Научная статья
УДК 343.98
doi: 10.17223/15617793/511/25

Формирование экосистем преступных сообществ как следствие цифровой трансформации организованной преступной деятельности

Виталий Викторович Поляков[1]

[1] *Алтайский государственный университет, Барнаул, Россия, agupolyakov@gmail.com*

Аннотация. Рассмотрена эволюция организованных преступных групп под воздействием цифровых инноваций. Выявлено распространение организованных групп, построенных на основе сетевых принципов управления и специализирующихся на совершении высокотехнологичных преступлений. Установлено формирование экосистем преступных сообществ, представляющих собой объединения автономных преступных групп, взаимодействующих посредством цифровых платформ в сети Даркнет. Проанализированы особенности и криминальные преимущества таких экосистем.
Ключевые слова: организованные преступные группы, теория экосистем, высокотехнологичные преступления, компьютерные преступления, цифровые платформы, цифровизация, уголовное судопроизводство

Для цитирования: Поляков В.В. Формирование экосистем преступных сообществ как следствие цифровой трансформации организованной преступной деятельности // Вестник Томского государственного университета. 2025. № 511. С. 229–236. doi: 10.17223/15617793/511/25

Original article
doi: 10.17223/15617793/511/25

The formation of ecosystems of criminal groups due to the digital transformation of organized crime

Vitaly V. Polyakov[1]

[1] *Altai State University, Barnaul, Russian Federation, agupolyakov@gmail.com*

Abstract. The article examines the problem of digital transformation within organized criminal groups. This transformation results from the introduction of innovative digital technologies into criminal activities and is manifested in the formation of decentralized organizational structures for criminal groups based on network management principles. It is shown that the transition from traditional hierarchical structures to alternative structures based on network interaction among participants is primarily typical of criminal groups specializing in high-tech crimes. In practice, the evolution of organized criminal activity has led to the emergence of groups with complex symbiotic structures, characterized by a combination of network interaction among the group's structural elements while maintaining a hierarchical structure within its governing core. The factors characterizing criminal groups with decentralized mixed structures are described, including a higher level of self-organization, increased group stability, adaptability to external conditions, responsiveness in addressing emerging issues, and enhanced anonymization of participants. The phenomenon of forming a new organizational structure for criminal groups has been revealed. This form is most accurately described by the concept of an ecosystem of criminal communities. It is shown that ecosystems of criminal communities are network associations of autonomous criminal groups interacting with one another based on the principle of "Crime as a Service", similar to the interaction principles found in business ecosystems within the digital economy. The technological basis for these ecosystems consists of digital platforms created and operating on the Darknet, which represent a shadow information environment that unites network services, data, and digital resources, facilitating the joint activities of ecosystem participants. The formation of ecosystems of criminal communities appears to be a qualitatively new and dangerous phenomenon. The criminal advantages gained from this transformation include the ease of attracting resources through the development of a global network market for criminal services and products on the Darknet; the "division of labor" through the narrow specialization of autonomous groups entering into cooperative and collaborative relationships; access to advanced means for committing high-tech crimes through the commercialization of criminal innovations; the rapid incorporation of new participants; the ease of overcoming interregional and interstate borders to commit transnational criminal acts; a combination of globalization and glocalization factors; and a significant reduction in the risk of criminal prosecution due to maximum anonymization of participants. The article concludes that the formation of ecosystems of criminal communities is becoming the dominant trend in the evolution of modern organized crime.
Keywords: organized crime, ecosystem theory, high-tech crimes, computer crimes, digital platforms, digitalization, criminal justice

***For citation*:** Polyakov, V.V. (2025) The formation of ecosystems of criminal groups due to the digital transformation of organized crime. *Vestnik Tomskogo gosudarstvennogo universiteta – Tomsk State University Journal*. 511. pp. 229–236. (In Russian). doi: 10.17223/15617793/511/25

Введение

Одним из следствий кардинальных изменений в информационной сфере, произошедших в 2000-е гг., стало появление качественно новых форм организации различных социальных и экономических систем [1]. Отличительная особенность этих форм заключается в формировании децентрализованной сетевой структуры управления, заменяющей традиционную вертикальную иерархическую структуру. Технологической основой для реализации сетевых принципов управления и взаимодействия стали глобальные информационные сети (прежде всего сеть Интернет), обеспечившие децентрализованный оперативный обмен информацией и эффективную интеграцию информационных ресурсов.

Переход к сетевой модели взаимодействия в социальных и экономических системах стал в последние годы доминирующей мировой тенденцией. Наиболее отчетливо этот переход наблюдается в современной цифровой экономике, проявившись в быстром распространении качественно новых форм организации бизнес-структур. Динамичными социальными группами, восприимчивыми к происходящим в экономической сфере общества изменениям, являются преступные сообщества. Как справедливо отметили В.Д. Ларичев и Т.В. Якушева, «наивно было бы полагать, что организованная преступность... в цифровую эпоху продолжит действовать традиционными способами и сохранит свою прежнюю структуру» [2. С. 84]

Для исследования закономерностей, характеризующих новые формы управления в социальных системах, плодотворной оказалась концепция экосистем. Понятие экосистемы, первоначально сформировавшееся в естественных науках, заняло прочное место в анализе тенденций развития современной цифровой экономики. Так, по мнению О.А. Зайцева и П.С. Пастухова, в цифровой экономике «фундаментальным элементом использования данных» являются экосистемы [3. С. 293]. Л.А. Раменская определяет экосистему как «совокупность автономных организаций, производящих взаимодополняющие компоненты ценности» без вертикальной интеграции, при этом внутри экосистемы происходит формирование «единой среды обмена информацией и ресурсами» [4. С. 20]. Важно отметить, что это понятие вошло в «Стратегию развития информационного общества в Российской Федерации на 2017–2030 годы», утвержденную Указом Президента Российской Федерации, где экосистема цифровой экономики определяется как «партнерство организаций, обеспечивающее постоянное взаимодействие» на основе технологических платформ, интернет-сервисов, информационных систем»[1].

Понятие экосистемы в силу его научной широты и междисциплинарности в последние годы было успешно применено и в правовых исследованиях. Так, С.В. Зуев рассматривает уголовное судопроизводство с позиций социальной экологии как социальную экосистему [5. С. 186]. А.Б. Смушкин считает, что цифровая трансформация формирует «экосистему всего уголовного судопроизводства – от подачи заявления о совершении преступления... до судебного приговора» [6. С. 243], включающую в себя криминалистический, уголовно-процессуальный и организационный блоки. Принципы построения экосистемы начального этапа уголовного судопроизводства рассмотрены в работе Л.Н. Масленниковой [7. С. 63].

Среди организованных преступных групп наиболее подготовленными к внедрению инновационных форм управления и взаимодействия оказались преступные сообщества, специализирующиеся на совершении высокотехнологичных преступлений [8] посредством использования специально разработанных программно-аппаратных средств [9] и применения информационно-коммуникационных сетей. В настоящее время можно говорить о том, что происходит цифровая трансформация таких преступных организаций. Эта трансформация выражается в качественных изменениях их внутренней структуры, способов управления и взаимодействия и детерминируется внедрением в криминальную деятельность передовых цифровых технологий.

Отражением происходящей цифровой трансформации выступает новое и опасное явление, которое может быть охарактеризовано как становление экосистем преступных сообществ. Структура экосистем преступных сообществ строится на принципах управления, сходных с бизнес-экосистемами и основанных на взаимодействии между участниками в соответствии с бизнес-моделью «преступление как услуга» («Crime-as-a-Service», модель CaaS) [10. P. 147; 11], отражающей появление теневого рынка криминальных киберуслуг, функционирующего в соответствии с экономическими законами обычного рынка.

Интересно отметить, что одними из первых на формирование экосистем обратили внимание специалисты-практики, занимающиеся расследованием компьютерных инцидентов. Так, аналитики АО «Лаборатория Касперского» изучили деятельность преступных сообществ, совершавших вымогательство денежных средств у крупных корпораций с помощью вредоносных программ. Сделанный вывод заключался в том, что такие сообщества – «лишь верхушка айсберга», поскольку в совершении каждого преступления задействовано множество автономных организованных групп, оказывающих друг другу преступные услуги посредством сервисов сети Даркнет и формирующих, по мнению аналитиков, «сложные экосистемы» [12], построенные по принципу бизнес-структур. На становление экосистем также обращалось внимание в исследованиях отечественных и зарубежных авторов. M. Chertoff M. и T. Simon считают, что формирование в сети Даркнет скрытой экосистемы («the hidden ecosystem») «способствует пропаганде, вербовке, финансированию и планированию» киберпреступлений [13. P. 5]. По мнению Р.И. Дремлюги и А.И. Коробеева, использование в криминальных целях сетевых платформ фактически поддерживает «экосистему для преступной деятельности» [14. С. 53].

Исследование цифровой трансформации организованных групп и преступных сообществ является сложной комплексной задачей, требующей привлечения теоретического аппарата всех наук криминального цикла.

В то же время специфика новых форм организованных преступных групп фактически остается не изученной. Представляется, что особая роль в решении этой задачи принадлежит криминалистике, являющейся, по выражению А.Н. Савенкова и Е.Р. Россинской, наукой «синтетической природы», интегрирующей «все новые достижения естественных, технических и гуманитарных наук» [15. С. 101].

В настоящей работе с криминалистических позиций рассматриваются понятие экосистем преступных сообществ, их структура, формирование и закономерности криминального функционирования.

Организованные преступные группы с сетевой структурой

Особенности преступных групп с традиционной внутренней структурой к настоящему времени изучены достаточно подробно [16, 17]. Классификация этих групп основывается на ст. 35 УК РФ и разъяснении Пленума Верховного Суда РФ от 10.06.2010 г. № 12[2]. В случае организованных групп к отличительным признакам относят устойчивость состава и наличие руководителя, для преступных сообществ добавляется сложная иерархическая внутренняя структура, включающая вертикальное соподчинение и наличие различных структурных элементов (подразделений или организованных групп) при устойчивых связях между структурными элементами и едином руководстве всем сообществом, причем все эти признаки являются при квалификации оценочными. Такой подход был заложен и обоснован в XX в., его можно проиллюстрировать следующим образом: «С точки зрения структуры преступное сообщество представляет собой систему разноуровневых организаций, находящихся в строгой иерархической зависимости друг от друга, с устойчивой внутренней структурой и распорядком» [18. С. 298]. Можно сказать, что главной особенностью организованных преступных групп с традиционной структурой является вертикальная система управления со строго иерархическим характером. На практике в тех случаях, когда иерархическая структура не находила подтверждения, суд, как правило, исключал из предъявленного обвинения квалифицирующий признак «организованная группа». В качестве примера можно привести типичное судебное решение в отношении участников преступной группы, обвинявшихся в хищении денежных средств из банкоматов с помощью скимминговых устройств. В описательно-мотивировочной части приговора содержится следующее основание для изменения предъявленного обвинения: поскольку из доказательств и справки-меморандума не следовало, что «среди подсудимых была создана и соблюдалась строгая иерархическая подчиненность»[3], суд исключил указание на совершение преступления организованной группой.

Появившиеся в 2000-е гг. информационно-коммуникационные технологии привели к возникновению преступных групп, специализирующихся на совершении высокотехнологичных преступных деяний [19]. В таких преступных группах стали использоваться инновационные формы управления, основанные не на иерархическом, а на альтернативном сетевом принципе. Эта трансформация была отмечена рядом исследователей. Так, А.Л. Осипенко обратил внимание на принципиальные отличия структуры этих групп от традиционных преступных формирований с иерархическим строением [20]. Для иллюстрации высокой общественной опасности такой эволюции можно указать быстрое формирование организованных групп с сетевой структурой, специализирующихся на распространении наркотических средств с помощью компьютерных технологий [21, 22]. В качестве типичного примера, подтверждающего распространение подобных преступных деяний, может быть приведено уголовное дело в отношении участников организованной преступной группы с сетевой структурой управления, занимавшейся незаконным оборотом наркотиков[4]. Распространение наркотических средств осуществлялось посредством сети Интернет без непосредственного контакта покупателей и продавцов, вырученные денежные средства поступали на виртуальные счета биржи криптовалют, при этом взаимодействие между соучастниками осуществлялось через анонимные мессенджеры.

Организованные преступные группы со смешанной структурой

Проведенный нами анализ материалов уголовных дел позволил прийти к выводу, что на практике в трансформации организованных преступных групп в Российской Федерации доминирующим направлением стало формирование групп с достаточно сложной симбиозной структурой. Эта организационная структура характеризуется сочетанием сетевого взаимодействия между структурными частями группы (преступными подразделениями) с сохранением элементов иерархического управления для ее руководящего ядра.

Приведем конкретный пример формирования организованных групп со смешанной организационной структурой. Организованная преступная группа специализировалась на совершении преступлений, заключавшихся в дистанционных хищениях денежных средств коммерческих банков[5]. Группа была создана неустановленными лицами, выступавшими под сетевыми псевдонимами, путем анонимного общения по информационной сети. С помощью вредоносных программ осуществлялся дистанционный сетевой доступ к управлению диспенсерами банкоматов, на которые подавались команды для выдачи наличных денег. Отдельные подразделения группы перемещались в районы расположения подвергшихся атаке банкоматов и забирали похищаемые денежные средства. Группа курьеров, специализировавшаяся на обороте средств платежа, забирала эти средства, обменивала их на чеки биржи криптовалюты «BTC-E» и передавала организаторам. Взаимодействие между структурными подразделениями осуществлялось исключительно дистанционно с помощью специальных программных средств, не допускавших идентификацию пользователей.

Правоохранительным органам удалось задержать руководителей и участников ряда подразделений и предъявить им обвинение по совокупности преступлений, подпадавших под ч. 4 ст. 159.6, ч. 3 ст. 272 и ч. 2 ст. 273 УК РФ. В описанном примере иерархическая структура отдельных групп и руководящего ядра сочеталась с сетевым характером взаимодействия между группами. Отметим также типичность того негативного обстоятельства, что организаторы преступной группы не были установлены.

Исследование судебно-следственной практики позволило выявить факторы, обеспечивающие криминальные преимущества организованных преступных групп с сетевой и смешанной структурой перед группами с иерархическим строением. К таким факторам могут быть отнесены:

– способность к самоорганизации, вследствие этого в зависимости от ситуации координирующим центром могут выступать структурные элементы, обладающие в конкретных условиях наибольшими ресурсами и возможностями;

– высокая устойчивость преступной группы в целом, связанная с децентрализацией управления и обеспечивающая быструю регенерацию после нейтрализации отдельных структурных элементов;

– повышенная адаптивность к меняющимся внешним условиям по сравнению с более «жесткой» иерархической структурой;

– оперативность в решении возникающих в процессе преступной деятельности задач за счет коммуникации по информационно-телекоммуникационным каналам;

– повышенная мотивированность участников как следствие добровольного участия в совершении преступления и легкости выхода из группы;

– высокая степень анонимизации входящих в преступную группу участников, достигаемая дистанционной формой контактов посредством информационно-телекоммуникационных сетей с привлечением специальных программно-аппаратных средств;

– снижение внутренних конфликтов вследствие дистанционного способа контактов, анонимности, добровольности выхода из группы и отсутствия иерархического неравенства.

Характерным примером, иллюстрирующим указанные преимущества, может служить следующее уголовное дело. Находившиеся в федеральном розыске лица посредством знакомства в сети Даркнет организовали преступное сообщество. С помощью специально разработанного вредоносного программного обеспечения они установили дистанционный контроль над компьютерными системами организаций, осуществлявших продажу железнодорожных билетов. Посредством неправомерного доступа к компьютерной информации за счет денежных средств этих организаций производилось оформление проездных документов на привлекаемых лиц, которые далее возвращали билеты в железнодорожные кассы, тем самым обналичивая похищенные средства. Через сайты в сети Даркнет в различных регионах Российской Федерации и ближнего зарубежья формировались структурные подразделения сообщества, реализовывавшие данный способ хищения денежных средств. Связь между соучастниками поддерживалась с использованием кросс-платформенной системы мгновенного обмена сообщениями ICQ, при этом руководители структурных подразделений оставались анонимными друг для друга и для низших звеньев. Как установил суд, данное преступное сообщество претерпело спад активности вследствие ликвидации правоохранительными органами части структурных подразделений, однако затем «регенерировалось путем привлечения в свои ряды новых участников и возобновило криминальную деятельность в прежних масштабах»[6].

Экосистемы преступных сообществ

Анализ эволюции преступных групп, специализирующихся на совершении высокотехнологичных преступлений, позволил выявить новое явление – формирование экосистем преступных сообществ. Именно понятие экосистемы позволяет наиболее точно описать новую форму организационной структуры организованных преступных групп, возникшую в условиях глобальной цифровой трансформации. При этом точно так же, как в цифровой экономике иерархические корпорации уступают дорогу «экономике, чья деятельность организована через платформы и экосистемы» [23. С. 462], так и традиционные иерархические преступные сообщества уступают место более эффективным объединениям, осуществляющим преступную деятельность путем формирования экосистем.

Полагаем, что основные отличительные признаки экосистем преступных сообществ заключаются в следующем:

1. Экосистемы преступных сообществ представляют из себя сетевые объединения автономных преступных групп, взаимодействующих в рамках экосистемы на основе принципа «преступление как услуга».

2. Технологической основой функционирования экосистем преступных сообществ служат цифровые платформы, создаваемые в сети Даркнет, являющейся теневым сегментом сети Интернет. *Такие ц*ифровые платформы представляют из себя информационную среду, объединяющую сетевые сервисы, услуги, информационные данные, цифровые ресурсы и предоставляющую техническую возможность для совместной деятельности автономных групп, входящих в экосистему.

Представляется, что именно появление цифровых платформ в сети Даркнет вызвало качественный скачок в организации высокотехнологичной преступной деятельности преступных сообществ. M. Chertoff и T. Simon отмечали, что скрытая в сети Даркнет экосистема с безопасной цифровой платформой обеспечивает неотслеживаемую инфраструктуру, используемую для огромного количества незаконных действий [13. P. 6]. Можно сказать, что формирование этих платформ привело к своеобразной «капитализации» преступного потенциала сети Даркнет. В силу этого пред-

ставляются совершенно обоснованными мнения о целесообразности криминализации создания и использования подобных платформ в преступных целях [2. С. 96] и о выделении подобной деятельности в качестве самостоятельного состава преступлений [14. С. 54].

В качестве примера экосистем преступных сообществ можно привести транснациональные преступные организации, которые специализировались на вымогательстве денежных средств у производственных и финансовых корпораций, осуществляя дистанционное шифрование содержащейся в компьютерах информации и требуя затем выкупа за ее восстановление. Согласно данным аналитической службы «Лаборатория Касперского», состав участников экосистем включал в себя такие автономные преступные группы, как разработчики вредоносного программного обеспечения; продавцы парольно-кодовой информации, обеспечивавшей доступ к объекту преступного посягательства; владельцы бот-сетей, собиравших данные о жертве; «упаковщики», обеспечивавшие вредоносной программе защиту от обнаружения; группы, занимавшиеся обналичиванием выплаченного в виде криптовалюты выкупа [12]. Взаимодействие между участниками внутри экосистемы поддерживалось в сети Даркнет через цифровые платформы анонимно и на условиях оплаты за оказанные преступные услуги.

Формирование экосистем преступных сообществ, специализирующихся на совершении высокотехнологичных преступлений, вызывает синергетический эффект, приводящий к значительным криминальным преимуществам. Полагаем, что эти преимущества заключаются в следующем.

1. *Легкость привлечения ресурсного обеспечения преступной деятельности.* Возникновение экосистем преступных сообществ фактически означает развитие в сети Даркнет глобального сетевого рынка преступных услуг, таких как заказ вредоносного программного обеспечения, и незаконно созданных продуктов, например конфиденциальной информации о юридических или физических лицах. Использование ресурсов этого сетевого рынка достигается с помощью сервисов Даркнет [24], что позволяет существенно снизить высокие затраты на подготовку высокотехнологичных преступлений и тем самым повысить криминальную эффективность преступной деятельности.

2. «*Разделение труда» между участниками экосистемы*. Такое «разделение труда», вообще говоря, возможно и в преступных организациях с традиционной структурой [25. С. 12], однако в экосистеме оно выступает в наиболее законченном виде как узкая специализация автономных преступных групп, объединенных более сложными отношениями кооперации и коллаборации.

3. *Доступ к новейшим цифровым средствам совершения преступлений*. Можно утверждать, что экосистемы преступных сообществ обеспечивают быструю и эффективную коммерциализацию преступных инноваций. Присоединение к цифровой платформе позволяет организованной преступной группе получить доступ к новейшим разработкам программных и программно-аппаратных средств, используемых при совершении высокотехнологичных преступлений.

4. *Возможности быстрого расширения.* Инкорпорация новых участников преступного сообщества достигается за счет возможностей, предоставляемых сетью Даркнет, и осуществляется с обеспечением анонимности привлекаемых участников. Отметим, что с помощью цифровых платформ преступные группы ведут активную рекламу своей деятельности для привлечения новых участников, а также предоставляемых преступных услуг и продуктов аналогично тому, как это делают обычные коммерческие организации.

5. *Легкость преодоления межрегиональных и межгосударственных границ.* Для экосистем преступных сообществ характерна географическая диверсификация преступной деятельности, основанная на специфике функционирования цифровых платформ в сети Даркнет и проявляющаяся в распространении преступных посягательств, осуществляемых транснациональными преступными группами, на разные регионы и государства. В качестве примера указанных особенностей можно привести следующее достаточно типичное уголовное дело. В. на цифровой платформе интернет-биржи программистов с территории Королевства Таиланд заказывал через обезличенные разовые аккаунты вредоносное программное обеспечение, реализующее несанкционированное копирование парольно-кодовой информации от серверов юридических лиц[7]. Получаемая информация распространялась заказчикам через сайт, сервер которого был расположен в России, при этом сама вредоносная программа функционировала за счет соединения с дата-центром хостинговой компании в США. Администрирование интернет-ресурсов проводилось через компании, расположенные в Германии, а для оплаты использовалась система электронных платежей WebMoney с идентификатором, зарегистрированным на гражданина Республики Узбекистан. Можно сказать, что наличие межгосударственных границ практически не сказывается на осуществлении подобной преступной деятельности, однако оно создает труднопреодолимые барьеры для законной деятельности правоохранительных органов.

6. Сочетание факторов глобализации и глокализации преступной деятельности. Географическая диверсификация ускоряет процессы глобализации организованной преступной деятельности, происходящие под воздействием цифровых инноваций. В то же время выход на международные преступные рынки региональных преступных сообществ, специализирующихся в совершении высокотехнологичных преступлений, существенно повышает роль нового фактора, практически не изученного науками криминального цикла. Таким фактором является глокализация преступной деятельности, выражающаяся в усилении ее локальных (государственных, региональных и иных) особенностей [10]. В экосистемах преступных сообществ происходит объединение и взаимодополнение одновременно протекающих процессов глобализации и глокализации, что создает дополнительные конкурентные преимущества.

7. *Снижение риска уголовного преследования.* В экосистемах преступных сообществ достигается максимальная анонимизация участников, при которой

остаются лично не знакомыми даже руководители автономных преступных групп, входящих в экосистему. Для повышения законспирированности привлекаются дополнительные способы противодействия возможному расследованию, например, безопасность экосистемы повышается путем исключения преступных посягательств в зоне юрисдикции государства, являющегося местом основной дислокации сообщества.

Приведенные факторы, обеспечивающие существенные преимущества новой формы организационной структуры преступных групп, позволяют объяснить причины быстрого становления экосистем преступных сообществ.

Развитие уголовного законодательства в целях противодействия современной организованной преступной деятельности

Организованные группы и преступные сообщества, построенные на сетевых принципах взаимодействия и управления, не полностью соответствуют тем признакам, которыми характеризуются традиционные преступные группы с иерархической структурой. Можно сказать, что они не укладываются в рамки сложившихся правовых представлений, исходящих из требований строгого иерархического соподчинения, устойчивости состава и связей между участниками, единого руководства. В то же время принципиально важно то, что такие группы продолжают оставаться организованными формированиями, только приобретшими иные качества. Более того, в силу существенных криминальных преимуществ они способны не менее, а более эффективно осуществлять высокотехнологичную преступную деятельность и тем самым представляют более серьезную общественную опасность.

Полагаем, что для приведения уголовного законодательства в соответствие с новыми формами организованной преступности из действующих уголовно-правовых норм целесообразно исключить избыточные признаки, сужающие возможность привлечения к уголовной ответственности участников организованных преступных групп с сетевой структурой или объединенных в экосистемы преступных сообществ. Такие предложения уже высказывались отечественными учеными. Так, В.С. Овчинский считает, что «в условиях цифрового мира с всеобщей телекоммуникационной связанностью, вероятно, пора отказаться в определении ОПГ от признака непосредственной связи и личного взаимодействия участников ОПГ» [26. С. 204].

Отметим, что имеются и позитивные примеры адекватного реагирования Законодателя на происходящие изменения, прежде всего – затрагивающие сферу национальной безопасности. Именно, возросшие угрозы от террористической деятельности в определенной степени связаны с тем обстоятельством, что в структуре террористических групп наблюдается переход от иерархического к сетевому принципу [27. С. 80]. Оперативный учет данного обстоятельства проведен в ч. 1 ст. 205.4 УК РФ, в которой дано определение террористического сообщества без указания на признаки его структурированности.

Заключение

Начавшаяся в 2000-е гг. глобальная цифровизация привела к появлению организованных преступных групп, построенных на основе сетевых принципов управления и взаимодействия и в силу этого обладающих конкурентными преимуществами по сравнению с преступными группами с традиционной структурой. В последние годы произошла дальнейшая цифровая трансформация организованной преступной деятельности, проявляющаяся в таком качественно новом явлении, как формирование экосистем преступных сообществ. Это явление означает становление и развитие наиболее высокоорганизованных и опасных форм преступных организаций, специализирующихся на совершении высокотехнологичных преступлений и имеющих межрегиональный и транснациональный характер.

Можно полагать, что данная тенденция в трансформации организованной преступной деятельности в ближайшие десятилетия станет доминирующей в Российской Федерации и других высокоразвитых странах. В связи с этим представляется, что в исследованиях современной организованной преступности *назрел перенос центра внимания на новые явления, проявляющиеся в быстром становлении новых форм организованных групп и преступных сообществ. Такие исследования призваны стать надежной теоретической базой для разработки практических рекомендаций, предназначенных для правоохранительных органов и направленных на эффективное противодействие высокотехнологичной преступной деятельности.*

Примечания

[1] Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы (Утв. Указом Президента Российской Федерации от 09.05.2017 № 203). Ч. 4. Пункт с). URL: http://static.kremlin.ru/media/acts/files/0001201705100002.pdf

[2] Постановление Пленума Верховного Суда РФ от 10 июня 2010 г. № 12 «О судебной практике рассмотрения уголовных дел об организации преступного сообщества (преступной организации) или участии в нем (ней)» // Верховный суд Российской Федерации. URL: https://vsrf.ru/documents/own/33243/ (дата обращения: 24.10.2024).

[3] См.: Приговор Орджоникидзевского районного суда г. Екатеринбурга № 1-22/2014 1-523/2013 от 17.06.2014 по делу № 1-22/2014 // Судебные и нормативные акты РФ. URL: https://sudact.ru/regular/doc/JOwYYTmt8u51/ (дата обращения: 16.01.2024).

[4] См.: Уголовное дело № 1-12/2016 // Архив Центрального районного суда г. Кемерово.

[5] См.: Приговор Якутского городского суда Республики Саха (Якутия) № 1-681/2019 от 26.08.2019 по делу № 1-1462/2018 // Судебные и нормативные акты РФ. URL: https://sudact.ru/regular/doc/8jIATe7oVfNK/ (дата обращения: 16.01.2024).

[6] См.: Приговор Смольнинского районного суда г. Санкт-Петербурга № 1-41/2016 1-501/2015 от 02.02.2016 по делу № 1-41/2016 // Судебные и нормативные акты РФ. URL: https://sudact.ru/regular/doc/VKr2k6rRHcot/ (дата обращения: 16.01.2024).

[7] См.: Уголовное дело № 1-222/2016 // Архив Советского районного суда г. Владивостока.

Список источников

1. Кастельс М. Становление общества сетевых структур // Новая постиндустриальная волна на Западе. Антология / под ред. В.Л. Иноземцева. М. : Academia, 1999. С. 494–505.
2. Ларичев В.Д., Якушева Т.В. Организованная преступность и киберпреступность: вопросы соотношения и законодательного урегулирования // Журнал российского права. 2023. Т. 27, № 3. С. 82–99. doi: 10.12737/jrp.2023.031
3. 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.
4. Раменская Л.А. Применение концепции экосистем в экономико-управленческих исследованиях // Управленец. 2020. Т. 11, № 4. С. 16–27.
5. Зуев С.В. Уголовное судопроизводство как цифровая социальная экосистема // Университетские правовые диалоги «Право и экология» : материалы Междунар. науч.-практ. конфер. Челябинск, 25–26 марта 2021 г. Челябинск : Изд-во Южно-Уральского гос. ун-та (нац. исслед. ун-та), 2021. С. 186–189.
6. Смушкин А.Б. Об экосистеме предварительного расследования // Вестник Томского государственного университета. 2023. № 488. С. 242–247. doi: 10.17223/15617793/488/26
7. Масленникова Л.Н. Концептуальный подход к построению уголовного судопроизводства, обеспечивающего доступ к правосудию в условиях развития цифровых технологий // Вестник Университета им. О.Е. Кутафина (МГЮА). 2020. № 10 (74). С. 52–65. doi: 10.17803/2311-5998.2020.74.10.052-065
8. 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
9. Поляков В.В. Тенденции развития средств совершения высокотехнологичных преступлений // Информационное право. 2023. № 4 (78). С. 26–28. doi: 10.55291/1999-480X-2023-4-26-28
10. Lavorgna A., Antonopoulos G.A. Criminal markets and networks in Cyberspace // Trends Organ Crime. 2022. Vol. 25, Is. 2. P. 145–150. doi: 10.1007/s12117-022-09450-5
11. Третьяков Г.М. Модель «преступление как услуга» в системе способов совершения преступлений с использованием компьютерной техники и информационных технологий // Актуальные проблемы развития правовых институтов в контексте глобальных вызовов : сб. науч. ст. Гродно : ГрГУ, 2024. С. 267–270.
12. Безвершенко Л., Галов Д., Квятковски И. Шифровальщики: кто, как и зачем использует их в 2021 году // АО «Лаборатория Касперского». URL: https://securelist.ru/ransomware-world-in-2021/101425/ (дата обращения: 24.10.2024).
13. Chertoff M., Simon T. The Impact of the Dark Web on Internet Governance and Cyber Security. Centre for International Governance Innovation and Chatham House, 2015. No. 6. February 2015. 8. p. URL: https://www.cigionline.org/sites/default/files/gcig_paper_no6.pdf
14. Дремлюга Р.И., Коробеев А.И. Уголовно-правовая политика в сфере противодействия платформизации преступной деятельности // Всероссийский криминологический журнал. 2022. Т. 16, № 1. С. 47–56. doi: 10.17150/2500-4255.2022.16(1).47-56
15. Савенков А.Н., Россинская Е.Р. Вектор развития криминалистической науки в условиях глобальной цифровизации // Государство и право. 2023. № 5. С. 100–110. doi: 10.31857/S102694520025650-6
16. Яблоков Н.П. Расследование организованной преступной деятельности. М., 2002. 172 с.
17. Скуратов Ю.И., Глазкова Л.В., Грудинин Н.С., Незнамова А.А. Развитие организованной преступности в России: системный анализ // Всероссийский криминологический журнал. 2016. Т. 10, № 4. С. 638–648. doi: 10.17150/2500-4255.2016.10(4).638-648
18. Организованная преступность / под ред. А.И. Долговой, С.В. Дьякова. М., 1989. 352 с.
19. 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
20. Осипенко А.Л. Организованная преступность в сети Интернет // Вестник Воронежского института МВД России. 2012. № 3. С. 10–16.
21. Глушков Е.Л. Сбыт наркотических средств бесконтактным способом посредством сети Интернет: пути выявления и раскрытия // Проблемы правоохранительной деятельности. 2018. № 2. С. 45–53. doi: 10.21681/2226-0692-2019-1-54-60
22. Давыдов С.И., Кондратьев М.В., Поляков В.В. Противодействие транснациональным организованным группам, использующим информационно-коммуникационные технологии для незаконного сбыта наркотических средств // Правоприменение. 2024. Т. 8, № 1. С. 111–120. doi: 10.52468/2542-1514.2024.8(1).111-120
23. Захаров В.Я., Трофимов О.В., Фролов В.Г., Новиков А.В. Управление экосистемой: механизмы интеграции компаний в соответствии с концепцией «Индустрия 4.0» // Лидерство и менеджмент. 2019. Т. 6, № 4. С. 453–468. doi: 10.18334/lim.6.4.41197
24. 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, № 3. P. 30–43.
25. Воронин Ю.А. Анализ феномена организованной преступности в России: криминологические аспекты // Вестник Южно-Уральского государственного университета. Серия: Право. 2017. Т. 17, № 1. С. 12–18. doi: 10.14529/law170102
26. Овчинский В.С. Криминология цифрового мира : учебник. М. : Норма ; ИНФРА-М, 2018. 352 с.
27. Петров В.И. Основные тенденции современного терроризма в условиях глобализации // Вестник Южно-Уральского государственного университета. Серия: Социально-гуманитарные науки. 2007. № 24 (96). С. 78–82.

References

1. Castells, M. (1999) Stanovlenie obshchestva setevykh struktur [Formation of a Society of Network Structures]. In: Inozemtsev, V.L. (ed.) *Novaya postindustrial'naya volna na Zapade. Antologiya* [New Post-Industrial Wave in the West. Anthology]. Moscow: Academia. pp. 494–505.
2. Larichev, V.D. & Yakusheva, T.V. (2023) Organizovannaya prestupnost' i kiberprestupnost': voprosy sootnosheniya i zakonodatel'nogo uregulirovaniya [Organized Crime and Cybercrime: Issues of Relationship and Legislative Regulation]. *Zhurnal rossiyskogo prava*. 3 (27). pp. 82–99. doi: 10.12737/jrp.2023.031
3. Zaytsev, O.A. & Pastukhov, P.S. (2022) Tsifrovoy profil' litsa kak element informatsionno-tekhnologicheskoy strategii rassledovaniya prestupleniy [Digital Facial Profile as an Element of an Information Technology Strategy for Crime Investigation]. *Vestnik Permskogo universiteta. Yuridicheskie nauki*. 56. pp. 281–308. doi: 10.17072/1995-4190-2022-56-281-308
4. Ramenskaya, L.A. (2020) Primenenie kontseptsii ekosistem v ekonomiko-upravlencheskikh issledovaniyakh [Application of the ecosystem concept in economic and managerial research]. *Upravlenets*. 4 (11). pp. 16–27.
5. Zuev, S.V. (2021) [Criminal proceedings as a digital social ecosystem]. *Universitetskie pravovye dialogi "Pravo i ekologiya"* [University Legal Dialogues "Law and Ecology"]. Proceedings of the International Conference. Chelyabinsk. 25–26 March 2021. Chelyabinsk: South Ural State University. pp. 186–189. (In Russian).
6. Smushkin, A.B. (2023) On the ecosystem of the preliminary investigation. *Vestnik Tomskogo gosudarstvennogo universiteta – Tomsk State University Journal*. 488. pp. 242–247. (In Russian). doi: 10.17223/15617793/488/26
7. Maslennikova, L.N. (2020) Kontseptual'nyy podkhod k postroeniyu ugolovnogo sudoproizvodstva, obespechivayushchego dostup k pravosudiyu v usloviyakh razvitiya tsifrovykh tekhnologiy [Conceptual approach to the construction of criminal proceedings ensuring access to justice in the

context of the development of digital technologies]. *Vestnik Universiteta im. O.E. Kutafina (MGYuA)*. 10 (74). pp. 52–65. doi: 10.17803/2311-5998.2020.74.10.052-065
8. Polyakov, V.V. (2023) Ponyatie "vysokotekhnologichnye prestupleniya" v kriminalistike [The concept of "high-tech crimes" in forensic science]. *Kriminalistika: vchera, segodnya, zavtra*. 4. pp. 151–162. doi: 10.55001/2587-9820.2023.19.44.015
9. Polyakov, V.V. (2023) Tendentsii razvitiya sredstv sovershеniya vysokotekhnologichnykh prestupleniy [Trends in the development of means of committing high-tech crimes]. *Informatsionnoe pravo*. 4 (78). pp. 26–28. doi: 10.55291/1999-480X-2023-4-26-28
10. Lavorgna, A., & Antonopoulos, G.A. (2022) Criminal markets and networks in Cyberspace. *Trends Organ Crime*. 2 (25). pp. 145–150. doi: 10.1007/s12117-022-09450-5
11. Tret'yakov, G.M. (2024) Model' "prestuplenie kak usluga" v sisteme sposobov sovershеniya prestupleniy s ispol'zovaniem komp'yuternoy tekhniki i informatsionnykh tekhnologiy [The "crime as a service" model in the system of methods for committing crimes using computer equipment and information technologies]. In: *Aktual'nye problemy razvitiya pravovykh institutov v kontekste global'nykh vyzovov* [Current Problems of Development of Legal Institutions in the Context of Global Challenges]. Grodno: Grodno State University. pp. 267–270.
12. Bezvershenko, L., Galov, D. & Kvyatkovski, I. (2021) Shifroval'shchiki: kto, kak i zachem ispol'zuet ikh v 2021 godu [Ransomware: who, how, and why uses it in 2021]. *Securelist by Kaspersky*. [Online] Available from: https://securelist.ru/ransomware-world-in-2021/101425/ (Accessed: 24.10.2024).
13. Chertoff, M. & Simon, T. (2015) The Impact of the Dark Web on Internet Governance and Cyber Security. *Centre for International Governance Innovation and Chatham House*. 6. [Online] Available from: https://www.cigionline.org/sites/default/files/gcig_paper_no6.pdf.
14. Dremlyuga, R.I. & Korobeev, A.I. (2022) Ugolovno-pravovaya politika v sfere protivodeystviya platformizatsii prestupnoy deyatel'nosti [Criminal legal policy in the sphere of counteracting the platformization of criminal activity]. *Vserossiyskiy kriminologicheskiy zhurnal*. 1 (16). pp. 47–56. doi: 10.17150/2500-4255.2022.16(1).47-56
15. Savenkov, A.N. & Rossinskaya, E.R. (2023) Vektor razvitiya kriminalisticheskoy nauki v usloviyakh global'noy tsifrovizatsii [Vector of development of forensic science in the context of global digitalization]. *Gosudarstvo i pravo*. 5. pp. 100–110. doi: 10.31857/S102694520025650-6
16. Yablokov, N.P. (2002) *Rassledovanie organizovannoy prestupnoy deyatel'nosti* [Investigation of Organized Criminal Activity]. Moscow: Yurist.
17. Skuratov, Yu.I. et al. (2016) Razvitie organizovannoy prestupnosti v Rossii: sistemnyy analiz [Development of organized crime in Russia: systems analysis]. *Vserossiyskiy kriminologicheskiy zhurnal*. 4 (10). pp. 638–648. doi: 10.17150/2500-4255.2016.10(4).638-648
18. Dolgova, A.I. & D'yakov, S.V. (eds) (1989) *Organizovannaya prestupnost'* [Organized Crime]. Moscow: Yuridicheskaya literatura.
19. Polyakov, V.V. (2023) Gruppovaya forma sovershеniya prestupleniy kak odin iz priznakov vysokotekhnologichnoy prestupnosti [Group form of committing crimes as one of the features of high-tech crime]. *Rossiyskiy yuridicheskiy zhurnal*. 1 (148). pp. 117–126. doi: 10.34076/20713797_2023_1_117
20. Osipenko, A.L. (2012) Organizovannaya prestupnost' v seti Internet [Organized Crime on the Internet]. *Vestnik Voronezhskogo instituta MVD Rossii*. 3. pp. 10–16.
21. Glushkov, E.L. (2018) Sbyt narkoticheskikh sredstv beskontaktnym sposobom posredstvom seti Internet: puti vyyavleniya i raskrytiya [Contactless sale of narcotics via the Internet: ways of detection and disclosure]. *Problemy pravookhranitel'noy deyatel'nosti*. 2. pp. 45–53. doi: 10.21681/2226-0692-2019-1-54-60
22. Davydov, S.I., Kondrat'ev, M.V. & Polyakov, V.V. (2024) Protivodeystvie transnatsional'nym organizovannym gruppam, ispol'zuyushchim informatsionno-kommunikatsionnye tekhnologii dlya nezakonnogo sbyta narkoticheskikh sredstv [Counteracting transnational organized groups using information and communication technologies for the illegal sale of narcotic drugs]. *Pravoprimenenie*. 1 (8). pp. 111–120. doi: 10.52468/2542-1514.2024.8(1).111-120
23. Zakharov, V.Ya. et al. (2019) Upravlenie ekosistemoy: mekhanizmy integratsii kompaniy v sootvetstvii s kontseptsiey "Industriya 4.0" [Ecosystem management: mechanisms for integrating companies in accordance with the Industry 4.0 concept]. *Liderstvo i menedzhment*. 4 (6). pp. 453–468. doi: 10.18334/lim.6.4.41197
24. 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 (7). pp. 30–43.
25. Voronin, Yu.A. (2017) Analiz fenomena organizovannoy prestupnosti v Rossii: kriminologicheskie aspekty [Analysis of the phenomenon of organized crime in Russia: criminological aspects]. *Vestnik Yuzhno-Ural'skogo gosudarstvennogo universiteta. Seriya: Pravo*. 1 (17). pp. 12–18. doi: 10.14529/law170102
26. Ovchinskiy, V.S. (2018) *Kriminologiya tsifrovogo mira* [Criminology of the Digital World]. Moscow: Norma; INFRA-M.
27. Petrov, V.I. (2007) Osnovnye tendentsii sovremennogo terrorizma v usloviyakh globalizatsii [Main trends of modern terrorism in the context of globalization]. *Vestnik Yuzhno-Ural'skogo gosudarstvennogo universiteta. Seriya: Sotsial'no-gumanitarnye nauki*. 24 (96). pp. 78–82.

Информация об авторе:
Поляков В.В. – канд. юрид. наук, доцент кафедры уголовного процесса и криминалистики Алтайского государственного университета (Барнаул, Россия). E-mail: agupolyakov@gmail.com

Автор заявляет об отсутствии конфликта интересов.

Information about the author:
V.V. Polyakov, Cand. Sci. (Law), associate professor, Altai State University (Barnaul, Russian Federation). E-mail: agupolyakov@gmail.com

The author declares no conflicts of interests.

Статья поступила в редакцию 06.01.2025;
одобрена после рецензирования 10.02.2025; принята к публикации 28.02.2025.

The article was submitted 06.01.2025;
approved after reviewing 10.02.2025; accepted for publication 28.02.2025.