ISSN 2500-4255

УДК 343.9
DOI 10.17150/2500-4255.2020.14(1).96-105

ОРГАНИЗАЦИЯ ХАКЕРСКОГО СООБЩЕСТВА: КРИМИНОЛОГИЧЕСКИЙ И УГОЛОВНО-ПРАВОВОЙ АСПЕКТЫ

И.Р. Бегишев[1], З.И. Хисамова[2], С.Г. Никитин[1]
[1] Казанский инновационный университет им. В.Г. Тимирясова (ИЭУП), г. Казань, Российская Федерация
[2] Краснодарский университет Министерства внутренних дел Российской Федерации, г. Краснодар, Российская Федерация

Информация о статье

Дата поступления
23 сентября 2019 г.

Дата принятия в печать
10 февраля 2020 г.

Дата онлайн-размещения
28 февраля 2020 г.

Ключевые слова
Кибербезопасность; киберкриминология; киберпреступление; киберпреступность; организация преступного сообщества (преступной организации) или участие в нем; уголовная ответственность; преступная организация; преступное сообщество; хакер; хакерское сообщество; хакерская группа; хактивизм; цифровые технологии; цифровая криминология

Аннотация. Цифровые технологии являются неотъемлемой частью нашей повседневной жизни. Независимо от того, есть ли у нас дома компьютер, используем ли мы возможность получения государственных и муниципальных услуг в цифровой форме или просто эксплуатируем электронные гаджеты, зависимость общества от технологий возрастает. Безопасная цифровая среда повышает доверие населения и способствует созданию стабильного и процветающего государства. Правительство и бизнес-сообщество также используют возможности технологической революции за счет более широкого внедрения и применения цифровых технологий. Традиционные формы преступности тоже эволюционировали. Преступные объединения начинают перемещаться в информационно-телекоммуникационную сеть Интернет. Цифровая преступность развивается невероятно быстрыми темпами, постоянного появляются новые виды преступных деяний. Поэтому мы должны идти в ногу с цифровыми технологиями, понимать возможности, которые они создают для киберпреступников, и то, как их можно использовать в качестве инструмента для борьбы с киберпреступностью. На фоне активного проникновения цифровых технологий на протяжении последних трех десятилетий во все сферы жизни общества происходило формирование особой категории правонарушителей — так называемых хакеров. Преступные группы хакеров общественно опасны, поскольку, объединившись, они способны спланировать мощную компьютерную атаку, в том числе и в отношении объектов критической информационной инфраструктуры. Кроме того, хакерские группы стали вполне реальной угрозой как для правительств, крупных корпораций и военных ведомств, так и для частных лиц. Прогнозировавшаяся несколько лет назад экспертами тенденция к размытию граней между хакерскими группами и организованной преступностью стала явью. И сейчас фактически можно говорить о возникновении нового самостоятельного вида организованной преступности — хакерского сообщества. Указанные обстоятельства обусловливают необходимость создания специальной нормы, предусматривающей ответственность за организацию хакерского сообщества и участие в нем. Наличие такой нормы позволит обеспечить комплексный подход к уголовно-правовому противодействию деятельности таких преступных сообществ и адекватную уголовно-правовую оценку действий лиц, выступающих в качестве организаторов — координаторов хакерских организаций.

THE ORGANIZATION OF HACKING COMMUNITY: CRIMINOLOGICAL AND CRIMINAL LAW ASPECTS

Ildar R. Begishev[1], Zarina I. Khisamova[2], Sergey G. Nikitin[1]
[1] Kazan Innovative University named after V.G. Timiryasov (IEML), Kazan, the Russian Federation
[2] Krasnodar University of the Ministry of Internal Affairs of the Russian Federation, Krasnodar, the Russian Federation

Article info

Received
2019 September 23

Accepted
2020 February 10

Available online
2020 February 28

Abstract. Digital technology is an integral part of our daily lives. Regardless of whether we have a computer at home, whether we use the possibilities of obtaining state and municipal services in digital form or simply operate electronic gadgets, society's dependence on technology is increasing. A secure digital environment enhances trust and contributes to the creation of a stable and prosperous nation. Government and the business community are also taking advantage of the technological revolution through greater adoption and use of digital technologies. Traditional forms of crime have also evolved, as criminal associations increasingly use the information and telecommunications network — the Internet — to commit cybercrimes and increase

ISSN 2500-4255

Keywords
Cybersecurity; cybercriminology; cybercrime; organization of a criminal community (criminal organization) or participation in it; criminal responsibility; criminal organization; criminal community; hacker; hacking community; hacker group; hacktivism; digital technologies; digital criminology

their profits. Digital crime is developing at an incredibly fast pace, and new types of criminal acts are constantly emerging. So we need to keep up with digital technologies, understand the opportunities they create for cybercriminals, and how they can be used as a tool to combat cybercrime. The active use of digital technologies in all spheres of social life in the last three decades formed a background for the emergence of a special type of criminals — the so-called hackers. Criminal groups of hackers pose a public danger because, if they unite, they are capable of planning a large-scale computer attack which could target, among other things, critically important information infrastructure objects. Besides, hacker groups have become a real danger for both governments, large corporations, the military, and for private persons. The trend for blurring the boundaries between hacker groups and organized crime, that the experts predicted a few years ago, has now become a reality. In fact, it is possible to say that a new independent type of organized crime has emerged — the hacking community. These circumstances make it necessary to develop a special norm that provides for the liability for organizing hacking community or participating in it. Such a norm will allow for a complex approach to the criminal law counteraction against such criminal groups by ensuring an adequate criminal law assessment of the actions of the organizers and coordinators of hackers' organizations.

Проникновение цифровых технологий в нашу жизнь носит по-настоящему глобальный характер. Цифровые преступления достаточно опасны еще и тем, что сегодня современные IT-технологии полностью вошли во все сферы деятельности людей и инициировали преобразование индустриального социума в информационное общество.

В настоящее время борьба с цифровой преступностью является одной из наиболее актуальных проблем во всем мире. Увеличивающееся количество киберпреступников, постоянное развитие цифровых технологий и, как следствие, новые возможности «совершенствования» этих преступлений создают очередные угрозы для глобальных информационных сетей и в целом для общества [1, с. 29]. Угроза киберпреступности продолжает расти, поскольку преступники адаптируются к новым мерам безопасности, берут «на вооружение методы социальной инженерии» [2, p. 5] и вообще активно трансформируются в условиях развития цифровой экономики [3, p. 8] и применения искусственного интеллекта [4].

По прогнозам авторитетного американского исследовательского центра по вопросам кибербезопасности Cybersecurity Ventures, мировой оборот киберпреступности к 2021 г. достигнет 6 трлн дол. в год по сравнению с 3 трлн дол. в 2015 г. [5]. Ожидается, что через три года киберпреступность будет более прибыльной, чем глобальная торговля всеми основными нелегальными наркотиками, вместе взятыми [6]. Киберпреступность является существенной угрозой для абсолютно любой организации в мире и одной из самых больших проблем человечества [7].

Стоит особо подчеркнуть, что рост киберпреступности неразрывно связан с увеличением числа лиц, вовлеченных в преступную деятельность, в том числе в ее организованных формах. Отсутствие физических границ в сети Интернет позволяет использовать ее в целях совершения транснациональных преступлений [8].

На фоне активного проникновения цифровых технологий на протяжении последних трех десятилетий во все сферы жизни общества происходило формирование особой категории правонарушителей — так называемых хакеров (от англ. hack — разрубать). Термин «хакерство» впервые был применен в конце 1950-х гг. в протоколе заседания клуба Tech Model Rail Road в Массачусетском технологическом институте. Сегодня данный термин широко употребляется в значении взлома защиты компьютерных сетей и систем, создания вредоносных программ и совершения компьютерных атак.

Следует отметить, что такое столь часто используемое понятие, как «хакер», на сегодняшний день не получило единого толкования, которое бы устраивало как специалистов в IT-сфере, так и представителей юридического и научного сообщества.

В широком смысле хакеры — лица, совершающие киберпреступления (мошенничество в сфере компьютерной информации, незаконное собирание сведений, составляющих коммерческую, налоговую либо банковскую тайну, и др.) посредством неправомерного доступа к компьютерной информации либо с использованием вредоносного программного обеспечения в киберпространстве (вирусов, троянских программ, DDoS-программ и т.д.) [9, с. 12].

В свою очередь отметим, что рассматриваемый термин сегодня используется для обозначения двух диаметрально противоположных направлений деятельности в цифровой сфере. Его первое значение характеризует личность с противоправными установками, чья деятельность носит ярко выраженный криминальный характер; второе значение подразумевает специалиста в области информационных технологий, профессионального программиста и разработчика компьютерных систем [10, с. 116].

Поддержим точку зрения Е.А. Маслаковой, согласно которой ставить знак равенства между хакерами и лицами, совершающими преступления в сфере компьютерной информации или с использованием цифровых технологий, не совсем верно [там же, с. 117]. Указанные понятия соотносятся как частное и общее.

Длительное время учеными-криминологами предлагались различные типологии хакеров, выделяемые как по мотивам [11; 12], так и по характеру преступной деятельности [13; 14]. При этом акцент в исследованиях в основном делался на личность хакера как одиночного преступника.

Интересной и отражающей современные тенденции представляется криминологическая типология хакеров, описанная в отчете The Business of Hacking, подготовленном известной американской компанией Hewlett Packard Enterprise[1]. В документе подчеркивается, что хакеры стараются работать совместно, ведут себя как небольшие корпорации со службами поддержки клиентов и бухгалтерией. При этом их организационный состав идентичен сложной бизнес-структуре, в которой помимо программистов и разработчиков есть и те, кто занимается обслуживанием клиентов и финансовыми вопросами. Кроме того, «сотрудники» набираются и проверяются так же, как и в любой другой серьезной организации.

Так, в отчете выделяются следующие типы хакеров:

– государственные «хакеры», движимые идеей патриотизма или воинским долгом, чья деятельность координируется государством;

– хактивисты — идеологически мотивированные лица, преследующие определенные цели, зачастую деструктивные и направленные на разрушение учреждений и объектов инфраструктуры;

– киберпреступники — лица, мотивированные на получение прибыли;

– хакеры-эгоисты — лица, желающие стать знаменитыми и получить всеобщее признание своей деятельности;

– хакеры с хобби или профессионалы, для которых хакинг выступает в качестве забавного времяпрепровождения [15].

С данной типологией нельзя не согласиться.

Е.А. Маслаковой приводится классификация, представленная в указе президента США, направленном на борьбу с компьютерной преступностью:

– неорганизованные субъекты (сотрудники организаций, хакеры);

– организованные субъекты (представители организованной преступности, промышленного шпионажа, террористы);

– представители специальных служб других государств [10, с. 116].

С этим мнением мы также солидарны. Вместе с тем сегодня становится очевидным, что хакерские группы представляют собой вполне реальную угрозу как для крупных корпораций, военных ведомств и правительств, так и для частных лиц. Причем речь идет не о хакерах-любителях, а об их серьезных, профессиональных группах. Они вызывают опасения у организаций, над защитой информационных систем которых трудятся целые подразделения [16].

Как справедливо отмечают зарубежные исследователи из Обсерватории киберпреступности Австралийского национального университета, что могут сделать люди, могут сделать и организации, и зачастую гораздо лучше. Очевидно, что многие, если не все, виды преступных организаций способны заниматься киберпреступностью. Интернет и связанные с ним технологии прекрасно подходят для координации действий лиц, находящихся в разных точках земного шара [17].

Хакеры, объединившись в группы, способны спланировать мощную компьютерную атаку, в том числе и в отношении объектов критической информационной инфраструктуры. Вопросами противодействия таким преступлениям обеспокоено все мировое сообщество, ведь атаки против объектов жизнеобеспечения и обороны страны могут привести к глобальным жертвам и разрушениям [18, с. 10], утрате конфиденциальной цифровой информации [19].

Длительное время среди ученых-криминологов доминировало мнение, что большинство

[1] The Business of Hacking. URL: https://www.hpe.com/h30683/ww/en/hpe-technology-now/The-business-of-hacking_1589130.html.

организованных киберпреступлений является работой квалифицированных технических специалистов, которые применяют свои знания в целях осуществления преступной деятельности в информационно-телекоммуникационной сети Интернет. Отдельные ученые выделяли традиционные преступные группы, которые используют цифровые технологии для достижения преступных целей.

В исследовании А.Л. Осипенко названо три укрупненных типа лиц, осуществляющих противоправную деятельность в глобальных сетях:

– представители традиционной преступности, осознавшие преимущества информационно-телекоммуникационных технологий при осуществлении традиционных посягательств;

– представители хакерского сообщества, обладающие специальной подготовкой и совершающие преступления, возможные только в глобальных компьютерных сетях;

– организованная преступность, все более активно привлекающая для достижения своих целей первые две категории лиц [20, с. 209].

По мнению А.Ю. Чупровой, «преступные группы, занимающиеся информационным криминальным бизнесом, можно подразделить на:

– традиционные группы, структура и связи которых аналогичны тем, что действуют и в иных преступных группах;

– виртуальные преступные группы, участники которых объединены друг с другом посредством информационно-телекоммуникационных сетей и не вступают друг с другом в непосредственные личные контакты;

– смешанные группы, участники которых могут вступать в коммуникации как непосредственно, так и исключительно с использованием информационных технологий» [21].

Не умаляя достоинств приведенных классификаций, все же отметим, что прогнозировавшаяся несколько лет назад экспертами тенденция к размытию граней между хакерскими группами и организованной преступностью сегодня стала явью [17]. И фактически сейчас можно говорить о возникновении нового вида организованной преступности — хакерского сообщества.

М. Макгуайр по результатам анализа большой выборки преступных посягательств в IT-сфере констатирует, что до 80 % киберпреступлений может быть результатом той или иной формы организованной деятельности. Однако это не означает, что данные группы принимают форму традиционных иерархических организованных преступных групп или что эти группы совершают исключительно цифровые преступления. По мнению исследователя, более вероятно, что традиционные организованные преступные группы стали частью цифрового мира [22].

Преступные группы демонстрируют различные уровни организации в зависимости от того, направлена ли их деятельность исключительно на онлайн-цели, используются ли онлайн-инструменты для совершения преступлений в реальном мире и едины ли цели у преступной деятельности в Сети и реальном мире [там же]. Цифровые технологии в руках даже одного человека, не говоря уже об организованных преступных группах, могут превратиться в небывалое по мощности орудие совершения преступлений [23, с. 261].

Несмотря на то что эксперты в области обеспечения информационной безопасности[2] наряду с научным сообществом [24–28] отмечают все большее слияние киберпреступности с организованной преступностью вплоть до полной трансформации одной в другую, уголовно-правовые подходы к регулированию рассматриваемых отношений все еще не отражают объективной картины происходящего.

С точки зрения Пленума Верховного Суда Российской Федерации, «организованная преступность в ее различных проявлениях посягает на общественную безопасность, жизнь и здоровье граждан, собственность, нарушает нормальное функционирование государственных, коммерческих и иных организаций и общественных объединений»[3], ввиду чего адекватная законодательная реакция на такие преступные проявления и грамотное применение норм об ответственности за создание преступного сообщества (преступной организации) представляются первостепенной задачей. К сожалению, действующее уголовное законодательство за создание преступного сообщества нельзя признать удовлетворительным и отвечающим современным реалиям.

[2] ISTR Internet Security Threat Report // Symantec Corporation. 2019. Vol. 24. URL: https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf.

[3] О судебной практике рассмотрения уголовных дел об организации преступного сообщества (преступной организации) или участии в нем (ней) : постановление Пленума Верхов. Суда РФ от 10 июня 2010 г. № 12 // Российская газета. 2010. № 130.

Общепринятые определения и характеристики организованной преступности очевидно устарели, поскольку эволюция этого явления сама по себе уже произошла. Справедливости ради стоит отметить ряд попыток законодателя усилить ответственность за создание отдельных разновидностей преступных групп — террористического и экстремистского сообществ, незаконного вооруженного формирования, а также за бандитизм. Стремление законодателя дать четкое определение указанным видам сообществ вполне оправданно и разумно, однако многочисленные изменения и дополнения уголовного законодательства по-прежнему оставили нерешенными некоторые вопросы их соотношения [29, с. 175].

Между тем угроза от деятельности хакерских организаций ничуть не меньше угрозы от деятельности традиционных преступных групп и сообществ, а порой в разы превосходит ее. Вместе с тем применение положений ст. 210 «Организация преступного сообщества (преступной организации) или участие в нем (ней)» Уголовного кодекса Российской Федерации[4] и иных положений института соучастия в преступлении в форме совершения преступления преступным сообществом (преступной организацией) невозможно.

Такое положение дел вызвано сложившейся в науке и практике традиционной характеристикой преступного сообщества (преступной организации) и вытекающими из нее признаками данного сообщества (данной организации), которые являются обязательными для правоприменителей при квалификации преступления. Так, «преступление признается совершенным преступным сообществом (преступной организацией), если оно совершено структурированной организованной группой или объединением организованных групп, действующих под единым руководством, члены которых объединены в целях совместного совершения одного или нескольких тяжких либо особо тяжких преступлений для получения прямо или косвенно финансовой или иной материальной выгоды» (ч. 4 ст. 35 УК РФ).

Таким образом, преступное сообщество (преступная организация) в силу существующей судебной практики характеризуется тремя отличительными признаками:

– структурированность;

– организованность, т.е. четкое распределение функций между соучастниками, тщательное планирование преступной деятельности, наличие внутренней жесткой дисциплины;

– цель создания — совершение тяжких и особо тяжких преступлений для получения прямо или косвенно финансовой или иной материальной выгоды[5].

При отсутствии одного из признаков преступное объединение нескольких лиц не может быть признано преступным сообществом, и ответственность для них наступает лишь как за совершение преступлений организованной группой [30].

Отдельные из перечисленных признаков преступной организации вполне применимы для характеристики хакерского сообщества, но, к сожалению, не все.

Следует поддержать позицию отдельных исследователей, состоящую в том, что структурированность, выраженная в форме иерархичного построения преступных групп, не всегда имеет место в системе построения современных преступных организаций, в особенности существующих в киберпространстве. В правоприменительной практике достаточно примеров, когда отдельные ячейки (группировки) различной криминальной «квалификации» действовали в условиях добровольного объединения партнерских усилий.

Мы согласны с мнением А.Ю. Чупровой о том, что «отмирание соподчиненности в таких группах связано с фактической анонимностью участников, использующих для решения общих задач современные коммуникации, не требующие непосредственных контактов» [21].

А.Ю. Чупровой также выделены ключевые характеристики «виртуальной преступной группы»:

– тщательная подготовка к совершению преступления;

– использование сложных способов совершения преступлений;

– распределение ролей при совершении преступлений при равенстве всех ее участников;

– наличие координирующего звена;

– наличие единого криминального пространства в Сети;

[4] Уголовный кодекс Российской Федерации : федер. закон РФ от 13 июня 1996 г. № 63-ФЗ // Собрание законодательства РФ. 1996. № 25. Ст. 2954.

[5] О судебной практике рассмотрения уголовных дел об организации преступного сообщества (преступной организации) или участии в нем (ней) : постановление Пленума Верхов. Суда РФ от 10 июня 2010 г. № 12.

– использование информационных технологий в качестве инструмента формирования преступного процесса [21].

Однако автор резюмирует: несмотря на то что на практике зачастую речь идет о совершении преступлений преступным сообществом, объединяющим как группы, существующие в офлайн-пространстве, так и виртуальные группы, согласно букве закона такие сообщества нельзя характеризировать как организованные преступные сообщества ввиду отсутствия устойчивых связей у групп, существующих в киберпространстве, а также по причине единичных фактов участия ее членов в эпизодах преступной деятельности. В результате автор приходит к выводу о целесообразности «оценивать деятельность виртуальных криминальных структур, осуществляющих преступную деятельность в сфере электронной коммерции исключительно в информационно-телекоммуникационных сетях, в частности сети Интернет, как преступления, совершенные организованной группой» [там же].

Выражая солидарность с позицией А.Ю. Чупровой по отдельным аспектам, касающимся признаков рассматриваемых преступных образований, все же позволим себе не согласиться с высказанным мнением относительно правил квалификации.

На наш взгляд, трудности выявления и квалификации совершения преступлений в составе организованных преступных сообществ обусловлены рядом объективных причин. Во-первых, это несовершенство устоявшегося определения преступного сообщества, не отвечающего современным реалиям. Во-вторых, преступная деятельность хакерских сообществ отличается высокой латентностью, из-за чего установление и доказывание наличия устойчивых связей, их характеризующих, становится для правоохранительных органов неразрешимой задачей. В-третьих, латентность преступной деятельности хакерских сообществ неразрывно связана с проблемой низкой эффективности деятельности правоохранительных органов, а точнее, с отсутствием у них достаточного уровня компетенций для выявления сложных иерархических связей, ввиду чего в материалах судебной практики имеют место лишь случаи совершения преступлений только в составе группы лиц либо организованной группой, в большинстве случаев являющейся лишь отдельной ячейкой преступного синдиката.

Между тем, не исключая возможности объединения отдельных преступных групп для совершения единичных преступлений, все же отметим, что существуют хакерские сообщества, обладающие устойчивыми связями и внутренней структурой, чья деятельность осуществлялась в целях реализации общих преступных намерений единым руководством. Как справедливо подметил Д. Мэнки, «киберпреступность превратилась в сложную, высокоорганизованную иерархию, включающую лидеров, инженеров, пехоту и наемных денежных мулов» [31].

Рассмотрим подробнее особенности построения и организации деятельности хакерского сообщества на примере преступной организации, занимавшейся хищениями денежных средств через системы дистанционного банковского обслуживания, чья деятельность была прекращена сотрудниками ФСБ России и МВД России совместно с Group-IB, международной компанией по предотвращению и расследованию киберпреступлений [32].

Описываемый случай уникален, так как впервые в мировой правоохранительной практике удалось установить всю преступную цепочку, включая организатора группы, который владел бот-сетью, и отдельные группы: «заливщиков», проводящих мошеннические операции; «дропов» — лиц, непосредственно осуществляющих обналичивание похищенных денежных средств. В преступной организации также выделялись администраторы, отвечавшие за организационное обеспечение: аренду, настройку, обслуживание и работоспособность серверов; разработчики, занимавшиеся разработкой вредоносного программного обеспечения и эксплойтов[6]; «трафферы», обеспечивавшие поступление вредоносного трафика, и поставщики[7]. От действий хакерской группы пострадали клиенты свыше 100 банков по всему миру [там же].

Злоумышленники взламывали сайты, которые активно используют в своей деятельности бухгалтеры, а также сайты популярных СМИ и крупных магазинов и заражали их вредонос-

[6] Эксплойт — компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении, которые применяются для проведения компьютерной атаки на информационную систему.

[7] Схема преступной деятельности рассматриваемой хакерской группы предоставлена компанией Group-IB исключительно в научных целях.

ными программами Win32/Carberp и Win32/Rdpdor. Установив скрытный удаленный доступ к компьютеру потенциальной жертвы и обнаружив на нем программы и реквизиты для работы с банковскими счетами, «заливщики» формировали мошенническое платежное поручение о перечислении денежных средств на заранее подготовленный счет. После чего похищенные деньги обналичивались посредством банковских карт, оформленных на подставных физических или юридических лиц, «обнальщиками», отвечавшими за организацию работы «дропов» («мулов») — лиц, непосредственно открывавших банковские счета или платежные карты, на которые переводились похищенные денежные средства, и впоследствии снимавших похищенные денежные средства для последующей их передачи «обнальщику» [32].

В числе характеристик нормативно закрепленной трактовки преступного сообщества (преступной организации), не позволяющих применять к хакерским сообществам положения ст. 35 УК РФ, отдельными экспертами отмечалось наличие объединенного умысла на совершение тяжких и (или) особо тяжких преступлений [10]. Позволим себе не согласиться с указанным мнением в силу ряда объективных причин, в первую очередь ввиду наметившейся уголовной политики по усилению ответственности за преступления, совершаемые с использованием цифровых технологий.

Хакерское сообщество, за исключением сообщества хактивистов[8], создается и функционирует в основном для совершения цифровых преступлений с целью материального обогащения. Анализ санкций особо квалифицированных составов статей УК РФ, предусматривающих ответственность за совершение наиболее распространенных хакерских преступлений, позволяет заключить, что большая часть из них относится к категории тяжких преступлений: п. «г» ч. 3 ст. 158, ч. 4 ст. 159.3, ч. 4 ст. 159.6, ч. 3 ст. 171.2, ч. 4 ст. 174.1, ч. 4 ст. 274.1 УК РФ.

Однако, как отмечалось нами ранее, устоявшаяся в законе и теории трактовка признаков организованного преступного сообщества (организации) не позволяет применять указанные положения закона к хакерским сообществам. В связи с этим видится целесообразным внести изменения в ч. 4 ст. 35 УК РФ и в положения постановления Пленума Верховного Суда Российской Федерации «О судебной практике рассмотрения уголовных дел об организации преступного сообщества (преступной организации) или участии в нем (ней)», расширив толкование признаков такой формы соучастия, как организованное преступное сообщество (организация), с учетом признаков хакерского сообщества: необязательность иерархичного построения взаимоотношений между членами организованного преступного сообщества и структурированности, использование информационно-телекоммуникационных технологий как основного средства коммуникации, более широкое толкование роли организатора, выступающего в качестве координатора деятельности отдельных ячеек, возможная географическая распределенность структурных подразделений преступного сообщества вплоть до транснациональности.

Вместе с тем санкции за непосредственно «компьютерные» преступления, т.е. преступления в сфере компьютерной информации (ст. 272–274 УК РФ), не превышают пяти лет лишения свободы, т.е. относятся к категории средней тяжести. В свою очередь, совершение деяний, предусмотренных ст. 272, 273 УК РФ, зачастую является промежуточным этапом в цепочке незаконных действий на пути к достижению преступного результата. Однако при пресечении деятельности отдельных ячеек преступной организации, специализировавшихся только на неправомерном доступе либо создании, использовании и распространении вредоносных компьютерных программ, применение к ним положений ч. 4 ст. 35 УК РФ становится практически невозможным по причине трудноказуемости наличия умысла на совершение тяжкого преступления у участников сообщества, не имеющих прямых контактов между собой и находящихся на значительном удалении друг от друга.

Указанные обстоятельства обусловливают необходимость создания специальной нормы, предусматривающей ответственность за создание хакерского сообщества и участие в нем. Наличие такой нормы позволит обеспечить комплексный подход к уголовно-правовому противодействию деятельности таких преступных сообществ, обеспечив адекватную уголовно-правовую оценку действий лиц, выступающих в качестве организаторов — координаторов хакерских организаций.

[8] Хактивизм — политическое протестное движение против государственного контроля в информационно-телекоммуникационной сети Интернет.

Являясь сторонниками умеренного и конструктивного подхода, считаем целесообразным отметить, что инициируемая уголовно-правовая норма должна носить универсальный характер, что предопределяет исключение из ее диспозиции описания конкретных преступлений, для совершения которых была создана преступная организация. В условиях всеобщей цифровизации общественных отношений такой подход будет обладать превентивным эффектом с «определенным запасом прочности».

Подводя итог нашему исследованию, заключим, что хакерское сообщество сегодня становится самостоятельным видом преступного сообщества, которое посягает на национальную безопасность, собственность, нарушает нормальное функционирование государственных, коммерческих и иных организаций и в отдельных случаях наносит вред жизни и здоровью граждан. Существующие тенденции в преступном мире свидетельствуют не только о сращивании криминальных методов, но и о глубокой трансформации классической преступности в цифровую. В условиях несовершенства правоприменительной практики создание понятных, исключающих пробелы уголовно-правовых мер противодействия созданию хакерских сообществ и участию в них становится одним из ключевых и необходимых способов реагирования государства на растущие угрозы в цифровом пространстве.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Протасевич А.А. Борьба с киберпреступностью как актуальная задача современной науки / А.А. Протасевич, Л.П. Зверянская // Криминологический журнал Байкальского государственного университета экономики и права. — 2011. — № 3. — С. 28–33.

2. Eddolls M. Making Cybercrime Prevention the Highest Priority / M. Eddolls. — DOI: 10.1016/S1353-4858(16)30075-7 // Network Security. — 2016. — Vol. 2016, iss. 8. — P. 5–8.

3. Lee L. Cybercrime has evolved: it's time cyber security did too / L. Lee. — DOI: 10.1016/S1361-3723(19)30063-6 // Computer Fraud & Security. — 2019. — Vol. 2019, iss. 6. — P. 8–11.

4. Хисамова З.И. Правовое регулирование искусственного интеллекта / З.И. Хисамова, И.Р. Бегишев. — DOI: 10.17150/2411-6262.2019.10(2).19 // Baikal Research Journal. — 2019. — Т. 10, № 2. — URL: http://brj-bguep.ru/reader/article.aspx?id=23011.

5. Morgan S. Cybercrime Damages $6 Trillion By 2021 / S. Morgan // Cybersecurity Ventures. — URL: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021.

6. Periman K. How to Prevent the Bank Robbery No One Can See / K. Periman // Cisco Blogs. — URL: https://blogs.cisco.com/financialservices/how-to-prevent-the-bank-robbery-no-one-can-see.

7. Oyedele A. BUFFETT: This is 'the number one problem with mankind' / A. Oyedele // Business Insider. — URL: https://www.businessinsider.com/warren-buffett-cybersecurity-berkshire-hathaway-meeting-2017-5.

8. Антонов О.Ю. Выявление дополнительных эпизодов и новых видов порно-сексуальной преступной деятельности, совершаемой с использованием информационно-телекоммуникационных сетей / О.Ю. Антонов // Расследование преступлений: проблемы и пути их решения. — 2017. — № 3 (17). — С. 169–177.

9. Простосердов М.А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им : автореф. дис. … канд. юрид. наук : 12.00.08 / М.А. Простосердов. — Москва, 2016. — 28 с.

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

11. Parker D.B. Fighting Computer Crime / Donn B. Parker. — New York : Wiley Publisher, 1998. — 512 p.

12. Айков Д. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями / Д. Айков, К. Сейгер, У. Фонсторх. — Москва : Мир, 1999. — 351 с.

13. Rogers M. A New Hacker Taxonomy / M. Rogers. — Winnipeg : Univ. of Manitoba, 2000. — 85 p.

14. Buono L. Fighting cybercrime through prevention, outreach and awareness raising / L. Buono. — DOI: 10.1007/s12027-014-0333-4 // ERA Forum. — 2014. — Vol. 15, iss. 1. — P. 1–8.

15. Poremba S. Hackers Today Act More Like Small Businesses Than Thieves / S. Poremba // Hewlett Packard Enterprise Development LP. — URL: https://www.hpe.com/us/en/newsroom/blog-post/2017/03/hackers-today-act-more-like-small-businesses-than-thieves.html.

16. Волуйская М. Крупнейшие хакерские группировки мира. Инфографика / М. Волуйская // Аргументы и Факты. — 2017. — 11 марта.

17. Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime / R. Broadhurst, P. Grabosky, M. Alazab, S. Chon // International Journal of Cyber Criminology. — 2014. — Vol. 8, iss. 1. — P. 1–20.

18. Бегишев И.Р. Проблемы противодействия преступным посягательствам на информационные системы критически важных и потенциально опасных объектов / И.Р. Бегишев // Информационная безопасность регионов. — 2010. — № 1. — С. 9–13.

19. Бегишев И.Р. Уголовная ответственность за приобретение или сбыт цифровой и документированной информации, заведомо добытой преступным путем / И.Р. Бегишев // Актуальные проблемы экономики и права. — 2010. — № 1. — С. 123–126.

20. Осипенко А.Л. Сетевая компьютерная преступность: теория и практика борьбы / А.Л. Осипенко. — Омск : Ом. акад. МВД России, 2009. — 480 с.

21. Чупрова А.Ю. Особенности групповой преступности в сфере электронной коммерции / А.Ю. Чупрова // Преступность, уголовная политика, закон : материалы Всерос. науч.-практ. конф., Москва, 26–27 янв. 2016 г. / под ред. А.И. Долговой. — Москва, 2016. — С. 40–48.

22. McGuire M. Organised Crime in the Digital Age / M. McGuire. — London : John Grieve Centre for Policing and Security, 2012.

23. Суходолов А.П. Проблемы противодействия преступности в сфере цифровой экономики / А.П. Суходолов, Л.А. Колпакова, Б.А. Спасенников. — DOI: 10.17150/2500-4255.2017.11(2).258-267 // Всероссийский криминологический журнал. — 2017. — Т. 11, № 2. — С. 258–267.

24. Номоконов В.А. Киберпреступность как новая криминальная угроза / В.А. Номоконов, Т.Л. Тропина // Криминология: вчера, сегодня, завтра. — 2012. — № 24. — С. 45–55.

25. Скляров С.В. Современные подходы к определению понятия, структуры и сущности компьютерной преступности в Российской Федерации / С.В. Скляров, К.Н. Евдокимов. — DOI: 10.17150/1996-7756.2016.10(2).322-330 // Криминологический журнал Байкальского государственного университета экономики и права. — 2016. — Т. 10, № 2. — С. 322–330.

26. Grabosky P. Organized Cybercrime and National Security / P. Grabosky. — DOI: 10.1057/9781137474162_5 // Cybercrime Risks and Responses. Eastern and Western Perspectives / ed. R.G. Smith, R. Chak-Chung Cheung, L. Yiu-Chung Lau. — New York : Palgrave Macmillan, 2015. — P. 67–80.

27. Актуальные проблемы предупреждения преступлений в сфере экономики, совершаемых с использованием информационно-телекоммуникационных сетей / А.П. Суходолов, С.В. Иванцов, С.В. Борисов, Б.А. Спасенников. — DOI: 10.17150/2500-4255.2017.11(1).13-21 // Всероссийский криминологический журнал. — 2017. — Т. 11, № 1. — С. 13–21.

28. Узденов Р.М. Новые границы киберпреступности / Р.М. Узденов. — DOI: 10.17150/2500-4255.2016.10(4).649-655 // Всероссийский криминологический журнал. — 2016. — Т. 10, № 4. — С. 649–655.

29. Плешаков С.М. Экстремистское сообщество как разновидность организованной преступной группы / С.М. Плешаков // Актуальные проблемы взаимодействия общественности с органами государственной власти и органами местного самоуправления : материалы 2-й Всерос. науч.-практ. конф. — Саранск, 2017. — С. 174–177.

30. Научно-практический комментарий к Уголовному кодексу Российской Федерации от 13 июня 1996 г. № 63-ФЗ / Н.А. Агешкина, М.А. Беляев, Ю.В. Белянинова [и др.]. — Саратов : Ай Пи Эр Медиа, 2013. — 848 с.

31. Manky D. Cybercrime as a Service: a very Modern Business / D. Manky. — DOI: 10.1016/S1361-3723(13)70053-8 // Computer Fraud and Security. — 2013. — Vol. 2013, iss. 6. — P. 9–13.

32. Сомов С. Задержаны участники крупнейшей преступной группы, занимавшейся мошенничествами в системах интернет-банкинга / С. Сомов // Cnews Клуб. — URL: http://club.cnews.ru/blogs/entry/import_zaderzhany_uchastniki_krupnejshej_prestupnoj_gruppy_zanimavshejsya_moshennichestvami_v_sistemah_internetbankinga_420b.

REFERENCES

1. Protasyevich A.A., Zveryanskaya L.P. Fighting Cybercrimes as an Urgent Task for Contemporary Research. *Kriminologicheskii zhurnal Baikal'skogo gosudarstvennogo universiteta ekonomiki i prava = Criminology Journal of Baikal National University of Economics and Law*, 2011, no. 3, pp. 28–33. (In Russian).

2. Eddolls M. Making cybercrime prevention the highest priority. *Network Security*, 2016, vol. 2016, iss. 8, pp. 5–8. DOI: 10.1016/S1353-4858(16)30075-7.

3. Lee L. Cybercrime has evolved: it's time cyber security did too. *Computer Fraud & Security*, 2019, vol. 2019, iss. 6, pp. 8–11. DOI: 10.1016/S1361-3723(19)30063-6.

4. Khisamova Z.I., Begishev I.R. Legal Regulation of Artificial Intelligence. *Baikal Research Journal*, 2019, vol. 10, no. 2. DOI: 10.17150/2411-6262.2019.10(2).19. Available at: http://brj-bguep.ru/reader/article.aspx?id=23011. (In Russian).

5. Morgan S. Cybercrime Damages $6 Trillion By 2021. *Cybersecurity Ventures*. Available at: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021.

6. Periman K. How to Prevent the Bank Robbery No One Can See. *Cisco Blogs*. Available at: https://blogs.cisco.com/financialservices/how-to-prevent-the-bank-robbery-no-one-can-see.

7. Oyedele A. BUFFETT: This is 'the number one problem with mankind'. *Business Insider*. Available at: https://www.businessinsider.com/warren-buffett-cybersecurity-berkshire-hathaway-meeting-2017-5.

8. Antonov O.Yu. Detection of New Episodes of Porn-Related Criminal Activities Committed Using Information and Telecommunication Networks. *Rassledovanie prestuplenii: problemy i puti ikh resheniya = Criminal Investigation: Problems and Ways of Their Solution*, 2017, no. 3 (17), pp. 169–177. (In Russian).

9. Prostoserdov M.A. *Ekonomicheskie prestupleniya, sovershaemye v kiberprostranstve, i mery protivodeistviya im. Avtoref. Kand. Diss.* [Economic crimes in cyberspace and measures of counteracting them. Cand. Diss. Thesis]. Moscow, 2016. 28 p.

10. 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 (31), pp. 114–121. (In Russian).

11. Parker Donn B. *Fighting Computer Crime*. New York, Wiley Publisher, 1998. 512 p.

12. Aikov D., Seiger K., Fonstorkh U. *Komp'yuternye prestupleniya. Rukovodstvo po bor'be s komp'yuternymi prestupleniyami* [Crimes. Guidance on protection from computer crimes]. Moscow, Mir Publ., 1999. 351 p.

13. Rogers M. *A New Hacker Taxonomy*. Winnipeg, University of Manitoba, 2000. 85 p.

14. Buono L. Fighting cybercrime through prevention, outreach and awareness raising. *ERA Forum*, 2014, vol. 15, iss. 1, pp. 1–8. DOI: 10.1007/s12027-014-0333-4.

15. Poremba S. Hackers Today Act More Like Small Businesses Than Thieves. *Hewlett Packard Enterprise Development LP*. Available at: https://www.hpe.com/us/en/newsroom/blog-post/2017/03/hackers-today-act-more-like-small-businesses-than-thieves.html.

16. Voluiskaya M. Largest hacker groups of the world. Infographics. *Argumenty i Fakty*, 2017, March 11. (In Russian).

17. Broadhurst R., Grabosky P., Alazab M., Chon S. Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime. *International Journal of Cyber Criminology*, 2014, vol. 8, iss. 1, pp. 1–20.

18. Begishev I.R. Problems of Counter Action to the Criminal Encroachments on the Information Systems of Critical and Potentially Dangerous Objects. *Informatsionnaya bezopasnost' regionov = Information Security of Regions*, 2010, no. 1, pp. 9–13. (In Russian).

19. Begishev I.R. Criminal Liability for Purchasing or Marketing of Digital and Documented Information Knowingly Obtained with Criminal Means. *Aktual'niye problemy ekonomiki i prava = Actual Problems of Economics and Law*, 2010, no. 1, pp. 123–126. (In Russian).

20. Osipenko A.L. *Setevaya komp'yuternaya prestupnost': teoriya i praktika bor'by* [Network Digital Crimes: the Theory and Practice of Counteraction]. Omsk Academy of the Russian Ministry of the Interior Publ., 2009. 480 p.

21. Chuprova A.Yu. Specific features of group crimes in the sphere of e-commerce. In Dolgova A.I. (ed.). *Prestupnost', ugolovnaya politika, zakon. Materialy Vserossiiskoi nauchno-prakticheskoi konferentsii, Moskva, 26–27 yanvarya 2016 g.* [Criminality, Criminal Policy, Law. Materials of All-Russian Research Conference, Moscow, January 26–27, 2016]. Moscow, 2016, pp. 314–320. (In Russian).

22. McGuire M. *Organised Crime in the Digital Age*. London, John Grieve Centre for Policing and Security, 2012.

23. Sukhodolov A.P., Kolpakova L.A., Spasennikov B.A. Issues of Counteracting Crimes in the Sphere of Digital Economy. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2017, vol. 11, no. 2, pp. 258–267. DOI: 10.17150/2500-4255.2017.11(2).258-267. (In Russian).

24. Nomokonov V.A., Tropina T.L. Cybercrime as a New Criminal Threat. *Kriminologiya: vchera, segodnya, zavtra = Criminology: Yesterday, Today, Tomorrow*, 2012, no. 24, pp. 45–55. (In Russian).

25. Sklyarov S.V., Evdokimov K.N. Modern Approaches to the Concept, Structure and Nature of Computer Crime in the Russian Federation. *Kriminologicheskii zhurnal Baikal'skogo gosudarstvennogo universiteta ekonomiki i prava = Criminology Journal of Baikal National University of Economics and Law*, 2016, vol. 10, no. 2, pp. 322–330. DOI: 10.17150/1996-7756.2016.10(2).322-330. (In Russian).

26. Grabosky P. Organized cybercrime and national security. In Smith R.G., Chak-Chung Cheung R., Yiu-Chung Lau L. (eds.). *Cybercrime risks and responses. Eastern and Western Perspectives*. New York, Palgrave Macmillan, 2015, pp. 67–80. DOI: 10.1057/9781137474162_5.

27. Sukhodolov A.P., Ivantsov S.V., Borisov S.V., Spasennikov B.A. Topical Issues of Preventing Economic Crimes Committed with the Use of Information and Telecommunication Networks. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2017, vol. 11, no. 1, pp. 13–21. DOI: 10.17150/2500-4255.2017.11(1).13-21. (In Russian).

28. Uzdenov R.M. New Frontiers of Cybercrime. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2016, vol. 10, no. 4, pp. 649–655. DOI: 10.17150/2500-4255.2016.10(4).649-655. (In Russian).

29. Pleshakov S.M. Extremist Community as a Kind of Organized Criminal Group. *Aktual'nye problemy vzaimodeistviya obshchestvennosti s organami gosudarstvennoi vlasti i organami mestnogo samoupravleniya. Materialy 2-i Vserossiiskoi nauchno-prakticheskoi konferentsii* [Topical Problems of Interaction between the Community and State Power and Local Governance Bodies. Materials of 2nd All-Russian Research Conference]. Saransk, 2017, pp. 174–177. (In Russian).

30. Ageshkina N.A., Belyaev M.A., Belyaninova Yu.V., Biryukova T.A., Boldyrev S.A. *Nauchno-prakticheskii kommentarii k Ugolovnomu kodeksu Rossiiskoi Federatsii ot 13 iyunya 1996 g. № 63-ФЗ* [Research and Practice Comment to the Criminal Code of the Russian Federation of June 13, 1996 № 63-ФЗ]. Saratov, I.P.R. Media Publ., 2013. 848 p.

31. Manky D. Cybercrime as a Service: a very Modern Business. *Computer Fraud and Security*, 2013, vol. 2013, iss. 6, pp. 9–13. DOI: 10.1016/S1361-3723(13)70053-8.

32. Somov S. The police detained the participants of a major criminal group involved in internet banking fraud. *Cnews Klub*. Available at: http://club.cnews.ru/blogs/entry/import_zaderzhany_uchastniki_krupnejshej_prestupnoj_gruppy_zanimavshejsya_moshennichestvami_v_sistemah_internetbankinga_420b. (In Russian).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Бегишев Ильдар Рустамович — старший научный сотрудник Казанского инновационного университета им. В.Г. Тимирясова (ИЭУП), кандидат юридических наук, заслуженный юрист Республики Татарстан, г. Казань, Российская Федерация; e-mail: begishev@mail.ru.

Хисамова Зарина Илдузовна — начальник отделения планирования и координации научной деятельности научно-исследовательского отдела Краснодарского университета Министерства внутренних дел Российской Федерации, кандидат юридических наук, г. Краснодар, Российская Федерация; e-mail: alise89@inbox.ru.

Никитин Сергей Геннадьевич — заведующий научной частью Казанского инновационного университета им. В.Г. Тимирясова (ИЭУП), г. Казань, Российская Федерация; e-mail: nikitin@ieml.ru.

INFORMATION ABOUT THE AUTHORS

Begishev, Ildar R. — Senior Researcher, Kazan Innovative University named after V.G. Timiryasov (IEML), Ph.D. in Law, Honored Lawyer of the Republic of Tatarstan, Kazan, the Russian Federation; e-mail: begishev@mail.ru.

Khisamova, Zarina I. — Head, Department of Planning and Coordination of Research Activities, Research Department, Krasnodar University of the Ministry of Internal Affairs of the Russian Federation, Ph.D. in Law, Krasnodar, the Russian Federation; e-mail: alise89@inbox.ru.

Nikitin, Sergey G. — Head, Research Department, Kazan Innovative University named after V.G. Timiryasov (IEML), Kazan, the Russian Federation; e-mail: nikitin@ieml.ru.

ДЛЯ ЦИТИРОВАНИЯ

Бегишев И.Р. Организация хакерского сообщества: криминологический и уголовно-правовой аспекты / И.Р. Бегишев, З.И. Хисамова, С.Г. Никитин. — DOI: 10.17150/2500-4255.2020.14(1).96-105 // Всероссийский криминологический журнал. — 2020. — Т. 14, № 1. — С. 96–105.

FOR CITATION

Begishev I.R., Khisamova Z.I., Nikitin S.G. The organization of hacking community: criminological and criminal law aspects. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2020, vol. 14, no. 1, pp. 96–105. DOI: 10.17150/2500-4255.2020.14(1).96-105. (In Russian).