Секция «Обеспечение финансовой безопасности России: финансовые расследования в цифровой экономике»

Криминальная экономика в цифровую эпоху: вызовы и угрозы

Научный руководитель – Хабибулин Алик Галимзянович

Макиева Инна Зурабовна
Студент (магистр)
Московский государственный университет имени М.В.Ломоносова, Высшая школа государственного аудита, Кафедра экономических и финансовых расследований, Москва, Россия
E-mail: innamakieva@icloud.com

В условиях стремительной цифровизациисовременного общества криминальная экономика претерпевает значительные трансформации, адаптируясь к новым технологическим реалиям и создавая при этом беспрецедентные вызовы и угрозы для национальной и международной безопасности. Интеграция информационно-коммуникационных технологий в нелегальные экономические процессы способствует эволюции традиционных форм преступности, порождая новые, более изощренные методы противоправной деятельности.

Анализ статистических данных свидетельствует о существенном увеличении числа преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. В 2024 году на территории Российской Федерации зарегистрировано 765,4 тысячи таких преступлений, что демонстрирует значительный рост по сравнению с предыдущими периодами (в 2023 году зарегистрировано 676 тысяч преступлений). Экономический ущерб от киберпреступлений в 2023 году достиг 156 миллиардов рублей, превысив объем отечественного рынка информационной безопасности, оцененного в 145 миллиардов рублей. Данная диспропорция указывает на необходимость усиления мер по защите информационного пространства и разработки эффективных стратегий противодействия цифровой преступности.

Существенную угрозу представляет использование криптовалют в целях отмывания денежных средств и финансирования противоправных операций. Преступные организации все чаще обращаются к цифровым валютам для сокрытия незаконных финансовых потоков. Например, одна из международных наркоторговых группировок использовала крупнейшую в мире криптовалютную биржу(Binance) для отмывания десятков миллионов долларов, полученных от незаконного оборота наркотиков. Подобные случаи демонстрируют необходимость разработки и внедрения механизмов мониторинга и регулирования операций с криптовалютами для предотвращения их использования в криминальных целях.

Даркнет становится ключевой платформой для распространения запрещенных веществ, предоставляя анонимные площадки для торговли наркотиками. В России после закрытия крупнейшего даркнет-рынка Hydra в 2022 году наблюдается активная борьба между новыми площадками за доминирование на нелегальном рынке, сопровождающаяся кибератаками и агрессивными рекламными кампаниями. Такая динамика свидетельствует о высокой адаптивности криминальных структур к изменениям в цифровой среде и усложняет задачи правоохранительных органов по пресечению незаконного оборота наркотиков.

Международные криминальные сети активно используют криптовалюты для отмывания денежных средств и обхода санкционных режимов. В декабре 2024 года Национальное агентство по борьбе с преступностью Великобритании разоблачило масштабную сеть по отмыванию денег, использовавшую криптовалюту Tether для перевода крупных сумм, помогая российским элитам обходить международные санкции. Данная операция

подчеркнула глобальный характер современных финансовых преступлений и необходимость международного сотрудничества в борьбе с ними.

Цифровизация криминальной экономики порождает ряд серьезных вызовов и угроз, среди которых наиболее значимыми являются сложность отслеживания финансовых потоков, поскольку анонимность и децентрализация криптовалютзатрудняют идентификацию источников и получателей средств, что осложняет борьбу с финансовыми преступлениями, распространение запрещенных товаров и услуг через даркнет, который предоставляет платформу для торговли наркотиками, оружием и другими нелегальными товарами, увеличивая их доступность и распространение, а также угроза национальной безопасности, поскольку использование цифровых технологий криминальными структурами может подрывать экономическую и политическую стабильность государства, способствуя финансированию терроризма и других форм экстремизма.

Борьба с цифровой криминальной экономикой требует системного подхода, включающего правовые, технологические и международные механизмы. Необходимо совершенствование законодательства с акцентом на регулирование криптовалютных операций, идентификацию пользователей и блокировку нелегальных интернет-ресурсов. Внедрение алгоритмов машинного обучения и анализа больших данных позволит выявлять аномальные транзакции, прогнозировать криминальные схемы и автоматизировать финансовый мониторинг. Развитие технологий блокчейн-аналитики и интеграция KYC/AML-процедур на криптовалютных платформах снизят анонимность незаконных финансовых потоков. Ключевым фактором является международное сотрудничество, включающее унификацию нормативных стандартов, оперативный обмен данными и координацию усилий правоохранительных структур. Введение цифровых национальных валют (CBDC) создаст прозрачную финансовую среду и усложнит схемы отмывания средств. Дополнительно следует инвестировать в подготовку специалистов по кибербезопасности и развитие цифровой грамотности населения.

Источники и литература

1) Число киберпреступлений в России // TAdviser. URL: https://www.tadviser.ru/index.php/Статья:Число_киберпреступлений_в_России (дата обращения: 20.02.2025).
2) Ущерб от киберпреступлений в России превысил объем рынка информационной безопасности // ComNews. URL: https://www.comnews.ru/content/233687/2024-06-11/2024-w24/1008/uscherb-kiberprestupleniy-rossii-prevysil-obem-rynka-informacionnoy-bezopasnosti (дата обращения: 20.02.2025).
3) Потери от киберпреступности // TAdviser. URL: https://www.tadviser.ru/index.php/Статья:Потери_от_киберпреступности (дата обращения: 20.02.2025).
4) Киберпреступность в России и СНГ 2023–2024 // ICT.Moscow. URL: https://ict.moscow/research/kiberprestupnost-v-rossii-i-sng-2023-2024/ (дата обращения: 20.02.2025).