

Научная статья
УДК 343.352.4

ОПЕРАТИВНО-РОЗЫСКНОЕ ПРОТИВОДЕЙСТВИЕ ОБНАЛЬНЫМ ПЛОЩАДКАМ ХХI ВЕКА

Илья Сергеевич Марсаков,
Академия управления МВД России, Москва, Россия,
ilya.marsakov.94@mail.ru



Аннотация

Введение: в статье рассматриваются особенности оперативно-розыскного противодействия преступлениям, совершаемым в кредитно-финансовой сфере, подразделениями экономической безопасности и противодействия коррупции. Особое внимание уделено одному из видов преступлений в данной области – незаконной банковской деятельности с использованием обнальных площадок нового типа, представляющих собой одну из серьезных угроз экономической безопасности Российской Федерации.

Материалы и методы: эмпирической и теоретической основой исследования явились доктринальные положения юридической науки, касающиеся оперативно-розыскного противодействия преступлениям, совершаемым в кредитно-финансовой сфере. В качестве ключевых источников проанализированы нормативные правовые акты, научные труды, результаты анкетирования респондентов, а также следственно-судебная практика, посвященная вопросам борьбы с преступлениями в данной сфере. Методологическую основу исследования составили как общенаучные методы (анализ, синтез, индукция, дедукция), так и частнонаучные методы познания, включая конкретно-социологический, контент-анализ, статистический метод, моделирование, структурно-логический, диалектический и формально-юридический подходы.

Обзор литературы: проанализированы труды ученых в области оперативно-розыскной деятельности, а также приведены позиции Президента Российской Федерации В.В. Путина и Министра внутренних дел Российской Федерации В.А. Колокольцева по проблемным аспектам и оперативной обстановке в рассматриваемой сфере. Отражены результаты исследований, посвященных незаконной банковской деятельности. Значимыми для разработки данной проблематики являются работы П.И. Иванова, М.И. Мамаева, А.В. Телкова, Р.Г. Искалиева и других исследователей.

Результаты исследования: на основе проведенного исследования автором сформулированы теоретические и практические выводы в сфере оперативно-розыскного противодействия преступлениям в кредитно-финансовой сфере, в частности свидетельствующие о трансформации обнальных площадок в устойчивые и технологически оснащенные преступные структуры, активно использующие информационно-коммуникационные технологии, криптовалюты, блокчейн-платформы и виртуальные финансовые инструменты, что значительно усложняет противодействие таким площадкам и повышает латентность указанных видов преступлений.

Обсуждение и заключение: результаты исследования свидетельствуют о многослойности преступных схем, применяемых для обналичивания и вывода денежных средств, в том числе за пределы страны. Установлена необходимость внедрения инновационных подходов к оперативно-розыскному противодействию данным преступлениям. Практические аспекты исследования подтверждают значимость повышения уровня профессиональной компетентности сотрудников подразделений экономической безопасности и противодействия коррупции в части структурных элементов обнальных площадок нового типа, укрепления внутреннего и межведомственного взаимодействия, а также модернизации оперативно-розыскного законодательства и разработки аналитико-прогностических инструментов для своевременного выявления и раскрытия преступлений в указанной сфере.

Ключевые слова: оперативно-розыскное противодействие; органы внутренних дел Российской Федерации; обнальные площадки нового типа; преступления в кредитно-финансовой сфере; борьба; ин-

формационно-коммуникационные технологии; подразделения экономической безопасности и противодействия коррупции; незаконная банковская деятельность

© Марсаков И.С., 2025

Для цитирования: Марсаков И.С. Оперативно-розыскное противодействие обнальным площадкам XXI века // Вестник Казанского юридического института МВД России. 2025. Т. 16. № 2 (60). С. 123 – 132.

Scientific article

UDC 343.352.4

**OPERATIONAL INVESTIGATIVE ACTIVITIES
IN THE CONTEXT OF DIGITALIZATION TO COMBAT CRIMES
IN THE CREDIT AND FINANCIAL SECTOR:
COUNTERING CASH-OUT PLATFORMS
OF THE 21ST CENTURY**

Ilya Sergeevich Marsakov,
Academy of Management of the Ministry of Internal Affairs of Russia,
Moscow, Russia,
ilya.marsakov.94@mail.ru

Abstract

Introduction: the article examines the specifics of the operational investigative activities of the internal affairs bodies of the Russian Federation in the context of digitalization, in the framework of countering crimes in the credit and financial sphere. Special attention is paid to the activities of 21st century cash platforms as one of the forms of criminal financial infrastructure that threatens the economic security of the Russian Federation.

Materials and Methods: the empirical and theoretical basis of this research is the doctrinal provisions of legal science concerning the organization and implementation of operational investigative activities of the internal affairs bodies of the Russian Federation in the field of countering crimes committed in the credit and financial sphere. Regulatory legal acts, scientific papers, survey results of respondents, archival materials of inspections, judicial acts, as well as other materials devoted to combating crimes in the credit and financial sphere, including those committed using modern information and communication technologies, were analyzed as key sources. The methodological basis of the research was made up of both general scientific methods (analysis, synthesis, induction, deduction) and private scientific methods of cognition, including structural-logical, dialectical and formal-legal approaches.

Literature Review: the works of scientists in the field of operational investigative activities are analyzed, and the positions of the President of the Russian Federation V.V. Putin and the Minister of Internal Affairs of the Russian Federation V.A. Kolokoltsev on problematic aspects and the operational situation in this area are illustrated.

Results: of research on the use of information and telecommunication technologies for illegal purposes are noted. A significant contribution to the development of this issue was made by P.I. Ivanov, M.I. Mamaev, A.V. Timofeev and other researchers. Research results: based on the conducted research, the author formulated theoretical and practical conclusions indicating the transformation of new-type cash platforms into stable and technologically equipped criminal structures that actively use information and communication technologies, cryptocurrencies, blockchain platforms and virtual financial instruments, which significantly complicates their detection and increases the latency of crimes.

Discussion and Conclusions: the results of the study indicate the establishment of a multi-layered criminal schemes used to cash out and withdraw funds, including outside the country. The necessity of introducing innovative methods of operational investigative activities aimed at combating these types of crimes has been identified. The practical aspects of the study confirm the relevance of raising awareness among employees of economic security and anti-corruption units, strengthening interdepartmental cooperation, as well as modernizing legislation and developing analytical and predictive tools for the timely detection and suppression of crimes in this area.

Keywords: operational investigative activities; internal affairs bodies of the Russian Federation; new type of cash platforms; crimes in the credit and financial sphere; struggle; information and communication technologies; economic security and anti-corruption units

© Marsakov I.S., 2025

For citation: Marsakov I.S. Operational Investigative Activities in the Context of Digitalization of Crimes in the Credit and Financial Sphere: Countering Cash-Out Platforms of the 21st Century. Bulletin of the Kazan Law Institute of MIA of Russia. 2025;16(2): 123-132. (In Russ.).

Введение

В условиях стремительной цифровизации оперативно-розыскная деятельность (далее – ОРД) приобретает новые функциональные возможности, обусловленные разработкой, апробацией и внедрением современных информационных технологий [1, с. 62 – 63], включая системы на базе искусственного интеллекта, в оперативные подразделения органов внутренних дел Российской Федерации (далее – ОВД). Вместе с тем расширение технологического инструментария сопровождается ростом числа вызовов и угроз как внутреннего, так и трансграничного характера, с которыми сталкиваются оперативные подразделения ОВД.

Актуальность данных вызовов последовательно обозначается в стратегических документах государственной политики Российской Федерации, таких как Стратегия национальной безопасности¹, Стратегия экономической безопасности Российской Федерации до 2030 года², а также Концепция государственной системы противодействия противоправным действиям, совершаемым с использованием информационно-коммуникационных технологий³. Указанные документы фиксируют приоритетные направления обеспечения национальной, экономической и информационной безопасности, акцентируя внимание на росте цифровых форм преступной активности, высокой латентности противоправных действий и их трансформации. Особое внимание уделяется преступлениям, совершаемым в кредитно-финансовой сфере, включая хищения денежных средств посредством методов социальной инженерии, а также несанкционированного доступа к системам дистанционного банковского обслуживания и оформления займов от имени граждан в микрофинансовых организациях. В этих условиях деятельность оперативных подразделений ОВД требует пе-

реосмыслиния и модернизации подходов к оперативно-розыскному противодействию рассматриваемым преступлениям с ориентацией на проактивное выявление и раскрытие преступлений в соответствующей сфере, включая те, которые совершаются с использованием информационно-коммуникационных технологий (далее – ИКТ) [2, с. 86 – 87].

Обзор литературы

Анализ научной литературы по вопросам оперативно-розыскного противодействия в условиях цифровизации преступлений в кредитно-финансовой сфере [3, с. 103; 4, с. 12; 5, с. 121] позволил установить следующую закономерность: усиление технологической составляющей преступной деятельности прямо коррелирует с необходимостью трансформации сил, средств и методов ОРД, направленных на противодействие таким преступлениям, что обуславливает потребность в расширенной разработке и интеграции цифровых инструментов в деятельность оперативных подразделений ОВД.

Параллельно с этим соответствующие тезисы прозвучали в выступлении Президента Российской Федерации В.В. Путина 5 марта 2025 года на ежегодном расширенном заседании коллегии Министерства внутренних дел Российской Федерации (далее – МВД России, Ведомство), где было подчеркнуто: «Масштабные, долгосрочные планы развития России требуют надежного обеспечения экономической безопасности, а значит, системной работы по очищению отраслей экономики и финансового сектора от криминала, от схем отмывания преступных доходов»⁴. В свою очередь, на том же мероприятии Министр внутренних дел Российской Федерации В.А. Колокольцев указал, что ведомством предпринимаются дальнейшие меры по стабилизации оперативной обстановки в кредитно-финансовой сфере, включая выявление фактов противоправной деятельности со стороны

¹ О Стратегии национальной безопасности Российской Федерации: указ Президента Российской Федерации от 02.07.2021 № 400 // Собрание законодательства Российской Федерации. 2021. № 27 (Ч. II), ст. 5351.

² О Стратегии экономической безопасности Российской Федерации на период до 2030 года: указ Президента Российской Федерации от 13.05.2017 № 208 // Собрание законодательства Российской Федерации. 2017. № 20, ст. 2902.

³ Об утверждении Концепции государственной системы противодействия противоправным действиям, совершаемым с использованием информационно-коммуникационных технологий: распоряжение Правительства Российской Федерации от 30.12.2024 № 4154-р.

⁴ Владимир Путин выступил на ежегодном расширенном заседании коллегии Министерства внутренних дел России. URL: <http://www.kremlin.ru/events/president/news/76408/videos> (дата обращения: 28.03.2025).

руководства и собственников кредитных организаций¹.

Проведенное исследование свидетельствует, что в Российской Федерации ключевую роль в противодействии преступлениям в кредитно-финансовой сфере играют подразделения экономической безопасности и противодействия коррупции (далее – ЭБиПК), входящие в структуру правоохранительной системы страны. Значимость их деятельности и вклад в стабилизацию оперативной обстановки в указанной сфере подтверждаются ежегодными статистическими данными МВД России.

Материалы и методы

Методологическую основу исследования составили: диалектический метод научного познания объективной действительности, а также основанные на нем общенаучные методы: наблюдение (при подборке первичной информации в государственных органах исполнительной власти), описание, обобщение, анализ, синтез, индукция и дедукция (при подборке и исследовании всей информации, отраженной в статье); частнонаучные методы: формально-логический (при определении особенностей оперативно-розыскного противодействия, осуществляемого подразделениями ЭБиПК в борьбе с преступлениями в кредитно-финансовой сфере), конкретно-социологический (при анкетировании начальников (заместителей начальников) подразделений ЭБиПК территориальных органов МВД России на окружном, межрегиональном и региональном уровнях за период 2024-2025 гг.), контент-анализ (при изучении следственно-судебной практики), статистический (при изучении статистических сведений, отражающих результаты работы подразделений ЭБиПК).

Согласно статистическим сведениям ГИАЦ МВД России, в 2024 г. ОВД было расследовано 6 408 преступлений, что на 0,6% меньше по сравнению с предыдущим годом. В суд направлено 6 182 уголовных дела, что также на 0,4% ниже, чем в предыдущем периоде. В то же время количество выявленных лиц, причастных к совершению преступлений, составило 6 200 человек (+1%), из которых 3 041 преступник направлен в суд, что на 25,8% меньше по сравнению с прошлым годом. Размер причиненного материального ущерба превысил 39 млрд руб².

Данные свидетельствуют о сохраняющейся высокой криминальной активности в кредитно-финансовой сфере, что требует усиленного

внимания со стороны правоохранительных органов. Несмотря на снижение общего числа расследуемых преступлений и направленных в суд уголовных дел, рост выявленных лиц, а также значительные объемы ущерба указывают на высокую эффективность проводимых оперативно-розыскных мероприятий (далее – ОРМ). Это подтверждает необходимость продолжения и дальнейшей оптимизации оперативно-розыскного противодействия по соответствующему направлению.

Результаты исследования

Особую значимость и обеспокоенность вызывает проблема снижения числа предварительно расследованных уголовных дел и сокращения объема материалов, направленных в суд. Эта негативная тенденция, выявленная не только на основе статистических данных, но и следственно-судебной практики, может свидетельствовать о растущей сложности получения информации в соответствующей сфере, а также о недостаточной материально-технической оснащенности подразделений ЭБиПК в условиях цифровизации преступной деятельности. Высокий уровень латентности преступлений, совершаемых с использованием ИКТ, указывает на необходимость научного переосмысления подходов к оперативно-розыскному противодействию в рассматриваемой сфере, связанной с функционированием облачных площадок нового типа. Устранение пробелов в правоприменительной практике требует не только модернизации оперативно-розыскного законодательства, но и внедрения интеллектуальных аналитических инструментов (аналитико-прогностических моделей), способных эффективно адаптироваться к быстро меняющимся схемам незаконных финансовых операций. Кроме того, оперативно-розыскное противодействие указанным общественно опасным деяниям, по нашему мнению, невозможно без эффективного внутриведомственного и межведомственного взаимодействия с Федеральной службой по финансовому мониторингу России (Росфинмониторинг) [6, с. 105 – 106], Банком России, сотрудниками ЭКЦ МВД России [7, с. 55 – 56] и другими заинтересованными государственными органами исполнительной власти.

При этом следует констатировать, что практический опыт подразделений ЭБиПК, обобщенный в рамках настоящего исследования, позволяет утверждать, что оперативно-розыскное противодействие облачным площадкам нового

¹ Текст официального выступления В.А. Колокольцева на расширенном заседании коллегии МВД России. URL: <https://mvd.ru/news/item/9628493?year=2023&month=4&day=5> (дата обращения: 04.04.2025).

² Статистические данные ГИАЦ МВД России. «Состояние преступности в России за январь – декабрь 2024 г.». URL: <https://mvd.ru/reports/item/60248328/> (дата обращения: 05.03.2025).

типа должно быть признано одним из приоритетных направлений в структуре оперативно-розыскной политики [7, с. 177], поскольку оно напрямую связано с необходимостью усиления мер по борьбе с преступлениями в кредитно-финансовой сфере

На наш взгляд, обнальные площадки XXI века (нового типа) – это трансформировавшиеся в устойчивые, технологически оснащенные организованные группы и преступные сообщества, активно использующие цифровые технологии, теневую отчетность, транзитные и трансграничные операции с использованием криптообменников, криптовалютных бирж, криптоматов, а также вовлекающие как юридических, так и физических лиц. Эти схемы характеризуются многомиллиардными оборотами и наносят значительный ущерб не только гражданам, но и бюджету страны, поскольку включают в себя уклонение от уплаты налогов, легализацию (отмывание) преступных доходов и другие противоправные действия, скзывающиеся на финансовой стабильности государства.

По словам директора Росфинмониторинга Ю.А. Чиханчина, оборот площадок, используемых для незаконного обналичивания денежных средств, за последнее время сократился. Однако эта позитивная тенденция заключает определенный риск, связанный с переходом части клиентов в банковский сектор. По оценкам некоторых экспертов, на конец 2024 года на территории Российской Федерации действуют более 200 обнальных площадок нового типа, в деятельность которых вовлечено более 3 000 физических лиц, на долю которых приходится почти половина общего объема сомнительных операций. При этом значительно возросло число несовершеннолетних, вовлекаемых в совершение незаконных операций¹.

Согласно результатам исследования, организаторы обнальных площадок нового типа оказывают незаконные услуги по обналичиванию и выводу денежных средств за рубеж представителям онлайн-казино, кибер- и телефонным мошенникам, коррупционерам, наркоторговцам, торговым сетям и другим преступным группам. Например, ежегодный оборот денежных средств онлайн-казино составляет не менее 350 млрд руб., от незаконной реализации наркотических и психотроп-

ных веществ – не менее 1 трлн руб., а общий теневой оборот денежных средств составляет порядка 5 трлн руб., что за последние четыре года в полтора раза превысило данный показатель и в пять раз – среднемировой уровень².

В рамках проведенного исследования не ставилась задача охарактеризовать все существующие схемы обнальных площадок нового типа, поскольку это невозможно из-за объема публикации. Однако в статье рассматривается один из видов противоправной деятельности – осуществление незаконной банковской деятельности, ответственность за которую предусмотрена ст. 172 УК РФ³. Результаты анкетирования руководителей и сотрудников подразделений ЭБиПК территориальных органов МВД России на окружном, межрегиональном и региональном уровнях дают основание утверждать, что респонденты выделяют незаконную банковскую деятельность как особо проблемную при оперативно-розыскном противодействии преступлениям такого рода. Это обусловлено тем, что преступники используют современные ИКТ, что значительно усложняет процесс выявления и раскрытие противоправной деятельности в данной сфере⁴.

Итоги проведенного исследования, включая данные анкетирования сотрудников подразделений ЭБиПК, подтверждают необходимость эффективной и системной борьбы с рассматриваемым видом преступлений. В связи с этим, на наш взгляд, крайне важно, чтобы сотрудники указанных подразделений имели четкое представление о возможной структуре обнальных площадок нового типа, их функциональных, технических и иных особенностях. Это позволит оперативно реагировать на противоправные проявления и эффективно применять весь доступный инструментарий ОРД для их противодействия [8, с. 145].

Следует отметить, что представленное описание офисов обнальных площадок нового типа носит в значительной степени предположительный характер и основано на результатах анализа публичной информации, экспертных мнений и открытых научных взглядов. По нашему мнению, в силу высокой степени адаптивности и гибкости подобных преступных структур их организационные модели не являются окончательными и могут

¹ Директор Росфинмониторинга Ю.А. Чиханчин увидел риск перехода клиентов обнальных площадок в банки. URL: https://nby.ru/pubs/rosfinmonitoring_uvidel_risk_perekhoda_kli/59137/ (дата обращения: 02.03.2025).

² Эксперты оценили долю нелегального оборота в РФ в 10% от всей розницы. URL: <https://ria.ru/20240116/obnalichivanie-1921655571.html>; <https://ria.ru/20240716/dengi-1959934623.html> (дата обращения: 24.04.2025).

³ Уголовный кодекс Российской Федерации: Федеральный закон Российской Федерации от 13.06.1996 № 63-ФЗ // Собрание законодательства Российской Федерации. 1996. № 25. Ст. 2954.

⁴ Сведения о результатах анкетирования начальников (заместителей начальников) подразделений ЭБиПК территориальных органов МВД России на окружном, межрегиональном и региональном уровнях за период 2024-2025 гг., вопрос 29.

варьироваться в зависимости от конкретных условий.

На основе проведенного исследования можно выделить несколько ключевых аспектов функционирования офисов обнальных площадок нового типа. Эти площадки представляют собой организованные группы людей, которые действуют в непосредственной близости от криптообменников, а их деятельность осуществляется с учетом использования современных цифровых финансовых инструментов. Как показали результаты исследования, офисы таких обнальных площадок, как правило, состоят из 10 – 15 человек. Важнейшей фигурой является руководитель офиса, который координирует взаимодействие с трейдерами для выбора платежных платформ, условий сотрудничества и размещения депозитов. Также он несет нагрузку за координацию действий с так называемыми «дроповодами» – лицами, занимающимися подбором дропов – анонимных участников, которых организаторы вовлекают в схему. Помимо руководителя, в офисах работают операторы, чья задача заключается в контроле соответствия информации о платежах, размещенной на платформе, с данными, поступающими в личные кабинеты дропов через push-уведомления. Другие лица в таких офисах осуществляют обналичивание средств с дропов через банкоматы или в банковских или кредитных учреждениях, в том числе опираясь на доверенности, выданные самими дропами.

Кроме того, организаторы обнальных площадок нового типа используют различные схемы, основанные на применении цифровых финансовых инструментов. Преступники приобретают SIM-карты, анкетные данные, а также платежные карты, оформленные на подставных лиц. Эти данные используются для регистрации электронных средств платежа (далее – ЭСП), таких как виртуальные банковские карты, токены и другие аналогичные инструменты, которые затем оформляются в различных коммерческих банках, включая ПАО Сбербанк, Альфа-Банк, Т-Банк, Точка-Банк, Райффайзенбанк и других.

Таким образом, в обобщенном виде один из возможных механизмов функционирования обнальных площадок нового типа может быть описан следующим образом: денежные средства, поступающие от потерпевших, зачисляются на ЭСП, оформленные на дропов. Далее денежные средства многократно транзитируются между различными ЭСП с целью затруднения отслежи-

вания их движения. На последующих этапах они обналичиваются через банкоматы либо иными доступными способами. Завершающая стадия схемы, как правило, включает конвертацию средств в криптовалюту с использованием криптообменников и криптобирж, после чего полученные активы поступают в теневой финансовый оборот, в том числе на криптокошельки организаторов и заказчиков противоправной деятельности.

В контексте изучения современных форм незаконной банковской деятельности особый интерес, на наш взгляд, представляет выявленная сотрудниками ГУЭБиПК МВД России схема обналичивания денежных средств, реализованная посредством почтовых денежных переводов с последующим получением наличности в отделениях ФГУП «Почта России». Организатором противоправной деятельности выступал 53-летний житель г. Москвы, возглавлявший устойчивую организованную группу из 15 человек, включая номинальных руководителей подконтрольных юридических лиц, бухгалтеров, инкассаторов и получателей наличных средств. В структуру группы также входил гражданин Турецкой Республики, обеспечивавший открытие расчетных счетов в банках с иностранным участием. За определенный период денежные средства клиентов, маскируемые под оплату фиктивных услуг, поступали на счета фирм-«однодневок», после чего направлялись почтовыми переводами участникам группы и обналичивались. Полученная наличность передавалась заказчикам через офис «подпольного банка». По документально подтвержденным данным, годовой оборот данной схемы превышал 1 млрд руб. В ходе ОРМ проведено 25 обысков, изъяты печати фиктивных организаций, электронные носители, первичная документация и ключи систем «банк-клиент»¹.

Одним из ключевых признаков функционирования такой площадки является необходимость постоянного использования большого количества ЭСП-дропов. В связи с этим преступники нередко приобретают у дропов средства доступа к открытому на их имя банковскому счету (включая банковскую карту, SIM-карту и мобильный телефон, на который поступают одноразовые SMS-пароли), после чего используют данный счет в противоправных целях. Кроме того, у нотариусов оформляются доверенности на активных участников организованных групп или преступных сообществ (проверенных), что позволяет последним

¹ В Москве пресечена незаконная деятельность крупной «обнальной площадки» с годовым оборотом свыше 1 млрд рублей. URL: https://mvd.ru/mvd/structure1/Glavnie_upravlenija/Glavnoe_upravlenie_jeconomicheskoy_bezop/Publikacii_i_vistuplenija/item/7126892/ (дата обращения: 21.03.2025).

снимать наличные денежные средства в банке даже при блокировке счета.

Следует отметить, что приведенная выше информация носит ориентировочный характер для сотрудников подразделений ЭБиПК и основана на анализе обобщенных сведений. Важной составляющей понимания возможных особенностей функционирования обнальных площадок нового типа, в том числе контингента, с которым приходится работать сотрудникам указанных подразделений, являются так называемые дропы. Согласно результатам анкетирования, к их числу, как правило, относятся лица, находящиеся в затруднительном финансовом положении: должники, мигранты, студенты, а также граждане с судимостью. Руководители площадок, осуществляющих противоправную деятельность, нередко находят таких лиц через объявления в сети Интернет, предлагая работу с формулировками типа: «Требуется сотрудник для удаленной работы с денежными переводами. Серьезный заработка за несколько часов в день. Трудоустройство без проверок и заполнения документов. Опыт работы не требуется». Подобные объявления ориентированы на социально уязвимые категории населения и маскируют противоправную суть предполагаемой деятельности, что существенно затрудняет своевременное оперативно-розыскное противодействие.

Кроме того, следует отметить, что в современных условиях государство достаточно жестко реагирует на создание обнальных площадок нового типа, что подталкивает руководителей офисов постоянно совершенствовать противоправные схемы организации своей деятельности. Например, для обмена противоправным практическим опытом («ноу-хау») используются как открытые, так и законспирированные тематические форумы и чаты (большинство из которых находятся в мессенджере Telegram). Здесь также размещаются многие площадки для поиска клиентов – заказчиков услуг по незаконному обналичиванию денежных средств и предварительному согласованию условий трансфера.

Основываясь на массиве исследованной информации, мы сформулировали авторский подход к оперативно-розыскному противодействию обнальным площадкам нового типа в целях расширения компетенций и профессиональных знаний, в том числе сотрудников подразделений ЭБиПК, с указанием основных признаков, свидетельствующих о возможном наличии на территории того или иного субъекта Российской Федерации обнальной площадки такого типа, к которым возможно относятся:

- наличие криптообменника;
- скопление большого числа статичных SIM-карт и ID устройств в одном месте, на которые не поступают звонки (используется только интернет-трафик);
- использование одних и тех же ID устройств для управления SIM-картами и онлайн-банками;
- ежедневное снятие крупных сумм в одних и тех же банкоматах;
- наличие информации о преступлениях по ст. 126 и 163 УК РФ (возможны случаи похищения членами обнальных площадок дропов для вымогательства похищенных денежных средств, поступивших на счета дропов);
- большое количество объявлений в сети Интернет о предоставлении соответствующих услуг, а также о проведении лекций (семинаров) о зарплатке в области P2P-платежей и т.п.;
- большое количество выданных доверенностей на одних и тех же поверенных.

Обсуждение и заключение

Основываясь на проведенном исследовании, мы пришли к следующим теоретическим и практическим выводам.

1. Теоретические выводы.

1.1. Эволюция обнальных площадок нового типа: обнальные площадки XXI века представляют собой трансформированные, технологически оснащенные организованные группы и преступные сообщества, активно использующие современные ИКТ, криптовалюты и криптообменники. Применение новых финансовых инструментов и методов обналичивания значительно затрудняет оперативно-розыскное противодействие противоправной деятельности и способствует росту латентности преступлений в данной сфере.

1.2. Многослойность преступных схем: современные обнальные площадки строят схемы посредством использования криптообменников, виртуальных карт, а также создания скрытых транзакций с применением блокчейн-платформ. Это позволяет преступным организованным группам и преступным сообществам выводить значительные суммы денежных средств, зачастую минуя традиционные финансовые инструменты, находящиеся под контролем государственных органов.

1.3. Актуальность внедрения новых подходов оперативно-розыскного противодействия: для эффективной борьбы с обнальными площадками нового типа необходимы инновационные подходы в ОРД. На наш взгляд, ключевое значение имеет понимание структуры таких площадок, а также их функциональных, технических и организационных особенностей, что позволит подразделени-

ям ЭБиПК своевременно выявлять и раскрывать данные преступления.

2. Практические выводы.

2.1. Актуализируется необходимость повышения компетентности сотрудников ЭБиПК, работающих на объектах кредитно-финансовой сферы, в части понимания структурных элементов обнальных площадок нового типа, что позволит оперативно реагировать на изменения в их деятельности и эффективно применять комплекс ОРМ.

2.2. Развитие межведомственного взаимодействия: одним из ключевых факторов борьбы с обнальными площадками нового типа является координация действий как внутри ведомства, так и между различными государственными структурами, в частности Росфинмониторингом и Бан-

ком России. Это обеспечит комплексный подход к оперативно-розыскному противодействию и позволит разработать единую стратегию мониторинга финансовых транзакций.

2.3. Адаптация законодательства и правоприменительной практики: необходимо модернизировать подходы к оперативно-розыскному противодействию рассматриваемым преступлениям, включая внесение изменений в оперативно-розыскное законодательство с учетом появления новых форм и способов осуществления незаконной банковской деятельности. Разработка аналитико-прогностических моделей и иных цифровых инструментов позволит оперативным подразделениям ЭБиПК более эффективно выявлять, отслеживать и пресекать преступления указанного вида.

СПИСОК ИСТОЧНИКОВ

1. Марсаков И.С. Использование информационных технологий в деятельности оперативных подразделений органов внутренних дел в рамках оперативно-розыскного противодействия преступлениям коррупционной направленности, совершаемым в сфере закупок для государственных и муниципальных нужд // Криминалистическое обеспечение безопасности Российской Федерации в финансовой сфере (65-е ежегодные Криминалистические чтения): сборник научных статей по материалам международной научно-практической конференции. В 2-х частях, Москва, 24 мая 2024 года. Москва: Академия управления МВД России, 2024. С. 60 – 69.
2. Саркисян Г.Г. Алгоритм выявления и раскрытия преступлений, совершенных с использованием информационно-коммуникационных технологий (киберпреступлений) // Актуальные вопросы осуществления оперативно-розыскной деятельности органов внутренних дел: сборник научных статей Всероссийского круглого стола, Орёл, 24 октября 2024 года. Орловский юридический институт МВД РФ им. В.В. Лукьянова, 2024. С. 86 – 90.
3. Мамаев М.И. Уголовно-правовые меры противодействия незаконному обналичиванию денежных средств в условиях инновационной экономики // Закон и право. 2021. № 7. С. 102 – 104.
4. Иванов П.И. Проблемы противодействия легализации преступных доходов и пути их решения // Вестник Белгородского юридического института МВД России имени И.Д. Путилина. 2020. № 3. С. 9 – 19.
5. Искалиев Р.Г., Телков А.В. К вопросу о противодействии преступлениям экономической и коррупционной направленности, совершаемым с использованием it-технологий // Закон и право. 2021. № 11. С. 118 – 123.
6. Марсаков И.С. Особенности взаимодействия подразделений экономической безопасности и противодействия коррупции на этапе выявления преступлений коррупционной направленности, совершаемых в сфере закупок для государственных и муниципальных нужд // Философия права. 2023. № 1 (104). С. 103 – 110.
7. Марсаков И.С. Особенности взаимодействия подразделений экономической безопасности и противодействия коррупции с экспертно-криминалистическим центром МВД России в противодействии преступлениям экономической и коррупционной направленности // Ученые записки Казанского юридического института МВД России. 2025. Т. 10. № 1 (19). С. 54 – 60.
8. Марсаков И.С. Особенности оперативно-розыскной политики в эпоху применения искусственного интеллекта в борьбе с преступлениями экономической и коррупционной направленности, совершаемыми в сфере закупок для государственных и муниципальных нужд // Уголовная политика России на современном этапе: состояние, тенденции, перспективы: сборник научных трудов по материалам международной научно-практической конференции, посвященной 90-летию со дня рождения профессора Г.А. Аванесова. В 2-х частях, Москва, 27 сентября 2024 года. Москва: Академия управления МВД России, 2024. С. 175 – 187.

9. Марсаков И.С. Отдельные аспекты борьбы органов внутренних дел с преступлениями, совершаемыми с использованием информационно-коммуникационных технологий в кредитно-финансовой сфере // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2025. Т. 1, № 69. С. 143 – 150.

REFERENCES

1. Marsakov I.S. Ispol'zovanie informacionnyh tekhnologij v deyatel'nosti operativnyh podrazdelenij organov vnutrennih del v ramkah operativno-rozysknogo protivodejstviya prestupleniyam korrupcionnoj napravленности, sovershaemym v sfere zakupok dlya gosudarstvennyh i municipal'nyh nuzhd // Kriminalisticheskoe obespechenie bezopasnosti Rossijskoj Federacii v finansovoj sfere (65-e ezhegodnye Kriminalisticheskie chteniya): sbornik nauchnyh statej po materialam mezhdunarodnoj nauchno-prakticheskoy konferencii. V 2-h chastyah, Moskva, 24 maya 2024 goda. Moskva: Akademiya upravleniya MVD Rossii, 2024. S. 60 – 69.
2. Sarkisyan G.G. Algoritm vyyavleniya i raskrytiya prestuplenij, sovershennyh s ispol'zovaniem informacionno-kommunikacionnyh tekhnologij (kiberprestuplenij) // Aktual'nye voprosy osushchestvleniya operativno-razysknoy deyatel'nosti organov vnutrennih del: sbornik nauchnyh statej Vserossijskogo kruglogo stola, Oryol, 24 oktyabrya 2024 goda. Orlovskij yuridicheskij institut MVD RF im. V.V. Luk'yanova, 2024. S. 86 – 90.
3. Mamaev M.I. Ugolovno-pravovye mery protivodejstviya nezakonomu obnalichivaniyu denezhnyh sredstv v usloviyah innovacionnoj ekonomiki // Zakon i pravo. 2021. № 7. S. 102 – 104.
4. Ivanov P.I. Problemy protivodejstviya legalizacii prestupnyh dohodov i puti ih resheniya // Vestnik Belgorodskogo yuridicheskogo instituta MVD Rossii imeni I.D. Putilina. 2020. № 3. S. 9 – 19.
5. Iskaliev R.G., Telkov A.V. K voprosu o protivodejstvii prestupleniyam ekonomiceskoy i korupcionnoj napravленности, sovershaemym s ispol'zovaniem it-tehnologij // Zakon i pravo. 2021. № 11. S. 118 – 123.
6. Marsakov I.S. Osobennosti vzaimodejstviya podrazdelenij ekonomiceskoy bezopasnosti i protivodejstviya korrupcii na etape vyyavleniya prestuplenij korupcionnoj napravленности, sovershaemyh v sfere zakupok dlya gosudarstvennyh i municipal'nyh nuzhd // Filosofiya prava. 2023. № 1 (104). S. 103 – 110.
7. Marsakov I.S. Osobennosti vzaimodejstviya podrazdelenij ekonomiceskoy bezopasnosti i protivodejstviya korrupcii s ekspertno-kriminalisticheskim centrom MVD Rossii v protivodejstvii prestupleniyam ekonomiceskoy i korupcionnoj napravленности // Uchenye zapiski Kazanskogo yuridicheskogo instituta MVD Rossii. 2025. T. 10. № 1 (19). S. 54 – 60.
8. Marsakov I.S. Osobennosti operativno-rozysknoj politiki v epohu primeneniya iskusstvennogo intellekta v bor'be s prestupleniyami ekonomiceskoy i korupcionnoj napravленности, sovershaemymi v sfere zakupok dlya gosudarstvennyh i municipal'nyh nuzhd // Ugolovnaya politika Rossii na sovremennom etape: sostoyanie, tendencii, perspektivy: sbornik nauchnyh trudov po materialam mezhdunarodnoj nauchno-prakticheskoy konferencii, posvyashchennoj 90-letiyu so dnya rozhdeniya professora G.A. Avanesova. V 2-h chastyah, Moskva, 27 sentyabrya 2024 goda. Moskva: Akademiya upravleniya MVD Rossii, 2024. S. 175 – 187.
9. Marsakov I.S. Otdel'nye aspekty bor'by organov vnutrennih del s prestupleniyami, sovershaemymi s ispol'zovaniem informacionno-kommunikacionnyh tekhnologij v kreditno-finansovoj sfere // Yuridicheskaya nauka i praktika: Vestnik Nizhegorodskoj akademii MVD Rossii. 2025. T. 1, № 69. S. 143 – 150.

Информация об авторе:

Марсаков Илья Сергеевич, кандидат юридических наук, старший преподаватель кафедры организации оперативно-разыскной деятельности Академии управления МВД России, e-mail: ilya.marsakov.94@mail.ru

Автор прочитал и одобрил окончательный вариант рукописи.

Information about the author:

Marsakov Ilya S., Candidate of Law (Research doctorate), Senior Lecturer at the Department of Organization of Operational and Investigative Activities of the Academy of Management of the Ministry of Internal Affairs of Russia, e-mail: ilya.marsakov.94@mail.ru

The author has read and approved the final version of the manuscript.

Статья получена: 23.04.2025.

Статья принята к публикации: 26.06.2025.

Статья опубликована онлайн: 27.06.2025.

Против размещения полнотекстовой версии статьи в открытом доступе в сети Интернет не возражаю.