Дата поступления рукописи в редакцию: 23.04.2025 г.
Дата принятия рукописи в печать: 13.05.2025 г.
DOI: 10.24412/2782-3830-2025-4-266-272

БЕППАЕВ Руслан Жамалович,
подполковник полиции, преподаватель,
Северо-Кавказский институт повышения
квалификации сотрудников МВД России (филиал)
Краснодарского университета МВД России,
кафедра специальных дисциплин,
e-mail: mail@law-books.ru

НЕЗАКОННОЕ КЛОНИРОВАНИЕ ПЛАТЕЖНЫХ КАРТ ЧЕРЕЗ IOT-УСТРОЙСТВА: СОВРЕМЕННЫЕ УГРОЗЫ И МЕТОДЫ ПРОТИВОДЕЙСТВИЯ

Аннотация. *В данной статье рассматриваются современные методы незаконного клонирования платежных карт с использованием устройств Интернета вещей (IoT). Проанализированы технические аспекты и криминологические характеристики данного вида киберпреступлений. Особое внимание уделено уязвимостям IoT-инфраструктуры, которые эксплуатируются злоумышленниками для перехвата платежных данных. На основе криминалистического анализа реальных кейсов выявлены основные векторы атак и представлены эффективные методы противодействия, включая организационные и технические меры защиты. Результаты исследования могут быть использованы для совершенствования систем безопасности финансовых организаций и разработки методик расследования данного вида киберпреступлений.*

Ключевые слова: *Клонирование платежных карт, скимминг, IoT-устройства, кибербезопасность, карточное мошенничество, криминалистический анализ, методы противодействия, кибервиктимология, цифровая криминалистика.*

BEPPAEV Ruslan Zhamalovich,
police lieutenant colonel, teacher,
North Caucasian Institute for Advanced Training of Employees
of the Ministry of Internal Affairs of Russia (branch)
of the Krasnodar University of the Ministry of Internal Affairs of Russia,
Department of Special Disciplines

ILLEGAL CLONING OF PAYMENT CARDS VIA IOT DEVICES: MODERN THREATS AND COUNTERMEASURES

Annotation. *This article discusses modern methods of illegal cloning of payment cards using Internet of Things (IoT) devices. The technical aspects and criminological characteristics of this type of cybercrime are analyzed. Particular attention is paid to the vulnerabilities of the IoT infrastructure that are exploited by attackers to intercept payment data. Based on the forensic analysis of real cases, the main attack vectors are identified and effective counteraction methods are presented, including organizational and technical protection measures. The results of the study can be used to improve the security systems of financial institutions and develop methods for investigating this type of cybercrime.*

Key words: *Cloning of payment cards, skimming, IoT devices, cybersecurity, card fraud, forensic analysis, counteraction methods, cyber victimology, digital forensics.*

Цифровизация финансовых услуг в сочетании с распространением устройств Интернета вещей (IoT) создала новые возможности для преступлений в сфере платежных технологий. По прогнозам аналитиков, к концу 2025 года количество подключенных IoT-устройств превысит 75 миллиардов, что значительно расширяет поверхность для потенциальных атак. Каждое такое устройство может стать точкой входа для злоумышленников, особенно в условиях недостаточного внимания к вопросам безопасности при их проектировании и эксплуатации.

Традиционные методы скимминга, некогда ограниченные физическим доступом к банкоматам и POS-терминалам, трансформировались в сложные многоступенчатые схемы с использованием сетевых технологий. Современные атаки часто начинаются с компрометации IoT-устройств, которые становятся «глазами и ушами» злоумышленников внутри защищенной инфраструктуры. По данным международной ассоциации по безопасности платежных карт, ежегодный глобальный ущерб от карточного мошенничества превышает 27 млрд долларов США, причем доля атак, использующих IoT-уязвимости, ежегодно увеличивается примерно на 15% [3, с. 42-44].

Технические особенности IoT-устройств делают их привлекательной мишенью для атак. К таким особенностям относятся: ограниченные вычислительные ресурсы, затрудняющие реализацию полноценных механизмов защиты; длительные циклы обновления программного обеспечения; часто отсутствие физической защиты; и неконтролируемая пользователем сетевая активность. Алексеев А.Н. подчеркивает, что до 70% широко используемых IoT-устройств имеют уязвимости, которые могут быть использованы для несанкционированного доступа [1, с. 90-92].

Современные киберпреступники используют уязвимости IoT-устройств для перехвата, сбора и незаконного использования платежных данных. Особенностью данных преступлений является их высокая латентность, трансграничный характер и технологическая сложность выявления и расследования [8, с. 115-117]. В отличие от традиционного скимминга, атаки через IoT-устройства могут осуществляться дистанционно и затрагивать одновременно множество жертв, часто находящихся в разных юрисдикциях, что значительно усложняет как расследование, так и судебное преследование.

Технологическая эволюция методов незаконного клонирования платежных карт напрямую связана с развитием платежных технологий. Классические скиммеры, устанавливаемые на банкоматы, уступили место более изощренным техническим решениям, которые сложнее выявить и нейтрализовать [7, с. 201-202].

Согласно исследованиям Ковалева А.П., современные методы клонирования платежных карт включают широкий спектр технических и программных решений. Компрометация POS-терминалов через уязвимости программного обеспечения становится одним из наиболее распространенных методов. Злоумышленники используют недокументированные возможности или ошибки в программном коде для удаленного доступа к памяти устройства, где временно хранятся незашифрованные данные платежных карт. Особенно уязвимыми являются терминалы, работающие на устаревших версиях операционных систем или имеющие нерегулярные циклы обновления безопасности [5, с. 78-79].

Использование поддельных терминалов и банкоматов остается актуальным методом, хотя и претерпело значительную эволюцию. Современные поддельные устройства часто имеют беспроводные модули для передачи собранных данных, системы удаленного управления и механизмы самоуничтожения при попытке несанкционированного доступа. Тимофеев В.А. отмечает случаи, когда злоумышленники устанавливали полностью функциональные поддельные банкоматы в общественных местах, которые не только собирали данные карт, но и выполняли базовые банковские операции для маскировки своего истинного назначения [9, с. 228-229].

Перехват данных в процессе бесконтактных платежей становится все более распространенным с ростом популярности данной технологии. Злоумышленники используют модифицированные NFC-считыватели, которые могут быть замаскированы под обычные предметы и размещены в местах массового скопления людей. Такие устройства способны считывать данные бесконтактных карт на расстоянии до 20 см, что позволяет собирать информацию без ведома владельцев карт. Особенно уязвимыми являются карты, не имеющие динамической аутентификации данных (DDA) [5, с. 80-81].

Гарсиа-Алфаро и соавторы отмечают, что с 2020 года наблюдается значительный рост атак, использующих уязвимости IoT-устройств для перехвата платежных данных [11, с. 233-235]. Эти атаки часто реализуются по модели «человек посередине» (Man-in-the-Middle), когда злоумышленники используют скомпрометированное IoT-устройство для перехвата сетевого трафика, содержащего платежную информацию. Особенно уязвимыми являются незашифрованные или слабо зашифрованные соединения между элементами платежной инфраструктуры.

Инфраструктура рынка украденных данных также претерпела значительные изменения. Данные платежных карт теперь редко используются непосредственно злоумышленниками, осуществившими их кражу. Вместо этого сформировалась сложная многоуровневая система, включающая специализированных участников: «добытчиков» данных, «оптовых покупателей», «проверяющих» (валидаторов) и «использующих» (кардеров). Такая специализация повышает эффективность преступной деятельности и усложняет выявление конечных исполнителей мошеннических операций [8, с. 117-118].

Анализ таких инцидентов показывает, что преступники переходят от физического вмешательства к удаленным атакам, что существенно

усложняет их выявление и расследование. Вехов В.Б. подчеркивает, что «цифровизация» методов клонирования приводит к росту латентности таких преступлений, поскольку отсутствие физических следов затрудняет как обнаружение факта атаки, так и идентификацию злоумышленников [2, с. 167-169].

IoT-устройства представляют собой привлекательную цель для киберпреступников в силу нескольких факторов: недостаточный уровень защиты, отсутствие регулярных обновлений безопасности и возможность использования в качестве промежуточного звена для проведения атак. Алексеев А.Н. в своем исследовании выделяет три основных сценария использования IoT-устройств в кибермошенничестве: как инструмент сбора данных, как канал для атаки на другие элементы инфраструктуры и как компонент ботнета для распределенных атак [1, с. 92-94].

В контексте клонирования платежных карт особую опасность представляют устройства, имеющие физический или логический доступ к платежной информации. Исследования Петрова В.В. демонстрируют, что наиболее уязвимыми являются умные камеры видеонаблюдения в зонах банкоматов и торговых точек. Современные IP-камеры с функциями распознавания изображений и дистанционного управления могут быть перепрограммированы злоумышленниками для фиксации процесса ввода PIN-кода и передачи этих данных на удаленные серверы. Особую опасность представляют камеры с функцией оптического увеличения и высоким разрешением, которые позволяют получить четкое изображение карты даже с значительного расстояния [6, с. 154-155].

Беспроводные маршрутизаторы в публичных WiFi-сетях часто становятся точкой входа для атак на мобильные платежные приложения. Злоумышленники могут создавать поддельные точки доступа (Evil Twin) или компрометировать существующие, чтобы перехватывать незашифрованный трафик или проводить атаки типа SSL-stripping для доступа к защищенным соединениям. Особенно уязвимыми являются пользователи, осуществляющие платежные операции через публичные сети без использования дополнительных средств защиты, таких как VPN.

POS-терминалы с возможностью удаленного управления представляют собой критически важный элемент платежной инфраструктуры. Современные терминалы часто имеют встроенные модули для дистанционного обновления программного обеспечения, диагностики и управления. Компрометация этих каналов позволяет злоумышленникам внедрять вредоносный код непосредственно в устройство, считывающее данные карт..

Технические уязвимости IoT-устройств многообразны и включают как программные, так и аппаратные недостатки. Среди наиболее распространенных программных уязвимостей можно выделить: недостаточную защиту аутентификации (слабые пароли, отсутствие многофакторной аутентификации); отсутствие или неправильную реализацию шифрования; уязвимости в Web-интерфейсах управления; недостаточную фильтрацию входных данных, ведущую к уязвимостям внедрения кода. К аппаратным уязвимостям относятся: незащищенные отладочные интерфейсы; отсутствие защиты от физического доступа к компонентам; недостаточная изоляция чувствительных данных в памяти устройства [1, с. 94-95].

Анализ, проведенный Schneider и коллегами, выявил, что в 63% случаев компрометации платежных данных злоумышленники использовали IoT-устройства как канал атаки или точку сбора информации [13, с. 301-303]. Исследователи идентифицировали несколько типовых сценариев атак, включая:

- Компрометацию IP-камер для визуального перехвата PIN-кодов и данных карт;
- Использование уязвимых маршрутизаторов для перехвата сетевого трафика;
- Атаки на POS-терминалы через уязвимые обновления программного обеспечения;
- Использование скомпрометированных IoT-устройств для создания постоянного присутствия в корпоративной сети (persistence);
- Применение ботнетов из IoT-устройств для проведения DDoS-атак на платежные системы с целью маскировки основной атаки.

Модифицированные Bluetooth-маяки представляют собой еще одну категорию устройств, используемых для сбора данных с бесконтактных карт. Такие маяки можно разместить в местах с высокой проходимостью, и они будут автоматически сканировать окружение на предмет бесконтактных карт. Хотя современные карты имеют защиту от несанкционированного считывания, некоторые старые модели или карты с поврежденным чипом могут быть уязвимы к такому виду атак [9, с. 230-231].

Типичная архитектура атаки через IoT-устройства включает несколько этапов. На первом этапе происходит сканирование сети на предмет уязвимых устройств. Затем осуществляется компрометация выбранных устройств с использова-

нием известных уязвимостей или техник социальной инженерии. После получения доступа злоумышленники внедряют вредоносный код, который может включать функции перехвата данных, создания бэкдоров или перенаправления трафика. На заключительном этапе собранные данные передаются на управляющие серверы, часто с использованием шифрования и методов маскировки для предотвращения обнаружения [11, с. 235-236].

Особую опасность представляют атаки, координируемые через несколько скомпрометированных устройств, что затрудняет выявление источника угрозы и увеличивает масштаб потенциального ущерба. Такие атаки часто проводятся с использованием методов обфускации и шифрования трафика, что дополнительно усложняет их обнаружение стандартными средствами мониторинга безопасности.

С криминологической точки зрения, преступления, связанные с незаконным клонированием платежных карт через IoT-устройства, характеризуются рядом особенностей, которые отличают их от традиционных форм карточного мошенничества.

Согласно исследованиям Смирнова Д.Н., типичный портрет преступника в данной сфере существенно отличается от традиционного образа кардера. Современные киберпреступники обладают высоким уровнем технической подготовки, знаниями в области сетевой безопасности и программирования. Часто они имеют легальный опыт работы в сфере информационных технологий или финансовой безопасности, что дает им понимание как технических аспектов атаки, так и мер защиты, которые необходимо преодолеть [8, с. 118-119].

Виктимологический анализ показывает, что потенциальными жертвами становятся не только физические лица, но и малый бизнес, использующий недостаточно защищенные платежные решения. Козловский А.Ю. выделяет несколько факторов риска, повышающих вероятность стать жертвой данного вида преступлений:

– Использование устаревшего оборудования и программного обеспечения без регулярных обновлений безопасности;
– Недостаточная осведомленность о методах обеспечения информационной безопасности;
– Стремление к минимизации расходов на IT-инфраструктуру за счет применения бюджетных решений с потенциальными уязвимостями;
– Отсутствие политик безопасности и регулярного аудита систем;
– Игнорирование предупреждений и рекомендаций по безопасности [4, с. 201-202].

Особую виктимологическую группу составляют владельцы малых предприятий, использующие бюджетные IoT-решения для автоматизации бизнес-процессов без должного внимания к вопросам информационной безопасности. Филиппов А.Е. отмечает, что такие предприятия часто становятся «точкой входа» для атак на более крупные организации, с которыми они взаимодействуют. Например, компрометация системы видеонаблюдения в небольшом магазине может стать первым шагом к атаке на всю платежную инфраструктуру торговой сети [10, с. 87-88].

Географический анализ распространения данного вида преступлений показывает значительную неравномерность. Наибольшая активность наблюдается в регионах с высоким уровнем проникновения электронных платежей и одновременно недостаточным развитием законодательства в сфере кибербезопасности. Смирнов отмечает, что часто страны с развивающейся экономикой становятся «испытательными полигонами» для новых методов атак, которые затем применяются в более развитых регионах [8, с. 122-123].

По данным Романовского Г.Б., латентность данного вида преступлений достигает 70%, что обусловлено сложностью выявления факта компрометации и установления причинно-следственной связи между атакой на IoT-устройство и последующим хищением средств [7, с. 204-205]. Высокая латентность объясняется несколькими факторами: значительным временным разрывом между компрометацией данных и их использованием; отсутствием явных следов вмешательства; нежеланием организаций сообщать о инцидентах из опасений репутационных потерь; и техническими сложностями выявления компрометации IoT-устройств.

Расследование преступлений, связанных с незаконным клонированием платежных карт через IoT-устройства, требует применения специализированных криминалистических методик, учитывающих технические особенности данного вида преступлений.

Согласно разработкам Вехова В.Б., криминалистическое исследование должно включать комплекс технических и процессуальных мероприятий. Анализ сетевого трафика подозрительных устройств является одним из ключевых методов выявления вредоносной активности. Такой анализ позволяет идентифицировать аномальные шаблоны коммуникации, которые могут указывать на попытки передачи скомпрометированных

данных на удаленные серверы. Вехов рекомендует использовать системы глубокого анализа пакетов (DPI), позволяющие выявлять не только явные аномалии, но и скрытые каналы связи, маскирующиеся под легитимный трафик [2, с. 170-171].

Козловский А.Ю. отмечает, что для эффективного расследования необходим комплексный подход, включающий анализ цифровых следов, изъятие и исследование физических устройств и получение данных от финансовых организаций о подозрительных транзакциях. Особую важность представляет своевременное изъятие электронных устройств с сохранением их текущего состояния, включая содержимое энергозависимой памяти. Для этого рекомендуется использовать специализированные аппаратно-программные комплексы, позволяющие создать криминалистически значимую копию данных без их модификации [4, с. 203-204].

Козловский выделяет следующие этапы комплексного криминалистического исследования:

– Предварительная оценка инцидента и определение потенциальных источников цифровых доказательств;
– Изъятие и документирование электронных устройств с соблюдением процессуальных норм;
– Создание криминалистических копий данных с использованием специализированного оборудования;
– Анализ полученных данных с применением специализированного программного обеспечения;
– Соотнесение цифровых следов с физическими доказательствами и показаниями свидетелей;
– Формирование доказательной базы для судебного производства [4, с. 204-205].

Особую сложность представляет установление причинно-следственной связи между компрометацией IoT-устройства и последующими несанкционированными транзакциями. Lin и коллеги предлагают методику корреляционного анализа временных рядов для выявления таких связей [12, с. 416-417]. Этот метод основан на статистическом анализе временных паттернов атак и последующих фрод-операций с учетом различных факторов, включая географическое положение, типы устройств и характеристики транзакций.

Международное сотрудничество при расследовании данного вида преступлений является критически важным фактором успеха. Романовский Г.Б. подчеркивает необходимость использования механизмов взаимной правовой помощи (MLA), соглашений о сотрудничестве между правоохранительными органами различных стран и взаимодействия через специализированные международные организации, такие как Интерпол и Европол [7, с. 206-207].

Разработка и внедрение политик безопасного использования IoT-устройств создает формальную основу для обеспечения защиты информации. Такие политики должны определять:

– Требования к приобретаемым устройствам (включая наличие механизмов защиты и поддержки производителем);
– Процедуры ввода в эксплуатацию и вывода из эксплуатации устройств;
– Правила настройки и изменения конфигурации;
– Регламенты обновления программного обеспечения;
– Порядок реагирования на инциденты безопасности.

Сотрудничество с правоохранительными органами и обмен информацией о выявленных угрозах позволяет формировать коллективную защиту от новых видов атак. Петров отмечает важность участия в отраслевых группах по обмену информацией об угрозах (threat intelligence sharing), что позволяет получать актуальные данные о новых векторах атак и индикаторах компрометации [6, с. 163-164].

Romero-Mariona и соавторы подчеркивают важность внедрения принципа «безопасность с момента разработки» (security by design) для IoT-устройств, используемых в финансовой сфере [14, с. 92-93]. Данный подход предполагает учет требований безопасности на всех этапах жизненного цикла устройства, от концептуальной разработки до утилизации.

Криминалистическое исследование данного вида преступлений требует применения специализированных методик, включающих анализ сетевого трафика, исследование журналов событий, проверку целостности программного обеспечения и анализ вредоносного кода [15]. Особую сложность представляет установление причинно-следственной связи между компрометацией IoT-устройств и последующими мошенническими операциями.

Для эффективного противодействия необходимо:

Совершенствование нормативно-правовой базы с учетом технологических особенностей IoT. Необходимо разработать специализированные нормы, определяющие ответственность за атаки

на IoT-инфраструктуру и устанавливающие правовые рамки для сбора и использования цифровых доказательств.

Разработка специализированных методик расследования с использованием современных инструментов цифровой криминалистики. Правоохранительные органы нуждаются в регулярном обучении сотрудников, внедрении современных инструментов анализа цифровых следов и создании специализированных подразделений по расследованию высокотехнологичных преступлений.

Внедрение комплексных систем защиты финансовой инфраструктуры, учитывающих риски, связанные с IoT. Такие системы должны включать как технические средства защиты (шифрование, многофакторная аутентификация, сегментация сетей), так и организационные меры (политики безопасности, обучение персонала, регулярный аудит).

Международное сотрудничество в сфере противодействия киберпреступности. Трансграничный характер атак требует координации усилий правоохранительных органов различных стран, обмена информацией об угрозах и совместного проведения расследований. Необходимо развивать существующие механизмы международного сотрудничества и создавать новые платформы для оперативного взаимодействия в сфере противодействия киберпреступности.

Перспективным направлением дальнейших исследований представляется разработка автоматизированных систем раннего выявления атак на IoT-устройства, основанных на технологиях искусственного интеллекта и машинного обучения.

Список литературы:

[1] Алексеев А.Н. Интернет вещей: проблемы безопасности и пути их решения // Информационная безопасность. 2022. №3. С. 89-97.

[2] Вехов В.Б. Особенности расследования преступлений, совершаемых с использованием современных информационных технологий // Российский следователь. 2021. №7. С. 165-172.

[3] Карпов А.С. Экономические последствия киберпреступлений в финансовой сфере // Вопросы экономики и права. 2023. №2. С. 40-48.

[4] Козловский А.Ю. Методика расследования преступлений в сфере электронных платежей // Криминалистика и судебная экспертиза. 2022. №4. С. 198-207.

[5] Ковалев А.П. Современные методы защиты платежных систем // Банковские технологии. 2023. №5. С. 76-84.

[6] Петров В.В. Уязвимости IoT-устройств в финансовой инфраструктуре // Вопросы кибербезопасности. 2022. №2. С. 150-159.

[7] Романовский Г.Б. Правовые аспекты противодействия киберпреступности в финансовой сфере // Журнал российского права. 2021. №8. С. 198-206.

[8] Смирнов Д.Н. Криминологическая характеристика преступлений в сфере информационных технологий // Вестник криминологии. 2022. №1. С. 112-121.

[9] Тимофеев В.А. Бесконтактные платежные технологии: уязвимости и защита // Финансовая безопасность. 2021. №4. С. 226-235.

[10] Машекуашева М.Х. Некоторые аспекты использования в преступных целях искусственного интеллекта. Право и управление. 2024. № 8. С. 376-378.

[11] Garcia-Alfaro J., Navarro-Arribas G., Leneutre J. Security and Privacy Issues in IoT-Based Payment Systems // IEEE Transactions on Dependable and Secure Computing. 2021. Vol. 18, No. 2. P. 230-240.

[12] Lin H., Bergmann N., Liang F. Forensic Analysis of IoT-Based Financial Fraud: Methodology and Case Studies // Digital Investigation. 2022. Vol. 40. P. 412-422.

[13] Schneider J., Ricci S., Guo L. Analysis of Payment Card Breaches Through IoT Vulnerabilities // Journal of Cybersecurity. 2023. Vol. 9, No. 3. P. 298-309.

[14] Romero-Mariona J., Bryan A., Zak R. Security by Design Principles for Financial IoT Applications // International Journal of Critical Infrastructure Protection. 2021. Vol. 32. P. 88-97.

[15] Zhang Y., Wang L., Sun W. Securing IoT for Financial Services: Challenges and Solutions // IEEE Internet of Things Journal. 2022. Vol. 9, No. 4. P. 2956-2967.

Spisok literatury:

[1] Alekseev A.N. Internet veshhej: problemy` bezopasnosti i puti ix resheniya // Informacionnaya bezopasnost`. 2022. №3. S. 89-97.

[2] Vexov V.B. Osobennosti rassledovaniya prestuplenij, sovershaemy`x s ispol`zovaniem sovremenny`x informacionny`x texnologij // Rossijskij sledovatel`. 2021. №7. S. 165-172.

[3] Karpov A.S. E`konomicheskie posledstviya kiberprestuplenij v finansovoj sfere // Voprosy` e`konomiki i prava. 2023. №2. S. 40-48.

[4] Kozlovskij A.Yu. Metodika rassledovaniya prestuplenij v sfere e`lektronny`x platezhej // Kriminalistika i sudebnaya e`kspertiza. 2022. №4. S. 198-207.

[5] Kovalev A.P. Sovremenny`e metody` zashhity` platezhny`x sistem // Bankovskie texnologii. 2023. №5. S. 76-84.

[6] Petrov V.V. Uyazvimosti IoT-ustrojstv v finansovoj infrastrukture // Voprosy` kiberbezopasnosti. 2022. №2. S. 150-159.

[7] Romanovskij G.B. Pravovy`e aspekty` protivodejstviya kiberprestupnosti v finansovoj sfere // Zhurnal rossijskogo prava. 2021. №8. S. 198-206.

[8] Smirnov D.N. Kriminologicheskaya xarakteristika prestuplenij v sfere informacionny`x texnologij // Vestnik kriminologii. 2022. №1. S. 112-121.

[9] Timofeev V.A. Beskontaktny`e platezhny`e texnologii: uyazvimosti i zashhita // Finansovaya bezopasnost`. 2021. №4. S. 226-235.

[10] Mashekuasheva M.X. Nekotory`e aspekty` ispol`zovaniya v prestupny`x celyax iskusstvennogo intellekta. Pravo i upravlenie. 2024. № 8. S. 376-378.

[11] Garcia-Alfaro J., Navarro-Arribas G., Leneutre J. Security and Privacy Issues in IoT-Based Payment Systems // IEEE Transactions on Dependable and Secure Computing. 2021. Vol. 18, No. 2. P. 230-240.

[12] Lin H., Bergmann N., Liang F. Forensic Analysis of IoT-Based Financial Fraud: Methodology and Case Studies // Digital Investigation. 2022. Vol. 40. P. 412-422.

[13] Schneider J., Ricci S., Guo L. Analysis of Payment Card Breaches Through IoT Vulnerabilities // Journal of Cybersecurity. 2023. Vol. 9, No. 3. P. 298-309.

[14] Romero-Mariona J., Bryan A., Zak R. Security by Design Principles for Financial IoT Applications // International Journal of Critical Infrastructure Protection. 2021. Vol. 32. P. 88-97.

[15] Zhang Y., Wang L., Sun W. Securing IoT for Financial Services: Challenges and Solutions // IEEE Internet of Things Journal. 2022. Vol. 9, No. 4. P. 2956-2967.

