ISSN 2500-1442

Научная статья
УДК 343.98
EDN YNQHDZ
DOI 10.17150/2500-4255.2024.18(5).494-503

ОСОБЕННОСТИ ЛИЦ, СОВЕРШАЮЩИХ ВЫСОКОТЕХНОЛОГИЧНЫЕ ПРЕСТУПЛЕНИЯ В СОСТАВЕ ОРГАНИЗОВАННЫХ ГРУПП

В.В. Поляков
Алтайский государственный университет, г. Барнаул, Российская Федерация

Информация о статье

Дата поступления
14 марта 2024 г.

Дата принятия в печать
26 ноября 2024 г.

Дата онлайн-размещения
6 декабря 2024 г.

Ключевые слова

Групповые преступления; расследование преступлений; компьютерные преступления; высокотехнологичные преступления; соучастники преступления; организованные преступные группы

Аннотация. Статья посвящена исследованию характерных особенностей лиц, совершающих высокотехнологичные преступления в составе организованных преступных групп и сообществ. Обращено внимание на своеобразие в распределении ролей в таких группах и специфику отличительных черт соучастников этих деяний. Для построения типовых моделей лиц, совершающих высокотехнологичные преступления, в работе использовалась уголовно-правовая типизация членов преступных групп. Отмечена такая важная для нейтрализации противозаконной деятельности особенность организаторов (руководителей) указанных групп, как крайне высокая анонимизация, позволяющая им оставаться лично неизвестными для большинства членов группы и достигаемая с помощью специальных сетевых сервисов и анонимных мессенджеров. Среди соучастников-исполнителей особое внимание уделяется специалистам в сфере цифровых технологий, занимающимся разработкой в преступных целях и применением программно-аппаратных и программных средств преступления. Наличие в преступной группе таких специалистов является необходимым условием для совершения высокотехнологичного преступления. На основе анализа материалов судебно-следственной практики показано, что зачастую эти лица обладают, наряду с высоким уровнем профессиональных знаний и навыков, невысоким общекультурным уровнем и слабыми морально-волевыми качествами. Среди соучастников-пособников выделена отдельная группа инсайдеров, связанных с организацией, подвергшейся дистанционному посягательству, соучастников высокотехнологичных преступлений, обусловленных специализацией организованной группы. В качестве одной из таких специализаций рассмотрено бесконтактное распространение наркотических средств с использованием информационно-телекоммуникационных сетей. Приведены характерные особенности лиц — участников групп, специализирующихся на использовании в противоправных целях методов и технологий социальной инженерии. Для исследования личностных качеств участников указанных групп, сформированных по этническому принципу, предложено учитывать явление глокализации организованной преступной деятельности, проявляющееся наряду и одновременно с процессами ее глобализации. Полученные в настоящей работе результаты призваны способствовать преодолению негативных факторов, усложняющих расследование и предупреждение высокотехнологичных преступлений.

Original article

SPECIFIC FEATURES OF PERSONS COMMITTING HIGH-TECH CRIMES IN AN ORGANIZED GROUP

Vitaly V. Polyakov
Altai State University, Barnaul, the Russian Federation

Article info

Received
2024 March 14

Accepted
2024 November 26

Available online
2024 December 6

Abstract. The author examines specific features of persons who commit high tech crimes in an organized criminal group or community. Special attention is paid to the distribution of roles in such groups, as well as the specific distinctive features of accomplices involved in these actions. The author used the criminal law typification of criminal group members to construct typical models of persons who commit high tech crimes. It is noted that the feature crucial for the neutralization of unlawful actions of the organizers (leaders) of such groups is their extreme anonymization, which allows them to stay unknown to most members of the group; this is achieved through special online services or anonymous messengers. Regarding accomplices-perpetrators,

Keywords
Group crimes; crime investigation; computer crimes; high-tech crimes; accomplices in a crime; organized criminal groups

special attention is paid to digital technology specialists who develop and use hardware and software means of committing crimes. The presence of such specialists in a criminal group is a necessary condition for committing high tech crimes. The analysis of court and investigation practice shows that such persons, while having a high level of professional knowledge and skills, are often characterized by a low level of general culture and weak moral and volition qualities. Regarding accomplices-abettors, the author singles out a special group of insiders connected with the organizations that became the target of a distance assault, accomplices of high-tech crimes driven by the specialization of the organized group. One of such analyzed specializations is the contactless sale of narcotic substances through information-telecommunication networks. The author presents specific features of group participants specializing in the unlawful use of methods and technologies of social engineering. It is suggested that, in order to research the personal qualities of the participants of such groups based on the ethnic principles, the phenomenon of glocalization of organized criminal activities should be taken into account, as it is manifested together and simultaneously with the processes of their globalization. The obtained results should contribute to overcoming the negative factors that hinder the investigation and prevention of high-tech crimes.

Введение

В 2000-е гг. произошли качественные изменения в организованной преступной деятельности, проявившиеся в появлении и быстром распространении организованных преступных групп и сообществ, использующих для совершения преступных посягательств информационно-телекоммуникационные технологии. Отличительными признаками совершаемых ими высокотехнологичных преступлений являются: дистанционный характер доступа к объекту посягательства с помощью информационных сетей; использование специально разработанных в криминальных целях программных, программно-аппаратных и аппаратных средств преступления; обязательное наличие тщательной подготовки к преступлению и действий по сокрытию его следов; а также активное противодействие расследованию.

Для характеристики организованных преступных групп, специализирующихся на совершении высокотехнологичных преступлений, требуется определенный пересмотр традиционных подходов [1; 2, с. 288; 3, с. 87]. В полной мере это относится к составу и распределению ролей между участниками таких групп. В силу высокой сложности технологий, используемых при совершении этих преступлений, в состав преступных групп включаются участники, представленные, как показали А.Н. Савенков и Е.Р. Россинская, разными типами лиц [1, с. 105] и выполняющие существенно разные роли. Эти обстоятельства затрудняют противодействие высокотехнологичным преступлениям, выдвигая на первый план решение таких задач, как выявление организационной структуры группы и специфических ролей ее участников, установление особенностей организаторов и руководителей, индивидуализация вины соучастников [4, с. 118].

Таким образом, новой и актуальной задачей, направленной на противодействие современной организованной противоправной деятельности, является выявление специфических черт лиц, совершающих высокотехнологичные преступления в составе организованных преступных групп.

Типовые модели лиц, совершающих высокотехнологичные преступления

Классификация соучастников высокотехнологичного преступления может проводиться по различным основаниям, отражающим выполняемые участниками роли и решаемые ими задачи. В то же время в качестве основы всех возможных классификаций выступает уголовно-правовая типизация, исходящая из четырех видов соучастия, представленных в ст. 33 УК РФ: организаторы, исполнители, подстрекатели и пособники. Выделение характерных черт, отражающих важнейшие особенности лиц, входящих в эти четыре группы, производится путем обобщения данных имеющейся судебно-следственной практики. Полагаем, что получаемые в результате такого обобщения результаты могут рассматриваться как типовые криминалистические модели лиц, отражающие особенности тех или иных групп соучастников. Такая трактовка успешно применялась, в частности, Н.И. Малыхиной при систематизации лиц, совершивших преступление, в составе определенных групп [5, с. 143].

Модель лица, участвующего в совершении высокотехнологичного преступления, представ-

ляет собой систему взаимосвязанных и взаимообусловленных данных, состоящую, во-первых, из сведений общего характера, таких как возраст, пол, образование, психофизические особенности, волевые качества и т.д. [6, с. 156], во-вторых, из сведений, характерных именно для участников групп, специализирующихся на совершении таких преступных деяний (например, опыт в использовании компьютерных устройств, профессиональные знания в сфере защиты информации и программировании и т.п.). Необходимость учета наравне с техническими элементами «человеческого фактора киберпреступности» отмечалась и в зарубежной литературе [7, с. 496]. Построение таких моделей в условиях исследуемой проблематики сопряжено с рядом дополнительных трудностей. Эти трудности имеют объективный характер и связаны с неизбежным отставанием академических исследований от изменений, происходящих вследствие качественной трансформации противоправной деятельности [8, с. 97; 9, с. 220], а также с высокой латентностью высокотехнологичных преступлений [10], снижающей репрезентативность данных судебно-следственной практики и тем самым препятствующей теоретическим обобщениям.

Сложность расследования и предупреждения высокотехнологичных преступлений приводит к тому, что среди преступных деяний, связанных с использованием информационных технологий, раскрываются в первую очередь не высокотехнологичные, а наиболее простые виды преступлений. Как следствие, данные предварительного расследования и судебного разбирательства прежде всего относятся к лицам, совершившим такие преступления. Именно для них были достаточно надежно установлены отличительные особенности, описанные, в частности, В.В. Евдокимовым в отношении «среднестатистического хакера» [11, с. 89] и в публикациях других авторов [12; 13].

В то же время характерные особенности лиц, совершающих высокотехнологичные преступления в составе организованных преступных групп и сообществ, обладают весьма существенной спецификой и практически не изучены. Опишем возможные модели этих лиц, типизированные в соответствии с уголовно-правовыми видами соучастия.

Характерные особенности соучастников высокотехнологичного преступления

Организаторы. Исследование характерных черт лица, являющегося организатором (руководителем) преступной группы, имеет крайне важное значение для эффективности расследования. Как справедливо отмечала А.В. Бутырская, установление личностных качеств организатора требуется для установления самого факта создания такой группы [14, с. 38]. Более того, проведенный нами анализ судебно-следственной практики показал, что нейтрализация только руководства организованной преступной группы, специализирующейся на совершении высокотехнологичных преступлений, может привести к полной ликвидации деятельности всей группы. В противном случае даже привлечение к уголовной ответственности значительной части остальных соучастников не препятствует последующей регенерации группы[1].

В качестве типичных черт руководителя организованной группы, совершающей высокотехнологичные преступления, можно привести характеристику Ш., создавшего группу, совершавшую хищения денежных средств из банкоматов с помощью скимминговых устройств. Согласно приговору суда, Ш. обладал «настойчивостью, целеустремленностью, коммуникабельностью, организаторскими качествами, способностью влиять на волю других людей», умел «ориентироваться и принимать решения в сложных ситуациях, действуя из корыстных побуждений»[2]. Вследствие подобных особенностей личности выявление руководителей и доказывание их роли является одной из наиболее сложных задач.

Значителен негативный вклад от такой специфики высокотехнологичных преступлений, как высокая анонимизация участников преступных групп [15], достигаемая за счет использования сервисов Даркнет [16], VPN-сервисов, технологий TOR, анонимных децентрализованных сетей и виртуальных машин. Наконец, руководители транснациональных организованных групп зачастую находятся за пределами Российской Федерации, осуществляя руководство с помощью анонимных мессенджеров[3].

Как следствие, в случае высокотехнологичных преступлений руководителей организованных преступных групп и сообществ далеко не

[1] Приговор Смольнинского районного суда г. Санкт-Петербурга № 1-41/2016 1-501/2015 от 02.02.2016 г. по делу № 1-41/2016 // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru/regular/doc/VKr2k6rRHcot (дата обращения: 15.03.2024).

[2] Уголовное дело № 1-329/2013 // Архив Центрального районного суда г. Барнаула.

[3] Там же.

всегда удается установить и привлечь к уголовной ответственности. Нужно признать, что более типичными являются случаи[4], когда уголовные дела возбуждаются в отношении рядовых участников, а руководители остаются неустановленными следствием.

Исполнители. Лица, участвующие в высокотехнологичной преступной деятельности в качестве исполнителей, могут выполнять различные роли и решать широкий круг конкретных задач: подготавливать средства преступления, осуществлять его непосредственное совершение и сокрытие следов, а также выполнять ряд других функциональных обязанностей. Для большинства соучастников-исполнителей справедливо мнение, согласно которому мотивом участия в преступной группе является личная материальная выгода, при этом нравственность и правовое сознание «деформировано или ослаблено» [11, с. 87]. Полагаем, что среди исполнителей ключевую роль в осуществлении именно высокотехнологичных преступлений играют специалисты в области информационных технологий, владеющие знаниями и навыками, позволяющими применять, разрабатывать новые и модифицировать в преступных целях имеющиеся программные, программно-аппаратные и аппаратные средства преступлений.

После появления преступлений, основанных на использовании компьютерных технологий, в конце 90-х гг. возникли и в 2000-х гг. оформились определенные представления о лицах, совершающих эти преступные деяния. Они характеризовались как «увлеченные компьютерной техникой лица, преимущественно из числа молодежи» [12, с. 180]. Утверждалось, что «они весьма любознательны, обладают незаурядным интеллектом» [12, с. 181], что «эти люди, как правило, являются яркими, мыслящими личностями» [13, с. 115] и т.д. Однако проведенное нами исследование материалов уголовных дел показывает, что специалисты в сфере компьютерных технологий, участвующие в составе организованных преступных групп, в большинстве случаев отличаются совершенно иными личностными качествами. Для таких лиц, действительно, характерен высокий уровень профессиональных знаний в области разработки компьютерных программ, главным образом вредоносных, и программно-аппаратных средств, они свободно владеют международным компьютерным сленгом, склонны к самообразованию в сфере цифровых технологий, быстро перенимают новейшие достижения в этой сфере. В то же время, как показал анализ их переписки, им свойственен низкий общекультурный уровень, что находит свое отражение во множестве элементарных грамматических ошибок, примитивной лексике, постоянном использовании нецензурных выражений. Анализ материалов уголовных дел, прежде всего протоколов допросов, свидетельствует о весьма слабых морально-волевых качествах, что находит свое отражение в неспособности выстроить убедительную и непротиворечивую систему защиты. Характерным для этой группы исполнителей является то, что с целью смягчения уголовной ответственности они при предъявлении обвинения обычно дают признательные показания и помогают изобличению руководителей и других соучастников преступления. Кроме того, указанные лица на предварительном следствии достаточно часто ходатайствуют о заключении досудебного соглашения о сотрудничестве (гл. 40.1 УПК РФ), что существенно способствует успеху расследования.

Вот ряд достаточно типичных примеров, иллюстрирующих приведенную характеристику. Н., разрабатывавший по заказу руководства организованной преступной группы оригинальное вредоносное программное обеспечение, в ходе предварительной проверки пытался исказить обстоятельства преступления, но при допросах в качестве подозреваемого объяснил свое поведение сильным волнением и дал подробные показания по существу предъявленного ему обвинения. Само уголовное дело рассматривалось согласно ст. 314 УПК РФ в особом порядке[5]. Другой пример — уголовное дело, возбужденное в отношении Р. по обвинению в мошенничестве в сфере компьютерной информации (ст. 159.6 УК РФ). Р., будучи участником организованной преступной группы, согласно отведенной ему роли отвечал за нейтрализацию программных средств компьютерной защиты объектов преступного посягательства (коммерческих организаций). В процессе предварительного расследования с ним было заключено досудебное соглашение о сотрудничестве, и уголовное дело

[4] Приговор Якутского городского суда Республики Саха (Якутия) № 1-681/2019 от 26.08.2019 г. по делу № 1-1462/2018 // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru/regular/doc/8jIATe7oVfNK (дата обращения: 15.03.2024).

[5] Уголовное дело №1-411/2017 // Архив Феодосийского городского суда Республики Крым.

рассматривалось в особом порядке принятия судебного решения (гл. 40.1 УПК РФ)[6].

Пособники. Согласно «Конвенции против транснациональной организованной преступности», в случае преступлений, совершаемых организованными группами, умышленные пособничество и подстрекательство рассматриваются как уголовно наказуемые деяния[7]. При этом в отечественной научной литературе доминирует позиция, что лицо, непосредственно не входящее в такую группу, но оказывавшее помощь в совершении преступления, должно рассматриваться как пособник [17, с. 15].

Наиболее значимую помощь в совершении высокотехнологичных преступлений оказывают пособники, связанные с организациями — жертвами преступных посягательств. Это так называемые инсайдеры, обладающие информацией о деятельности и средствах защиты организации. Согласно данным, приводимым Ю.В. Трунцевским, максимальную угрозу создает инсайдерская деятельность сотрудников, связанных с обслуживанием корпоративных сетей организации и обеспечением ее информационной безопасности, поскольку они обладают наибольшими профессиональными знаниями и возможностями для содействия преступлениям [18, с. 20]. Вывод о значительном вкладе инсайдеров в пособничество подтверждается проведенным нами анализом материалов судебно-следственной практики, содержащей многочисленные сведения в отношении лиц, трудоустроенных в коммерческих организациях, в которых они имели доступ к охраняемой законом компьютерной информации[8].

Отметим также, что в роли пособников могут выступать собственники и администраторы цифровых платформ, действующих в сети Даркнет и предоставляющих на условиях анонимности сетевые сервисы, базы данных и различные информационные ресурсы для совершения высокотехнологичных преступлений. Как отмечают M. Chertoff и T. Simon, такие цифровые платформы могут использоваться преступными сообществами для совершения большого числа различных незаконных действий [19, p. 6]. Кроме того, пособники могут участвовать в уничтожении следов уже совершенного преступления, например, удаляя криминалистически значимую информацию об использовании виртуальных машин.

Подстрекатели. Участие подстрекателей выражается в склонении других лиц к участию в преступной деятельности [16; 20]. В случае высокотехнологичных преступлений действия подстрекателей могут проявляться в виде целенаправленного воздействия на молодых специалистов в сфере компьютерных технологий, имеющих склонность к девиантному поведению и желающих получать большие доходы. Отметим, что соответствующие действия могут проводиться не только путем непосредственного общения, но и анонимно на закрытых форумах и цифровых платформах. Подстрекатели достаточно часто привлекаются для вербовки специалистов в сфере цифровых технологий, которые нужны для выполнения технически сложных задач, например, для проведения целевых атак. Подстрекатели обычно ищут специалистов-исполнителей среди молодых меркантильных людей, отличающихся девиантным поведением. В дальнейшем лица, привлеченные подстрекателями к соучастию в преступлении, могут принуждаться к продолжению противоправных действий с помощью криминальных связей и угроз.

Особенности личности соучастников преступления в специализированных организованных преступных группах

Наибольшую сложность вызывает расследование преступлений, совершаемых организованными группами и преступными сообществами, отличающимися специализацией этой деятельности. В таком случае установление организаторов, исполнителей, пособников наиболее затруднено и требует большого объема оперативно-технических, оперативно-розыскных и следственных мероприятий.

[6] Приговор Железнодорожного районного суда г. Красноярска № 1-325/2015 от 28.09.2015 по делу № 1-325/2015 // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru/regular/doc/9kMFPk1qxOrr (дата обращения: 15.03.2024).

[7] Конвенция против транснациональной организованной преступности : принята 15.11.2000 г. Резолюцией 55/25 на 62-м пленар. заседании 55-й сессии Генер. Ассамблеи ООН. П. 1b ст. 5. URL: https://www.un.org/ru/documents/decl_conv/conventions/ orgcrime.shtml (дата обращения: 15.03.2024).

[8] Приговор Орджоникидзевского районного суда г. Екатеринбурга № 1-405/2012 1-405/2017 от 25.07.2017 г. по делу № 1-405/2012 // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru/regular/doc/89NiHUPYjCWw (дата обращения: 15.03.2024) ; Приговор Звениговского районного суда Республики Марий Эл № 1-21/2015 от 25.06.2015 г. по делу № 1-21/2015 // Там же. URL: https://sudact.ru/regular/doc/35dUap3XPB5R (дата обращения: 15.03.2024).

Преступные группы, осуществляющие сбыт наркотических средств. Дистанционные способы распространения наркотических веществ, основанные на использовании информационно-телекоммуникационных сетей, совершаются, как правило, организованными преступными группами с детальным распределением ролей между соучастниками преступления. Это обусловлено обеспечением функционирования сложной организационно-технической инфраструктуры, создаваемой такими группами, и привлечением передовых информационных разработок [21, с. 47]. Именно использование указанных разработок является важнейшей особенностью современного наркобизнеса [22, с. 183]. В таких группах достигается весьма высокая степень анонимизации соучастников, при которой рядовые исполнители, как правило, непосредственно не знакомы ни с организаторами, ни друг с другом.

В преступных сообществах, специализирующихся в распространении наркотических средств с помощью информационных сетей, имеет место специфическое распределение ролей соучастников преступления. Одни соучастники заказывают и получают наркотические вещества, другие их фасуют и распределяют на отдельные партии, третьи передают мелкооптовым торговцам и т.д. В качестве типичного примера можно привести уголовное дело в отношении участников преступного сообщества, выявленных и осужденных за совершение особо тяжких преступлений по ч. 2 ст. 210, ч. 3 ст. 228.1 и ч. 3 ст. 174.1 УК РФ[9].

Знание типичных особенностей личности сбытчиков наркотических средств представляет несомненную ценность для выявления используемых способов подготовки, совершения и сокрытия наркопреступлений, для планирования и организации оперативно-розыскных мероприятий и выбора тактики следственных действий [23, с. 115]. Проведенный анализ материалов уголовных дел позволяет установить характерные черты лиц, выступающих в роли исполнителей, непосредственно сбывающих наркотики. В большинстве случаев ими являются молодые люди в возрасте от 18 до 30 лет, при этом успешно ориентирующиеся в таких возможностях современной банковской системы, как осуществление безналичных финансовых операций с помощью электронных средств платежа.

Отдельно нужно отметить, что вербовка таких исполнителей, находящихся на нижнем уровне преступной иерархии, все чаще осуществляется также с использованием информационно-телекоммуникационных сетей. Для иллюстрации можно привести следующий типичный пример. Ш. подыскивал работу с помощью сети Интернет и получил от не установленного следствием лица предложение участвовать в бесконтактном сбыте наркотических средств. После того как Ш. дал согласие, с ним осуществил анонимное общение другой участник организованной преступной группы, представившийся «оператором» по г. Кемерово. Далее этот участник направлял Ш. по анонимному мессенджеру сообщения с указанием местонахождения наркотических средств, которые Ш. размещал в тайниках и затем высылал «оператору» фотографии тайников с их адресами[10].

Преступные группы, использующие технологии социальной инженерии. В последние годы в России и за рубежом произошло стремительное распространение преступных посягательств, в которых используются технологии социальной инженерии [24, с. 83; 25]. В силу этого заслуживают отдельного исследования специфические черты лиц, совершающих эти деяния.

Для участников преступных групп, специализирующихся на применении технологий социальной инженерии, характерна достаточно узкая специализация с выполнением «определенных ролей (моделей поведения)» [26, с. 91]. Эта специализация достигается на этапе подготовки незаконного деяния путем разработки типовых сценариев общения с жертвами посягательства, включающих в себя овладение начальными познаниями в сфере соответствующей деятельности [27, с. 7], например, знаниями организационной структуры и правил функционирования финансовых организаций или правоохранительных органов, навыками достаточно свободного владения профессиональной терминологией, умением импровизировать в зависимости от развивающейся при общении ситуации.

Особая роль отводится работникам коммерческих и государственных организаций, подвергшихся преступному посягательству. Эти работники, и прежде всего те из них, кто не обладает необходимыми знаниями в сфере защиты компьютерной информации, непреднамеренно открывают в корпоративной сети организации заинтересовавшие их фишинговые письма, содержащие вредоносные программы, перехо-

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

[10] Уголовное дело № 1-454/2017 // Там же.

дят на зараженные веб-сайты в соответствии со специально направленными им ссылками [28] и т.п., тем самым обеспечивая преступникам преодоление средств защиты компьютерной информации. Представляется, что эти лица, не имеющие злого умысла и не понимающие своего вклада в преступную деятельность, выполняют своеобразную роль «невольных пособников» преступления.

Этнические преступные группы. Самостоятельной и малоизученной задачей является выявление характерных особенностей членов организованных групп, совершающих высокотехнологичные преступления и организованных на этнической основе. Формирование этнических преступных групп, как подчеркивают А.Г. Ахмедов и Т.О. Бозиев, происходит путем выстраивания системы связей, предусматривающей «разграничение функций и полномочий» [29, с. 95]. Эти обстоятельства вносят дополнительные сложности в организацию расследования и доказывание совершенных преступлений.

Среди исследованных нами материалов судебно-следственной практики в качестве достаточно типичного можно привести следующее уголовное дело. С целью незаконного обогащения Ф., пользующийся повышенным доверием со стороны сограждан узбекской диаспоры, создал группу, сформированную по признаку национальности из уроженцев Республики Узбекистан. Этой группой совершались преступные деяния, выражавшиеся в виде неправомерного доступа к компьютерной информации, содержащейся в фискальной памяти контрольно-кассовых машин (ч. 3 ст. 272 УК РФ). По итогам судебного разбирательства суд указал, что формирование по этническому принципу смогло обеспечить «общность интересов, единообразие моральных принципов и образа мышления, а также в силу национальных особенностей способствовало устойчивости»[11].

Полагаем, что при исследовании характерных черт лиц, состоящих в современных этнических преступных группах, необходимо учитывать появление новых процессов, влияющих на трансформацию противоправной деятельности в условиях цифровизации общества. К ним, на наш взгляд, нужно в первую очередь отнести процессы глокализации, развивающиеся одновременно и наряду с процессами глобализации организованной преступности и приводящие к усилению региональных различий в деятельности незаконных формирований. Такой подход успешно применили E. Van Hellemont и J. Densley при исследовании характерных особенностей лиц, входивших в состав этнических преступных групп [30]. Представляется, что выявление специфики участников указанных групп, действующих в Российской Федерации, учитывающее процессы глокализации, является одной из новых задач, требующих своего решения.

Выводы

Цифровая революция одним из своих следствий вызвала качественную трансформацию преступной деятельности, проявившуюся в появлении организованных групп, совершающих высокотехнологичные преступления и характеризующихся своеобразным распределением ролей и спецификой отличительных черт соучастников таких деяний.

В соответствии с уголовно-правовой типизацией описаны отличительные особенности лиц, совершающих в составе преступных групп высокотехнологичные преступления. Важной отличительной особенностью руководителей этих групп является исключительно высокая анонимизация, достигаемая путем использования анонимных сетевых технологий и сервисов. Среди лиц, выступающих в качестве исполнителей, выделена группа специалистов в области компьютерных технологий, характерная именно для высокотехнологичных преступлений. Сделан вывод, что для этих лиц характерен, наряду с наличием профессиональных знаний, низкий общекультурный уровень и слабые морально-волевые качества. При рассмотрении пособников обращено внимание на роль инсайдеров, обладающих информацией о средствах защиты объекта незаконного посягательства.

Описаны роли и характерные черты лиц, связанные со специализацией организованных групп, совершающих бесконтактное распространение наркотических веществ. Выявлена ролевая специфика членов групп, практикующих преступные посягательства, основанные на технологиях социальной инженерии. Отмечено своеобразие личностных качеств участников этнических группировок и обращено внимание на важность учета такого нового явления, как глокализация преступной деятельности.

[11] Приговор Перовского районного суда г. Москвы № 1-975/2014 от 10.10.2016 г. по делу № 1-975/2014 // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru/regular/doc/t73YIZLoVMQJ (дата обращения: 15.03.2024).

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Савенков А.Н. Вектор развития криминалистической науки в условиях глобальной цифровизации / А.Н. Савенков, Е.Р. Россинская. — DOI https://doi.org /10.31857/S102694520025650-6. — EDN WRFJCQ // Государство и право. — 2023. — № 5. — С. 100–110.

2. Leukfeldt E.R. Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime / E.R. Leukfeldt, A. Lavorgna, E.R. Kleemans. — DOI 10.1007/s10610-016-9332-z // European Journal on Criminal Policy and Research. — 2017. — Vol. 23, iss. 3. — P. 287–300.

3. Поляков В.В. Источники и принципы формирования частной методики расследования высокотехнологичных преступлений / В.В. Поляков. — DOI 10.17803/1729-5920.2022.187.6.085-096. — EDN UQUDGM // Lex russica. — 2022. — Т. 75, № 6. — С. 85–96.

4. Поляков В.В. Групповая форма совершения преступлений как один из признаков высокотехнологичной преступности / В.В. Поляков. — DOI 10.34076/20713797_2023_1_117. — EDN KPAJNY // Российский юридический журнал. — 2023. — № 1 (148). — С. 117–126.

5. Малыхина Н.И. Особенности построения модели лица, совершившего преступление / Н.И. Малыхина. — EDN ULNPBT // Правовое государство: теория и практика. — 2015. — № 3 (41). — С. 141–144.

6. Сибилькова А.В. Криминалистическое моделирование личности неизвестного преступника / А.В. Сибилькова. — DOI 10.17803/1994-1471.2016.64.3.152-160. — EDN VVBSPN // Актуальные проблемы российского права. — 2016. — № 3 (64). — С. 152–160.

7. Bossler A.M. Introduction: New Directions in Cybercrime Research / A.M. Bossler, T. Berenblum. — DOI 10.1080/0735648X.2019.1692426 // Journal of Crime and Justice. — 2019. — Vol. 42, No. 5. — P. 495–499.

8. Лопашенко Н.А. О кризисе российского уголовного права (перечитывая А.Э. Жалинского) / Н.А. Лопашенко. — DOI 10.31857/S102694520027656-2 // Государство и право. — 2023. — № 9. — С. 97–111.

9. Тишутина И.В. Современные проблемы криминалистической методики в свете идей профессора Н.П. Яблокова / И.В. Тишутина. — DOI 10.55001/2587-9820.2023.35.47.020. — EDN AOJCLR // Криминалистика: вчера, сегодня, завтра. — 2023. — Т. 25, № 1. — С. 218–226.

10. Dupont B. Enhancing the Effectiveness of Cybercrime Prevention Through Policy Monitoring / B. Dupont. — DOI 10.1080/0735648X.2019.1691855 // Journal of Crime and Justice. — 2019. — Vol. 42, iss. 5. — P. 500–515.

11. Евдокимов К.Н. Особенности личности преступника, совершающего неправомерный доступ к компьютерной информации (на примере Иркутской области) / К.Н. Евдокимов. — EDN NDIGVX // Сибирский юридический вестник. — 2011. — № 1. — С. 86–90.

12. Мегрелишвили Г.Т. Криминологический и психологический портрет личности преступников в сфере высоких технологий / Г.Т. Мегрелишвили. — EDN KHNGHL // Вестник Томского государственного университета. — 2007. — № 299. — С. 180–181.

13. Маслакова Е.А. Лица, совершающие преступления в сфере информационных технологий: криминологическая характеристика / Е.А. Маслакова. — EDN SFPTEN // Среднерусский вестник общественных наук. — 2014. — № 1 (31). — С. 114–121.

14. Бутырская А.В. Значение исследования личности организатора преступного сообщества (преступной организации) в процессе расследования / А.В. Бутырская. — EDN QAVVUV // Российский следователь. — 2013. — № 10. — С. 38–40.

15. Сергеев С.М. Некоторые проблемы противодействия использованию в преступной деятельности средств обеспечения анонимизации пользователя в сети Интернет / С.М. Сергеев. — EDN ZDUGUF // Вестник Санкт-Петербургского университета МВД России. — 2017. — № 1 (73). — С. 137–140.

16. Смушкин А.Б. Криминалистические аспекты исследования даркнета в целях расследования преступлений / А.Б. Смушкин. — DOI 10.17803/1994-1471.2022.136.3.102-111. — EDN WEFQBU // Актуальные проблемы российского права. — 2022. — Т. 17, № 3. — С. 102–111.

17. Овчинникова Г.В. Комментарий к постановлению Пленума Верховного Суда РФ «О судебной практике рассмотрения уголовных дел об организации преступного сообщества (преступной организации) или участии в нем (ней)» от 10 июня 2010 года № 12 / Г.В. Овчинникова. — Санкт-Петербург : С.-Петерб. юрид. ин-т (фил.) Акад. Генер. прокуратуры Рос. Федерации, 2011. — 31 с. — EDN QSGPGN.

18. Трунцевский Ю.В. Киберпреступления в корпоративной среде: риски, оценка и меры предупреждения / Ю.В. Трунцевский. — EDN RAXGMJ // Российский следователь. — 2014. — № 21. — С. 19–22.

19. Chertoff M. The Impact of the Dark Web on Internet Governance and Cyber Security / M. Chertoff, T. Simon // Centre for International Governance Innovation and Chatham House. Paper Series. — 2015. — No. 6. — P. 1–8.

20. Саблина М.А. Подстрекательство: терминологический и квалификационный аспекты / М.А. Саблина. — DOI 10.17323/2072-8166.2016.4.129.139. — EDN XRJWCV // Право. Журнал Высшей школы экономики. — 2016. — № 4. — С. 129–139.

21. Глушков Е.Л. Сбыт наркотических средств бесконтактным способом посредством сети Интернет: пути выявления и раскрытия / Е.Л. Глушков. — EDN XTXKZN // Проблемы правоохранительной деятельности. — 2018. — № 2. — С. 45–53.

22. Осипенко А.Л. Организованная преступная деятельность в киберпространстве: тенденции и противодействие / А.Л. Осипенко // Юридическая наука и практика: Вестник Нижегородской академии МВД России. — 2017. — № 4 (40). — С. 181–188.

23. Давыдов С.И. Противодействие транснациональным организованным группам, использующим информационно-коммуникационные технологии для незаконного сбыта наркотических средств / С.И. Давыдов, М.В. Кондратьев, В.В. Поляков. — DOI 10.52468/2542-1514.2024.8(1).111-120 // Правоприменение. — 2024. — Т. 8, № 1. — С. 111–120.

24. Давыдов В.О. Об актуальных проблемах криминалистического обеспечения раскрытия и расследования мошенничеств, совершенных с использованием информационно-телекоммуникационных технологий / В.О. Давыдов, И.В. Тишутина. — DOI 10.24411/2587-9820-2020-10030 // Криминалистика: вчера, сегодня, завтра. — 2020. — № 2 (14). — С. 81–91.

25. Поляков В.В. Применение методов социальной инженерии при совершении высокотехнологичных преступлений / В.В. Поляков. — DOI 10.55001/2587-9820.2023.81.15.018 // Криминалистика: вчера, сегодня, завтра. — 2023. — № 3 (27). — С. 175–188.

26. Старостенко Н.И. Криминалистическая характеристика личности преступника, совершающего хищения с применением методов социальной инженерии / Н.И. Старостенко // Вестник Краснодарского университета МВД России. — 2022. — № 4 (58). — С. 89–95.

27. Головин А.Ю. Социальная инженерия в механизме преступной деятельности в сфере информационно телекоммуникационных технологий / А.Ю. Головин, Е.В. Головина. — DOI 10.24412/2071-6184-2021-2-3-13 // Известия Тульского государственного университета. Экономические и юридические науки. — 2021. — № 2. — С. 3–13.

28. Сабырбаева А.Б. О мерах по противодействию мошенничеству (на примере фишинга) / А.Б. Сабырбаева. — DOI 10.31857/S102694520017465-2 // Государство и право. — 2021. — № 1. — С. 181–185.

29. Ахмедов А.Г. Организованная этническая преступность: оперативно-розыскная характеристика, тенденция, вопросы, требующие разрешения / А.Г. Ахмедов, Т.О. Бозиев. — DOI 10.35750/2071-8284-2022-1-89-97. — EDN VYTJWK // Вестник Санкт-Петербургского университета МВД России. — 2022. — № 1 (93). — С. 89–97.

30. Van Hellemont E. Gang Glocalization: How a Global Mediascape Creates and Shapes Local Gang Realities / E. Van Hellemont, J.A. Densley. — DOI 10.1177/1741659018760107 // Crime, Media, Culture: An International Journal. — 2019. — Vol. 15, iss. 1. — P. 169–189.

REFERENCES

1. Savenkov A.N., Rossinskaya E.R. The Development Vector of Criminalistic Science in the Conditions of Global Digitalization. *Gosudarstvo i pravo = State and Law*, 2023, no. 5, pp. 100–110. (In Russian). EDN: WRFJCQ. DOI: https://doi.org /10.31857/S102694520025650-6.

2. Leukfeldt E.R., Lavorgna A., Kleemans E.R. Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime. *European Journal on Criminal Policy and Research*, 2017, vol. 23, iss. 3, pp. 287–300. DOI: 10.1007/s10610-016-9332-z.

3. Polyakov V.V. Sources and Principles of Private Methods Development for High-Tech Crimes Investigation. *Lex Russica*, 2022, vol. 75, no. 6, pp. 85–69. (In Russian). EDN: UQUDGM. DOI: 10.17803/1729-5920.2022.187.6.085-096.

4. Polyakov V. A Group Form of Committing Crimes as one of the Signs of High-Tech Crimes. *Rossiiskii yuridicheskii zhurnal = Russian Law Journal*, 2023, no. 1, pp. 117–126. (In Russian). EDN: KPAJNY. DOI: 10.34076/20713797_2023_1_117.

5. Malykhina N.I. Peculiarities of Building the Offender Model. *Pravovoe gosudarstvo: teoriya i praktika = The Rule-of-Law State: Theory and Practice*, 2015, no. 3, pp. 141–144. (In Russian). EDN: ULNPBT.

6. Sibilkova A.V. Forensic Modelling of an Unknown Criminal Personality. *Aktual'nye problemy rossiiskogo prava = Topical Problems of Russian Law*, 2016, no. 3, pp. 152–160. (In Russian). EDN: VVBSPN. DOI: 10.17803/1994-1471.2016.64.3.152-160.

7. Bossler A.M., Berenblum T. Introduction: New Directions in Cybercrime Research. *Journal of Crime and Justice*, 2019, vol. 42, no. 5, pp. 495–499. DOI: 10.1080/0735648X.2019.1692426.

8. Lopashenko N.O. On The Crisis of Russian Criminal Law (Re-Reading A.E. Zhalinsky). *Gosudarstvo i pravo = State and Law*, 2023, no. 9, pp. 97–111. (In Russian). DOI: 10.31857/S102694520027656-2.

9. Tishutina I.V. Modern Problems of Criminalistic Methodology in the Light of Professor N.P. Yablokov's Ideas. *Kriminalistika: vchera, segodnya, zavtra = Criminalistics: Yesterday, Today, Tomorrow*, 2023, vol. 25, no. 1. Pp. 218–226. (In Russian). EDN: AOJCLR. DOI: 10.55001/2587-9820.2023.35.47.020.

10. Dupont B. Enhancing the Effectiveness of Cybercrime Prevention Through Policy Monitoring. *Journal of Crime and Justice*, 2019, vol. 42, iss. 5, pp. 500–515. DOI: 10.1080/0735648X.2019.1691855.

11. Yevdokimov K.N. Personal Features of a Criminal Committing Illegal Access to Computer Information (By the Example of Irkutsk Region). *Sibirskii yuridicheskii vestnik = Siberian Legal Bulletin*, 2011, no. 1, pp. 86–90. (In Russian). EDN: NDIGVX.

12. Megrelishvili G.T. Criminological and Psychological Characteristic of a Criminal Identity in High Technology Sphere. *Vestnik Tomskogo gosudarstvennogo universiteta = Tomsk State University Journal*, 2007, no. 299, pp. 180–181. (In Russian). EDN: KHNGHL.

13. Maslakova E.A. Perpetrators Committing Crimes in the Sphere of Information Technologies: Criminological Characteristics. *Srednerusskii vestnik obshchestvennykh nauk = Central Russian Journal of Social Sciences*, 2014, no. 1, pp. 114–121. (In Russian). EDN: SFPTEN.

14. Butyrskaya A.V. The Significance of Studying the Personality of a Criminal Group (Criminal Organization) Organizer in the Process of Investigation. *Rossiiskii sledovatel' = Russian Investigator*, 2013, no. 10, pp. 38–40. (In Russian). EDN: QAVVUV.

15. Sergeev S.M. Some Problems of Counteraction to the Use in Criminal Activities of Means to Ensure the User's Anonymization on the Internet. *Vestnik Sankt-Peterburgskogo universiteta MVD Rossii = Saint-Petersburg University of Ministry of Internal Affairs of Russia Bulletin*, 2017, no. 1, pp. 137–140. (In Russian). EDN: ZDUGUF.

16. Smushkin A.B. Forensic Aspects of the Dark Net Study for Crimes Investigation Purposes. *Aktual'nye problemy rossiiskogo prava = Topical Problems of Russian Law*, 2022, vol. 17, no. 3, pp. 102–111. (In Russian). EDN: WEFQBU. DOI: 10.17803/1994-1471.2022.136.3.102-111.

17. Ovchinnikova G.V. *Comments to the Decree of the Plenary Session of the Supreme Court of the Russian Federation "On Court Practice of Examining Criminal Cases on the Organization of a Criminal Group (Criminal Organization) and the Participation in it" of June 10, 2010, No 12.* Saint Petersburg Law Institute of the Office of the Prosecutor General of the Russian Federation Publ., 2011. 31 p. EDN: QSGPGN.

18. Truntsevskij Yu.V. Cybercrime in Corporate Sphere: Risks, Evaluation and Measures of Prevention. *Rossiiskii sledovatel' = Russian Investigator*, 2014, no. 21, pp. 19–22. (In Russian). EDN: RAXGMJ.

19. Chertoff M., Simon T. The Impact of the Dark Web on Internet Governance and Cyber Security. *Centre for International Governance Innovation and Chatham House. Paper Series*, 2015, no. 6. pp. 1–8.

20. Sablina M. Incitement: Terminology and Qualification Aspects. Pravo. *Zhurnal Vysshey shkoly ekonomiki = Law. Journal of the Higher School of Economics*, 2016, no. 4, pp. 129–139. (In Russian). EDN: XRJWCV. DOI: 10.17323/2072-8166.2016.4.129.139.

21. Glushkov E.L. About Some Questions of Distribution in a Contactless Manner of Drugs Via the Internet: Ways of Identification and Disclosure. *Problemy pravookhranitel'noi deyatel'nosti = Problems of Law-Enforcement Work*, 2018, no. 2, pp. 45–53. (In Russian). EDN: XTXKZN.

22. Osipenko A.L. Organized Criminal Activities in Cyberspace: Trends and Fighting. *Yuridicheskaya nauka i praktika: Vestnik Nizhegorodskoi akademii MVD Rossii = Legal Science and Practice: Journal of Nizhniy Novgorod Academy of the Ministry of the Interior of the Russian Federation*, 2017, no. 4, pp. 181–188. (In Russian).

23. Davidov S.I., Kondratev M.V., Polyako V.V. Countering Transnational Organized Groups Using Information and Communication Technologies for the Illegal Sale of Drugs. *Pravoprimenenie = Law Enforcement Review*, 2024, vol. 8, no. 1, pp. 111–120. (In Russian). DOI: 10.52468/2542-1514.2024.8(1).111-120.

24. Davydov V.O., Tishutina I.V. About Topical Problems of Forensic Skills of Investigation and Detection of Fraud Committed Using Information and Telecommunication Technologies. *Kriminalistika: vchera, segodnya, zavtra = Criminalistics: Yesterday, Today, Tomorrow*, 2020, no. 2, pp. 81–91. (In Russian). DOI: 10.24411/2587-9820-2020-10030.

25. Polyakov V.V. Using the Methods of Social Engineering when Committing High Tech Crimes. *Kriminalistika: vchera, segodnya, zavtra = Criminalistics: Yesterday, Today, Tomorrow*, 2023, no. 3, pp. 175–188. (In Russian). DOI: 10.55001/2587-9820.2023.81.15.018.

26. Starostenko N.I. Criminalistic Characteristics of the Identity of a Criminal Committing Theft by Social Engineering Methods. *Vestnik Krasnodarskogo universiteta MVD Rossii = Bulletin of the Krasnodar University of Ministry of Internal Affairs of Russia Bulletin*, 2022, no. 4, pp. 89–95. (In Russian).

27. Golovin A.Yu., Golovina E.V. Social Engineering in the Mechanism of Criminal Activity in the Field of Information and Telecommunications Technologies. *Izvestiya Tul'skogo gosudarstvennogo universiteta. Ekonomicheskie i yuridicheskie nauki = Izvestiya of the Tula State University. Economic and Legal Sciences*, 2021, no. 2, pp. 3–13. (In Russian). DOI: 10.24412/2071-6184-2021-2-3-13.

28. Sabyrbaeva A.B. On Measures to Counteract Fraud (Using the Example of Phishing). *Gosudarstvo i pravo = State and Law*, 2021, no. 1, pp. 181–185. (In Russian). DOI: 10.31857/S102694520017465-2.

29. Ahmedov A.G., Boziev T.O. Organized Ethnic Crime: Criminal Intelligence Analysis, Trends, and Challenges. *Vestnik Sankt-Peterburgskogo universiteta MVD Rossii = Saint-Petersburg University of Ministry of Internal Affairs of Russia Bulletin*, 2022, no. 1, pp. 89–97. (In Russian). EDN: VYTJWK. DOI: 10.35750/2071-8284-2022-1-89-97.

30. Van Hellemont E. Gang Glocalization: How a Global Mediascape Creates and Shapes Local Gang Realities. *Crime, Media, Culture: An International Journal*, 2019, vol. 15, iss. 1, pp. 169–189. DOI: 10.1177/1741659018760107.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Поляков Виталий Викторович — доцент кафедры уголовного процесса и криминалистики Алтайского государственного университета, кандидат юридических наук, г. Барнаул, Российская Федерация; e-mail: agupolyakov@gmail.com.

INFORMATION ABOUT THE AUTHORS

Polyakov, Vitaly V. — Ass. Professor, Department of Criminal Procedure and Criminalistics, Altai State University, Ph.D. in Law, Barnaul, the Russian Federation; e-mail: agupolyakov@gmail.com.

ДЛЯ ЦИТИРОВАНИЯ

Поляков В.В. Особенности лиц, совершающих высокотехнологичные преступления в составе организованных групп / В.В. Поляков. — DOI 10.17150/2500-4255.2024.18(5).494-503. — EDN YNQHDZ // Всероссийский криминологический журнал. — 2024. — Т. 18, № 5. — С. 494–503.

FOR CITATION

Polyakov V.V. Specific Features of Persons Committing High-Tech Crimes in an Organized Group. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2024, vol. 18, no. 5, pp. 494–503. (In Russian). EDN: YNQHDZ. DOI: 10.17150/2500-4255.2024.18(5).494-503.