УДК 343.34 Вестник СПбГУ. Право. 2022. Т. 13. Вып. 1

Уголовная ответственность за организацию устойчивой группы лиц, созданной для совершения преступлений в сфере компьютерной информации

И. Н. Мосечкин

Вятский государственный университет,
Российская Федерация, 610000, Киров, ул. Московская, 36

Для цитирования: Мосечкин, Илья Н. 2022. «Уголовная ответственность за организацию устойчивой группы лиц, созданной для совершения преступлений в сфере компьютерной информации». *Вестник Санкт-Петербургского университета. Право* 1: 28–45.
https://doi.org/10.21638/spbu14.2022.102

В статье анализируются правовые проблемы, возникающие в связи с установлением уголовной ответственности за организацию устойчивой группы лиц, созданной для совершения преступлений в сфере компьютерной информации. Актуальность темы исследования обусловлена негативной динамикой преступлений, связанных с использованием компьютерных технологий и совершенных преступными сообществами или преступными организациями, а также постоянным ростом ущерба от них. Автор осуществляет оценку действующих уголовно-правовых мер противодействия организованной киберпреступности, выявляя их недостатки. Проанализированы положения отечественного и зарубежного уголовного законодательства, что позволило установить некоторые правовые пробелы и выявить пути их преодоления. В статье доказывается, что Уголовный кодекс РФ не в полной мере охватывает случаи создания организованных преступных формирований, созданных для совершения противоправной деятельности в сфере компьютерной информации. В частности, не дифференцирована ответственность между группой лиц по предварительному сговору и организованной группой; категория преступлений и отсутствие цели извлечения прибыли не позволяют квалифицировать деяние как совершенное преступным сообществом или преступной организацией. По мнению автора, целесообразно признать отдельным деликтом сам факт создания противоправных организованных формирований, как это сделано в законодательстве отдельных стран семьи общего права, а также в отечественных нормах, регулирующих противодействие терроризму и экстремизму. Предлагается включить в УК РФ норму, предусматривающую ответственность за организацию устойчивой группы лиц в целях совершения преступлений в сфере компьютерной информации. Сформулирована редакция соответствующей статьи, которая может быть использована как рекомендация при совершенствовании законодательства.

Ключевые слова: компьютерная информация, компьютерное преступление, организованная группа, преступное сообщество, киберпреступление, общественная безопасность.

1. Введение

Преобразования в информационно-телекоммуникационной среде оказывают существенное влияние на преступность. Представители криминальных сообществ

достаточно быстро реагируют на появление новых технологий и предпринимают попытки их использования в противоправных целях. Если не так давно киберпреступления представляли собой новое, неизученное явление, то к настоящему времени они получили значительное распространение, а противодействие им стало предметом исследований ряда отечественных и зарубежных ученых (Xiaobing, Yongfeng 2018, 794; Бегишев, Хисамова, Никитин 2020; Грачева, Маликов, Чучаев 2020). Более того, такие традиционные для человечества преступления, как кража или мошенничество, перетекают в интернет-среду, поскольку она обеспечивает достаточную прибыль и высокий уровень латентности. Появление компьютерной преступности, как правильно отмечают С. В. Скляров и К. Н. Евдокимов, стало одной из социальных проблем технократического общества, а проблема информационной безопасности физических и юридических лиц все более актуализируется (Скляров, Евдокимов 2016, 322). Если изначально компьютерные преступления совершались одиночками, то сейчас можно говорить о тенденции возрастания групповой и организованной преступности в данной сфере.

Организованная преступность, являясь одной из самых опасных разновидностей преступности, также претерпевает серьезные изменения. Основной ее целью выступает, как правило, извлечение материальных выгод. При этом деятельность скрывается от правоохранительных органов, например, с помощью коррупции или иных методов криминальной маскировки (Rose-Ackerman, Palifka 2018, 75–76). Цифровая среда становится все более привлекательной для организованной преступности как раз потому, что позволяет извлекать значительные материальные выгоды и избегать внимания со стороны органов власти.

Как показывают статистические сведения Генеральной прокуратуры РФ, наблюдается рост преступлений, совершенных организованной группой или преступным сообществом. Так, в 2016 г. число подобных деликтов составило 12 581, в 2017 г. — 13 232, в 2018 г. — 15 628, в 2019 г. — 16 290. При этом за январь — декабрь 2019 г. правоохранительными органами РФ зарегистрировано 294 409 преступлений (на 68,5 % больше, чем в 2018 г.), совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации[1]. Таким образом, даже по показателям официальной статистики можно отметить рост организованной и компьютерной преступности, определенную связь между которыми отрицать невозможно. Вместе с тем следует учитывать высокую латентность, которая составляет от нескольких десятков до нескольких тысяч процентов по разным видам преступных деяний (Скляров, Евдокимов 2016, 323–324). Не останавливаясь на уровне скрытой и скрываемой преступности, а также методиках ее оценки, согласимся с общепринятой позицией: реальное число таких преступлений выше, чем отраженное в официальной статистике (как в России, так и за рубежом).

В странах Европейского союза возрастают расходы на противодействие так называемым сложным организованным преступным группам (Serious and Organized Crime Threat Assessment, SOCTA). Европол в настоящее время ведет борьбу против более чем 5000 международных преступных групп. Для сравнения, в 2013 г. это чис-

[1] Состояние преступности в России за январь — декабрь 2019 г. Сборник Генеральной прокуратуры Российской Федерации. *Генеральная прокуратура РФ*. 2020. Дата обращения 15 июня, 2020. https://genproc.gov.ru/upload/iblock/034/sbornik_12_2019.pdf.

ло составляло около 3600. Значительная часть преступных формирований использует компьютерные технологии для осуществления своей деятельности (Jirovský et al. 2018, 2–3).

По справедливому мнению А. Л. Осипенко, криминальную активность в интернет-пространстве проявляют преимущественно две категории лиц:

— «обычные» преступники, переносящие в цифровую среду отдельные виды преступной деятельности (наркоторговля, мошенничество и др.);
— киберпреступники, обладающие навыками в сфере информационных технологий, позволяющими совершать преступления, возможные только в киберпространстве (несанкционированный дистанционный доступ к информационным ресурсам, нарушение функционирования сетевых объектов и т. п.) (Осипенко 2017, 183).

В настоящее время и «обычные», и киберпреступники объединяются в преступные формирования, поскольку это облегчает совершение преступлений и обеспечивает более высокую вероятность успеха.

В зарубежных научных трудах подчеркивается, что многие киберпреступники тесно связаны между собой, объединяются для совершения преступлений и изучают противоправную деятельность других лиц (Hutchings 2014, 3–4). Другие авторы провели продолжительное, многолетнее исследование (включающее анализ уголовных дел в нескольких странах и анонимные интервью), по итогам которого были сделаны выводы, заслуживающие пристального внимания. Ученые полагают, что, с одной стороны, роль организованной киберпреступности среди других видов чрезмерно преувеличена, с другой — она существует и активно проявляет себя в корыстных преступлениях. В большинстве случаев преступные формирования состояли из стабильной группы основных членов, т. е. совершали преступления с одинаковым составом в течение определенного времени. Вместе с тем имели место группы, объединившиеся в социальных сетях на непродолжительный период (Leukfeldt, Lavorgna, Kleemans 2017, 288–289).

Несмотря на кратковременность существования киберпреступности, можно заметить не только количественные, но и качественные ее изменения. Появилось множество видов, которые продолжают развиваться и совершенствоваться. Сложилась компьютерная преступность, отвечающая всем признакам профессиональной. В цифровой среде осуществляют деятельность лица, специализирующиеся на компьютерных мошенничествах, кражах, вымогательствах, незаконном доступе к информации, создании вредоносных программ, фишинге и других высокотехнологических преступлениях (Boddy 2018, 9).

Одним из наиболее новых и наименее изученных направлений является «хактивизм» (от англ. hack — взламывать и activism — активность). Изначально хактивисты занимались политическими акциями в информационно-телекоммуникационных сетях, что часто сопровождалось компьютерными атаками. Так, с 2008 г. группа «Аноним» (Anonymous) совершила ряд кибератак в поддержку некоторых политических и общественных целей. Мишенями стали государственные и религиозные организации, а также отдельные юридические лица. Поводы для атак были самыми разными: поддержка политических движений, уголовные дела по отношению к активистам, религиозная деятельность (Li 2013, 302).

Хактивисты отличаются от представителей организованной киберпреступности тем, что, как правило, не преследуют корыстных целей. Однако нельзя исключать и пересечения этих видов противоправных организаций. Хотя существует множество трудов о киберпреступности, кибертерроризме и иных преступлениях в цифровой среде, хактивизму посвящено не так много исследований. Отдельные криминологи считают это движение новой, уникальной и вместе с тем опасной формой девиации (Tanczer 2016, 1614–1615).

Достаточно трудно говорить о статистике хактивизма. Как следует из зарубежной литературы, по мнению опрошенных респондентов, хактивизм составлял 58 % всех нарушений, связанных с незаконным доступом к компьютерной информации в 2011 г. В то же время, по данным опросов, проводившихся с 2004 по 2010 г., ни один из респондентов не называл хактивизм в качестве причины таких нарушений[2]. К сожалению, небольшое число исследований не позволяет получить объективное представление о данной разновидности организованной преступности.

Ученые подчеркивают, что существует необходимость в уникальном подходе к различным формам хактивизма (Webber, Yip 2018, 253–254). Думается, с этим мнением можно согласиться, причем даже в более широком масштабе. В последнее время в науке преобладает позиция, согласно которой компьютерные атаки совершаются, как правило, в корыстных целях (McDaniel 2018, 161–162). Вместе с тем можно наблюдать случаи создания целых противоправных групп, занимающихся взломом компьютерных систем. Речь идет не только о хактивистах, но и об иных преступных формированиях, проявляющихся в цифровой среде. Они хорошо организованы, владеют необходимыми навыками, а их цели и задачи не связаны (по крайней мере прямо) с получением финансовой или иной материальной выгоды. Таким образом, возможно, сам факт создания подобных формирований должен влечь наступление уголовной ответственности?

Целью настоящего исследования выступает разрешение отдельных теоретических и прикладных проблем применения уголовно-правовых норм, охраняющих безопасность компьютерной информации. Задачи исследования: проанализировать зарубежное законодательство, связанное с регулированием сферы компьютерной информации, а также мнения ученых по поводу его состояния; оценить уголовно-правовые нормы об ответственности за компьютерные преступления в контексте их противодействия организованной преступности; обосновать и сформулировать предложения по совершенствованию главы Уголовного кодекса РФ от 13.06.1996 № 63-ФЗ[3] (далее — УК РФ) о преступлениях в сфере компьютерной информации.

Методологической основой работы традиционно выступили универсальные принципы и требования диалектического метода познания (объективности и всесторонности рассмотрения объекта познания, всеобщей связи явлений, системности и др.). Для исследования особенностей правового регулирования организованной киберпреступности в зарубежных странах использовался сравнительно-правовой метод. Для изучения эмпирического материала применен документальный метод (исследованы известные факты совершения общественно опасных деяний

[2] 2012 Data Breach Investigations Report. Дата обращения 24 июня, 2020. https://www.wired.com/images_blogs/threatlevel/2012/03/Verizon-Data-Breach-Report-2012.pdf.

[3] Здесь и далее все ссылки на российские нормативно-правовые акты и судебную практику приводятся по СПС «КонсультантПлюс». Дата обращения 29 июля, 2020. http://www.consultant.ru.

организованными преступными формированиями, изучен законодательный материал). Применен формально-юридический метод, который позволил должным образом оценить правовые категории, выявить и истолковать их признаки. Для оценки состояния организованной и компьютерной преступности использовались статистические методы.

2. Основное исследование

Изучение зарубежного опыта уголовно-правового противодействия организованной преступности может внести большой вклад в разработку направлений совершенствования отечественного законодательства. Кроме того, заслуживают внимания выводы ученых, исследовавших нормативные акты различных стран. В частности, в одной из работ, посвященных сравнительно-правовой характеристике, указывается, что законодательство США и Великобритании позволяет применять меры уголовной ответственности не только в случае совершения конкретного компьютерного преступления, но и за создание преступных формирований в противоправных целях (Мосечкин 2021, 166).

В указанных странах действуют похожие правовые положения: в США в 1986 г. принят Закон о компьютерном мошенничестве и злоупотреблениях[4], а в Великобритании применяется Закон о неправомерном использовании компьютеров 1990 г.[5] Ученые подчеркивают, что уголовное законодательство США охватывает в качестве отдельных преступлений подстрекательство и сговор, что увеличивает вероятность привлечения к ответственности. Вместе с тем в правоприменительной практике Великобритании встречаются факты назначения наказания за сговор и дачу советов в совершении компьютерных преступлений. Такая деятельность признается отдельным нарушением (Karagiannopoulos 2018, 135–136).

Ученые, посвятившие труды законодательству Ямайки, отмечают, что в перечень противоправных деяний, установленный Законом о компьютерных преступлениях 2015 г., включены все виды соучастия в совершении таких преступлений (в качестве самостоятельного деликта). Важная особенность заключается в том, что все соучастники независимо от роли подлежат наказанию, как и исполнитель (Barclay 2017, 85).

В Австралии действует Уголовный закон от 1995 г., в котором использован подход, характерный для вышеуказанных стран: соучастие в совершении каких-либо преступлений само по себе является отдельным преступлением[6]. Однако имеются и специальные нормы. В частности, ст. 478.4 предусматривает наказание за разновидности соучастия в совершении киберпреступлений. Похожим образом, как следует из зарубежной литературы, регулируется ответственность в странах Южной Африки, где с 2002 г. действует Закон об электронных коммуникациях и сделках (ECT Act) (Shultz 2016).

---

[4] H. R. 4718 — Computer Fraud and Abuse Act of 1986. Дата обращения 25 июня, 2020. https://www.congress.gov/bill/99th-congress/house-bill/4718.

[5] Computer Misuse Act 1990. Дата обращения 25 июня, 2020. https://www.legislation.gov.uk/ukpga/1990/18/contents.

[6] Criminal Code Act 1995. Дата обращения 29 июня, 2020. https://www.legislation.gov.au/Details/C2017C00235.

Для англосаксонской правовой семьи достаточно характерно установление ответственности за разновидности соучастия в тех или иных преступлениях. Иначе говоря, лица, объединившиеся для совершения противоправных деяний, привлекаются к ответственности независимо от того, удалось ли им достигнуть желаемых результатов. Для борьбы с организованной киберпреступностью в уголовный закон часто вводятся специальные нормы, что отражает особенное отношение к ним со стороны законодателя. Ученые, анализирующие зарубежное законодательство, говорят о неуловимом характере киберпреступности, который привел к широко распространенной криминализации любой подготовки (сговор, владение техническими устройствами). Авторы поддерживают такую криминализацию, но отмечают, что многие страны не рассматривают простую подготовку преступного поведения как наказуемое деяние (Viano 2016, 21–22).

Настоящее исследование не было бы объективным без изучения нормативно-правовых актов зарубежных стран, входящих в группу романо-германской правовой семьи (в контексте выявления особенностей уголовно-правового противодействия хакерским сообществам).

В уголовном законе Венгрии не содержится норм, устанавливающих ответственность лишь за создание объединений с целью совершения компьютерных преступлений. Однако в зарубежной литературе отмечается, что налицо правовой пробел, который должен быть преодолен посредством внесения соответствующих изменений. Вместе с тем подчеркивается, что новые статьи должны действовать только в комплексе с мерами криминологического характера (Béla 2016, 173–174).

Уголовный закон Финляндии усиливает ответственность за совершение компьютерных преступлений посредством закрепления различных видов соучастия в качестве квалифицирующего признака. При этом само противоправное объединение не образует отдельного состава преступления, а рассматривается как неоконченная стадия. Однако исследователи подчеркивают, что законодательство сталкивается все с большими вызовами со стороны киберпреступности и нуждается в совершенствовании. Это отвечает действующей Директиве Европейского парламента и Совета от 12.08.2013, согласно п. 13 которой целесообразно предусмотреть более суровые меры наказания, если нападение на информационную систему совершено преступной организацией (Calcara, Sund, Tolvanen 2019, 94–97).

Как отмечает А. В. Пелевина, ст. 216.1 Пенитенциарного кодекса Эстонии устанавливает уголовную ответственность за подготовку компьютерного преступления (Пелевина 2017, 246). Любопытно, что данное правонарушение может быть вменено юридическим лицам, т. е. к ответственности привлекаются не только конкретные физические лица, но и общность людей.

Исследование нормативных актов иных стран, принадлежащих к правовой семье континентального права, позволяет сделать вывод о том, что организация группы лиц, направленной на совершение преступлений в сфере компьютерной информации, чаще признается квалифицирующим признаком, чем отдельным составом преступления. Среди таких стран можно назвать ФРГ, Нидерланды, Французскую Республику, Социалистическую Республику Вьетнам, Китайскую Народную Республику, Чешскую Республику и др. (Мосечкин 2021, 167). В основном уголовное законодательство данных стран охватывает создание таких организаций

через институты соучастия и неоконченных преступлений, т. е. ответственность наступает за приготовление или покушение.

Изложенное позволяет сформулировать промежуточный вывод: в законодательстве ряда зарубежных стран использован подход, в соответствии с которым любое соучастие, возникшее для совершения компьютерных преступлений, признается отдельным оконченным деянием. Как правило, такие страны входят в группу англосаксонской правовой семьи. Для законодательства стран, принадлежащих к романо-германской правовой семье, более характерно конструирование квалифицирующих составов с помощью признаков, охватывающих тот или иной вид соучастия. При этом часть ученых указывает на то, что законы нуждаются в совершенствовании и должны включать отдельные нормы, учитывающие организованную киберпреступность.

Разумеется, в науке существуют мнения и о том, что влияние организованной киберпреступности чрезмерно преувеличено. Так, отдельные авторы, критикуя законодательство Великобритании, отмечают, что терминология в нормативных актах далека от действительности и при принятии изменений в законодательстве не было должного понимания соотношения форм соучастия в совершении компьютерных преступлений (Lavorgna, Sergi 2016, 182–183). Другие ученые полагают, что такие формы объединения, как хактивизм, не нуждаются в репрессивном регулировании, поскольку выступают своеобразной разновидностью протеста, на которую распространяется свобода слова (Li 2013, 311–312).

Думается, что общественная опасность и нанесенный вред от деятельности киберпреступности, тем более организованной, будут только возрастать. В связи с этим следует поднять вопрос о криминализации самого факта объединения в преступное формирование в целях совершения компьютерных преступлений. Решение данного вопроса невозможно без учета оснований криминализации деяния. В науке уголовного права сложился ряд парадигм, в которых количество и виды оснований определяются неоднозначно: плюралистическая, монистическая, смешанная, волюнтаристская (Нечаев 2017, 91–92). Среди оснований наиболее часто выделяются следующие: общественная опасность криминализуемого деяния, реже — широкая распространенность; ожидаемые положительные последствия, превышающие отрицательные последствия; отсутствие противоречия действующему законодательству и др.

Наличие общественной опасности в противоправной деятельности организованных преступных формирований в сфере компьютерной информации вполне очевидно. Наличие в УК РФ гл. 28 уже указывает на то, что компьютерные преступления способны наносить существенный вред общественным отношениям, иначе законодатель не стал бы вводить в уголовный закон ст. 272–274[1]. Ущерб от таких преступлений ежегодно возрастает, а соучастие еще более повышает общественную опасность. Распространенность организованной киберпреступности является достаточно спорным моментом. По данным официальной статистики, приведенным выше, преступления в сфере компьютерной информации не отличаются значительным количеством, но имеют тенденцию к возрастанию (в том числе в соучастии). Не следует забывать и о высокой латентности подобных деликтов.

Правовые аспекты криминализации следует рассмотреть более подробно. Уголовный закон предусматривает деяния, которые связаны с компьютерными тех-

нологиями, но посягают на другие охраняемые объекты. К ним можно отнести, например, мошенничество в сфере компьютерной информации (ст. 159[6] УК РФ), неправомерный оборот средств платежей (ст. 187 УК РФ) и иные. Хотя в зарубежной литературе (и в ряде трудов отечественных авторов, разделяющих широкий подход) подобные деяния часто включаются в понятие киберпреступности, настоящее исследование сосредоточено на преступлениях в сфере компьютерной информации, включенных в гл. 28 УК РФ (Fortes, Boff 2017, 7–8). Иными словами, компьютерная преступность далее будет пониматься в контексте узкого подхода.

Анализ отечественного уголовного законодательства позволяет сделать вывод, что оно охватывает практически все возможные виды противоправной деятельности в сфере компьютерной информации, обладающие высокой общественной опасностью. Вместе с тем отдельные ученые указывают на необходимость криминализации иной деятельности, например, связанной с неправомерным воздействием на информационную систему (Грачева, Маликов, Чучаев 2020, 196) или приобретением вредоносных программ (Гребенкин, Коврижных 2017, 75).

Различные формы соучастия охватываются квалифицирующими признаками ст. 272–274[1] УК РФ. Так, ч. 3 ст. 272 УК РФ предусматривает ответственность за неправомерный доступ к компьютерной информации, совершенный группой лиц по предварительному сговору или организованной группой. Часть 2 ст. 273 УК РФ признает наказуемым создание, использование и распространение вредоносных компьютерных программ, совершенные группой лиц по предварительному сговору или организованной группой. Одна из самых новых статей в этой главе — ст. 274[1] УК РФ — в ч. 4 также содержит квалифицирующий признак, связанный с совершением преступления группой лиц по предварительному сговору или организованной группой.

Хотя законодатель включил различные формы соучастия как квалифицирующие признаки, представляется не совсем логичным отсутствие дифференциации в зависимости от степени организованности. Думается, что совершение преступления организованной группой является более опасным деянием, чем совершение группой лиц по предварительному сговору. Соответственно, должно быть предусмотрено более строгое наказание.

Тем не менее анализ статей, охватывающих преступления в сфере компьютерной информации, показывает, что совершение деяния в соучастии влечет наступление более строгой уголовной ответственности. Правда, вид и форма соучастия не влияют на квалификацию, поскольку охватываются одной частью статьи. Вместе с тем пока не совершено общественно опасное деяние (а в ряде случаев — пока не наступило общественно опасное последствие), не образуется оконченного преступления, даже если планировалось его совершение группой лиц по предварительному сговору или организованной группой. В этом случае речь может идти только о приготовлении или покушении.

Действующий уголовный закон содержит нормы, предусматривающие ответственность за сам факт создания отдельных видов организованных групп или за участие в них. Так, ст. 205[4] УК РФ закрепляет противоправность создания террористических сообществ или участия в них. В ст. 282[1] УК РФ похожим образом устанавливается ответственность за организацию экстремистского сообщества. В пояснительной записке к проекту Федерального закона № 203317-3 «О внесении

изменений и дополнений в законодательные акты РФ в связи с принятием Федерального закона "О противодействии экстремистской деятельности"», результатом которого стало принятие ст. 282^1 УК РФ, отмечалось, что «лица, объединившиеся для осуществления экстремистской деятельности, являясь, по сути, членами организованной группы лиц, заранее объединившимися для совершения преступления (ч. 3 ст. 35 УК РФ), должны подлежать аналогичному преследованию».

Введением данных статей законодатель подчеркнул: общественная опасность объединения в определенных преступных целях столь велика, что необходимо привлечение к ответственности даже без реализации деликтов, ради которых создана группа. Диспозиция указанных статей неоднократно подвергалась заслуженной критике. В частности, одним из недостатков называется смешение различных форм соучастия — организованной группы и преступного сообщества (Абдулатипов 2016, 93). С. М. Кочои относительно ст. 205^4 и 205^5 УК РФ отмечает, что законодательные разночтения вносят лишь путаницу в теорию и практику применения уголовного закона, касающегося форм соучастия в «террористических преступлениях» (Кочои 2016, 743). Ю. А. Клименко, анализируя ст. 282^1 и 282^2 УК РФ, подчеркивает, что легальная дефиниция экстремистского сообщества сформулирована законодателем весьма противоречиво. С одной стороны, в ч. 1 ст. 282^1 УК РФ говорится о том, что экстремистское сообщество — это организованная группа лиц. Следовательно, можно отнести данное объединение к разновидности организованной группы. С другой стороны, в норме указано, что сообщество имеет части или входящие в него структурные подразделения, а это означает наличие у экстремистского сообщества такой же структуры, как у преступного сообщества (Клименко 2017, 125).

Ученые подчеркивают некоторую нелогичность и бессистемность конструирования рассматриваемых уголовно-правовых норм. Вместе с тем многие авторы не отрицают их необходимости. Напротив, наличие соответствующих статей в уголовном законе позволяет привлекать к уголовной ответственности лиц, объединившихся для совершения преступлений, обладающих повышенной общественной опасностью. Как отмечают представители науки, до введения ст. 205^4 УК РФ иногда складывалась несколько абсурдная ситуация: факт существования террористического сообщества выявлялся, но запретить деятельность этого сообщества не представлялось возможным, и оно продолжало существование. Кроме того, криминализация организаторской деятельности при создании террористического сообщества имела и имеет большое профилактическое значение (Аулов 2016, 102). Наконец, в связи с указанием на цель организации террористических и экстремистских сообществ производится их отграничение от других организованных групп и преступных сообществ (преступных организаций).

Несмотря на сохраняющееся несовершенство ст. 205^4 и 282^1 УК РФ, а также критику со стороны научных работников (с которыми во многом следует согласиться), закрепленные нормы не являются «мертвыми» и применяются в практике. Так, по ст. 205^4 УК РФ в 2016 г. осуждены 2 чел., в 2017 г. — 1, в 2018 г. — 1, в 2019 г. — 1. По ст. 282^1 УК РФ в 2016 г. осуждены 16 чел., в 2017 г. — 4, в 2018 г. — 4, в 2019 г. — 6[7].

[7] Уголовное судопроизводство. Данные о назначенном наказании по статьям УК. Дата обращения 23 июля, 2020. http://stat.xn----7sbqk8achja.xn--p1ai/stats/ug/t/14/s/17.

Подчеркнем: речь идет о лицах, в отношении которых вступил в силу приговор суда. В то же время в данной статистике не отражены граждане, уголовное производство по делам которых было прекращено на более ранней стадии, а также скрытая часть преступности. Таким образом, ст. 205^4 и 282^1 УК РФ весьма трудно назвать «нерабочими». Следовательно, вышеуказанные недостатки не оказывают существенного влияния на востребованность статей и необходимость ответственности за организацию и участие в отдельных преступных формированиях. Изучение ст. 205^4 и 282^1 УК РФ позволило рассмотреть подходы законодателя к противодействию различным проявлениям организованной преступности посредством уголовного права. Соответственно, такие подходы могли бы быть использованы и в борьбе с киберпреступностью.

Для решения этого вопроса вновь следует обратиться к содержанию гл. 28 УК РФ. Действующий уголовный закон не позволяет охватить в полной мере деятельность по организации хакерских сообществ, как и участие в них. Статьями данной главы предусматривается ответственность за совершение преступлений группой лиц по предварительному сговору или организованной группой. Если же в противоправных целях были созданы преступное сообщество или преступная организация, то при наличии всех признаков возможно привлечение к уголовной ответственности по ст. 210 УК РФ. Именно здесь наблюдается одна из возможных правовых проблем. В соответствии со ст. 210 УК РФ, преступное сообщество (преступная организация) создается в целях совершения одного или нескольких тяжких или особо тяжких преступлений, а ст. 35 УК РФ указывает на намерение получения прямо или косвенно финансовой или иной материальной выгоды.

Если соотносить хакерское сообщество с преступным сообществом, то в ряде случаев могут отсутствовать признаки, предусмотренные ч. 4 ст. 35 УК РФ. Как уже отмечалось ранее, хакерские сообщества, пусть и в большинстве случаев, но не всегда создаются с корыстной целью. Так, большую известность получили публикации в средствах массовой информации о преступлениях, совершенных организованной группой «Шалтай-Болтай». Целью группы было получение незаконного доступа к компьютерной информации должностных лиц. Полученная информация публиковалась в ряде источников цифровой среды и средствах массовой информации. При совершении первых преступлений участники группы действовали не в целях получения материальной выгоды, а скорее из хулиганских побуждений. В дальнейшем полученная информация стала использоваться для извлечения прибыли, в основном путем вымогательства[8].

Таким образом, данный пример показывает, что в отдельных случаях лица действительно объединяются в группы для совершения компьютерных преступлений не в корыстных целях. Наличие специальной нормы, предусматривающей ответственность за создание таких групп и участие в них, могло бы оказать профилактический эффект и установить меру наказания, соответствующую деянию.

Также обратим внимание на тот факт, что преступления, предусмотренные ч. 1–3 ст. 272, ч. 1 и 2 ст. 273 УК РФ, относятся к категориям небольшой и средней тяжести. Как указано в п. 2 Постановления Пленума Верховного Суда РФ от

[8] Мосгорсуд огласил приговор лидеру хакерской группировки «Шалтай-Болтай». 2017. Дата обращения 24 июля, 2020. https://www.gazeta.ru/social/2017/07/06/10775462.shtml.

10.06.2010 № 12 «О судебной практике рассмотрения уголовных дел об организации преступного сообщества (преступной организации) или участии в нем (ней)», преступное сообщество (преступная организация) отличается от иных видов преступных групп, в том числе от организованной группы, помимо прочего, более сложной внутренней структурой, а также возможностью объединения двух или более организованных групп. Следовательно, может сложиться ситуация, при которой преступное формирование будет обладать сложной внутренней структурой, сплоченностью и целью совершения преступлений, предусмотренных ст. 272 и 273 УК РФ. Такое формирование нельзя признать преступным сообществом или преступной организацией в связи с тем, что данные деяния относятся к категориям небольшой и средней тяжести.

В связи с этим необходимо попробовать соотнести противоправные хакерские объединения с организованной группой, особенности которой раскрыты в ч. 3 ст. 35 УК РФ. Очевидно, что бóльшая часть признаков совпадет. Правда, организованная группа не обладает структурированностью, сплоченностью и целями, как преступное сообщество. Вместе с тем если признать хакерское объединение организованной группой лиц, объединившихся для совершения компьютерных преступлений, то возможно их привлечение к ответственности только за приготовление или покушение на преступление.

Думается, что хакерские сообщества еще несколько лет назад были значительно менее опасными, чем террористические или экстремистские, поэтому сложившиеся правовое регулирование и практика применения норм на тот момент достаточно адекватно отвечали обстановке. В настоящее время цифровизация продолжает охватывать все больше сфер человеческой жизни, а ущерб от компьютерных преступлений возрастает. Соответственно, можно говорить о повышенной общественной опасности хакерских сообществ.

В науке уголовного права предлагаются соответствующие рекомендации по криминализации. В зарубежной литературе отмечается, что объединения людей способны совершать то же самое, что и отдельные лица, и зачастую лучше. При этом почти все виды преступных формирований (включая высокоорганизованные традиционные формирования) потенциально могут участвовать в совершении компьютерных преступлений (Broadhurst et al. 2014, 2). В связи с этим объединение в целях совершения киберпреступлений должно наказываться строже.

Так, И. Р. Бегишев, З. И. Хисамова и С. Г. Никитин подчеркивают, что необходимы изменения в уголовном законе, специально охватывающие ответственность за создание хакерского сообщества и участие в нем. По мнению авторов, введение новой нормы обеспечит адекватную правовую оценку деятельности участников организаций, связанных с совершением преступлений в сфере компьютерной информации. В новой норме для придания ей универсального характера следует избегать описания конкретных преступлений, на совершение которых направлена организация (Бегишев, Хисамова, Никитин 2020, 102–103).

Похожего мнения придерживается Л. В. Глазкова, подчеркивая, что «уголовно-правовые меры противодействия преступности нуждаются в разработке новых понятий, соответствующих изменениям в способах формирования организованных групп и сообществ». Она предлагает дополнить гл. 28 УК РФ нормами об ответственности за создание организованной преступной группы (кибергруппы)

и за создание преступного сообщества, имеющего цели совершения преступлений в сфере компьютерной информации (Глазкова 2019, 58–59).

Думается, что позиции вышеуказанных ученых стоит поддержать. Действительно, правильным решением было бы привлечение к уголовной ответственности с момента организации преступного формирования, созданного для совершения компьютерных преступлений, как за оконченное преступление. С учетом реального существования хакерских организаций (сообществ), совершения ими различных преступлений (в том числе некорыстной направленности) необходимо усовершенствовать уголовный закон путем внесения в него положений, закрепляющих ответственность за создание таких формирований, руководство ими или участие в них.

Вместе с тем не в полной мере можно поддержать мнение о том, что следует избегать описания конкретных преступлений, на совершение которых направлена организация. Напротив, следует уделить большое внимание способам законодательного отграничения от иных видов преступных формирований, например террористических или экстремистских. Именно так поступил законодатель при конструировании ст. 205^4 и 282^1 УК РФ. В диспозиции перечислены либо конкретные деяния (в ст. 205^4 УК РФ), либо общий признак преступлений (в ст. 282^1 УК РФ).

В случае криминализации ответственности за создание хакерских групп также необходимо указание на вид преступлений, ради совершения которых такие группы образовываются. В противном случае возникнут сложности при разграничении отдельных составов преступлений со сходными признаками. Так, общими чертами с хакерским сообществом могут обладать организованные группы, объединившиеся для совершения дистанционных мошенничеств или краж. Однако считаем оправданным напомнить, что лица, объединившиеся для совершения компьютерных преступлений, не всегда преследуют корыстные цели. Вместе с тем их сходство заключается в противоправном посягательстве на компьютерную информацию.

В связи с этим при формулировании статьи, предусматривающей ответственность за организацию хакерского сообщества, следует указать цель как обязательный признак. Такой целью может быть совершение преступлений в сфере компьютерной информации, что позволит отграничить киберпреступность от общеуголовной преступности, реализуемой с применением компьютерных технологий, а также от других разновидностей сообществ.

При конструировании соответствующей статьи вряд ли оправданно использовать слова «хакер» или «хакерский», поскольку действующий уголовный закон, а также иные нормативные правовые акты их не используют и не раскрывают. Законодатель, регулируя отношения, связанные с неправомерными действиями в сфере компьютерной информации, использует другие конструкции, а введение новых определений целесообразно только в тех случаях, когда применяющиеся формулировки не соответствуют новым явлениям. Полагаем, именно цель, указанная выше, поможет избежать неоправданного использования слов «хакер» или «хакерский» в уголовном законе.

Как уже отмечалось ранее, действующие редакции ст. 205^4 и 282^1 УК РФ подвергаются аргументированной критике, связанной в основном со смещением форм соучастия. К сожалению, при конструировании статьи, предусматривающей ответственность за организацию хакерского сообщества, не избежать тех же спорных

решений, в том числе смешения таких форм соучастия, как преступное сообщество и организованная группа. В соответствии с принципами системности и языковой стандартизированности конструкции вводимых в уголовный закон статей должны соответствовать уже существующим статьям. В связи с этим предлагаемая редакция статьи не может существенным образом отличаться от ст. 205^4 и 282^1 УК РФ. Их преобразование и устранение недостатков допустимы только единовременно, однако данную проблему следует отнести к предмету отдельного, гораздо более объемного научного исследования.

Вместе с тем полагаем возможным отказаться от термина «сообщество», поскольку именно оно сбивает с толку многих ученых и практиков (в силу его различающихся значений), а его исключение не окажет негативного влияния на правоприменение.

3. Выводы

Проведенное исследование, дополняющее уже имеющиеся научные труды, подтвердило, что организованная преступность продолжает развиваться, в том числе в области совершения деяний в цифровой среде. В отечественной и зарубежной литературе отмечается рост киберпреступлений, совершенных в различных формах соучастия, в то время как уголовное законодательство не всегда адекватно отражает регулирование существующих отношений.

Одна из существующих проблем связана с ответственностью за создание преступных формирований с целью совершения компьютерных преступлений. В зарубежном законодательстве сложились разные подходы к мерам уголовно-правового противодействия таким явлениям. В странах, относящихся к семье общего права, достаточно распространены положения, позволяющие привлекать к уголовной ответственности за любое объединение с целью совершить компьютерное преступление как за оконченное деяние. В странах континентальной правовой семьи более характерно закрепление форм соучастия в качестве квалифицирующих признаков, в том числе в составах преступления, связанных с компьютерной информацией.

В науке также сложилась дискуссия о целесообразности криминализации создания хакерских сообществ. Имеются аргументированные мнения за и против. В рамках проведенного исследования мы привели дополнительные доводы в пользу криминализации хакерских сообществ. Такое изменение в законодательстве представляется весьма актуальным и отвечающим сложившейся ситуации противодействия киберпреступности.

В УК РФ статью, предусматривающую ответственность за указанное деяние, можно разместить в гл. 28 под номером 274^2. Предлагаем следующую формулировку ее диспозиций:

> Статья 274^2. Организация устойчивой группы лиц в целях совершения преступлений в сфере компьютерной информации
>
> 1. Создание устойчивой группы лиц, заранее объединившихся в целях совершения преступлений в сфере компьютерной информации, а равно руководство такой группой, ее частью или входящими в такую группу структурными подразделениями…

2. Участие в устойчивой группе лиц, заранее объединившихся в целях совершения преступлений в сфере компьютерной информации…

Предложенная рекомендация по совершенствованию уголовного закона является лишь примерной и, безусловно, нуждается в уточнении после проведения соответствующих научных изысканий. При формулировании диспозиции ст. 274^2 УК РФ был принят во внимание подход законодателя, который уже использовался при создании ст. 205^4 и 282^1. Законодатель допустил противоречия между признаками террористических и экстремистских сообществ, и признаками, закрепленными в ст. 35 УК РФ. В таком случае получается, что все будущие предложения по криминализации разных видов преступных сообществ не будут соответствовать действующим статьям либо Общей части, либо Особенной части.

В свою очередь, при формулировании ст. 274^2 УК РФ мы вынуждены занять одну из позиций в дискуссионном вопросе, посчитав недопустимым отклонение от тех методов, которые уже были использованы и показали свою эффективность, даже если в науке обращается внимание на противоречия с положениями, закрепленными в ст. 35 УК РФ. Если использовать кардинально различающиеся способы закрепления в законе похожих явлений, то нарушается целостность уголовного закона, затрудняются квалификация и применение норм, что ведет к снижению эффективности борьбы с организованной преступностью.

Вместе с тем выбранное направление уголовно-правового противодействия организованной киберпреступности представляется правильным. Очевидно, что разработка уголовно-правовых норм, регулирующих данную сферу, должна носить комплексный и всесторонний характер. При этом желательно единство подхода со стороны не только отечественных, но и зарубежных ученых, что обусловлено транснациональным характером компьютерной преступности. В связи с изложенным надеемся, что данное исследование пробудит научный интерес иных ученых и это приведет к оптимальному решению о совершенствовании закона.

Библиография

Абдулатипов, Абдулатип М. 2016. «Организация террористического сообщества и участие в нем (уголовно-правовые аспекты)». *Юридический вестник Дагестанского государственного университета* 18 (2): 91–99.

Аулов, Артем Н. 2016. «Организация террористического сообщества (ч. 1 ст. 205^4 УК РФ): вопросы уголовно-правового содержания». *Теория и практика общественного развития* 6: 101–104.

Бегишев, Ильдар Р., Зарина И. Хисамова, Сергей Г. Никитин. 2020. «Организация хакерского сообщества: криминологический и уголовно-правовой аспекты». *Всероссийский криминологический журнал* 14 (1): 96–105.

Глазкова, Лилия В. 2019. «Особенности современных организованных преступных групп». *Мониторинг правоприменения* 1 (30): 54–60.

Грачева, Юлия В., Сергей В. Маликов, Александр И. Чучаев. 2020. «Предупреждение девиаций в цифровом мире уголовно-правовыми средствами». *Право. Журнал Высшей школы экономики* 1: 188–210.

Гребенкин, Федор Б., Любовь А. Коврижных. 2017. «Некоторые проблемные вопросы объективных признаков состава преступления, предусмотренного ст. 273 УК РФ». *Вестник гуманитарного образования* 2: 71–77.

Клименко, Юрий А. 2017. «Организация экстремистского сообщества: проблемы квалификации». *Lex Russica* 3 (124): 123–132.

Кочои, Самвел М. 2016. «Пробелы в законодательстве о терроризме и предложения по их устранению». *Всероссийский криминологический журнал* 10 (4): 740–749.

Мосечкин, Илья Н. 2021. «Уголовная ответственность за создание организованных групп, направленных на совершение компьютерных преступлений, по законодательству зарубежных стран». *Наука, технологии, общество — НТО–2021*: сборник научных статей по материалам Всероссийской научной конференции, 165–168. Красноярск: Красноярский краевой Дом науки и техники Российского союза научных и инженерных общественных объединений.

Нечаев, Алексей Д. 2017. «Основания и поводы (де)криминализации». *Российский юридический журнал* 4 (115): 91–101.

Осипенко, Анатолий Л. 2017. «Организованная преступная деятельность в киберпространстве: тенденции и противодействие». *Юридическая наука и практика: Вестник Нижегородской академии МВД России* 4 (40): 181–188.

Пелевина, Алла В. 2017. «Ответственность за преступления в сфере компьютерной информации в странах Балтии». *Татищевские чтения: актуальные проблемы науки и практики:* материалы XIV Международной научно-практической конференции: в 4 т. Т. 2, 245–248. Тольятти, Волжский университет имени В. Н. Татищева (институт).

Скляров, Сергей В., Константин Н. Евдокимов. 2016. «Современные подходы к определению понятия, структуры и сущности компьютерной преступности в Российской Федерации». *Криминологический журнал Байкальского государственного университета экономики и права* 10 (2): 322–330.

Barclay, Corlane. 2017. "Cybercrime and legislation: A critical reflection on the Cybercrimes act, 2015 of Jamaica". *Commonwealth Law Bulletin* 43 (1): 77–107.

Béla, Simon. 2016. "Hacktivism and its status in Hungary". *Magyar Rendészet* 16 (2): 161–174.

Boddy, Matt. 2018. "Phishing 2.0: The new evolution in cybercrime". *Computer Fraud & Security* 11: 8–10.

Broadhurst, Roderic, Peter Grabovsky, Mamoun Alazab, Brigitte Bouhours, Steve Chon. 2014. "An analysis of the nature of groups engaged in cyber crime". *International Journal of Cyber Criminology* 8 (1): 1–20.

Calcara, Giulio, Peter Sund, Matti Tolvanen. 2019. *Cybercrime, law and technology in Finland and beyond*. Tampere, Police University College of Finland Publ.

Fortes, Vinícius B., Salete O. Boff. 2017. "An analysis of cybercrimes from a global perspective on penal law". *Revista Brasileira de Direito* 13 (1): 7–24.

Hutchings, Alice. 2014. "Crime from the keyboard: Organised cybercrime, co-offending, initiation and knowledge transmission". *Crime, Law and Social Change* 62 (1): 1–20.

Jirovský, Václav, Andrej Pastorek, Max Mühlhäuser, Andrea Tundis. 2018. "Cybercrime and organized crime". *Proceedings of the 13th International Conference on Availability, Reliability and Security — ARES 2018*. Hamburg: Association for Computing Machinery Publ. Accessed August 14, 2020. https://dl.acm.org/doi/pdf/10.1145/3230833.3233288.

Karagiannopoulos, Vasileios. 2018. "Contemporary norms and law and hacktivism". *Living with Hacktivism*, 91–142. Cham, Palgrave Macmillan.

Lavorgna, Anita, Anna Sergi. 2016. "Serious, therefore organised? A critique of the emerging 'cyber-organised crime' rhetoric in the United Kingdom". *International Journal of Cyber Criminology* 10 (2): 170–187.

Leukfeldt, Rutger E., Anita Lavorgna, Edward R. Kleemans. 2017. "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* 23 (3): 287–300.

Li, Xiang. 2013. "Hacktivism and the First Amendment: Drawing the line between cyber protests and crime". *Harvard Journal of Law & Technology* 27 (1): 302–323.

McDaniel, Brandon. 2018. "An in-depth look into cybercrime". *Themis: Research Journal of Justice Studies and Forensic Science* 6 (1): 148–162.

Rose-Ackerman, Susan, Bonnie J. Palifka. 2018. "Corruption, organized crime, and money laundering". *Institutions, Governance and the Control of Corruption*, 75–111. Cham, Palgrave Macmillan.

Shultz, Charlotte B. 2016. "Cybercrime: An analysis of current legislation in South Africa". LLM diss., University of Pretoria.

Tanczer, Maria L. 2016. "Hacktivism and the male-only stereotype". *New Media & Society* 18 (8): 1599–1615.

Viano, Emilio C. 2016. "Cybercrime: Definition, typology, and criminalization". *Cybercrime, Organized Crime, and Societal Responses*, 3–22. Cham, Springer.
Webber, Craig, Michael Yip. 2018. "The rise of Chinese cyber warriors: Towards a theoretical model of online hacktivism". *International Journal of Cyber Criminology* 12 (1): 230–254.
Xiaobing, Li, Yongfeng Qin. 2018. "Research on criminal jurisdiction of computer cybercrime". *Procedia Computer Science* 131: 793–799.

Статья поступила в редакцию 16 августа 2020 г.;
рекомендована к печати 10 декабря 2021 г.

Контактная информация:

Мосечкин Илья Николаевич — канд. юрид. наук, доц.; weretowelie@gmail.com

Criminal liability for organizing a stable group of persons aimed at committing crimes in the field of computer information

I. N. Mosechkin

Vyatka State University,
36, ul. Moskovskaya, Kirov, 610000, Russian Federation

For citation: Mosechkin, Ilya N. 2022. "Criminal liability for organizing a stable group of persons aimed at committing crimes in the field of computer information". *Vestnik of Saint Petersburg University. Law* 1: 28–45. https://doi.org/10.21638/spbu14.2022.102 (In Russian)

The article analyzes legal problems arising in connection with the establishment of criminal liability for organizing a stable group of persons for committing crimes in the field of computer information. The urgency of this topic is due to the negative dynamics of crimes associated with computer technology and committed by criminal communities or organizations as well as the constant growth of damage from them. The author evaluates the current criminal law measures to counter organized cybercrime, identifying their shortcomings. The provisions of domestic and foreign criminal legislation were analyzed, which made it possible to identify some legal gaps and identify ways to overcome them. The article proves that the Criminal Code of the Russian Federation does not fully cover cases of the creation of organized criminal groups aimed at committing illegal activities in the field of computer information. In particular, responsibility is not differentiated between a group of persons by prior conspiracy and an organized group; the category of crimes and the absence of the purpose of making profit do not allow qualifying the act as committed by a criminal community or a criminal organization. It is advisable to recognize the very fact of the creation of illegal organized formations as a separate tort, as is done in the legislation of individual countries of the "common law" legal family, as well as in domestic norms regulating countering terrorism and extremism. It is proposed to include in the Criminal Code of the Russian Federation a norm providing for responsibility for organizing a stable group of persons aimed at committing crimes in the field of computer information. The wording of the corresponding article has been formulated, which can be used as a recommendation when improving legislation.

Keywords: computer information, computer crime, organized group, criminal community, cybercrime, public safety.

References

Abdulatipov, Abdulatip M. 2016. "Organizing a terrorist community and participating in it (criminal-legal aspects)". *Iuridicheskii vestnik Dagestanskogo gosudarstvennogo universiteta* 18 (2): 91–99. (In Russian)

Aulov, Artem N. 2016. "Organization of terrorist community (part 1 of the Article 205[4] of the Russian Federation Criminal Code): Questions of criminal legal content". *Teoriia i praktika obshchestvennogo razvitiia* 6: 101–104. (In Russian)
Barclay, Corlane. 2017. "Cybercrime and legislation: A critical reflection on the Cybercrimes act, 2015 of Jamaica". *Commonwealth Law Bulletin* 43 (1): 77–107.
Begishev, Il'dar R., Zarina I. Khisamova, Sergei G. Nikitin. 2020. "The Organization of hacking community: Criminological and criminal law aspects". *Vserossiiskii kriminologicheskii zhurnal* 14 (1): 96–105. (In Russian)
Béla, Simon. 2016. "Hacktivism and its status in Hungary". *Magyar Rendészet* 16 (2): 161–174.
Boddy, Matt. 2018. "Phishing 2.0: The new evolution in cybercrime". *Computer Fraud & Security* 11: 8–10.
Broadhurst, Roderic, Peter Grabovsky, Mamoun Alazab, Brigitte Bouhours, Steve Chon. 2014. "An analysis of the nature of groups engaged in cyber crime". *International Journal of Cyber Criminology* 8 (1): 1–20.
Calcara, Giulio, Peter Sund, Matti Tolvanen. 2019. *Cybercrime, law and technology in Finland and beyond*. Tampere, Police University College of Finland Publ.
Fortes, Vinícius B., Salete O. Boff. 2017. "An analysis of cybercrimes from a global perspective on penal law". *Revista Brasileira de Direito* 13 (1): 7–24.
Glazkova, Liliia V. 2019. "Features of modern organised criminal groups". *Monitoring pravoprimeneniia* 1 (30): 54–60. (In Russian)
Gracheva, Iuliia V., Sergei V. Malikov, Aleksandr I. Chuchaev. 2020. "Preventing deviations in the digital world by criminal law means". *Pravo. Zhurnal Vysshei shkoly ekonomiki* 1: 188–210. (In Russian)
Grebenkin, Fedor B., Liubov' A. Kovrizhnykh. 2017. "Some of the problems of objective evidence of a crime under Article 273 of the Criminal Code of Russian Federation". *Vestnik gumanitarnogo obrazovaniia* 2: 71–77. (In Russian)
Hutchings, Alice. 2014. "Crime from the keyboard: Organised cybercrime, co-offending, initiation and knowledge transmission". *Crime, Law and Social Change* 62 (1): 1–20.
Jirovský, Václav, Andrej Pastorek, Max Mühlhäuser, Andrea Tundis. 2018. "Cybercrime and organized crime". *Proceedings of the 13th International Conference on Availability, Reliability and Security — ARES 2018*. Hamburg, Association for Computing Machinery Publ. Accessed August 14, 2020. https://dl.acm.org/doi/pdf/10.1145/3230833.3233288.
Karagiannopoulos, Vasileios. 2018. "Contemporary norms and law and hacktivism". *Living with Hacktivism*, 91–142. Cham, Palgrave Macmillan.
Klimenko, Iurii A. 2017. "Extremist community formation: Qualification problems". *Lex Russica* 3 (124): 123–132. (In Russian)
Kochoi, Samvel M. 2016. "Gaps in anti-terrorism legislation and proposals for bridging them". *Vserossiiskii kriminologicheskii zhurnal* 10 (4): 740–749. (In Russian)
Lavorgna, Anita, Anna Sergi. 2016. "Serious, therefore organised? A critique of the emerging "cyber-organised crime" rhetoric in the United Kingdom". *International Journal of Cyber Criminology* 10 (2): 170–187.
Leukfeldt, Rutger E., Anita Lavorgna, Edward R. Kleemans. 2017. "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* 23 (3): 287–300.
Li, Xiang. 2013. "Hacktivism and the First Amendment: Drawing the line between cyber protests and crime". *Harvard Journal of Law & Technology* 27 (1): 302–323.
McDaniel, Brandon. 2018. "An in-depth look into cybercrime". *Themis: Research Journal of Justice Studies and Forensic Science* 6 (1): 148–162.
Mosechkin, Ilya N. 2021. "Criminal liability for the creation of organized groups aimed at committing computer crimes under the laws of foreign countries". *Nauka, tekhnologii, obshchestvo — NTO–2021*: Sbornik nauchnykh statei po materialam Vserossiiskoi nauchnoi konferentsii, 165–168. Krasnoyarsk, Krasnoiarskii kraevoi Dom nauki i tekhniki Rossiiskogo soiuza nauchnykh i inzhenernykh obshchestvennykh ob"edinenii Publ. (In Russian)
Nechaev, Aleksei D. 2017. "The grounds and occasions of (de)criminalization". *Rossiiskii iuridicheskii zhurnal* 4 (115): 91–101. (In Russian)
Osipenko, Anatolii L. 2017. "Organized criminal activities in cyberspace: Trends and fighting". *Iuridiches-*

kaia nauka i praktika: Vestnik Nizhegorodskoi akademii MVD Rossii 4 (40): 181–188. (In Russian)
Pelevina, Alla V. 2017. "Accountability for crimes in the field of computer information in the Baltic States". *Tatishchevskie chteniia: Aktual'nye problemy nauki i praktiki*: materialy XIV Mezhdunarodnoi nauchno-prakticheskoi konferentsii: in 4 vols. Vol. 2, 245–248. Tolyatti, Volzhskiy universitet imeni V. N. Tatishcheva (institut) Publ. (In Russian)
Rose-Ackerman, Susan, Bonnie J. Palifka. 2018. "Corruption, organized crime, and money laundering". *Institutions, Governance and the Control of Corruption*, 75–111. Cham, Palgrave Macmillan.
Shultz, Charlotte B. 2016. "Cybercrime: An analysis of current legislation in South Africa". LLM diss., University of Pretoria.
Skliarov, Sergei V., Konstantin N. Evdokimov. 2016. "Modern approaches to the concept, structure and nature of computer crime in The Russian Federation". *Kriminologicheskii zhurnal Baikal'skogo gosudarstvennogo universiteta ekonomiki i prava* 10 (2): 322–330. (In Russian)
Tanczer, Maria L. 2016. "Hacktivism and the male-only stereotype". *New Media & Society* 18 (8): 1599–1615.
Viano, Emilio C. 2016. "Cybercrime: Definition, typology, and criminalization". *Cybercrime, Organized Crime, and Societal Responses*, 3–22. Cham, Springer.
Webber, Craig, Michael Yip. 2018. "The rise of Chinese cyber warriors: Towards a theoretical model of online hacktivism". *International Journal of Cyber Criminology* 12 (1): 230–254.
Xiaobing, Li, Yongfeng Qin. 2018. "Research on criminal jurisdiction of computer cybercrime". *Procedia Computer Science* 131: 793–799.

Received: August 16, 2020
Accepted: December 10, 2021

Author's information:

Ilya N. Mosechkin — PhD in Law, Associate Professor; weretowelie@gmail.com