

Использование цифровых платформ как технологическая основа формирования экосистем преступных сообществ

В. В. Поляков

*Алтайский государственный университет
пр. Ленина, 61, 656049, Барнаул, Россия. E-mail: agupolyakov@gmail.com*

В статье рассмотрены вопросы, связанные с формированием цифровых платформ, создаваемых организованными группами и преступными сообществами. Отмечено, что такие цифровые платформы функционируют в сети Даркнет как теневом сегменте сети Интернет, что обеспечивает повышенную анонимизацию пользователей за счет применения специальных средств и технологий. Отмечена важная роль цифровых платформ в развитии новых форм организованной преступной деятельности, основанных на сетевых принципах управления и взаимодействия в социальных группах. Проанализированы значительные криминальные преимущества, предоставляемые применением цифровых платформ при совершении высокотехнологичных преступлений, заключающихся в применении преступными группами специально создаваемых компьютерных средств для удаленного доступа к объектам преступного посягательства.

Выявлено и описано на основе предложенного понятийного аппарата такое качественно новое явление, как создание на базе цифровых платформ экосистем преступных сообществ. Эти экосистемы представляют собой сетевые объединения отдельных автономных преступных групп с разной криминальной специализацией, взаимодействующих друг с другом посредством информационно-телекоммуникационных сетей, при этом цифровые платформы выступают технологической основой функционирования экосистем преступных сообществ. Рассмотрены наиболее существенные факторы, обеспечивающие более высокую криминальную эффективность экосистем при осуществлении высокотехнологичной преступной деятельности по сравнению с организованными преступными группами с традиционной вертикальной иерархической структурой, а также перед аналогичными преступными группами с сетевой структурой управления. Описана связь формирующихся экосистем преступных сообществ с явлениями глобализации, выражающимися в транснациональном характере высокотехнологичной преступной деятельности, и с проявившимися в последние годы процессами глокализации преступности.

Ключевые слова: организованные группы, транснациональная преступность, высокотехнологичные преступления, цифровые платформы, экосистемы.

The Use of Digital Platforms as a Technological Basis for the Formation of Criminal Communities Ecosystems

V. V. Polyakov

*Altai State University
61 Lenin St., 656049, Barnaul, Russia. E-mail: agupolyakov@gmail.com*

The article discusses issues related to the formation of digital platforms created by organized groups and criminal communities. It notes that such digital platforms operate on the Darknet, a shadow segment of the Internet that provides increased user anonymization through the use of specialized software tools and technologies. The important role of digital platforms in the development of new forms of organized criminal activity, based on network principles of management and interaction within social groups, is highlighted. The significant criminal advantages provided by the use of digital platforms in the commission of high-tech crimes—specifically, the use of specially created computer tools for remote access to objects of criminal encroachment by criminal groups—are analyzed. Based on the proposed conceptual framework, a qualitatively new phenomenon has been identified and described: the creation of ecosystems of criminal communities based on digital platforms. These ecosystems are network associations of separate autonomous criminal groups with different specializations, interacting with each other through information and telecommunication networks, while digital platforms serve as the

technological foundation for the functioning of these ecosystems. The article considers the most significant factors that ensure a higher criminal efficiency of these ecosystems in implementing high-tech criminal activities compared to organized criminal groups with a traditional vertical hierarchical structure, as well as similar criminal groups with a network management structure. Finally, it describes the connection between the emerging ecosystems of criminal communities and the phenomena of globalization, expressed in the transnational nature of high-tech criminal activity, as well as the processes of glocalization of crime that have manifested in recent years.

Key words: organized criminal groups, transnational crime, high-tech crimes, digital platforms, ecosystems.

Происходящее в 2000-е годы распространение новых информационно-телекоммуникационных технологий, выразившееся в реализации качественно новых возможностей для обмена информацией, вызвало процессы трансформации различных социальных систем. Эта трансформация связана с формированием новых эффективных форм организационной структуры в таких системах и выражается в переходе от традиционного иерархического управления к взаимодействию, основанному на сетевом принципе. В последние годы данное явление стало одной из доминирующих мировых тенденций [Кастельс 1999], затрагивающей сферы экономики, государственного управления, социальных отношений.

Одним из негативных следствий происходящих изменений явилась трансформация организационной структуры преступных групп. Организованные группы и преступные сообщества во все большей степени ориентируются на новую структуру управления и взаимодействия, которая, используя выражение А. М. Каминского, является родственной «управлению в иных социальных системах» [Каминский 2023: 14], и прежде всего – в экономических. В первую очередь такую трансформацию совершают наиболее динамичные из организованных преступных групп, специализирующиеся на совершении **высокотехнологичных преступлений**. Такие преступления могут быть определены как общественно опасные деяния, совершаемые преступными группами с помощью специально созданных или модифицированных компьютерных средств преступления с применением удаленного доступа к объекту преступного посягательства [Поляков 2023: 156]. Достаточно быстрое внедрение в преступных группах новых форм организационной структуры, основанных на сетевом взаимодействии участников, было описано и проанализировано в ряде проводившихся в 2000-е годы исследований [Осипенко 2012; Осипенко 2009: 122, 237-239; Глазкова 2019; Овчинский 2018: 216; Коновалова, Есина 2021; Поляков 2023]. Представляется, что наблюдаемый быстрый рост количества высокотехнологичных преступных посягательств в отношении как юридических, так и физических лиц в определенной степени связан именно с развитием новых и более эффективных сетевых форм организационной структуры преступных групп. Данное обстоятельство делает актуальным и востребованным дальнейшее изучение феномена структурной трансформации организованных групп и преступных сообществ.

Анализ судебно-следственной практики последних лет показывает, что в эволюции преступных групп, специализирующихся на совершении высокотехнологичных преступлений, наметился следующий этап трансформации организационной структуры [Поляков 2023: 367-374]. Подобно тому, как формирование сетевой структуры имело своей технологической основой использование информационных сетей, так новая организационная структура стала возможной благодаря появлению и быстрому распространению **сетевых (цифровых) платформ**. Цифровые платформы получили широкое распространение прежде всего как один из наиболее эффективных инструментов современной цифровой экономики. В сфере экономических отношений цифровые платформы представляют из себя сетевую информационную среду, включающую интерактивные сайты с информацией о продуктах и услугах, обеспечивающие сетевое взаимодействие между различными группами партнеров – юридических и физических лиц, реализующих или приобретающих определенные товары и услуги. На роль цифровых платформ в этой сфере обращали внимание О. А. Зайцев и П. С. Пастухов, по мнению которых «фундаментальным элементом использования данных в цифровой экономике являются цифровые платформы» [Зайцев, Пастухов 2022: 293], и другие авторы. Цифровые платформы в расширяющемся масштабе внедряются и в сферу государственных отношений. В работе Э. Л. Сидоренко с соавторами [Сидоренко, Барциц, Хисамова 2019] была выделена и проанализирована роль цифровых платформ в повышении эффективности цифрового управления на общегосударственном и региональном уровне.

Высокая эффективность цифровых платформ обусловлена тем, что они обеспечивают наилучшие технологические возможности для эффективного сетевого взаимодействия автономных участников. В этом качестве они служат технологической основой для формирования и функционирования социально-экономических экосистем различной природы [Раменская 2020]. **Цифровые экосистемы** представляют из себя объединения автономных участников, осуществляющих совместную деятельность посредством цифровых платформ без иерархического вертикального соподчинения, характерного для традиционных форм взаимодействия. При этом цифровые экосистемы обладают целым рядом существенных преимуществ по сравнению с традиционными объединениями, среди которых можно выделить следующие:

- обеспечивают эффективную сетевую координацию деятельности участников экосистемы;
- способствуют оптимальному «разделению труда» между автономными участниками;
- позволяют легко и быстро соединять информационные ресурсы на базе цифровой платформы;
- создают условия для практически мгновенного обмена необходимой информацией посредством информационно-телекоммуникационных сетей;
- существенно облегчают привлечение новых участников.

Указанные преимущества привели к тому, что организованные группы и преступные сообщества, использующие в своей криминальной деятельности возможности, предоставляемые информационно-телекоммуникационными технологиями, перешли к созданию и эксплуатации цифровых платформ. Важной отличительной особенностью таких платформ является их функционирование, как правило, в сети **Даркнет**. Специфика сети Даркнет как теневого сегмента сети Интернет проявляется в применении специальных программных средств для защиты от свободного доступа к информационным ресурсам и в обеспечении высокой степени анонимизации пользователей. Размещение цифровых платформ, создаваемых преступными группами, именно в сети Даркнет обусловлено в первую очередь указанными особенностями. Отметим, что в последние годы правовым аспектам функционирования сети Даркнет было уделено значительное внимание отечественных и зарубежных исследователей, высказывавших различные взгляды на роль этой сети в высокотехнологичной преступной деятельности и на возможности ее правового регулирования сети [Протасевич, Скрыбикова 2021; Смушкин 2022; Бычков, Вехов 2023; Васильев, Ибрагимов, Васильева 2019; Beshiri, Susuri 2019].

На наш взгляд, цифровые платформы, созданные в сети Даркнет организованными группами и преступными сообществами, явились технологической основой для появления качественно новой формы управления и взаимодействия в преступных группах и обеспечили формирование **экосистем преступных сообществ**. Такие экосистемы представляют из себя объединения отдельных преступных групп, сохраняющих свою автономность, осуществляющих децентрализованное сетевое взаимодействие и криминальное «разделение труда» посредством анонимного использования цифровых ресурсов и услуг, представленных на соответствующих цифровых платформах.

Можно полагать, что возникновение экосистем преступных сообществ выступает в качестве одного из проявлений весьма общих процессов, связанных с глобализацией преступности. В случае экосистем преступных сообществ это проявляется, в частности, в транснациональном характере криминальной деятельности преступных групп, входящих в состав экосистемы. Можно отметить, что эволюция в организации высокотехнологичной преступной деятельности, приведшая к формированию экосистем, подтверждает правильность вывода А. Н. Савенкова и Е. Р. Россинской о появлении «новых цифровых сущностей и распределенного участия в преступном деянии» [Савенков, Россинская 2023: 103-104].

Экосистемы преступных сообществ обладают значительными криминальными преимуществами перед другими формами структурирования, как традиционными, так и сетевыми. Функционирующая в сети Даркнет экосистема обеспечивает возможности для скрытого и практически безопасного совершения различных криминальных действий, в число которых входят:

- разработка и распространение вредоносных программ, в том числе под конкретные заказы;
- обеспечение незаконными средствами связи и другими запрещенными к обороту устройствами;
- снабжение преступных групп информационными сведениями, полученными путем неправомерного воздействия на компьютерную информацию;
- распространение наркотических средств с использованием информационно-телекоммуникационных сетей, и т. д.

Отдельно нужно отметить высокие возможности самоорганизации преступных групп, объединенных в экосистемы, при изменении внешних условий. Такая самоорганизация отражает отмечавшуюся Т. Я. Хабриевой тенденцию усиления самоорганизации в сетевых коммуникациях, при взаимодействии в которых «формируются сетевые сообщества, потенциально способные образовывать саморегулируемую «криптосреду» [Хабриева 2018: 12].

В качестве примера организованных преступных групп, объединенных на основе цифровой платформы в экосистему, можно привести описанные аналитической службой «Лаборатории Касперского» преступные сообщества, специализировавшиеся на вымогательстве денежных средств у крупных компаний и корпораций с помощью программ-шифровальщиков [Безвершенко, Галов, Квятковский 2021: URL]. Входившие в экосистему автономные преступные группы обладали разным функционалом, включавшим в себя разработку вредоносных программ, непосредственное совершение DDOS-атак, обналичивание полученных от потерпевших средств и т. д. Связь между преступными группами осуществлялась анонимно, взаимодействие строилось по принципу так называемой бизнес-модели **RaaS** («программа – вымогатель как услуга»).

Становление экосистем преступных сообществ ведет к формированию глобального международного рынка преступных услуг, функционирующего посредством цифровых платформ в сети Даркнет. Этот сетевой рынок существенно расширяет криминальные возможности для подготовки, совершения и сокрытия высокотехнологичных преступлений. Полагаем, что при анализе закономерностей функционирования этого рынка необходимо учитывать, наряду с отмеченными процессами глобализации преступной деятельности, также заявившие о себе в последние годы процессы ее **глокализации** [Поляков 2024: 154]. Явление глокализации отражает развитие процессов, противоположных глобализации и выражающихся в усилении локальных идентичностей, связанных с отдельными регионами, государствами (объединениями государств), национальными группами. На важность учета процессов глокализации обращал внимание, в частности, Председатель Конституционного суда Российской Федерации В. Д. Зорькин [Зорькин 2014: 8]. Процессы глокализации проявляются, например, в специализации преступлений, совершаемых преступными группами этнических диаспор [Van Hellemont, Densley 2019], имеющих как в Российской Федерации, так и в большинстве других развитых стран. Представляется, что исследование влияния глокализации на организованную преступную деятельность является одним из новых и перспективных направлений развития для уголовно-правовых наук.

В заключение нужно отметить, что противодействие организованным группам и преступным сообществам, объединенным посредством цифровых платформ в экосистемы, является чрезвычайно сложной практической

задачей, стоящей перед правоохранительными органами. В связи с этим, как представляется, перед криминалистической теорией стоит важная задача по разработке и апробации рекомендаций, предназначенных для расследования совершенных такими преступными объединениями высокотехнологичных преступлений.

Литература

- Безвершенко Л., Галов Д., Квятковский И. Шифровальщики: кто, как и зачем использует их в 2021 году. URL: <https://securelist.ru/ransomware-world-in-2021/101425/>
- Бычков В. В., Вехов В. Б. Некоторые аспекты противодействия преступлениям экстремистской направленности, совершенным с использованием даркнет / Расследование преступлений: проблемы и пути их решения. – 2023. – № 2. – С. 89–94. DOI: 10.54217/2411-1627.2023.40.2.010.
- Васильев А. А., Ибрагимов Ж. И., Васильева О. В. Даркнет как ускользающая сфера правового регулирования / Юрислингвистика. – 2019. – № 12. С. 10-12.
- Глазкова Л. В. Особенности современных организованных преступных групп / Мониторинг правоприменения. – 2019. – №1 (30). – С. 54-60.
- Зайцев О. А., Пастухов П. С. Цифровой профиль лица как элемент информационно-технологической стратегии расследования преступлений / Вестник Пермского университета. Юридические науки. – 2022. Вып. 56. – С. 281–308. DOI: 10.17072/1995-4190-2022-56-281-308.
- Зорькин В. Д. Проблемы конституционно-правового развития России (к 20-летию Конституции Российской Федерации) / Вестник Московского университета. Сер. 11. Право. – 2014. – № 1. – С. 3-21.
- Каминский А. М. Теоретические основы криминалистического анализа организованности преступной деятельности и возможности его практического использования: автореф. дисс. д-ра юрид. наук. Нижний Новгород, 2008.
- Кастельс М. Становление общества сетевых структур / Новая постиндустриальная волна на Западе. Антология / под ред. В. Л. Иноземцева. М., 1999. - С. 494-505.
- Коновалова Е. А., Есина А. С. Сравнительно-правовой анализ категории «организованная преступная группа» / Вестник Московского университета МВД России. – 2021. – № 6. – С. 161–165. DOI: 10.24412/2073-0454-2021-6-161-165.
- Овчинский В. С. Криминология цифрового мира : учебник для магистратуры. М., 2018.
- Осипенко А. Л. Организованная преступность в сети Интернет / Вестник Воронежского института МВД России. – 2012. – № 3. – С. 10-16.
- Осипенко А. Л. Сетевая компьютерная преступность: теория и практика борьбы: монография. Омск, 2009.
- Поляков В. В. Групповая форма совершения преступлений как один из признаков высокотехнологичной преступности / Российский юридический журнал. – 2023. – № 1 (148). – С. 117-126. DOI: 10.34076/20713797_2023_1_117.
- Поляков В. В. К вопросу о противодействии высокотехнологичной транснациональной преступности / Сб. мат. Междунар. науч.-практич. конф. «Актуальные проблемы отечественной криминалистики: современные тенденции», посвященной памяти проф. Н. П. Яблокова. 16 декабря 2022 г., г. Москва. М., 2023. – С. 367-374.
- Поляков В. В. Структура и содержание криминалистической характеристики высокотехнологичных преступлений / Актуальные проблемы российского права. – 2024. – № 6. – С. 147-159. DOI: 10.17803/1994-1471.2024.164.7.147-159.
- Поляков В. В. Понятие «высокотехнологичные преступления» в криминалистике / Криминалистика: вчера, сегодня, завтра. – 2023. – № 4. – С. 151-162. DOI: 10.55001/2587-9820.2023.19.44.015.
- Протасевич А. А., Скрябикова Ю. Б. О необходимости формирования единой дефиниции «даркнет» в криминалистике / Сибирские уголовно-процессуальные и криминалистические чтения. – 2021. – № 4. – С. 77–86. DOI: 10.17150/2411-6122.2021.4.77-86.
- Раменская Л. А. Применение концепции экосистем в экономико-управленческих исследованиях / Управленец. – 2020. – Т. 11, № 4. – С. 16-27.
- Савенков А. Н., Россинская Е. Р. Вектор развития криминалистической науки в условиях глобальной цифровизации / Государство и право. – 2023. – № 5. С. 100-110. URL: <http://gospravo-journal.ru/s102694520025650-6-1/>. DOI: 10.31857/S102694520025650-6.
- Сидоренко Э. Л., Барциц И. Н., Хисамова З. И. Эффективность цифрового государственного управления: теоретические и прикладные аспекты / Вопросы государственного и муниципального управления. – 2019. – № 2. – С. 93-114.
- Смушкин А. Б. Криминалистические аспекты исследования даркнета в целях расследования преступлений / Актуальные проблемы российского права. – 2022. – Т. 17, № 3. – С. 102-111. DOI: 10.17803/1994-1471.2022.136.3.102-111.
- Хабриева Т. Я. Право перед вызовами цифровой реальности / Журнал российского права. – 2018. – № 9. – С. 5–16. DOI: 10.12737/art_2018_9_1
- Beshiri A. S., Susuri A. Dark Web and Its Impact in Online Anonymity and Privacy: A Critical Analysis and Review / Journal of Computer and Communications. 2019. Vol.7. No. 3. P. 30-43. DOI: 10.4236/jcc.2019.73004.
- Van Hellemont E., Densley J. Gang globalization: How a global mediascape creates and shapes local gang realities / Crime, Media, Culture: An International Journal. 2019. Vol. 15. Issue 1. P. 1-20. DOI: 10.1177/1741659018760107.

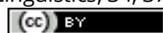
References

- Beshiri, A. S., Susuri, A. (2019). Dark Web and Its Impact in Online Anonymity and Privacy: A Critical Analysis and Review. *Journal of Computer and Communications*, 3, 30-43. DOI: 10.4236/jcc.2019.73004.
- Bezvershenko, L., Galov, D., Kvyatkovsky, I. Ransomware: who, how and why uses them in 2021. Available from: <https://securelist.ru/ransomware-world-in-2021/101425/> (in Russian).
- Bychkov, V. V., Vekhov, V. B. (2023). Some aspects of counteracting extremist crimes committed using the darknet. *Investigation of crimes: problems and solutions*, 2, 89-94. DOI: 10.54217/2411-1627.2023.40.2.010 (in Russian).
- Castells, M. (1999). Formation of a society of network structures / New post-industrial wave in the West. Anthology. Edited by V. L. Inozemtsev. Moscow, 494-505 (in Russian).
- Glazkova, L. V. (2019). Features of modern organized crime groups. *Monitoring of law enforcement*, 1 (30), 54-60 (in Russian).
- Kaminsky, A. M. (2008). Theoretical foundations of forensic analysis of the organization of criminal activity and the possibilities of its practical use: Abstract of the Dissertation of a Doctor of Law. Nizhny Novgorod (in Russian).
- Khabrieva, T. Ya. (2018). Law facing the challenges of digital reality. *Journal of Russian law*, 9, 5-16. DOI: 10.12737/art_2018_9_1 (in Russian)
- Konovalova, E. A., Esina, A. S. (2021). Comparative legal analysis of the category "organized criminal group". *Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia*, 6, 161–165. DOI: 10.24412/2073-0454-2021-6-161-165 (in Russian).
- Osipenko, A. L. (2009). Network computer crime: theory and practice of struggle: monograph. Omsk (in Russian).
- Osipenko, A. L. (2012). Organized crime on the Internet. *Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia*, 3, 10-16 (in Russian).
- Ovchinsky, V. S. (2018). Criminology of the digital world: a textbook for master's degree programs, Moscow (in Russian).
- Polyakov, V. V. (2023). Group form of committing crimes as one of the signs of high-tech crime. *Russian Law Journal*, 1 (148), 117-126. DOI: 10.34076/20713797_2023_1_117 (in Russian).
- Polyakov, V. V. (2023). On the issue of combating high-tech transnational crime. Coll. of materials. Int. scientific-practical. conf. "Actual problems of domestic forensic science: modern trends", dedicated to the memory of prof. N. P. Yablokov. December 16, 2022, Moscow. Moscow, 367-374 (in Russian).
- Polyakov, V. V. (2023). The concept of "high-tech crimes" in forensic science. *Forensic science: yesterday, today, tomorrow*, 4, 151-162. DOI: 10.55001 / 2587-9820.2023.19.44.015 (in Russian).
- Polyakov, V. V. (2024). Structure and content of forensic characteristics of high-tech crimes. *Actual problems of Russian law*, 6, 147-159. DOI: 10.17803/1994-1471.2024.164.7.147-159 (in Russian).
- Protasevich, A. A., Skryabikova, Yu. B. (2021). On the need to form a single definition of "darknet" in forensic science. *Siberian criminal procedure and forensic readings*, 4, 77-86. DOI: 10.17150 / 2411-6122.2021.4.77-86 (in Russian).
- Ramenskaya, L. A. (2020). Application of the ecosystem concept in economic and managerial research. *Manager*, 4, 16-27 (in Russian).
- Savenkov, A. N., Rossinskaya, E. R. (2023). Vector of Development of Forensic Science in the Context of Global Digitalization. *State and Law*, 5, 100-110. Available from: <http://gospravo-journal.ru/s102694520025650-6-1/>. DOI: 10.31857/S102694520025650-6 (in Russian).
- Sidorenko, E. L., Bartsits, I. N., Khisamova, Z. I. (2019). Efficiency of Digital Public Administration: Theoretical and Applied Aspects. *Issues of State and Municipal Administration*, 2, 93-114 (in Russian).
- Smushkin, A. B. (2022). Forensic aspects of darknet research for the purposes of crime investigation. *Actual problems of Russian law*, 3, 102-111. DOI: 10.17803/1994-1471.2022.136.3.102-111 (in Russian).
- Van, Hellemont E., Densley, J. (2019). Gang glocalization: How a global mediascape creates and shapes local gang realities. *Crime, Media, Culture: An International Journal*, 1, 1-20. DOI: 10.1177/1741659018760107.
- Vasiliev, A. A., Ibragimov, Zh. I., Vasilyeva, O. V. (2019). Darknet as an elusive sphere of legal regulation. *Jurilinguistics*, 12, 10-12 (in Russian).
- Zaitsev, O. A., Pastukhov, P. S. (2022). Digital face profile as an element of the information technology strategy for investigating crimes. *Bulletin of Perm University. Legal sciences*, 56, 281–308. DOI: 10.17072/1995-4190-2022-56-281-308 (in Russian).
- Zorkin, V. D. (2014). Problems of constitutional and legal development of Russia (on the 20th anniversary of the Constitution of the Russian Federation). *Bulletin of Moscow University. Series 11. Law*, 1, 3-21 (in Russian).

Citation:

Поляков В. В. Использование цифровых платформ как технологическая основа формирования экосистем преступных сообществ // Юрислингвистика. – 2024. – 34. – С. 37-41.

Polyakov V. V. (2024) The Use of Digital Platforms as a Technological Basis for the Formation of Criminal Communities Ecosystems. *Legal Linguistics*, 34, 37-41.



This work is licensed under a Creative Commons Attribution 4.0. License