УДК 004.42,004.75
DOI 10.52575/2687-0932-2025-52-4-873-886
EDN PRAXZD

Эмуляция программного модуля имитации атаки на беспроводную сеть

Борисенко А.В., Акапьев В.Л., Ковалева Е.Г., Новикова Е.А.
Белгородский юридический институт МВД России имени И.Д. Путилина
Россия, 308024, г. Белгород, ул. Горького, 71
borisenko02.94@mail.ru

Аннотация. Актуальность исследования определяется необходимостью увеличения эффективности противодействия киберпреступности. Целью данной статьи является попытка эмуляции программного модуля симулятора-тренажера, имитирующего процесс проникновения в беспроводную сеть Wi-Fi с использованием принципов социальной инженерии, который может быть использован в процессе подготовки профильных специалистов. Для достижения поставленной цели необходимо решить следующие задачи: запустить разработанный программный модуль; выбрать программную среду; осуществить компиляцию программного модуля. В процессе решения сформулированных задач был проведен анализ криминогенной обстановки в части киберпреступности, были использованы обще- и частнонаучные методы познания (диалектический, анализ, синтез, аналогия, проецирование, прогнозирование и т. д.), главным из которых явился метод модульного проектирования аппаратно-программного комплекса. На основании выполненных работ был создан программный модуль симулятора. Проведенное исследование позволяет сделать вывод о необходимости использования подобных аппаратно-программных комплексов для подготовки сотрудников правоохранительных органов.

Ключевые слова: киберпреступность, имитация атаки на беспроводную сеть, симулятор-тренажер, эмуляция программного модуля, хендшейк

Для цитирования: Борисенко А.В., Акапьев В.Л., Ковалева Е.Г., Новикова Е.А. 2025. Эмуляция программного модуля имитации атаки на беспроводную сеть. *Экономика. Информатика*, 52(4): 873–886. DOI 10.52575/2687-0932-2025-52-4-873-886; EDN PRAXZD

Emulation of the Attack Simulation Software Module to a Wireless Network

Aleksander V. Borisenko, Viktor L. Akapyev,
Ekaterina G. Kovaleva, Ekaterina A. Novikova
Putilin Belgorod Law Institute of the Ministry of Internal Affairs of the Russian Federation
71 Gorky St., Belgorod 308024, Russia
borisenko02.94@mail.ru

Abstract. The relevance of the study is determined by the need to increase the effectiveness of countering cybercrime. The study attempts to emulate a simulator software module that imitates the process of penetration into a wireless Wi-Fi network applying principles of social engineering. Such a device may be indispensable to specialist training. To achieve this goal, it is necessary to solve the following tasks: launch the developed software module, select a software environment, and compile the software module. In the process of solving the formulated tasks, the authors analyzed the criminal situation in terms of cybercrime, employing general and private scientific methods of cognition (the dialectical method, analysis, synthesis, method of analogy, projection, forecasting, etc.), the main one being the method of modular design of the hardware and software complex. Based on the research findings, a simulator software module has been created. The study reveals the need to use such hardware and software complexes for training law enforcement officers.

Keywords: cybercrime, simulation of an attack on a wireless network, simulator, emulation of a software module, handshake

For citation: Borisenko A.V., Akapyev V.L., Kovaleva E.G., Novikova E.A. 2025. Emulation of the Attack Simulation Software Module to a Wireless Network. *Economics. Information technologies*, 52(4): 873–886 (in Russian). DOI 10.52575/2687-0932-2025-52-4-873-886; EDN PRAXZD

Введение

Рост использования цифровых решений в повседневной деятельности в сфере бизнеса и государственных услуг сопровождается увеличением количества цифровых устройств, которыми пользуются граждане. Сейчас люди регистрируются во множестве цифровых аккаунтов и проводят в интернете больше времени, чем когда-либо. В связи с этим растёт число кибератак и случаев цифрового мошенничества. Увеличивается не только количество компьютерных инцидентов, но и их сложность, а также степень негативного воздействия.

Статистические данные по состоянию киберпреступлений за январь – июль 2025 года хоть и свидетельствует о том, что общее количество зарегистрированных преступлений снизилось на 4,5 %, но позволяют считать данный вид противоправной деятельности как представляющий серьезную угрозу обществу [В России за январь-июль 2025 года ущерб от IT-преступлений вырос на 16 % и составил почти 120 млрд рублей, 2025].

Злоумышленники находят новые способы использования уязвимостей: от похитителей информации, взламывающих миллионы учётных записей, до банд вымогателей, меняющих тактику шантажа, и киберпреступников, использующих искусственный интеллект. Продолжает расти число платформ, предлагающих услуги DDoS-атак, что в современном мире, во многом полагающемся на онлайн-сервисы, может сделать платформы недоступными.

Рост количества сетевых атак и актов кибермошенничества с начала СВО актуализирует, в частности, необходимость качественного роста уровня профессиональной подготовки сотрудников правоохранительных органов.

Решение указанной задачи осложняется отсутствием необходимого аппаратного и программного обеспечения ведомственных вузов и неповоротливостью системы закупок товаров и услуг для государственных нужд.

Для применения в образовательном процессе профильных вузов и преодоления указанных препятствий предлагается вариант использования симулятора-тренажера, имитирующего сетевые проникновения.

Объекты и методы исследования

В современную цифровую эпоху беспроводные сети стали неотъемлемой частью нашей повседневной жизни. От смартфонов до «умных» домов [Ramadan, 2022; Abdalla, Tang, Marojevic, 2025], от предприятий до общественных мест – беспроводные технологии произвели революцию в том, как мы общаемся, работаем и живём. Эти сети обеспечивают беспрецедентное удобство, позволяя нам подключаться к интернету без проводов, что способствует удалённой работе, онлайн-покупкам, общению в социальных сетях и многому другому [Zhukabayeva, Karabayev, Nurusheva, Satybaldina, 2024].

Однако у этого удобства есть и обратная сторона: уязвимости в системе безопасности. Как и у всех технологий, у беспроводных сетей есть свои уязвимые места, которыми могут воспользоваться злоумышленники. Это палка о двух концах: беспроводные технологии невероятно удобны, но при этом создают потенциальные угрозы безопасности и открывают потенциальные возможности для киберпреступников.

Киберпреступность стала серьёзной проблемой, имеющей сложные социальные и экономические последствия, наносящие ущерб национальной безопасности. Растущая распространённость и диверсификация стратегий и методов киберпреступности стали

серьёзным препятствием как для понимания масштабов существующих рисков, так и для разработки эффективной политики предотвращения киберпреступлений для коммерческих структур, государственных учреждений и физических лиц.

Огромное количество финансово мотивированных вторжений, совершаемых ежедневно, также оказывает кумулятивный эффект, снижая конкурентоспособность национальной экономики и создавая огромную нагрузку на специалистов по кибербезопасности, что приводит к снижению их готовности к работе и выгоранию.

Правоохранительные органы стремятся разработать эффективные стратегии для предотвращения и расследования киберпреступлений [Yavorsky, Useev, Kurushin, 2021], но при этом необходимо учитывать, что процесс расследования киберпреступлений сложен и требует специальной подготовки, знаний о компьютерных системах и навыков сбора электронных доказательств.

Согласно статистике Kaspersky Threat Intelligence (рис. 1) наибольшую долю киберпреступлений за сентябрь 2025 года составляют попытки проникновения, под которыми подразумеваются попытки взлома системы извне с целью использования уязвимостей и потенциального совершения мошеннических действий, растраты или злоупотребления [Интерактивная карта киберугроз, 2025].

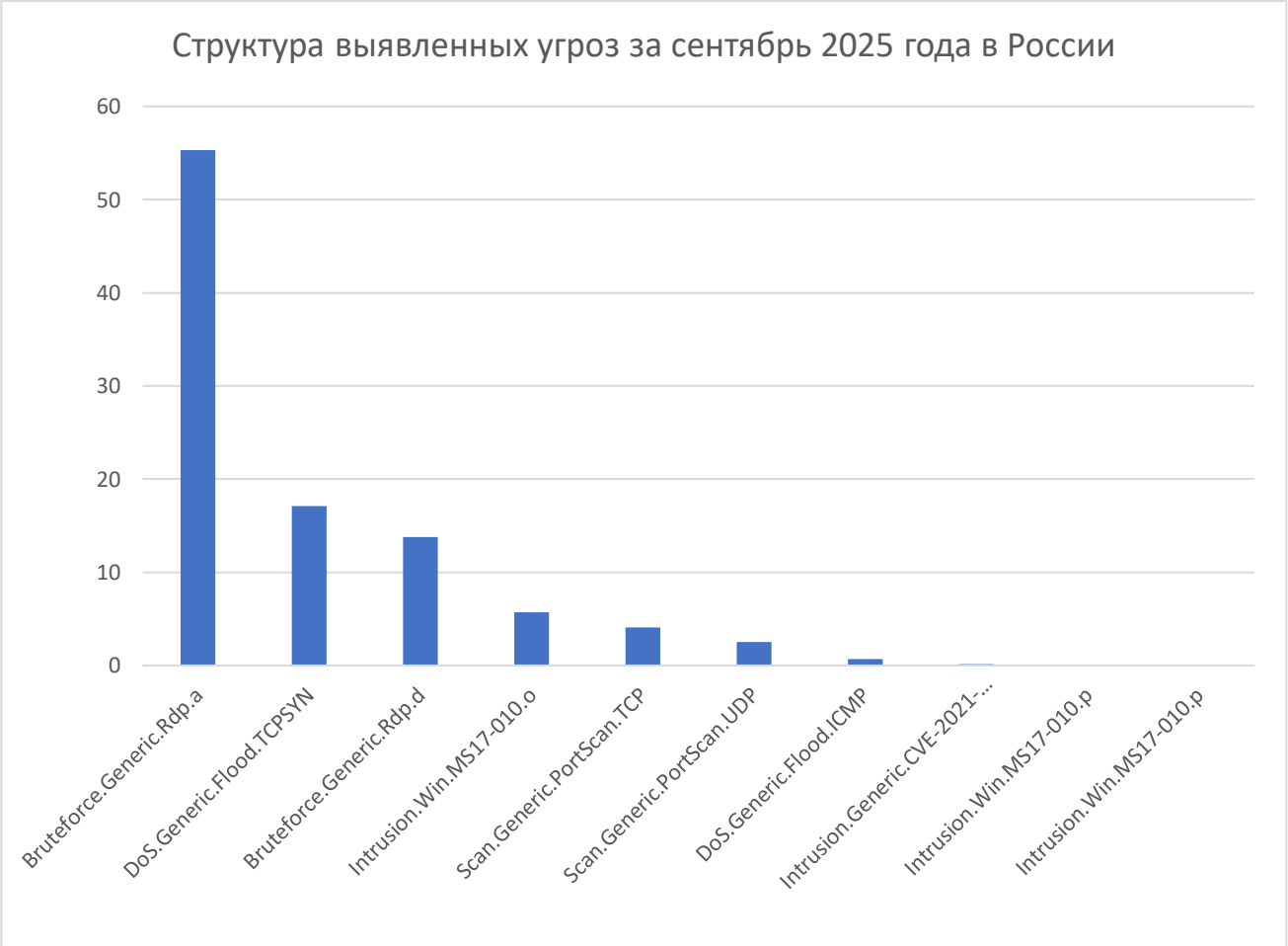

Рис. 1. Гистограмма сканирования выявленных угроз (в процентах)
Fig. 1. Histogram of the scan of identified threats (percentage)

Разновидностью проникновений являются атаки на беспроводную сеть, представляющие собой вредоносные действия или стратегии, направленные на использование уязвимостей систем беспроводной связи, включая сети Wi-Fi, мобильные сети передачи данных и Bluetooth-соединения.

Целью таких атак может быть что угодно: от несанкционированного перехвата и изменения данных до нарушения работы сети и управления устройствами. Поскольку беспроводные сети передают данные по радиоканалу, они по своей сути предоставляют потенциальным злоумышленникам больше возможностей для доступа, чем проводные сети. Следовательно, без надёжных мер безопасности эти сети могут быть уязвимы для несанкционированного доступа и неправомерного использования, что ставит под угрозу как персональные, так и корпоративные данные.

Наиболее эффективным средством противодействия проникновению в настоящее время является тестирование на проникновение (или пентест) [Teichmann, Boticiu, 2023; Torres-Trujillo, Meza-Alarcon, Ticona, 2024]. Тестирование на проникновение помогает организациям выявлять уязвимости и недостатки в своих системах, которые иначе они могли бы не обнаружить [Журавлева, Ткаченко, 2023]. Это позволяет предотвращать атаки до их начала [Bodenhausen, Mangel, Vogt, Henze, 2025], поскольку организации могут устранять выявленные уязвимости, что актуализирует необходимость использования в процессе подготовки правоохранительных кадров соответствующих аппаратно-программных имитаторов сетевых атак [Акапьев, Савотченко, 2015].

Однако проведение пентеста представляет собой довольно-таки дорогостоящее мероприятие [Prayatno, Tohari, Susilowati, 2024]. Именно это обуславливает необходимость разработки и использования в учебном процессе симуляторов проникновения.

Анализ готовых систем

Базовых знаний в области кибербезопасности сегодня недостаточно, поскольку злоумышленники с каждым днём становятся всё более организованными и изощрёнными. Необходимо применять безотлагательные меры для повышения эффективности формирования компетентности в области кибербезопасности у сотрудников правоохранительных органов и лучший способ сделать это – практические занятия с использованием симуляторов.

В настоящее время на отечественном и международном рынках присутствует целый ряд тренажеров и эмуляторов, которые могут быть использованы на различных уровнях подготовки сотрудников по кибербезопасности (табл. 1).

На отечественном рынке тренажеров и эмуляторов в сфере подготовки специалистов по защите информации выделяется продукция фирмы «Учтех-Профи», в перечне которой по рассматриваемой проблематике можно выделить виртуальные тренажеры «Системы контроля и управления доступом», «Средства программно-аппаратной защиты информации», «Межсетевые экраны нового поколения» и виртуальный учебник «Кибербезопасность. Анализ и управление уязвимостями». Его функциональность:

– теоретический раздел с демонстрацией различных процессов анализа и управления уязвимостями;

– структурированная навигация по разделам;

– настройки просмотра теоретического материала [Виртуальные тренажеры и эмуляторы, 2025].

Сравнительно новым направлением развития использования симуляторов в образовательном процессе является создание лабораторий кибербезопасности. Лаборатория кибербезопасности – это виртуальная среда, в которой можно пройти практическое обучение, выполняя смоделированные задания или сценарии. Обычно они используются для повышения уровня знаний и развития навыков.

Лаборатория кибербезопасности обладает теми же преимуществами, что и любое практико-ориентированное обучение работе с программным обеспечением, обеспечивая возможность проведения тренингов по информационной безопасности, предоставляя дополнительную защиту от атак с использованием социальной инженерии.

Таблица 1
Table 1

Виртуальные тренажеры и эмуляторы
Virtual simulators and emulators

Наименование и производитель	**Функционал**	**Условия приобретения**
Виртуальный тренажер «Системы контроля и управления доступом» (Учтех-Профи, Россия)	Предназначен для демонстрации и изучения принципов работы, а также монтажа и настройки системы контроля и управления доступом (СКУД)	Лицензия на 10 мест (цена требует уточнения)
Виртуальный тренажер «Применение средств программно-аппаратной защиты информации» (Учтех-Профи, Россия)	Предназначен для ознакомления с алгоритмами работы программных и программно-аппаратных средств борьбы с несанкционированным доступом.	Лицензия на 10 мест (цена требует уточнения)
Виртуальный тренажер «Кибербезопасность» (Учтех-Профи, Россия)	Предназначен для изучения принципов работы межсетевых экранов и обучения работе для защиты сетевой инфраструктуры	Лицензия на 10 мест (цена требует уточнения)
Виртуальный учебник «Кибербезопасность. Анализ и управление уязвимостями» (Учтех-Профи, Россия)	Предназначен для обучения теоретическим основам анализа и управления уязвимостями.	Лицензия на 10 мест (цена требует уточнения)
Лаборатория кибербезопасности (CloudShare, США)	Позволяет организациям проводить увлекательные практические занятия в любой отрасли кибербезопасности, моделировать угрозы	Информация закрыта
Лаборатория кибербезопасности (Hack the Box, Великобритания)	Комплексная платформа, которая помогает организациям развивать все аспекты кибербезопасности – от базовых знаний до продвинутых навыков	Информация закрыта
Лаборатории кибербезопасности (CyberDefenders, США)	Содержат реальные сценарии и библиотеку игровых задач по безопасности	Облачные лаборатории доступны по подписке
Платформа AttackDefense Labs, Pentester Academy	Содержит более 2000 уникальных лабораторных упражнений по кибербезопасности	Доступна по ежемесячной подписке на Pentester Academy
Project Juice Shop (Фонд OWASP, США)	Представляет собой намеренно небезопасное веб-приложение, предназначенное для обучения хакингу	Распространяется в соответствии с условиями лицензии MIT
Платформа для обучения навыкам кибербезопасности (Immersive Labs, Великобритания)	Геймифицированная среда для обучения, охватывающая все аспекты – от безопасности инфраструктуры и приложений до мониторинга угроз.	Информация закрыта
Центр управления безопасностью (SOC) на базе искусственного интеллекта (TryHackMe, Великобритания)	Обеспечивает управляемое иммерсивное обучение по кибербезопасности независимо от уровня подготовки.	Регистрация пользователя (от 25 долларов США за пользователя)

Лаборатории кибербезопасности могут существенно повлиять на процесс формирования профессиональной компетентности правоохранителей в части выявления угроз, реагирования на них и устранения их последствий.

На 2025 год среди лучших лабораторий по кибербезопасности выделяют платформу CloudShare, которая позволяет проводить практические занятия в области кибербезопасности. С ее помощью можно создавать собственные среды в любом облаке без написания кода и с минимальной настройкой, что позволяет моделировать угрозы, проводить тактические учения и получать полезную информацию об эффективности учебного процесса [The 8 Best Virtual Cybersecurity Practice Labs, 2025; Kumar, Niranjan, Reddy, Himanshu, Raju, Goud, 2025].

Комплексная платформа Hack the Box предоставляет широкий спектр задач для практики в области кибербезопасности: от базовых заданий до продвинутых кейсов. Платформа отлично использует геймификацию, примером которой является игра «Capture the Flag» – настраиваемая и захватывающая командная симуляция взлома. Hack the Box также предлагает широкий выбор киберполигонов, симуляций атак и практических лабораторий как для частных лиц, так и для компаний и преподавателей.

Будучи одной из ведущих компаний по обучению кибербезопасности в мире, Crybary располагает обширным каталогом обучающих материалов по кибербезопасности, разработанных отраслевыми экспертами. В библиотеке компании присутствует множество лабораторных работ, охватывающих все аспекты: от базового тестирования на проникновение и обнаружения вторжений до этичного взлома. Имеется несколько курсов о том, как создать и поддерживать собственную лабораторию.

Лаборатории Blue Team от CyberDefenders используют игровой подход, чтобы помочь специалистам по информационной безопасности развить правильное мышление и навыки для защиты от киберугроз. В лабораториях реальные сценарии сочетаются с элементами геймификации. Существует огромная библиотека игровых задач по безопасности, которые можно бесплатно загрузить и развернуть на виртуальной машине, а облачные лаборатории доступны по подписке.

Платформа AttackDefense Labs, доступная по ежемесячной подписке в Pentester Academy, включает более 2000 уникальных лабораторных упражнений. Лаборатории доступны через веб-браузер, и каждый обучающийся подключен к своей собственной выделенной лаборатории без каких-либо ограничений по использованию.

Project Juice Shop, разработанный фондом OWASP, представляет собой намеренно небезопасное веб-приложение, предназначенное для обучения хакерству. В приложении представлены десять основных уязвимостей OWASP, длинный список недостатков в системе безопасности и таблица результатов, в которой отслеживается прогресс пользователя.

Платформа Immersive Labs, признанная лидером в рейтинге Forrester Wave: платформы для обучения навыкам кибербезопасности в 2023 году, помогает как специалистам по безопасности, так и студентам вузов приобретать критически важные навыки в сфере безопасности. Платформа Immersive Labs представляет собой геймифицированную среду обучения, охватывающую все аспекты – от безопасности инфраструктуры и приложений до мониторинга угроз, – с возможностью выполнения упражнений на основе сценариев, направленных на развитие конкретных знаний и навыков. Образовательные учреждения также могут проводить полноценные симуляции кризисных ситуаций, чтобы проверить свои возможности по реагированию на инциденты.

TryHackMe – это центр управления безопасностью (SOC) на базе искусственного интеллекта, который обеспечивает управляемое иммерсивное обучение независимо от вашего уровня подготовки. Платформа с более чем 800 учебными лабораториями и множеством направлений обучения создана для того, чтобы изучение кибербезопасности было увлекательным и интересным [The 8 Best Virtual Cybersecurity Practice Labs, 2025].

При всем функциональном разнообразии и дидактической привлекательности перечисленные системы обладают одним существенным недостатком – они платные. Что

касается разработок зарубежных производителей, то их приобретение в настоящих условиях является практически невозможным.

Указанные предпосылки актуализируют необходимость реализации доктрины недорого симулятора сетевых атак. Не вдаваясь в подробности реализации аппаратной части, мы остановимся лишь на алгоритме эмуляции программного модуля симулятора.

Результаты исследования

Процедура запуска симулятора определяется, в первую очередь, выбором операционной системы (ОС) и начинается с ее настройки. Наш выбор ОС Kali Linux. Выбор обусловлен наличием в указанной ОС всех необходимых пакетов для проведения сетевых атак. Для интеграции драйверов в Kali Linux и проведения атаки на беспроводную сеть, будет использован разработанный программный модуль [Акапьев, Ковалева, Борисенко, Панарин, 2024].

Программирование процесса идентификации сетевого оборудования, после установки драйверов проверяем корректное определение адаптеров системой (рис. 2).

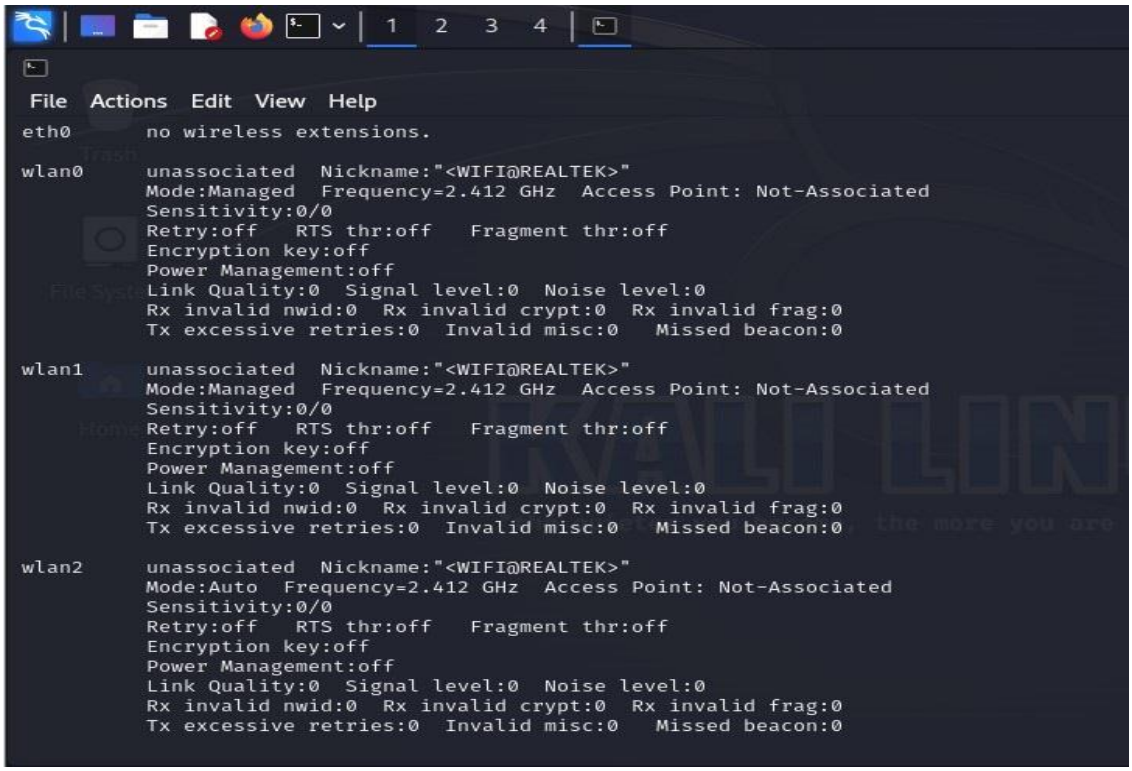

Рис. 2. Проверка корректного определения адаптеров системой
Fig. 2. Checking the correct identification of adapters by the system

Переход к запуску скрипта для имитации атаки на точку доступа (роутер). Далее осуществляются запуск и проверка с последующей установкой требуемых для работы компонентов.

После проведения процедуры включается полностью настроенная среда для проведения сетевой атаки и предлагается выбрать дальнейшее действие. Первым этапом будет перехват хендшейка [Perez, Selander, Mattsson, Watteyne, Vučinić, 2024] (т. е. процесс знакомства клиента и сервера, во время которого устройства идентифицируют друг друга и обмениваются секретными ключами [Saha, Ray, Dasgupta, 2024]) от клиентов атакуемой точки посредством их принудительного отключения [Montañez-Juan, Forteza-Domenici, García-Buades, Blahopoulou, Ortiz-Bonnin, 2025; An, Pan, Wen, Zhang, 2023]. Поэтому здесь выбирается пункт 2.

Далее выбирается интерфейс для поиска целевой точки (рис. 3).

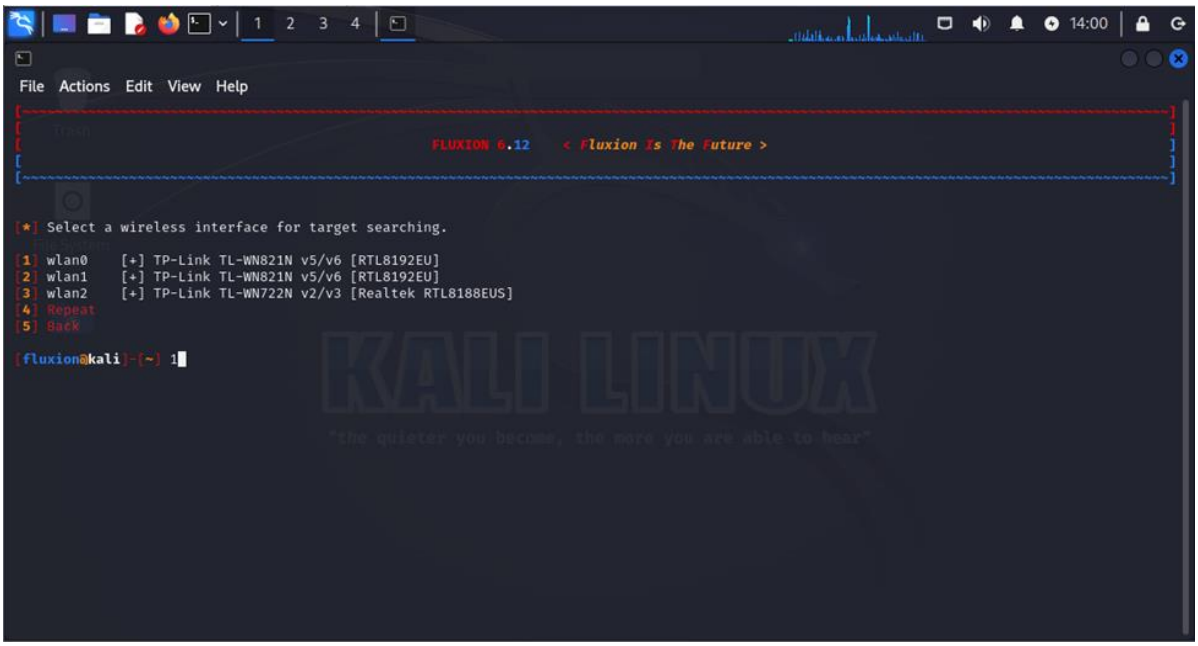

Рис. 3. Выбор интерфейса для поиска целевой точки
Fig. 3. Selecting the interface to search for a target point

В дальнейшем подбирается канал для поиска точки доступа (рис. 4). В описываемом варианте атаки роутер работает на частоте 2,4 ГГц, соответственно выбирается этот канал. Затем для поиска включается режим монитора и начинается поиск цели.

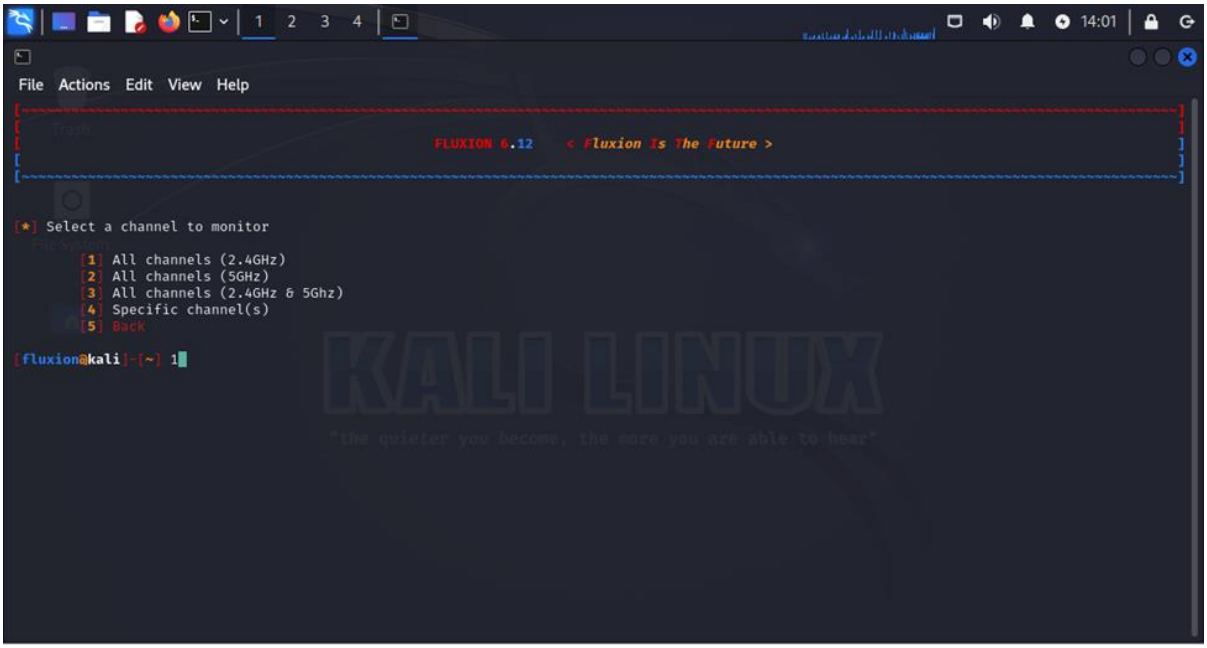

Рис. 4. Выбор канала
Fig. 4. Channel selection

Когда определены все точки доступа на канале, сканирование останавливается и на экран выводится список всех доступных точек и выбирается целевая точка (рис. 5).

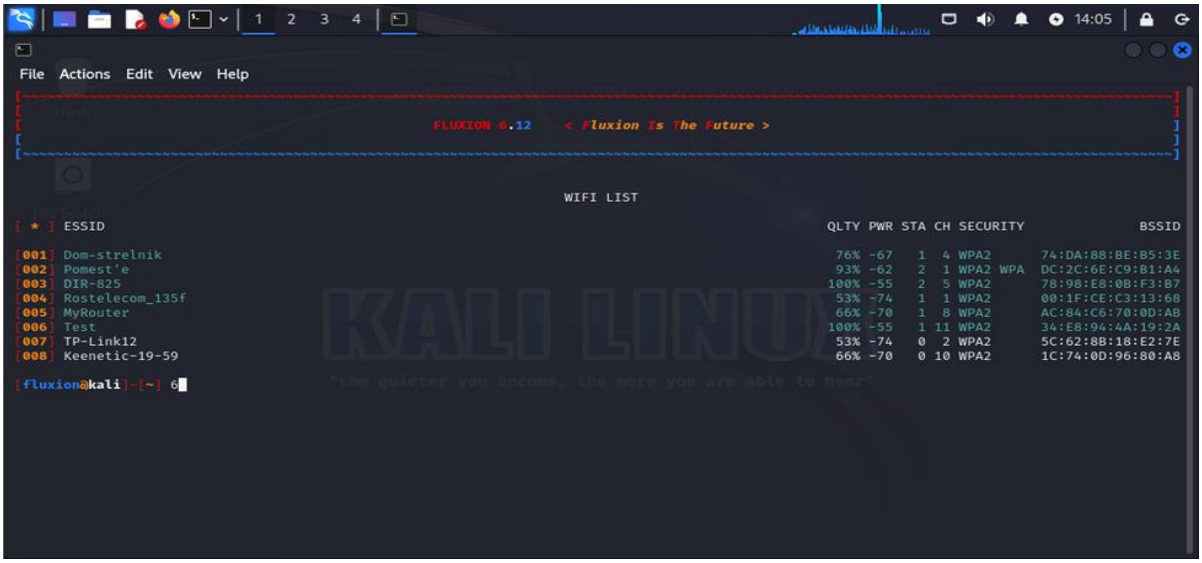

Рис. 5. Выбор целевой точки
Fig. 5. Target point selection

Теперь следует перейти к перехвату хендшейка, для чего необходимо назначить интерфейсы для отслеживания, деаутентификации и перехвата. Затем выбирается метод проверки перехваченного хендшейка (рис. 6).

Рис. 6. Выбор метода проверки перехваченного хендшейка
Fig. 6. Choosing the method of checking the intercepted handshake

После предварительной настройки оборудования можно переходить к запуску перехвата хендшейка посредством подавления целевой точки (рис. 7). Обычно это занимает одну-две минуты.

Хендшейк перехвачен, теперь необходимо сравнить его с введенным пользователем паролем, для этого поднимаем точку-двойник. Пока основная точка заглушена, клиент будет пытаться подключиться к двойнику и введет пароль, который будет сопоставлен с хендшейком.

Выбор второго этапа. Аналогично первому этапу назначаем интерфейсам функции и запускаем точку-двойник. Фейковая точка запущена, ждем подключения к ней пользователя. Тем временем у пользователя отключаются от интернета все клиенты атакуемой точки и

появляется идентичная в доступных сетях [Акапьев, Ковалева, Борисенко, Панарин, 2024], а при попытке подключения к ней выходит уведомление о необходимости ввода пароля (рис. 8).

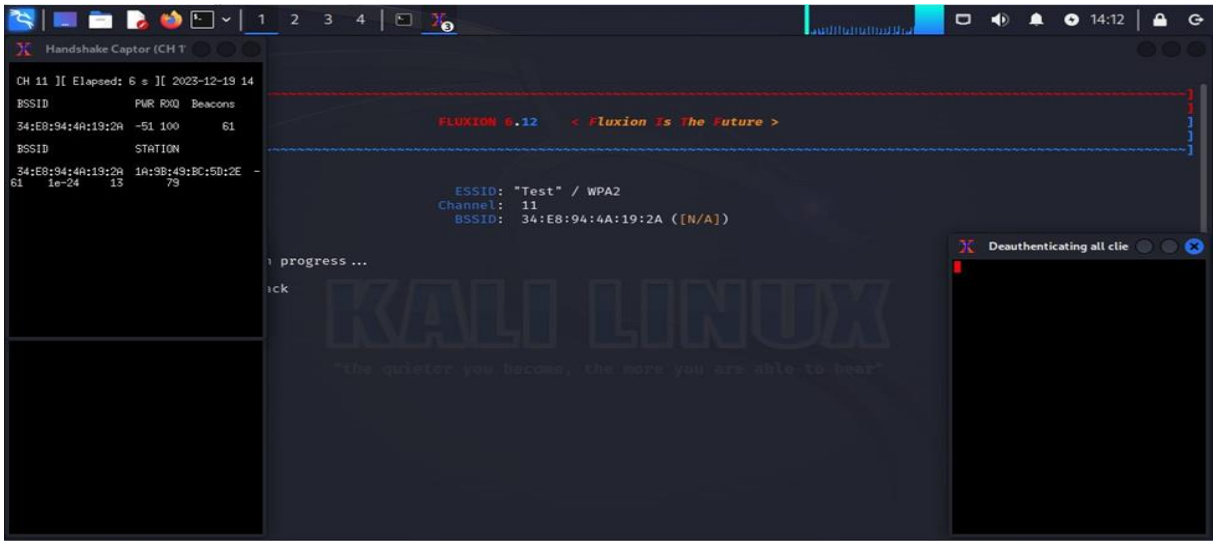

Рис. 7. Запуск перехвата хендшейка
Fig. 7. Launching the handshake interception

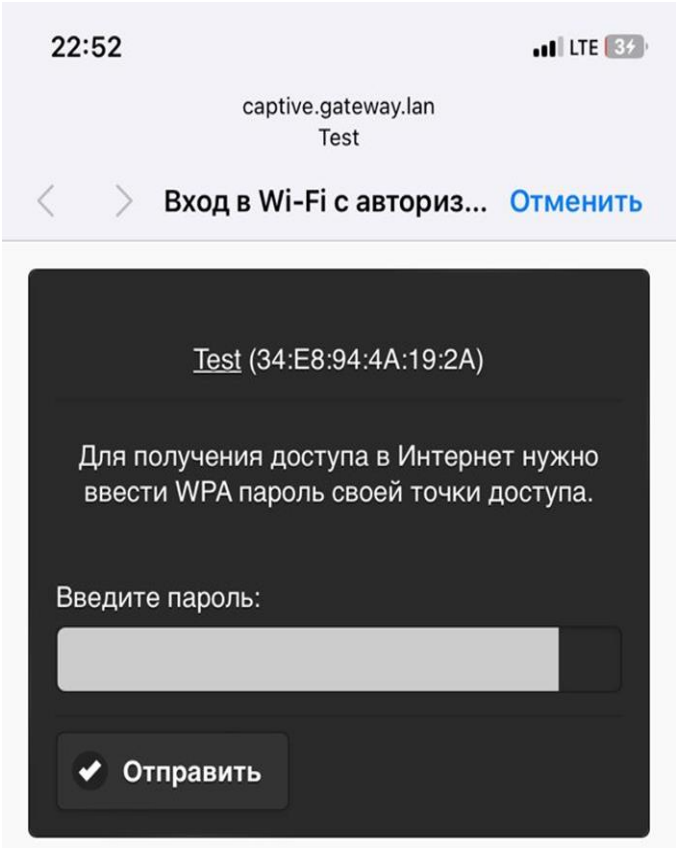

Рис. 8. Уведомление о необходимости ввода пароля
Fig. 8. Notification of the need to enter a password

Когда пароль введен и проверен, он сохраняется в системе (рис. 9).

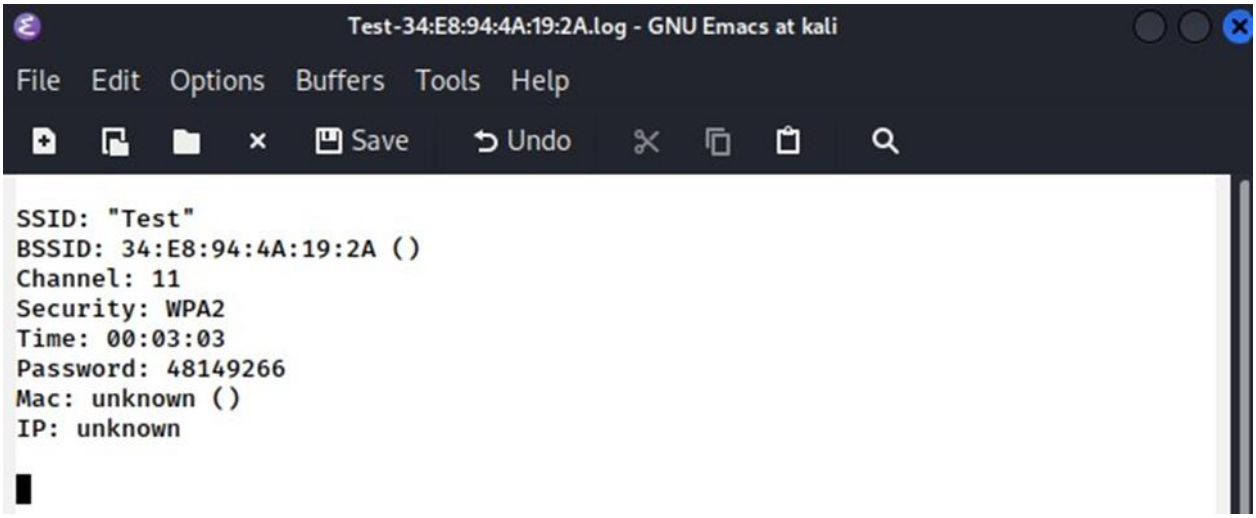

Рис. 9. Сохранение пароля
Fig. 9. Saving the password

Перехват реализован и поставленная учебная задача выполнена.

Заключение

Обеспечение информационной безопасности и противодействие киберпреступности являются непреходящими задачами, о которых в современных условиях забывать нельзя. Безусловно, невозможно защититься от попыток проникновения и воздействия на беспроводные сети на сто процентов, но можно использовать обязательные элементы защиты от атаки по Wi-Fi сети, к которым можно отнести обязательное применение сложных паролей, контроль подключения новых пользователей сети и обновление антивирусной защиты системы.

Но критическим, с точки зрения авторов, является формирование информационно-технологической компетентности специалиста в процессе подготовки его к профессиональной деятельности. В настоящее время реализация указанного процесса практически невозможна без использования обучающих тренажеров и симуляторов.

Предлагаемый авторами вариант эмуляции программного модуля имитации атаки на беспроводную сеть является малозатратным и быстрореализуемым способом демонстрации возможностей использования современных информационных технологий при подготовке сотрудников правоохранительных органов.

Таким образом, наиболее оптимальным вариантом имитации атаки на беспроводную сеть является эмуляция программного модуля симулятора-тренажера. Достигнута поставленная цель и подтверждена гипотеза исследования.

Список литературы

Акапьев В.Л., Ковалева Е.А., Борисенко А.В., Панарин В.В. 2024. Разработка симулятора атаки на беспроводную сеть. *Вестник Воронежского института ФСИН России*, 3: 22–34.

Акапьев В.Л., Савотченко С.Е. 2015. Актуальные проблемы импортозамещения программного обеспечения образовательных организаций в контексте информационной безопасности. *Дистанционное и виртуальное обучение*, 11(101): 113–125.

В России за январь – июль 2025 года ущерб от IT-преступлений вырос на 16 % и составил почти 120 млрд рублей. – URL: https://alrf.ru/news/v-rossii-za-yanvar-iyul-2025-goda-ushcherb-ot-it-prestupleniy-vyros-na-16-i-sostavil-pochti-120-mlrd (дата обращения 07.09.2025).

Виртуальные тренажеры и эмуляторы. – URL: https://labstand.ru/catalog/virtualnye-trenazhery-i-emulyatory-zashhita-informaczii (дата обращения 28.09.2025).

Журавлева В.В., Ткаченко А.Л. 2023. Пентест и его особенности. *Дневник науки*, 11: 83.

Интерактивная карта киберугроз. – URL: https://cybermap.kaspersky.com/ru/stats#country=213&type=IDS&period=m (дата обращения 08.10.2025).

Abdalla A.S., Tang B., Marojevic V. 2025. AI at the Physical Layer for Wireless Network Security and Privacy. *Artificial Intelligence for Future Networks*, 341–380. DOI:10.1002/9781394227952.ch10

An Z., Pan J., Wen Y., Zhang F. 2023. Secret handshakes: Full dynamicity, deniability and lattice-based design. *Theoretical Computer Science*, 940(3): 14–35. DOI:10.1016/j.tcs.2022.10.035

Bodenhausen J., Mangel S., Vogt T., Henze M. 2025. Bidirectional TLS Handshake Caching for Constrained Industrial IoT Scenarios. 2025 IEEE 50th Conference on Local Computer Networks (LCN). 1–10.

Kumar K.D., Niranjan D.K., Reddy P.P., Himanshu P., Raju K.S., Goud P. 2025. CloudShare: A Passwordless Cloud-Based File Storage and Sharing Framework. In 2025 International Conference on Computing Technologies (ICOCT). 1–6.

Montañez-Juan M., Forteza-Domenici C., García-Buades M.E., Blahopoulou J., Ortiz-Bonnin S. 2025. Virtual handshakes: team emotional intelligence and digital competences in virtual settings. *Behaviour & Information Technology*, 44(14): 3501–3513. DOI:10.1080/0144929X.2025.2535740

Perez E.L., Selander G., Mattsson J.P., Watteyne T., Vučinić M. 2024. EDHOC Is a New Security Handshake Standard: An Overview of Security Analysis. *Computer*, 57(9): 101–110.

Prayatno C., Tohari M., Susilowati T. 2024. The Impact of Using Technology and Innovation in Law Enforcement in the Era of Digitalization. *Jurnal Ekonomi Teknologi dan Bisnis (JETBIS)*, 3(8): 1026–1033.

Ramadan R. 2022. Internet of things (iot) security vulnerabilities: A review. *PLOMS AI*, 2(1).

Saha K.K., Ray S., Dasgupta M. 2024. ECMHP: ECC-based secure handshake protocol for multicasting in CCN-IoT environment. *IEEE Transactions on Network and Service Management*, 21(5): 5826–5842.

Teichmann F.M., Boticiu S.R. 2023. An overview of the benefits, challenges, and legal aspects of penetration testing and red teaming. *International Cybersecurity Law Review*, 4(4): 387–397.

The 8 Best Virtual Cybersecurity Practice Labs – URL: https://www.cloudshare.com/blog/cybersecurity-practice-labs (access data: 01.10.2025).

Torres-Trujillo J., Meza-Alarcon A.J., Ticona W. 2024. Test and Pentesting Methods for Identifying Vulnerabilities in IoT Devices: A Systematic Review. *Proceedings of the Computational Methods in Systems and Software*, 28–41.

Yavorsky M.A., Useev R.Z., Kurushin S.A. 2021. Information technologies in law enforcement: Overview of implements and opportunities. *European Proceedings of Social and Behavioural Sciences*.

Zhukabayeva T., Karabayev N., Nurusheva A., Satybaldina D. 2024. A method of vulnerability analysis in wireless internet of things networks for smart city infrastructures. *Scientific Journal of Astana IT University*. Vol. 20. DOI:10.37943/20VPSX8675

References

Akap'ev V.L., Kovaleva E.A., Borisenko A.V., Panarin V.V. 2024. Razrabotka simuljatora ataki na besprovodnuju set' [Development of a Wireless Network Attack Simulator.] *Vestnik Voronezhskogo instituta FSIN Rossii* [Bulletin of the Voronezh Institute of the Federal Penitentiary Service of Russia], 3: 22–34.

Akap'ev V.L., Savotchenko S.E. 2015. Aktual'nye problemy importozameshhenija programmnogo obespechenija obrazovatel'nyh organizacij v kontekste informacionnoj bezopasnosti [Current Issues of Import Substitution of Educational Software in the Context of Information Security]. *Distancionnoe i virtual'noe obuchenie* [Distance and Virtual Learning],11(101): 113–125.

V Rossii za janvar'-ijul' 2025 goda ushherb ot IT-prestuplenij vyros na 16 % i sostavil pochti 120 mlrd rublej [In Russia, damage from IT crimes increased by 16 % from January to July 2025, amounting to almost 120 billion rubles]. URL: https://alrf.ru/news/v-rossii-za-yanvar-iyul-2025-goda-ushcherb-ot-it-prestupleniy-vyros-na-16-i-sostavil-pochti-120-mlrd (access data: 07.09.2025).

Virtual'nye trenazhery i jemuljatory [Virtual simulators and emulators]. URL: https://labstand.ru/catalog/virtualnye-trenazhery-i-emulyatory-zashhita-informaczii (access data: 28.09.2025).

Zhuravleva V.V., Tkachenko A.L. 2023. Pentest i ego osobennosti [Pentesting and its features] *Dnevnik nauki* [Science Diary], 11: 83.

Abdalla A.S., Tang B., Marojevic V. 2025. AI at the Physical Layer for Wireless Network Security and Privacy. *Artificial Intelligence for Future Networks*, 341–380. DOI:10.1002/9781394227952.ch10

An Z., Pan J., Wen Y., Zhang F. 2023. Secret handshakes: Full dynamicity, deniability and lattice-based design. *Theoretical Computer Science*, 940(3): 14–35. DOI: 10.1016/j.tcs.2022.10.035

Bodenhausen J., Mangel S., Vogt T., Henze M. 2025. Bidirectional TLS Handshake Caching for Constrained Industrial IoT Scenarios. 2025 IEEE 50th Conference on Local Computer Networks (LCN). 1–10.

Kumar K.D., Niranjan D.K., Reddy P.P., Himanshu P., Raju K.S., Goud P. 2025. CloudShare: A Passwordless Cloud-Based File Storage and Sharing Framework. In 2025 International Conference on Computing Technologies (ICOCT). 1–6.

Montañez-Juan M., Forteza-Domenici C., García-Buades M.E., Blahopoulou J., Ortiz-Bonnin S. 2025. Virtual handshakes: team emotional intelligence and digital competences in virtual settings. *Behaviour & Information Technology*, 44(14): 3501–3513. DOI:10.1080/0144929X.2025.2535740

Perez E.L., Selander G., Mattsson J.P., Watteyne T., Vučinić M. 2024. EDHOC Is a New Security Handshake Standard: An Overview of Security Analysis. *Computer*, 57(9): 101–110.

Prayatno C., Tohari M., Susilowati T. 2024. The Impact of Using Technology and Innovation in Law Enforcement in the Era of Digitalization. *Jurnal Ekonomi Teknologi dan Bisnis (JETBIS)*, 3(8): 1026–1033.

Ramadan R. 2022. Internet of things (iot) security vulnerabilities: A review. *PLOMS AI*, 2(1).

Saha K.K., Ray S., Dasgupta M. 2024. ECMHP: ECC-based secure handshake protocol for multicasting in CCN-IoT environment. *IEEE Transactions on Network and Service Management*, 21(5): 5826–5842.

Teichmann F.M., Boticiu S.R. 2023. An overview of the benefits, challenges, and legal aspects of penetration testing and red teaming. *International Cybersecurity Law Review*, 4(4): 387–397.

The 8 Best Virtual Cybersecurity Practice Labs – URL: https://www.cloudshare.com/blog/cybersecurity-practice-labs (access data: 01.10.2025).

Torres-Trujillo J., Meza-Alarcon A.J., Ticona W. 2024. Test and Pentesting Methods for Identifying Vulnerabilities in IoT Devices: A Systematic Review. *Proceedings of the Computational Methods in Systems and Software*, 28–41.

Yavorsky M.A., Useev R.Z., Kurushin S.A. 2021.Information technologies in law enforcement: Overview of implements and opportunities. *European Proceedings of Social and Behavioural Sciences*.

Zhukabayeva T., Karabayev N., Nurusheva A., Satybaldina D. 2024. A method of vulnerability analysis in wireless internet of things networks for smart city infrastructures. *Scientific Journal of Astana IT University*, Vol. 20. DOI:10.37943/20VPSX8675

Конфликт интересов: о потенциальном конфликте интересов не сообщалось.
Conflict of interest: no potential conflict of interest related to this article was reported.

Поступила в редакцию 10.10.2025
Поступила после рецензирования 29.11.2025
Принята к публикации 02.12.2025

Received October 10, 2025
Revised November 29, 2025
Accepted December 02, 2025

ИНФОРМАЦИЯ ОБ АВТОРАХ

Борисенко Александр Васильевич, кандидат физико-математических наук, преподаватель кафедры информационно-компьютерных технологий в деятельности ОВД, Белгородский юридический институт Министерства внутренних дел Российской Федерации имени И.Д. Путилина, г. Белгород, Россия

Акапьев Виктор Львович, кандидат педагогических наук, доцент кафедры информационно-компьютерных технологий в деятельности ОВД, Белгородский юридический институт Министерства внутренних дел Российской Федерации имени И.Д. Путилина, г. Белгород, Россия

INFORMATION ABOUT THE AUTHORS

Aleksander V. Borisenko, Candidate of Physical and Mathematical Sciences, Lecturer at the Department of Information and Computer Technologies in the Activities of the Internal Affairs Directorate, Putilin Belgorod Law Institute of the Ministry of Internal Affairs of the Russian Federation, Belgorod, Russia

Viktor L. Akapyev, Candidate of Pedagogical Sciences, Associate Professor of the Department of Information and Computer Technologies in the Activities of the Internal Affairs Directorate, Putilin Belgorod Law Institute of the Ministry of Internal Affairs of the Russian Federation, Belgorod, Russia

Ковалева Екатерина Геннадьевна, кандидат технических наук, доцент кафедры информационно-компьютерных технологий в деятельности ОВД, Белгородский юридический институт Министерства внутренних дел Российской Федерации имени И.Д. Путилина, г. Белгород, Россия

Ekaterina G. Kovaleva, Candidate of Technical Sciences, Associate Professor of the Department of Information and Computer Technologies in the Activities of the Internal Affairs Directorate, Putilin Belgorod Law Institute of the Ministry of Internal Affairs of the Russian Federation, Belgorod, Russia

Новикова Екатерина Анатольевна, кандидат юридических наук, начальник кафедры информационно-компьютерных технологий в деятельности ОВД, Белгородский юридический институт Министерства внутренних дел Российской Федерации имени И.Д. Путилина, г. Белгород, Россия

Ekaterina A. Novikova, Candidate of Law Sciences, Head of the Department of Information and Computer Technologies in the Activities of the Internal Affairs Directorate, Putilin Belgorod Law Institute of the Ministry of Internal Affairs of the Russian Federation, Belgorod, Russia