Использование цифровых технологий организованной преступностью

Черявко Евгений Джонович, Северо-Западный институт управления Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации; факультет социальных технологий (Санкт-Петербург, Российская Федерация)
студент 3-го курса бакалавриата; e-mail: ont@myrambler.ru.

Научный руководитель:
Майборода Эльвира Тагировна, Северо-Западный институт управления Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации; кафедра правоведения (Санкт-Петербург, Российская Федерация)
кандидат философских наук, доцент; e-mail: mayboroda-et@ranepa.ru.

Аннотация
В данной статье ставится цель исследовать использование цифровых технологий организованной преступностью. В настоящий момент преступные сообщества активно пользуются потенциалом цифровых технологий, что позволяет им действовать анонимно, быстро и эффективно. Понимание того, как организованная преступность использует эти технологии, имеет решающее значение для разработки эффективных стратегий борьбы с этой растущей угрозой. Автор стремится пролить свет на то, как именно преступные организации используют технологии и какие сложности это создает для правоохранительных органов всего мира. Осуществляется это путем следующих методик: а) изучения соответствующих криминологических и уголовно-правовых исследований ученых, посвященных использованию цифровых технологий организованными преступными группировками; б) анализа законодательных актов и разбора публикаций по этой теме в российских и зарубежных СМИ, в которых сообщалось о реальных случаях использования этих технологий преступниками. Результаты исследования представлены несколькими ключевыми выводами. Во-первых, цифровые технологии служат катализатором для расширения влияния преступников, поскольку те используют такие достижения, как зашифрованные каналы связи, теневые веб-платформы и криптовалюты. Во-вторых, существуют проблемы, с которыми сталкиваются правоохранительные органы в борьбе с организованной преступностью, использующей цифровые технологии. В-третьих, в статье подчеркивается необходимость введения мер регулирования в отношении криптовалюты, являющейся основным средством расчета в преступных операциях, а также важность международного сотрудничества для ликвидации преступных сетей. Понимание того, как указанные технологии используются в преступной деятельности, имеет значение для разработки эффективных стратегий борьбы с организованной преступностью и защиты общества.

Ключевые слова: организованная преступность, цифровые технологии, анонимность, даркнет, криптовалюта, киберпреступления, Интернет.

Use of Digital Technologies by Organized Criminals

Evgeny J. Cheryavko, North-Western Institute of Management, Russian Academy of National Economy and Public Administration under the President of the Russian Federation; Faculty of Social Technologies (Saint Petersburg, Russian Federation)
BA student; e-mail: ont@myrambler.ru.

Academic Supervisor:
Mayboroda Elvira Tagirovna, North-Western Institute of Management, Russian Academy of National Economy and Public Administration under the President of the Russian Federation; Department of Law (Saint Petersburg, Russian Federation)
PhD in Philosophy, Associate Professor; e-mail: mayboroda-et@ranepa.ru.

Abstract
This article aims to investigate the employment of digital technologies by organized criminals. Criminal organizations are now actively exploiting the potential of digital technology to operate anonymously, quickly, and effectively. Being aware of the way the organized crime uses these technologies is crucial for developing effective strategies to combat this growing threat. The author seeks to highlight the specific ways of employing technology by criminal organizations as well as the challenges it creates for law enforcement agencies around the world.
This research has been done via the following techniques: a) studying the relevant criminological and criminal law academic papers on the use of digital technologies by organized criminal groups; b) analyzing the legislative acts and reviewing the publications on this topic in Russian and foreign media, featuring the actual cases of criminals using these technologies.
The author presents the study findings by drawing several key conclusions. Firstly, digital technologies serve as a catalyst for criminals to expand their influence as they utilize advances such as encrypted communication channels, shadow web platforms, and cryptocurrencies. Secondly, there are challenges faced by law enforcement agencies in combating organized criminals that uses digital technologies. Thirdly, the article emphasizes the need to introduce some regulatory measures for cryptocurrency, which is the main means of payment in criminal transactions, and the importance of international cooperation to dismantle criminal networks. Achieving the awareness of the way these technologies are used in criminal activities is important for the development of effective strategies to combat organized crime and to protect the society.

Keywords: organized crime, digital technologies, anonymity, darknet, cryptocurrency, cybercrime, Internet.

ВВЕДЕНИЕ

По определению А. И. Гурова, организованная преступность представляет собой относительно массовое функционирование устойчивых управляемых сообществ преступников, занимающихся совершением преступлений как промыслом (бизнесом) и создающих с помощью коррупции систему защиты от социального контроля [1, с. 5].

Влияние организованной преступности на общество обширно и охватывает широкий спектр преступной деятельности, такой как незаконный оборот наркотиков, торговля людьми, отмывание денег, коррупция, киберпреступность и т. д. Подобные деяния создают серьезные угрозы для общественного благополучия.

В последние годы цифровые технологии стали катализатором расширения и преобразования многих видов деятельности, в том числе и преступной.

Цель исследования — изучение применения цифровых технологий организованной преступностью.

Методология исследования базируется на анализе существующих криминологических и уголовно-правовых исследований ученых, а также на анализе публикаций по этой

теме в российских и зарубежных СМИ, в которых отражены реальные случаи использования цифровых технологий преступниками.

В данной статье под понятием «технологии» или «цифровые технологии» подразумеваются различные цифровые инструменты и веб-приложения, используемые организованными преступными группами для облегчения своей преступной деятельности.

СПОСОБЫ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИЙ ОРГАНИЗОВАННОЙ ПРЕСТУПНОСТЬЮ

В статье рассматриваются несколько видов цифровых технологий, связанных с организованной преступностью:

а) Инструменты киберпреступности: вредоносное программное обеспечение, которое используется организованными преступными группами.
б) Коммуникационные технологии: средства безопасной связи, используемые организованными преступными группами для координации своей деятельности и уклонения от обнаружения правоохранительными органами, в частности сеть Tor.
в) Финансовые технологии: инструменты, которые позволяют организованным преступным группам скрывать и переводить незаконно полученные средства.

Организованные преступные группировки используют технологии как мощный инструмент для усиления своей незаконной деятельности и преодоления традиционных барьеров. В этом разделе рассматриваются различные способы использования технологий преступными организациями для достижения своих целей, включая киберпреступность, отмывание денег, кражу личных данных, криптовалюту и использование теневых интернет-рынков.

а) Киберпреступность

Организованные преступные группы используют уязвимости в компьютерных сетях, системах и программном обеспечении для осуществления широкого спектра незаконных действий. Эти действия включают, среди прочего, взлом, утечку данных, атаки программ-вымогателей и распределенные атаки типа «отказ в обслуживании» (DDoS).

Наибольшее число преступлений в 2022 г. пришлось на атаки программ-вымогателей. Они по-прежнему являются киберугрозой номер один, причем не только для международных корпораций, но и российского бизнеса[1].

Помимо слабой законодательной основы противодействия киберпреступности одной из основных проблем является недостаточность компетентных лиц, выявляющих и предотвращающих киберпреступления [2, с. 141–143].

б) Отмывание денег

Отмывание денег — это процесс, в котором полученное имущество, приобретенное или аккумулируемое вследствие незаконной деятельности, перемещается или скрывается для того, чтобы прервать преступную цепочку [3, с. 262–268].

Отмывание денег является важнейшим компонентом организованной преступности, поскольку преступники стремятся скрыть происхождение своих незаконных доходов и интегрировать их в законную финансовую систему.

Согласно данным Центрального банка Российской Федерации (далее — ЦБ РФ), в последние годы объемы вывода денежных средств за рубеж в банковском секторе

[1] Киберцунами: как 2022 год изменил мир IT-преступлений в России [Электронный ресурс]. Известия IZ: [сайт]. URL: https://iz.ru/1447317/mariia-frolova/kibertcunami-kak-2022-god-izmenil-mir-it-prestuplenii-v-rossii (дата обращения: 11.05.2023).

значительно снизились: если в 2014 г. данная цифра составляла 816 млрд руб., то в 2018 г. — 73 млрд руб., в 2019 г. — 66 млрд руб., а в 2020 г. — 52 млрд руб. ЦБ РФ отмечает, что среди сомнительных банковских операций на сумму 52 млрд руб. 24 млрд руб. выведены за рубеж по авансовым платежам по импортируемым товарам [6, с. 44–46], что может косвенно свидетельствовать о переносе незаконных операций в криптоиндустрию, которая не контролируется финансовыми организациями.

Появление децентрализованных финансов (DeFi) и технологии блокчейна еще больше усложнило усилия по борьбе с отмыванием денег, поскольку преступники изучают новые способы использования этих новых финансовых экосистем.

в) Кража персональных данных

Персональные данные — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)[2].

Организованные преступные группы применяют различные методы для кражи таких данных, используя технологии для сбора личной информации и использования уязвимостей на онлайн-платформах. Фишинг, вредоносное ПО и тактика социальной инженерии используются для получения личных и финансовых данных отдельных лиц, которые затем используются для присвоения ложной личности или осуществления мошеннических действий [4, с. 2–3].

Посредством кражи персональных данных преступники могут открывать банковские счета, подавать заявки на кредиты и участвовать в других схемах финансового мошенничества. Технологии предоставляют им возможность выдавать себя за отдельных лиц, манипулировать цифровыми записями и совершать преступные действия в крупных масштабах, что приводит к значительным финансовым потерям и репутационному ущербу жертв.

г) Криптовалюта

Рост криптовалют произвел революцию в финансовом ландшафте и поставил новые задачи в борьбе с организованной преступностью. Преступные организации все чаще используют криптовалюты, поскольку эти цифровые активы обеспечивают повышенную анонимность и безопасность. Децентрализованный характер криптовалют в сочетании со сложностью отслеживания транзакций создает серьезные препятствия для правоохранительных органов, пытающихся отследить и арестовать незаконные средства.

На данный момент основные виды криптовалюты представлены следующими монетами: биткоин, Litecoin, Ethereum, NEM, DASH, Ripple, Monero и др. Самая популярная из всех выше представленных монет — биткоин, и именно с данной монетой проводится большая часть операций[3].

д) Теневые интернет-рынки

Развитие Интернета предоставило организованным преступным группам платформы для скрытного участия в незаконной деятельности. Эти подпольные торговые площадки способствуют продаже незаконных товаров и услуг, включая наркотики, поддельные документы, оружие, инструменты для взлома и украденные данные. Анонимность, обеспечиваемая сетью Tor, и использование криптовалют в качестве средства обмена усложнили для правоохранительных органов задачу эффективного проникновения в эти сети и их ликвидацию.

---

[2] О персональных данных: фед. закон от 27.07.2006 № 152-ФЗ (в ред. от 24.04.2020 № 123-ФЗ) [Электронный ресурс]. Доступ из СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_61801 (дата обращения: 12.05.2023).

[3] The Cryptocurrency Tumblers: Risks, Legality and Oversight [Электронный ресурс]. 2017. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3080361 (дата обращения: 22.09.2023).

ПРИМЕРЫ ГРОМКИХ ДЕЛ, В КОТОРЫХ ТЕХНОЛОГИИ ИГРАЛИ ЗНАЧИТЕЛЬНУЮ РОЛЬ В ДЕЯТЕЛЬНОСТИ ОРГАНИЗОВАННОЙ ПРЕСТУПНОСТИ

а) BTC-e была известной биржей криптовалют, которую обвиняли в содействии обширным операциям по отмыванию денег и использовании киберпреступниками платформы для конвертации своих нечестных доходов в криптовалюты[4].

Власти выявили, что BTC-e был причастен к отмыванию преступных доходов на миллиарды долларов, включая средства, полученные в результате хакерских атак, атак программ-вымогателей, незаконного оборота наркотиков и других незаконных действий. Биржа работала в условиях секретности, что позволяло пользователям проводить транзакции без предоставления подробной личной информации, тем самым сохраняя свою анонимность.

Сложная схема отмывания денег, используемая BTC-e, включала в себя многоуровневую цепочку транзакций и смешивание средств для дальнейшего запутывания денежного следа. Используя криптовалюты, преступники могли легко переводить средства через границы, минуя традиционные банковские системы и избегая проверки финансовых учреждений.

Этот случай высветил настоятельную необходимость усиления мер регулирования и международного сотрудничества для эффективной борьбы с отмыванием цифровой валюты. В то время как правительства и регулирующие органы приложили усилия для ужесточения надзора и введения более строгих правил «Знай своего клиента» (KYC) и «Противодействие отмыванию денег» (AML) в отношении бирж криптовалют, анонимный характер этих цифровых активов продолжает создавать проблемы.

б) Убийство подполковника следователя МВД Евгении Асцатуровны Шишкиной в 2018 г., заказанное через темную сеть[5], является пугающим примером того, как технологии сыграли значительную роль в содействии деятельности организованной преступности. Этот случай подчеркивает опасную конвергенцию киберпреступности и насилия в реальном мире, когда анонимность и охват Интернета создают питательную среду для преступных предприятий [5, с. 1–3].

Использование темной сети, скрытой части Интернета, доступной только через специальное программное обеспечение, позволяет преступникам действовать в тени, защищенной от традиционных правоохранительных мер. Это позволяет им общаться, планировать и осуществлять незаконные действия, включая акты насилия, с невообразимым ранее уровнем анонимности и безопасности.

В случае со следователем МВД Е. А. Шишкиной преступники использовали даркнет, чтобы заказать ее убийство. Они искали услуги киллера через онлайн-форумы, общались под псевдонимами и использовали методы шифрования, чтобы избежать обнаружения[6]. Это не только демонстрирует изощренный характер преступных операций, но и подчеркивает растущую изощренность организованной преступности в использовании технологий в своих целях. При этом важно отметить, что преступник был найден и осужден на 14 лет лишения свободы[7].

---

[4] ФБР против BTC-e: как рухнула крупнейшая русская криптобиржа [Электронный ресурс]. РБК: [сайт]. URL: https://www.rbc.ru/magazine/2018/01/5a2f1e0d9a7947f2b3ae49dc (дата обращения: 13.05.2023).

[5] Шишкина Евгения Асцатуровна [Электронный ресурс]. Управление на транспорте МВД России по Центральному федеральному округу. URL: https://цфоут.мвд.рф/PRESS_SLUZHBA/Nashi_geroi_2/item/18167788/ (дата обращения: 29.05.2023).

[6] Расправа за «дело»: кто убил следователя Шишкину [Электронный ресурс]. Газета.ru. URL: https://www.gazeta.ru/social/2019/04/22/12316279.shtml (дата обращения: 13.05.2023).

[7] Убийце следователя Шишкиной дали 14 лет: жуткие смски, равнодушие полиции [Электронный ресурс]. Московский комсомолец: [сайт]. URL: https://www.mk.ru/incident/2020/11/17/ubiyce-sledovatelya-shishkinoy-dali-14-let-zhutkie-smski-ravnodushie-policii.html (дата обращения: 29.05.2023).

ТРУДНОСТИ В БОРЬБЕ С ОРГАНИЗОВАННОЙ ПРЕСТУПНОСТЬЮ В ЭПОХУ ЦИФРОВЫХ ТЕХНОЛОГИЙ

Стремительное развитие технологий поставило перед правоохранительными органами множество сложностей в борьбе с организованными преступными группировками.

Одной из основных трудностей, с которыми сталкиваются правоохранительные органы, является анонимность и шифрование, обеспечиваемые даркнетом и различными каналами связи. Преступники используют эти платформы для безопасного общения, планирования своей деятельности и облегчения незаконных транзакций, что делает чрезвычайно сложной задачу для правоохранительных органов по отслеживанию и перехвату их сообщений.

Другой сложностью можно назвать глобальный охват сети Интернет, что создает серьезные проблемы юрисдикционного порядка. Лицо, нарушающее закон, может находиться в одной стране (в одной юрисдикции) и в то же время причинять вред обществу в другой стране (другой юрисдикции). Это не только препятствует расследованию и уголовному преследованию, но и создает юридические препятствия при сборе доказательств, выдаче подозреваемых и исполнении судебных решений в различных государствах.

Еще одним препятствием является вопрос разных уровней технологических возможностей и ресурсов стран. Это может создать сложности для эффективного сотрудничества. В развивающихся странах может не хватать необходимой инфраструктуры, технического опыта и ресурсов для борьбы со сложными киберпреступными сетями. Этот цифровой разрыв может усугубить проблемы международного сотрудничества, поскольку некоторым странам может быть трудно идти в ногу с развивающейся тактикой и технологиями, используемыми организованными преступными группами.

СОВЕРШЕНСТВОВАНИЕ ПРАВОВОЙ БАЗЫ И МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО

В ответ на растущую угрозу крайне важно разрабатывать эффективные меры для борьбы с преступной деятельностью, а именно реализовывать регуляторные меры для решения конкретных вопросов, связанных с использованием технологий организованными преступными группировками.

Одним из возможных подходов является совершенствование законодательства и нормативно-правовой базы для решения конкретных проблем, связанных с технологиями. Например, регулирование криптовалют.

Законодательная база, которая существует на данный момент в Российской Федерации, отражает некоторые проблемы, связанные с регулированием рынка криптовалют. Если обратиться к Федеральному закону «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»[8], а также иным актам, то можно отметить, что цифровая валюта обозначается в качестве имущества[9]. Но при этом, если обратиться к положениям Гражданского кодекса (ст. 128 ГК РФ), то цифровая валюта до сих пор не определена в качестве имущества и объекта гражданских

---

[8] О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: федер. закон от 31.07.2020 № 259-ФЗ (последняя редакция) [Электронный ресурс]. Доступ из СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_358753/ (дата обращения: 06.07.2023).

[9] Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ (последняя редакция) [Электронный ресурс]. Доступ из СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_5142/f7871578ce9b026c450f64790704bd48c7d94bcb/ (дата обращения: 07.07.2023).

прав[10]. Однако проблемное поле правового регулирования на данных вопросах не ограничивается — проблемы возникают также и в рамках уголовного права в контексте квалификации преступлений, которые связаны с обращением и использованием криптовалюты [7, с. 2].

Также усилия должны быть сосредоточены на содействии международному сотрудничеству и обмену информацией между правоохранительными органами для преодоления существующих ограничений и облегчения обмена информацией и опытом.

Однако на пути эффективного сотрудничества в борьбе с транснациональной организованной преступностью существуют определенные преграды. Одной из них являются различия в правоприменительной практике разных стран. Каждое государство имеет свою собственную правовую базу, стандарты сбора доказательной базы и процедуры, которые могут создавать значительные препятствия при обмене информацией и доказательствами. Отсутствие гармонизации и взаимного признания применяемых правовых мер часто приводит к задержкам, неэффективности и юридическим осложнениям в трансграничных расследованиях и судебных преследованиях.

ЗАКЛЮЧЕНИЕ

Исследование показывает, что постоянно развивающийся характер технологий представляет собой серьезное препятствие для правоохранительных органов в борьбе с организованной преступностью. Инструменты шифрования, глобальный характер Интернета, криптовалюты — все это создает трудности для противодействия преступным группам.

Так, в частности, были сделаны следующие выводы: во-первых, цифровые технологии служат катализатором для расширения влияния преступников, поскольку те используют такие достижения, как зашифрованные каналы связи, теневые веб-платформы и криптовалюты. Во-вторых, существуют проблемы, с которыми сталкиваются правоохранительные органы в борьбе с организованной преступностью, использующей цифровые технологии. В-третьих, существует необходимость введения мер регулирования в отношении криптовалюты, являющейся основным средством расчета в преступных операциях, а также важность международного сотрудничества для ликвидации преступных сетей.

Решение этих проблем требует реализации эффективных мер регулирования и международного сотрудничества. В частности, необходимо разработать законодательство и правила, регулирующие использование технологий, особенно в отношении криптовалюты, которая широко используется преступниками. Также расширение международного сотрудничества и обмена информацией между правоохранительными органами поможет преодолеть существующие ограничения.

Литература

1. *Гуров А. И.* Криминологическая характеристика и предупреждение преступлений, совершаемых организованными группами: учеб. пособие / под ред. Е. С. Жигарева; М-во внутр. дел РФ Моск. высш. шк. милиции. М.: МВШМ, 1992. 70 с.
2. *Жуков А. З.* Киберпреступность: актуальные проблемы и уголовно-правовая оценка в системе современного права. Проблемы экономики и юридической практики, 2019. Т. 15. № 4. С. 141–143.

[10] О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма: федер. закон от 07.08.2001 № 115-ФЗ (последняя редакция) [Электронный ресурс]. Доступ из СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_32834/ (дата обращения: 06.07.2023).

3. *Кирьянова Д. А.* Криптовалюта: угроза финансовой безопасности РФ. Сборник статей международной практической конференции «Проблемы обеспечения финансовой безопасности и эффективности экономических систем в XXI в.». Санкт-Петербургский университет технологий управления и экономики, 2017. С. 262–268.
4. *Кузьмин Ю. А.* Кража персональных данных (криминологический аспект) [Электронный ресурс]. Oeconomia et Jus, 2020. № 3. URL: https://cyberleninka.ru/article/n/krazha-personalnyh-dannyh-kriminologicheskiy-aspekt (дата обращения: 13.05.2023).
5. *Номоконов В. А., Тропина Т. Л.* Киберпреступность как новая криминальная угроза [Электронный ресурс]. Криминология: вчера, сегодня, завтра, 2012. № 24. URL: https://cyberleninka.ru/article/n/kiberprestupnost-kak-novaya-kriminalnaya-ugroza (дата обращения: 29.05.2023).
6. *Нугуманов А. Р.* Отмывание денег: оценка состояния и мер противодействия. Современная наука, 2022. № 1. С. 44–46.
7. *Баратов Ю. А.* Квалификация преступлений, совершенных с использованием криптовалюты. Право и управление, 2023. № 3.