Научная статья С. 84–88
УДК 343.9

ТРАНСНАЦИОНАЛЬНАЯ ОРГАНИЗОВАННАЯ ПРЕСТУПНОСТЬ В ЦИФРОВОЙ СФЕРЕ

Юрий Александрович Воронин
Южно-Уральский государственный университет (национальный исследовательский университет) Челябинск, Россия
voroninya@yandex.ru, ORCID: 0000-0001-9941-8316

Аннотация. Актуальной задачей криминологической науки и практики является анализ основных характеристик, а также состояния и динамики цифровой организованной преступности. В статье констатируется, что одной из самых примечательных особенностей ее развития сегодня выступает использование в цифровой среде (или посредством использования цифровых технологий) специфических приемов и методов, открывающих наиболее широкие возможности прежде всего для транснациональных криминальных сообществ, извлекающих из преступной деятельности баснословные барыши и причиняющих обществу огромный экономический ущерб. Авторы анализируют системообразующие признаки так называемой цифровой транснациональной организованной преступности,а также делают вывод об актуальности в сложившейся ситуации разработки и реализации целевых программ эффективного противодействия ей, подчеркивая, при этом, необходимость активизации межгосударственного сотрудничества в решении этой сложной задачи.

Ключевые слова: тенденции транснациональной организованной преступности, цифровая организованная преступность, использование информационных и телекоммуникационных технологий в преступлениях, компьютерная информация

Для цитирования: Воронин Ю. А. Транснациональная организованная преступность в цифровой сфере // Правопорядок: история, теория, практика. 2021. № 3 (30). С. 84–88.

Original article

TRANSNATIONAL ORGANIZED CRIME IN THE DIGITAL SPHERE

Yuriy A. Voronin
South Ural State University (National Research University), Chelyabinsk, Russia
voroninya@yandex.ru, ORCID: 0000-0001-9941-8316

Abstract. The actual task of criminological theory and practice is the analysis of the main characteristics, as well as the state and dynamics of digital organized crime. The article states that one of the most remarkable features of its development today is the use in the digital environment (or through the use of digital technologies) specific techniques and methods that open up the most widest opportunities first of all for transnational criminal communities, that extract fabulous profits from criminal activities and cause huge economic damage to society. The authors analyze the system-forming features of the so-called digital transnational organized crime, and also draw a conclusion about actuality in the current situation of developing and implementing targeted programs to effectively counter it, while emphasizing the need to intensify inter state cooperation in solving the complex problem.

Keywords: trends in transnational organized crime, digital organized crime, using of information and telecommunication technologies in criminality, computer information

For citation: Voronin Yu.A. Transnational Organized Crime in the Digital Sphere. *Pravoporyadok: istoriya, teoriya, praktika* [Legal Order: History, Theory, Practice]. 2021;(3):84-88. (In Russ.)

Введение

Одной из доминирующих особенностей современной криминогенной среды — как в России, так и в глобальных масштабах — является широкое распространение высокотехнологичной преступности во всех ее проявлениях. В частности, по словам руководителя отдела Следственного Комитета РФ по расследованию киберпреступлений К. Комарда (в его интервью ТАСС), уровень преступности с использованием информационных технологий или в киберпространстве за последние 7 лет (начиная с 2013 г.) вырос в 20 раз и продолжает увеличиваться, демонстрируя все большую агрессивность и, одновременно, высокую латентность[1]. Правоохранительные органы в России выявляют в среднем около 10 % преступлений, относящихся к данной категории. Не лучше обстоит дело в США: по данным нью-йоркской киберполиции, раскрываемость киберпреступлений в разные годы составляет в среднем всего лишь 4 %, подтверждая характеристику киберпреступности как высокодоходной и малорискованной криминальной деятельности [2, с. 138].

При этом одним из самых опасных и стремительно развивающихся сегментов высокотехнологичной киберпреступности в мире является транснациональная организованная преступность в сфере информационного пространства, использующая не существовавшие прежде и чрезвычайно эффективные сегодня информационно-цифровые технологии. В ст. 2 Конвенции ООН против транснациональной организованной преступности достаточно емко и вместе с тем четко раскрывается содержание этого понятия (и явления). В совокупности формализованных признаков оно означает функционирование структурно оформленных групп в составе трех или более лиц, существующих в течение определенного периода времени и действующих согласованно «с целью совершения одного или нескольких серьезных преступлений, или преступлений, признанных таковыми в соответствии с настоящей Конвенцией, с тем, чтобы получить прямо или косвенно финансовую или иную материальную выгоду»[2]. Криминологические исследования убедительно свидетельствуют, что во всем массиве высоко технологичных цифровых преступлений на долю именно организованных групповых форм их совершения — с четкой иерархией, распределением ролей участников и объединяющей их корыстной мотивацией — приходится более 87 %[3]. Не случайно, многочисленные конкретные примеры из реальной практики убедительно подтверждают, что все более распространенным становится осуществление транснациональной криминальной деятельности организованных преступных сообществ с использованием информационно-цифровых технологий именно в целях получения (упомянутой в Конвенции ООН) материальной выгоды. При этом материальные потери, причиняемые подобным криминальным бизнесом, существенно выше, по сравнению с традиционными разновидностями общеуголовной организованной преступности. Достаточно сказать, что, по некоторым экспертным оценкам, глобальный ущерб от таких преступлений в годовом исчислении составляет около 600 миллиардов долларов при росте на десятки процентов ежегодно [3, с. 1–7].

Описание исследования и обсуждение результатов

Как свидетельствует дальнейший анализ сложившейся ситуации, есть основания констатировать развитие сегодня в криминогенной среде следующей доминирующей тенденции, а именно: информационно-цифровые средства расширяют в первую очередь возможности международных криминальных структур, широко использующих высокие технологии в различных видах преступной деятельности с корыстной мотивацией, порождающей огромные экономические издержки. Подтверждением этого тезиса, на наш взгляд, являются следующие, достаточно хорошо различимые индикаторы.

Во-первых, развитие анализируемой тенденции нашло отражение в усилении диверсификации криминальной активности организованных преступных сообществ именно на международном, транснациональном уровне, т. е. на территории целого ряда государств, не ограничиваясь юрисдикцией какого-либо

[1] Комарда К. Интервью ТАСС // Эхо Москвы : [сайт]. URL: https://echo.msk.ru/?_ (дата обращения: 15.01.2021).

[2] United Nations Convention against Transnational Organized Crime And the Protocols Thereto. URL: https://www.un.org/ruleoflaw/files/UNConventionAgainst_TransnationalOrganizedCrime.pdf (дата обращения: 20.01.2021).

[3] Компьютерная преступность как разновидность организованной преступности // База знаний Allbest : [сайт]. URL: https://knowledge.allbest.ru/ (дата обращения: 20.01.2021).

из них. И такое развитие событий вполне логично: цифровизация криминальной среды (как отражение общемировой тенденции) неизбежно способствует интеграции преступных сообществ разных стран и, следовательно, усилению их транснационального характера, что является ярким свидетельством качественного изменения самой организованной преступности. Транснациональность данной категории преступлений выражается в том, что преступники, зачастую находясь на удаленном расстоянии от объекта посягательства на территории разных государств, тем самым во многом упрощают свою задачу. Как справедливо отмечают специалисты, преимущества упомянутой транснациональности заключаются, в частности, в том, что злоумышленники уходят от ответственности в силу ряда следующих довольно типичных обстоятельств, а именно: из-за различия или отсутствия соответствующего законодательства, регулирующего информационно-цифровую сферу в тех или ином государствах; отсутствия договора об экстрадиции между конкретными государствами; бюрократических и процессуальных сложностей, возникающих в связи с возбуждением уголовных дел в отношении именно иностранных граждан и т. д.[1]

Во-вторых, именно в силу перечисленных обстоятельств сегодняшние высокотехнологичные транснациональные преступные группы стремительно расширяют поле деятельности и, одновременно, демонстрируют все более высокие «показатели экономической эффективности». В результате, по мнению специалистов, на долю транснациональных преступных сообществ сегодня приходится в общей сложности от 15 до 20 %мирового ВВП чисто криминального оборота и не менее 25 % дополнительного легального оборота, контролируемого мафиозными сообществами. В целом же, «можно сделать вывод о том, что крупнейшими собственниками активов и держателями ресурсов на планете являются именно преступные синдикаты» [2, с. 137–138]. Вот лишь один из множества примеров, подтверждающих приведенную оценку складывающейся ситуации. Так, в своем релизе Министерство юстиции США в июне 2020 г. сообщило об осуждении окружным судом штата Невада лидеров транснациональной преступной группы Infraud Organization. Организация занималась крупномасштабным приобретением, продажей и распространением похищенных идентификационных данных, скомпрометированных дебетовых и кредитных карт, личной, финансовой и банковской информации, компьютерных вредоносных программ. Ущерб от ее деятельности был оценен примерно в 568 млн долларов [1, с. 8].

В-третьих, есть основания констатировать, что тенденция усиления транснациональности выразилась в ускорении динамики вовлечения в ряды организованных преступных сообществ этнических представителей самых разных стран, т. е. в своеобразную «интернационализацию» состава этих преступных группировок. Достаточно сказать, что в транснациональной криминальной активности организованных преступных формирований с различным этническим составом сегодня принимают участие выходцы примерно из 80 % стран. Причем, отличительная черта таких криминальных сообществ заключается в том, что их интернациональные соучастники могут находиться за тысячи километров друг от друга, им не мешает языковой барьер, поскольку компьютерные языки стандартны,а в цифровом мире не существует государственных границ. Характерным примером, в частности, явилась преступная деятельность транснациональной группировки, базировавшей свои структуры на территории Китая, России, Украины и ряда других стран Европы. Подразделениям Интерпола, Европола, при содействии «Лаборатории Касперского, удалось раскрыть киберпреступные операции этого криминального сообщества. Они продолжались два года и затронули около 100 финансовых организаций по всему миру, потерявших в результате хищенияв общей сложности около 1 млрд долларов[2].

В-четвертых, развитие тенденции цифровизации организованной преступности, обретая глобальный (транснациональный) характер, наряду с расширением специализации криминальных сообществ, несомненно, предполагает достаточно высокий уровень интеллектуальности и профессионализма их участников — субъектов этой преступной деятельности, определяя тем самым приток в нее высоко квалифицированного контингента. Именно в силу «продвинутости» этих (в отличие от традиционных) средств и способов криминальных действий, подобная активность является такой эффективной. Негативные преломления складывающейся ситуации при этом достаточно ясны. Ведь криминальный профессионализм и интеллектуальный уровень высококвалифицированного

[1] Компьютерная преступность как разновидность организованной преступности.

[2] Евгений Федуненко. Громкие киберпреступления последних лет // Коммерсантъ : [сайт]. URL: https://www.kommersant.ru/doc/3270122 (дата обращения: 20.01.2021).

контингента транснациональных криминальных сообществ одновременно определяют гораздо более высокий уровень их общественной опасности и результативности преступного бизнеса. Криминальные структуры, активно используют квалифицированных программистов, компьютерных взломщиков, специалистов по нелегальному манипулированию на рынке виртуальной валюты, получая громадные барыши от разного рода мошеннических операций.

Наряду со сказанным, высокий уровень профессионализма упомянутых субъектов зачастую обеспечивает им конспиративность и, следовательно, безнаказанность криминального бизнеса, позволяющего преступникам скрывать свои следы, сохранять анонимность, используя офшоры, препятствовать сбору доказательств. Ведь в подобных случаях, несмотря на предпринимаемые усилия, спецслужбы обладают сравнительно ограниченными возможностями для отслеживания денежных потоков нелегального характера, выявления и наказания подозреваемых в криминальных операциях лиц.

Кстати, ярким свидетельством сказанному как раз является активизация криминалитета в связи с операциями с использованием виртуальных денег. Транснациональные организованные преступные сообщества в условиях всеобщей цифровизации получили невиданную ранее возможность широкого использования новых финансовых инструментов — криптовалюты, блокчейна. Так, по сообщению BBC.com от 20.06.2020 г., ярким примером, отражающим указанную тенденцию, является создание и использование криминальными структурами биржевых площадок, на которых — в обход норм национального и международного права — они занимаются кибермошенничеством, отмыванием денежных средств, в особенности биткоинов, новакоинов и других цифровых (виртуальных) валют. Речь, в частности, идет о деятельности крупнейшей криптобиржи BTC-e, а также целого ряда других организаций подобного типа, которые, в отличие от легальных биржевых площадок, просто не требовали от клиентов серьезной авторизации для осуществления торгов. Как следует из оценки неправительственной организации Global Witness, совокупный суточный оборот BTC-e превышал 66 млн долларов, а с каждой сделки администраторы площадки получали 0,5 % комиссии. Причем, никто из многочисленных «клиентов» (более 20 тыс. пользователей) не знал, кто владеет этим прибыльным полулегальным бизнесом, поскольку бенефициары BTC-e скрывались за сетью офшоров. По оценкам Департамента криминальных расследований Службы внутренних доходов США, их совокупные активы к 2020 г. достигали 500 млн долларов [1, с. 9].

Наконец, в-пятых, есть веские основания констатировать, что, посредством использования цифровой среды (интернета, телекоммуникационной связи), для вербовки в свои ряды новых кадров, криминалитетом предпринимаются активные усилия по информационному воздействию прежде всего на молодежную аудиторию с целью «романтизации» профессиональной преступной деятельности в составе мафиозных сообществ. Такие пропагандистские материалы имеют форму мультимедийных коммуникаций и содержат, зачастую, виртуальные сообщения, презентации, журналы, аудио- и видеофайлы. Криминальная «романтика», как уже отмечалось, является центральной темой этой пропаганды. Специалисты отмечают, что широкая область влияния распространяемой через интернет подобной информации в геометрической прогрессии увеличивает аудиторию, на которую она может воздействовать со всеми вытекающими последствиями.

Заключение

Таким образом, как свидетельствуют криминологические исследования, данные уголовной статистики и следственно-судебная практика, цифровая экспансия во все сферы человеческого бытия, всеобщая телекоммуникационная взаимосвязанность наложили заметный отпечаток и способствовали небывалому развитию высокотехнологичной и весьма «интеллектуализированной» цифровой транснациональной (территориально) и многонациональной (по своему составу) организованной преступности, характеризующейся весьма болезненным для мирового сообщества и конкретных государств уровнем экономических потерь. В результате, сама мировая экономика все в большей степени приобретает черты мафиозной. В этой связи, существует острая необходимость в формулировании и реализации целевых программ противодействия возросшей активности цифровой транснациональной организованной преступности качественно нового поколения. Борьба с организованной преступностью в области информационных технологий должна быть одним из самых приоритетных направлений деятельности спецслужб. Без эффективного противодействия динамика данной категории преступлений будет и дальше нарастать с неослабевающей силой. Наряду с этим, все более очевидной становится также необходимость максимального

использования странами мирового сообщества не только их национального, но и международного опыта по разработке и реализации подобных программ в информационно-цифровой среде, а также их межгосударственной координации. Свидетельством возрастающего понимания значимости такого подхода является активная подготовка сегодня инициированной Российской Федерацией Конвенции ООН по противодействию киберпреступности.

Список источников

1. Воронин Ю. А., Беляева И. М., Кухтина Т. В. Современные тенденции преступности в цифровой среде // Вестник Южно-Уральского государственного университета. Серия «Право». 2021. Т. 21, № 1. С. 7–12.

2. Овчинский В. С. Преступность и борьба с ней в цифровом мире // Проектирование будущего. Проблемы цифровой реальности : труды 1-й Международной конференции (Москва, 8 — 9 февраля 2018 г.). Москва : ИПМ им. М. В. Келдыша, 2018. С. 137–138.

3. Сентюренко О. В. Цифровая среда: тренды и риски развития // Научно-техническая информация. Серия 1, Организация и методика информационной работы. 2015. № 2. С. 1–7.

References

1. Voronin Yu.A., Belyaeva I.M., Kuhtina T.V. Modern Trends of Crime in the Digital Environment. *Vestnik Yuzhno-Ural'skogo gosudarstvennogo universiteta. Seriya «Pravo»* [Bulletin of South Ural State University. Law Series]. 2021;21(1):7-12. (In Russ.)

2. Ovchinskij V.S. Crime and the fight against it in the digital world. *Proektirovanie budushchego. Problemy cifrovoj real'nosti: trudy 1-j Mezhdunarodnoj konferencii* [Designing the future. Problems of Digital Reality. Proceedings of the 1st International Conference]; 2018 Feb 8-9; Moscow. Moscow: M.V. Keldysh IPM Publ., 2018. p. 137-138. (In Russ.)

3. Sentyurenko O.V. Digital Environment: Trends and Risks of Development. *Nauchno-tekhnicheskaya informaciya. Seriya 1, Organizaciya i metodika informacionnoj raboty* [Scientific and Technical Information. Series 1, Organization and methodology of information work]. 2015;(2):1-7. (In Russ.)

Статья поступила в редакцию / The article was submitted: 11.03.2021.