru/en/content-6-2014/ (In Russ.).
14. Hakhanova I.V. Method of Pentest Synthesis and Vulnerability Detection. *Radio Electronics and Computer Science.* 2012;4:68-73.
15. Samarov Kh.Q., Salimov Z.I.O., Kasimov I.S. The relevance of creating a platform for performing laboratory training in cybersecurity-related disciplines. *In the World of Science and Education.* 2025;15. URL: https://ircels.com/docs/СБОРНИК%20МНЖ%2015%20ФЕВРАЛЯ%202025%20ТЕХНИЧЕСКИЕ%20НАУКИ.pdf (in Kz.).

ИНФОРМАЦИЯ ОБ АВТОРАХ / ABOUT THE AUTHORS

Артем Игоревич Любимов — студент факультета информационных технологий и анализа больших данных, Финансовый университет при Правительстве Российской Федерации, Москва, Российская Федерация
Artem I. Lyubimov — student of the Faculty of Information Technology and Big Data Analysis, Financial University under the Government of the Russian Federation, Moscow, Russian Federation
https://orcid.org/0009-0005-2633-7909
artem.lyubimov.harby@gmail.com

Сергей Анатольевич Резниченко — кандидат технических наук, доцент, кафедры информационной безопасности факультета информационных технологий и анализа больших данных, Финансовый университет при Правительстве Российской Федерации, Москва, Российская Федерация
Sergey A. Reznichenko — Cand. Sci. (Tech), Assoc. Prof., Department of Information Security, Faculty of Information Technology and Big Data Analysis, Financial University under the Government of the Russian Federation, Moscow, Russian Federation
https://orcid.org/0000-0002-1539-0457
Автор для корреспонденции / Corresponding author:
sareznichenko@fa.ru; rsa_5@bk.ru

Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.
Conflicts of Interest Statement: The authors have no conflicts of interest to declare.

Статья поступила 19.01.2026; после рецензирования 02.02.2026; принята к публикации 12.02.2026.
Авторы прочитали и одобрили окончательный вариант рукописи.
The article was submitted on 19.01.2026; revised on 02.02.2026 and accepted for publication on 12.02.2026.
The authors read and approved the final version of the manuscript.