ISSN 2500-4255

УДК 343.9
DOI 10.17150/2500-4255.2017.11(2).258-267

ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПНОСТИ В СФЕРЕ ЦИФРОВОЙ ЭКОНОМИКИ

А.П. Суходолов[1], Л.А. Колпакова[2], Б.А. Спасенников[3]
[1] Байкальский государственный университет, г. Иркутск, Российская Федерация
[2] Вологодский институт права и экономики Федеральной службы исполнения наказаний, г. Вологда, Российская Федерация
[3] Научно-исследовательский институт Федеральной службы исполнения наказаний, г. Москва, Российская Федерация

Информация о статье

Дата поступления
17 февраля 2017 г.

Дата принятия в печать
29 мая 2017 г.

Дата онлайн-размещения
21 июня 2017 г.

Ключевые слова
Цифровая экономика;
информационная безопасность;
противодействие преступности;
киберпреступность;
интернет-сервисы

Аннотация. Цель исследования состоит в формировании научно обоснованных предложений по совершенствованию системы мер противодействия преступности в сфере цифровой экономики. В работе использовались обще- и частнонаучные методы с превалированием социологических методов исследования. Авторами были проанализированы материалы 150 уголовных дел о преступлениях экономической направленности, совершаемых с применением цифровых технологий. Изучена статистика и аналитические данные, размещаемые на официальных сайтах МВД России и Судебного департамента при Верховном Суде Российской Федерации. Методом анкетирования опрошено 130 респондентов, в числе которых 43 сотрудника подразделений экономической безопасности и противодействия коррупции и отделов «К» МВД России, 45 представителей судейского корпуса и помощников судей, 42 научно-педагогических работника. В контексте общей концепции развития России в направлении информатизации экономики в статье обосновывается необходимость выделения преступности в сфере цифровой экономики в самостоятельную категорию для изучения. В целях разработки эффективных мер противодействия данному явлению определены его характерные черты и факторы, способствующие его развитию, проанализированы некоторые проблемы защиты конфиденциальной информации, выявления и уголовного преследования правонарушителя в условиях его деперсонификации в сети Интернет, многоэпизодности деяний при излишне лояльном подходе правоприменителя, разночтений при толковании норм уголовного закона, привлечения к юридической ответственности посредников в осуществлении информационного обмена. При формировании предложений учтены возможности глобальной интеграции и опыт стран, преуспевших в противодействии незаконному использованию цифровых технологий в экономике. Особое внимание уделено повышению превентивного потенциала национального уголовного законодательства и виктимологической профилактике.

ISSUES OF COUNTERACTING CRIMES IN THE SPHERE OF DIGITAL ECONOMY

Alexander P. Sukhodolov[1], Ludmila A. Kolpakova[2], Boris A. Spasennikov[3]
[1] Baikal State University, Irkutsk, the Russian Federation
[2] Vologda Institute of Law and Economics, Federal Penitentiary Service of Russia, Vologda, the Russian Federation
[3] Research Institute of Federal Penitentiary Service of Russia, Moscow, the Russian Federation

Article info

Received
2017 February 17

Accepted
2017 May 29

Available online
2017 June 21

Abstract. The goal of this research is to formulate scientifically grounded suggestions on improving the system of measures to counteract crimes in the sphere of digital economy. The authors used general and specific scientific methods, sociology methods being the prevalent ones. They analyzed 150 criminal cases of economic crimes committed with the use of digital technologies. They also studied the statistical and analytical materials found on the official websites of Russian Ministry of the Interior and the Court Department of the Supreme Court of the Russian Federation. They conducted a questionnaire survey that encompassed 130 respondents, including 43 employees of the economic security and anti-

Keywords
Digital economy; information security; crime counteraction; cybercrime; Internet services

corruption «K» departments of Russian Ministry of the Interior, 45 judges and their assistants, 42 university lecturers and researchers. The general concept of Russia's development towards digital economy makes it necessary to single out crimes in the sphere of digital economy as a separate crime category with the purpose of researching them. In order to develop effective measures for counteracting this phenomenon, the authors determine its specific features and factors that contribute to its development, analyze some problems of protecting confidential information, identifying and criminally prosecuting offenders in the conditions of their depersonification online, multiple offences when the attitude of the law enforcement bodies is excessively lax, different interpretations of criminal law norms, legal prosecution of intermediaries of information exchange. The formulated suggestions take into account the opportunities for a global integration and the experience of countries with a good record of counteracting illegal use of digital technologies in economy. The authors pay special attention to increasing the preventive potential of national criminal legislation as well as to victimological prevention.

Реализация концепции электронной (цифровой) экономики, появившейся в конце XX в. и стремительно обретающей новые формы, в настоящее время влечет поистине революционные изменения в классической модели хозяйствования и в бизнес-сфере. В силу переноса экономических отношений в интернет-пространство (виртуальную среду [1; 2], киберпространство [3]) и, как следствие, некоторого ослабления управленческого ресурса государства оценка ее размаха и доли в ВВП существенно затруднена, хотя и возможна. Согласно данным The Boston Consulting Group, тройку лидеров с наиболее развитой цифровой экономикой составляют Великобритания (12,4 % ВВП), Южная Корея (8,0 %) и Китай (6,9 %)[1]. Россия пока далека от лидирующих позиций (всего 2,8 %), но развитие в этом отношении определено сегодня как одно из приоритетных направлений. О значимости расширения применения цифровых технологий в экономике при одновременном обеспечении безопасности и конфиденциальности интеллектуальной собственности говорится и в Канкунской декларации ОЭСР 2016 г.[2]

Понятие цифровой экономики в узком смысле сводится к так называемой электронной коммерции, осуществляемой посредством информационных и коммуникационных технологий[3]. Сама же электронная коммерция представляет собой любые формы деловых сделок (бизнес — бизнес (B2B) и бизнес — потребитель (B2C)), при которых стороны взаимодействуют через электронные устройства и сети, прежде всего через Интернет [4]. Аналитический центр при Правительстве РФ в период с 12 по 25 января 2017 г. провел опрос. В его рамках экспертам из разных стран предлагалось проголосовать за одно из выработанных ранее определений данного явления либо сформулировать собственное. Весьма интересное определение дано Исследовательским центром журнала Economist и компанией IBM. Согласно ему, цифровая экономика представляет собой экономику, способную предоставить высококачественную ИКТ-инфраструктуру и мобилизовать возможности ИКТ на благо потребителей, бизнеса и государства[4]. Таким образом, рассматриваемое явление нельзя сводить к чистой коммерции. Оно имеет значительный социальный и культурный потенциал. Оценка влияния цифровой экономики на национальную и глобальную экономику, а также неизбежно на всю социальную сферу весьма важна ввиду нарастания проблем преступности, тоже модернизирующейся благодаря электронизации и цифровизации общества. В специальной литературе отмечается, что киберпреступность может быть ассоциирована не только с проблемами информационной безопасности, но и с угрозами государственности, военно-промышленному и производственному комплексу, инфраструктуре жизнеобеспечения [5].

Сегодня, говоря об экономических преступлениях, целесообразно выделять в само-

[1] The Boston Consulting Group (BCG) [Electronic resource]. URL: http://www.bcg.com.

[2] Ministral Declaration on the Digital Economy: Innovation, Growth and Social Prosperity («Cancún Declaration»), 21–23 June, 2016.

[3] Information Economy Report 2015: Unlocking the Potential of E-commerce for Developing Countries [Electronic resource]. URL: http://www.unic.ru/library/dokumenty-oon/information-economy-report-2015-unlocking-potential-e-commerce-developing-coun.

[4] Семь определений цифровой экономики [Электронный ресурс]. URL: https://www.crn.ru/news/detail.php?ID=116780.

стоятельную категорию преступность в сфере цифровой экономики. Не случайно в уголовной статистике при учете преступлений экономической направленности с начала 2017 г. отдельной строкой стали выделяться деяния, совершаемые с использованием компьютерных и телекоммуникационных технологий. За период с января по март 2017 г. таковых выявлено 2 572[5]. Однако заметим, что эта цифра не характеризует в полном объеме размах исследуемого явления во многом благодаря его высокой латентности, проистекающей главным образом из правовой неграмотности или инертности пострадавших от преступлений. На данный факт указал 121 эксперт (93 %) из 130 опрошенных нами представителей науки и практики. Кроме того, сложность состоит в том, что четко обозначить круг преступлений, так или иначе связанных с использованием электронной информации, автоматизированных средств ее обработки и хранения, практически невозможно, поскольку технические способы фиксации, обработки и хранения информации непрерывно эволюционируют, равно как способы совершения преступлений и объекты посягательств постоянно трансформируются. В ходе опроса эксперты высказывали разные мнения по этому поводу, называя чаще других статьи Особенной части УК РФ, где прямо указан элемент использования компьютерных и телекоммуникационных технологий, электронных средств платежей (ст. 159[3], 159[6], 171[2], 185[3], 187 УК РФ отметили 89,8 % опрошенных). Реже выделяли ст. 159, 172[1], 172[2], 174, 180, 183, 185[6] УК РФ. Мы также выяснили, что преступления, которые мы можем отнести к данной группе криминальных явлений, предусмотренных гл. 21 и 22 УК РФ, нередко образуют совокупность с иными деяниями, что затрудняет их классификацию по признакам родового, видового и непосредственного объектов, а соответственно, и их правильную квалификацию. Об этом свидетельствуют результаты изучения 150 обвинительных приговоров по уголовным делам о преступлениях, совершенных в сфере цифровой экономики. По обобщенным сведениям, наиболее часто деяния, предусмотренные статьями, указанными выше, соседствуют в формуле обвинения с деяниями, предусмотренными ст. 272–274 УК РФ (преступления в сфере компьютерной информации), что подчеркивает особенности экономических отношений, переведенных в цифровой формат. Отметим, что имеет место отставание правовой реакции государства от развития технических средств совершения преступлений. Помимо собственно вредоносных компьютерных программ, ответственность за создание, использование и распространение которых предусмотрена ст. 273 УК РФ, преступники могут применять программное обеспечение иного рода, предназначенное, например, для дешифрования информации, подбора паролей, а также различные электронные приспособления, такие как сканеры портов и пр. [6]. В условиях запрета на применение аналогии закона в уголовно-правовых отношениях считаем, что следует поддержать мнение ученых о криминализации действий по незаконному изготовлению, сбыту или приобретению специальных технических средств, предназначенных для нарушения систем защиты цифровой информации [там же; 7], что поможет снять ряд вопросов с квалификацией соответствующих деяний.

Проникновение информационных и телекоммуникационных технологий в экономику обострило проблемы охраны персональных данных, коммерческой, корпоративной и банковской тайны. В данном случае речь идет об информации конфиденциального свойства. К таковой, к примеру, относится инсайдерская информация, имеющая специальный правовой режим. Причем, предоставляя такой информации уголовно-правовую защиту, законодатель либо прямо предусматривает как криминообразующий признак использование для ее распространения или передачи электронных, информационно-телекоммуникационных сетей, включая сеть Интернет (ст. 185[3] УК РФ), либо презюмирует такую возможность, прибегая к менее казуистичному способу изложения диспозиции нормы (ст. 185[6] УК РФ). Однако и информация, находящаяся в свободном доступе, может представлять интерес для криминальных структур. Так, сведения, которые можно почерпнуть из реестра юридических лиц или с сайта службы судебных приставов об исполнительных производствах, могут быть использованы в целях подготовки рейдерских захватов. Заметим, что типичные механизмы маркетинговых операций в сети Интернет, таких как изучение текущего состояния социального коммерческого поиска, совместное создание стоимостных стратегий фирм, кобрендинг, стратегический маркетинг и др. [8], все чаще используются в мошеннических целях.

[5] Состояние преступности с января по март 2017 г. [Электронный ресурс]. URL: https://xn--b1aew.xn--p1ai/folder/101762/item/9871454.

В структуре преступлений экономической направленности значительно превалируют деяния в финансово-кредитной сфере (28 884 из 108 754 выявленных преступлений за 2016 г.)[6]. Учитывая активность цифровизации данной сферы и применяя метод экстраполяции, мы можем сделать вывод о том, что и эпицентр криминальных рисков совершения преступлений с использованием компьютерных и телекоммуникационных технологий находится именно здесь. По оценкам опрошенных сотрудников правоохранительных органов и ученых, наиболее уязвимы финансы юридических и физических лиц, размещенные на счетах кредитных учреждений. Так ответили 81,5 % респондентов. Еще 11,5 % поставили на первое место сами кредитные организации и оставшиеся 7,0 % — государственные финансовые институты. Материалы изученных уголовных дел тоже это подтверждают, а также показывают, что существенное изменение характера и способов совершения преступлений, в том числе и традиционно входящих в ядро преступности, напрямую коррелирует с состоянием информационной безопасности участников экономических отношений. Так, бреши в защитном поле банковской системы и хозяйствующих субъектов чреваты неправомерным доступом к клиентской базе, явлениями кардинга, фишинга, широким использованием при совершении деяний средств сотовой связи, платежных терминалов. В особенности страдают небольшие организации и индивидуальные предприниматели, которые, в отличие от крупных корпораций, не имеют возможности приобрести дорогостоящее программное обеспечение, способное оградить их от кибератак.

Так, в феврале 2017 г. сотрудниками Управления «К» МВД России во взаимодействии с МУ МВД «Раменское» была пресечена деятельность организованной преступной группы, которая посредством фишинговых сайтов с использованием методов социальной инженерии распространяла вредоносные программы. С их помощью она получала доступ к управлению банковскими счетами юридических лиц и совершила хищения денежных средств на общую сумму 100 млн р. Уголовное дело возбуждено по ч. 1 ст. 273 и ч. 3 ст. 159[6] УК РФ[7].

Электронная среда существенно затрудняет идентификацию правонарушителя, а значит, его изобличение и уголовное преследование, что влечет появление одной из характерных черт преступности в сфере цифровой экономики — многоэпизодность криминальной активности. Примером может служить уголовное дело в отношении Колонщакова и Гасанова, которые в сговоре с неустановленным лицом, выходящим в Интернет под псевдонимами DenAdel и Robusto, используя вредоносную программу и похищенные аутентификационные данные (электронно-цифровую подпись), получали незаконный доступ к счетам агентов систем электронных платежей, перечисляли с них средства на лицевые счета абонентских номеров телефонов, а после обналичивания переводили 25 % от похищенной суммы на неустановленный кошелек электронной платежной системы WebMoney Transfer, предоставленный неустановленным соучастником. За два часа ими было совершено более 130 незаконных операций по переводу денежных средств на общую сумму 1 597 600 р. В эти же и следующие сутки таким же способом было осуществлено хищение еще 1 480 000 р. Ввиду того что потерпевший — один (юридическое лицо), а деяния совершались в течение короткого промежутка времени, действия Колонщакова и Гасанова квалифицированы как единое преступление по ч. 3 ст. 159[6] УК РФ. Третий соучастник так и не был установлен[8].

Цифровые технологии в руках даже одного человека, не говоря уже об организованных преступных группах, могут превратиться в небывалое по мощности орудие совершения преступлений. Известны случаи, когда подросткам в одиночку удавалось дестабилизировать или полностью парализовать систему управления воздушным движением, вмешиваться в работу крупных онлайн-ретейлеров и манипулировать

[6] Состояние преступности с января по декабрь 2016 г. [Электронный ресурс]. URL: https://xn--b1aew.xn--p1ai/upload/site1/document_news/009/338/947/sb_1612.pdf.

[7] Сотрудниками Управления «К» МВД России пресечена деятельность организованной группы, которая похищала денежные средства с помощью модификации компьютерной информации [Электронный ресурс]. URL: https://xn--b1aew.xn--1ai/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii/Publikacii_i_vistuplenija/item/9552134.

[8] Приговор Савеловского районного суда г. Москвы по делу 1-226/13 [Электронный ресурс]. URL: https://savelovsky--msk.sudrf.ru/modules.php?name=sud_delo&name_op=doc&srv_num=1&number=218680299&delo_id=1540006&new=&text_number=1.

торгами на фондовой бирже Nasdaq. Групповая же преступность в условиях распространения электронного обмена информацией приобретает уникальные, ранее неизвестные формы. Например, среди зарубежных исследователей доминирует мнение о том, что утрачивается признак сплоченности таких групп, на смену ему приходит более эфемерная форма взаимодействия — криминальные макросети, их участниками становятся посетители форумов, чатов, закрытых онлайн-сообществ [9]. Но, чтобы стать вхожим в данные круги, требуется заслужить доверие, иметь определенный статус и репутацию, поэтому остается открытым вопрос, является ли подобное взаимодействие менее устойчивым, нежели общение в преступной группе традиционной формы [10].

Ведущим мотивом при совершении преступлений в сфере цифровой экономики выступает мотив обогащения. По результатам проведенного опроса, 98,4 % респондентов отвели ему первое место, лишь двое (1,6 %) указали в качестве основного игровой мотив. Однако и материалы практики, и экспертные оценки свидетельствуют, что в отдельных случаях людьми движут и иные побуждения. Так, в условиях кризиса, находясь на грани увольнения, некоторые сотрудники посягают на информационные ресурсы корпорации и передают коммерческие секреты конкурентам не столько из корысти, сколько из соображений мести. Материальная выгода при этом имеет второстепенное значение. К слову сказать, финансовые трудности компаний, как правило, влекут сокращение расходов на обновление программного обеспечения, что создает условия для кибератак и промышленного шпионажа. В результате могут пострадать не только корпоративные интересы, но и интересы клиентов, фискальная система.

Обращают на себя внимание разночтения при толковании норм уголовного закона, касающихся различных областей цифровой экономики. Это достаточно заметно при первичной квалификации преступлений, когда речь идет о выявлении оснований для возбуждения уголовных дел. Так, размещаемая на интернет-портале МВД РФ Управлением «К» информация об обнаруженных фактах преступлений, в целом сходных по криминообразующим признакам, демонстрирует и совершенно различные подходы к юридической оценке содеянного. Ситуация несколько выравнивается по результатам прокурорского надзора и судебного рассмотрения таких дел, когда итоговая формула обвинения более точно и предметно отражает вид и характер совершенного преступления. Иными словами, правовая оценка деяний (их квалификация), изложенная в итоговых решениях по соответствующим делам, отличается бóльшим единообразием, нежели в процессуальных решениях на подготовительном и первоначальном этапах расследования. С одной стороны, это объясняется тем, что на этапе проверки сообщений о преступлениях в сфере цифровой экономики, равно как и всех прочих, субъект расследования обладает лишь ограниченным объемом информации об обстоятельствах, входящих в предмет доказывания. К примеру, размер причиненного ущерба может уточняться вплоть до окончания судебных прений, а иногда этот вопрос выносится за рамки уголовной юрисдикции в порядке более точного определения суммы гражданского иска, но именно данный признак лежит в основе дифференциации ответственности за многие экономические преступления. Сотрудники подразделений по обеспечению экономической безопасности и отделов «К» МВД России в ходе проведения опроса (30 % от общего числа всех респондентов) отметили, что сложности с квалификацией рассматриваемых деяний на стадии возбуждения уголовного дела главным образом обусловлены тем, что ограниченные сроки проверки сообщений не позволяют проводить трудоемкие и затратные по времени следственные действия, такие как экспертизы. Кроме того, по делам рассматриваемой категории необходима обработка значительных объемов электронной информации, а для ее изъятия требуется производство выемки, которую можно осуществить лишь после возбуждения дела. Таким образом, мы можем сделать вывод о том, что не вполне точная квалификация преступлений рассматриваемой категории на первоначальном этапе расследования может быть обусловлена объективными причинами, связанными с установленными рамками процессуальной формы. Вместе с тем считаем нецелесообразным расширять сроки проверки сообщений о преступлениях, ибо в задачи стадии возбуждения уголовного дела входит лишь установление отдельных признаков криминала, а юридическая оценка деяния может уточняться неоднократно в ходе расследования.

Проведенный опрос выявил и иные причины затруднений с правильной квалификацией преступлений в сфере цифровой экономики.

Среди респондентов 48,5 % указали на особенности самих цифровых технологий, которые характеризуются постоянной модификацией и достаточной долей универсальности по сферам приложения. Обратили внимание на наличие посреднического звена при оказании информационных и телекоммуникационных услуг и на сложности с распределением ответственности между звеньями всей цепочки субъектов, вовлеченных в соответствующие правоотношения, 58,2 %. Еще больше опрошенных (87,0 %) отметили, что в криминологическом и криминалистическом отношении весьма значимы факторы анонимности и неограниченности числа пользователей цифровых технологий, что в контексте экономических отношений означает неперсонифицированность оферента, партнера, контрагента и т.п. Все чаще практикуется заключение договоров, в том числе и при совершении крупных сделок, посредством обмена электронными документами, заверенными факсимильными подписями (electronic data interchange (EDI)), или же при помощи протокола TCP / IP, позволяющего унифицировать «язык взаимодействия» в сетях [11]. При этом само бизнес-общение может строиться по поводу так называемых неовеществленных, а иногда и виртуальных объектов при использовании электронных как фиатных (выраженных в государственной валюте, например PayPal, Visa Cash), так и нефиатных (представленных негосударственными платежными сервисами WebMoney, «Яндекс.Деньги», RBK Money, Bitcoin и др.) денег. Заметим, что, в отличие от расчетов с помощью традиционных банковских платежных карт и систем интернет-банкинга, расчеты электронными деньгами чаще всего являются неперсонифицированными, что выступает самостоятельным криминологически важным фактором.

Вопрос в том, когда и при каких условиях данные экономические отношения могут перерасти в уголовно-правовые и уголовно-процессуальные. Во-первых, риск стать жертвой мошенников, использующих, к примеру, анонимные прокси-серверы, сайты-двойники и пр. в целях обмана и недоступности для идентификации, здесь весьма и весьма велик. Во-вторых, существует немалая опасность совершить так называемую бестоварную сделку, которая признается ничтожной и помимо гражданско-правовых последствий может повлечь за собой последствия уголовно-правовые. В-третьих, из-за транснационального характера электронного информационного обмена и значительного количества посреднических звеньев между источником и адресатом информации затруднена процедура установления правового статуса и добросовестности всех участников, вовлеченных в данный процесс. В этой связи сегодня все чаще предметом обсуждения в России и за рубежом становится проблема привлечения к юридической, в том числе и уголовной, ответственности интернет-провайдеров [12–15]. Вместе с тем звучат и предложения использовать их возможности для борьбы с киберпреступностью и применять поощрительные меры к тем, кто идет на сотрудничество с правоохранительными структурами [16; 17].

Еще один фактор, который следует учитывать при противодействии преступлениям в сфере цифровой экономики, — это колоссальная виктимность. С полной уверенностью можно заявить, что в условиях активного использования интернет-сервисов, электронных гаджетов и средств платежей никто не может чувствовать себя в безопасности. К примеру, получение СМС-сообщений, содержащих различного рода мошеннические уловки, стало сегодня неотъемлемым атрибутом повседневной жизни, при этом обывательская оценка общественной опасности подобных деяний редко выходит за границы мелкого бытового хулиганства. Отсюда их высочайшая естественная латентность, требующая серьезной разъяснительной работы с населением в рамках общей виктимологической профилактики. Обязанности по ее осуществлению следует возложить прежде всего на субъектов, предоставляющих соответствующие услуги. Например, банковский работник, оформляя клиенту платежную карту и подключая услугу «Мобильный банк», обязан разъяснить, от каких действий необходимо воздержаться, чтобы не стать жертвой мошенников, и как действовать, если это все же произошло. На уровне организаций виктимологическая профилактика может выстраиваться с помощью методов управления рисками цифровой безопасности[9].

Общность проблем противодействия преступности в сфере цифровой экономики за рубежом и в России позволяет сделать вывод о необходимости аккумулирования и анализа по-

[9] Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity. 17 September 2015 [Electronic resource]. URL: http://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf.

ложительного опыта таких стран, как Швейцария, Великобритания, Норвегия, Дания, которые преуспели не только в продвижении инноваций в экономике, но и в сфере противодействия их противозаконному использованию.

Министр по интеллектуальной собственности Великобритании баронесса Невилл-Рольф в рамках обсуждения проблем ИТ-безопасности в экономике среди наиболее эффективных механизмов противодействия киберкражам указала создание специализированного полицейского подразделения, реформирование судебных органов, создаваемых для рассмотрения экономических споров, связанных с применением информационных технологий (Enterprise Court IP), капитальное обновление правовой базы, в том числе затрагивающей вопросы авторского права на программное обеспечение[10]. В 2015 г. британским правительством был поставлен вопрос о повышении сроков лишения свободы за интернет-пиратство в промышленных масштабах с двух до десяти лет в целях защиты правообладателей. Тем самым оно уравняло в санкциях данные преступления с такими деяниями, как фальшивомонетничество и создание подделок[11].

В числе ведущих средств противодействия киберпреступности, частью которой является преступность в сфере цифровой экономики, М. Герке и его швейцарские коллеги называют модернизацию компьютерных систем и комплексных судебных программ для ускорения расследования и автоматизации процедур поиска в различных базах данных правоохранительных органов; интеграцию мер информационной безопасности на основе разработки и продвижения технических средств охраны; создание и совершенствование правовой базы, адекватной современным киберугрозам; соблюдение разумного баланса между уважением права на получение и распространение информации и контролем над информационными процессами [12].

Признавая особую незащищенность от киберугроз небольших фирм, занятых в торговле продовольственными товарами и в сфере питания, развлекательной индустрии и гостиничном бизнесе, авторы доклада по исследованию нарушений кибербезопасности Р. Клар, С. Амили, Д.Н. Шах, М. Батон, В. Ванг предложили следующие способы управления рисками в рассматриваемой сфере: применение брандмауэров новейших конфигураций (специального программного обеспечения) в целях фильтрации данных, противоречащих политике безопасности, ограничение прав пользователей администратором, исключение доступа к информационным ресурсам фирмы через посторонние электронные устройства, создание корпоративных беспроводных сетей, мониторинг активности пользователей, шифрование личных данных [18].

Поскольку значительная часть экономических сделок сегодня совершается в так называемом интернациональном пространстве — сети Интернет [19], преступность в сфере цифровой экономики имеет трансграничный характер. Исходя из этого нельзя обойти вниманием вопрос о международном сотрудничестве в сфере противодействия данному явлению. На сегодняшний день существует довольно много соглашений, затрагивающих вопросы безопасности в киберпространстве, однако большинство из них относится к источникам «мягкого» права и не позволяет решить возникающие юрисдикционные коллизии, на что неоднократно указывали отечественные и зарубежные исследователи [20; 21]. К таковым актам, в частности, можно отнести ряд рекомендаций, выработанных Советом Европы[12]. Попыткой внести правовую определенность в процесс противодействия преступности, использующей электронные и телекоммуникационные системы, в условиях международной интеграции стало принятие Конвенции Совета Европы о киберпреступности от 30 мая 2002 г., регламентирующей вопросы материального и процессуального характера. Однако, сделав робкий шаг в сторону ратификации Конвенции в 2005 г., Россия все же отказа-

[10] Cyber crime and IP theft Protecting the digital economy [Electronic resource]. URL: http://www.newstatesman.com/sites/default/files/files/NS%20Cybercrime%20Supplement%20Dec%202014.pdf.

[11] Британское правительство рассматривает вариант увеличения срока лишения свободы за пиратство в сети Интернет с 2 до 10 лет в черновиках [Электронный ресурс]. URL: http://www.geeks.izula.ru/post/259082.

[12] Recommendation № R (89) 9 of the Committee of Ministers of the Council of Europe to member States for the Computer-Related Crime and Final Report of the European Commitee on Crime Problems (adopted by the Committee of Ministers on 13 September 1989 at the 428th meeting of the Ministers' Deputies). Strasbourg, 1990 ; Recommendation № R (95) 13 of the Committee of Ministers of the Council of Europe to member States for the 11 concerning problems of criminal procedural law connected with Information Technology (adopted by the Committee of Ministers on 11 September 1995 at the 543rd meeting of the Ministers' Deputies). Strasbourg, 1995.

лась от участия в ней[13], усмотрев в ее положениях (прежде всего в ст. 32) угрозу национальной безопасности. Признавая ценность указанного документа для объединения усилий в области противодействия преступности в сфере цифровой экономики, мы присоединяемся к мнению аналитиков, считающих более перспективным и приемлемым для нашей страны сотрудничество в рамках Международного многостороннего партнерства против киберугроз (ИМПАКТ). Данная организация предлагает техническую поддержку Глобального центра реагирования, ориентированного на сетевую систему раннего предупреждения угроз и располагающего ресурсом электронной защищенной прикладной платформы взаимодействия экспертов (ESCAPE), с общей и постоянно обновляемой базой знаний по вопросам обеспечения кибербезопасности[14].

В последние годы российский законодатель уделяет особое внимание признаку использования при совершении преступлений различных электронных устройств, информационно-телекоммуникационных сетей, в том числе сети Интернет, рассматривая его либо как альтернативный способ совершения преступления, либо как основание дифференциации ответственности. В гл. 21 и 22 УК РФ при конструировании составов преступлений в сфере экономики напрямую он применяется редко (ст. 171^2 и 185^3). Ряд диспозиций норм данных глав содержит указание на использование определенных объектов, находящихся в неразрывной функциональной связи с электронными устройствами для хранения, обработки и передачи информации (ст. 159^3, 159^6, 187 УК РФ). Еще больше норм прямо не называют, но предполагают как одно из возможных средств совершения преступления использование цифровых технологий и информационно-телекоммуникационных сетей.

Из числа новелл последнего времени наибольшее количество вопросов вызывают, пожалуй, санкции за отдельные виды мошенничества, которые были выделены в самостоятельные статьи УК РФ. В рамках данной темы исследования интерес представляют ст. 159^3 («Мошенничество с использованием платежных карт») и 159^6 («Мошенничество в сфере компьютерной информации»). Так, если базовый состав преступления (ст. 159 УК РФ) предусматривает максимально возможное наказание в виде двух лет лишения свободы, то ч. 1 ст. 159^3 и ч. 1 ст. 159^6 — арест сроком до четырех месяцев. Считаем, что степень общественной опасности двух последних деяний несколько выше, чем в первом случае, поскольку здесь страдают не только отношения собственности, но и такие дополнительные объекты, как безопасность в сфере электронных средств платежей и компьютерная информация. Логичнее было бы усилить элемент санкций, а не поощрять данные виды мошенничества. Судебная практика в этом отношении еще менее понятна и буквально поражает своей лояльностью. Так, сроки лишения свободы за рассматриваемые деяния чаще всего не превышают трех лет, а штрафы обычно ограничиваются суммами до 100 тыс. р. Еще чаще суды, проявляя удивительное единодушие, применяют ст. 73 УК, назначая испытательный срок в виде одного года, если деяние единичное, и, как правило, двух лет шести месяцев за совокупность таковых. При этом для судов особенной роли не играет количество эпизодов — 3 или 11[15]. В этой связи считаем, что, реализуя установку на либерализацию уголовной политики, не следует абсолютно нивелировать требования справедливости и индивидуализации уголовно-правовых мер воздействия на преступника. Возвращаясь к результатам опроса, отметим, что мнения здесь несколько разнятся. Так, большинство представителей науки и профессорско-преподавательского состава наряду с сотрудниками органов предварительного расследования разделяют наше мнение об излишне мягкой позиции законодателя и судов (78,0 % от их числа); представители же судейского корпуса и аппаратов судов поддерживают сложившуюся практику (81,4 %), мотивируя свое решение преимущественно с позиций целесообразности, т.е. делая привязку к возмещению материального ущерба и загруженности уголовно-исполнительной системы.

Разделяя мнение первой группы респондентов, считаем, что следует положительно

[13] О подписании Конвенции о киберпреступности : распоряжение Президента РФ от 15 нояб. 2005 г. № 557-рп // Собрание законодательства РФ. 2005. № 47. Ст. 4929 ; О признании утратившим силу Распоряжения Президента РФ от 15 ноября 2005 г. «О подписании Конвенции о киберпреступности» : распоряжение Президента РФ от 22 марта 2008 г. № 144-рп // Там же. 2008. № 13. Ст. 1295.

[14] ИМПАКТ воздействует на глобальную кибербезопасность [Электронный ресурс]. URL: http://www.itu.int/net/itunews/issues/2009/08/pdf/200908_22-ru.pdf.

[15] См., напр.: Приговор по делу № 1-749/2013 Кузьминского районного суда г. Москвы [Электронный ресурс]. URL: https://kuzminsky--msk.sudrf.ru/modules.php?name=sud_delo&name_op=doc&srv_num=1&number=179797288&delo_id=1540006&new=&text_number=1 ; Приговор по делу № 1-52/2010 Брянского районного суда [Электронный ресурс]. URL: https://sudrf.ru.

оценить усиление ответственности за мошенничество, сопряженное с преднамеренным неисполнением договорных обязательств в сфере предпринимательской деятельности (ч. 5–7 ст. 159 УК РФ)[16]. В условиях развития цифровой экономики это особенно актуально, поскольку, как мы указывали ранее, возникают дополнительные сложности с проверкой чистоты сделок и идентификацией контрагента.

В завершение попытаемся наметить некоторые направления противодействия преступности в сфере цифровой экономики:

– совершенствование правовой защиты в виде усиления санкций за использование при совершении преступлений информационно-коммуникационной среды и специальных инструментов цифровой экономики;

– виктимологическая профилактика;

– техническая поддержка правоохранительных органов, включая регулярное обновление программного обеспечения, криминалистической техники, вливание новых ИТ-специалистов в ряды соответствующих подразделений по противодействию преступности;

– международная интеграция, упорядочение на правовой основе информационного обмена;

– обобщение и учет зарубежного опыта стран с развитой цифровой экономикой в сфере противодействия преступности в данной сфере;

– управление рисками цифровой безопасности в экономической сфере на уровне мировой интеграции, государства, отдельных отраслей, корпораций, предприятий.

[16] О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации по вопросам совершенствования оснований и порядка освобождения от уголовной ответственности : федер. закон от 3 июля 2016 г. № 323-ФЗ // Российская газета. 2016. 8 июля.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Фатьянов А.А. Актуальные проблемы информационной безопасности в виртуальной среде Интернета / А.А. Фатьянов // Реферативный журнал ВИНИТИ. — 2001. — № 10. — С. 6–8.

2. Рассолов И.М. Интернет-право / И.М. Рассолов. — М. : Закон и право, 2012. — 143 с.

3. Menthe D. Jurisdiction in cyberspace: a theory of international spaces / D. Menthe // Michigan Telecommunications and Technology Law Review. — 1998. — Vol. 4, iss. 1. — 103 p.

4. Wang F.F. Internet Jurisdiction and Choice of Law: Legal Practices in the EU, US and China / F.F. Wang. — Cambridge, 2010. — 276 p.

5. Boes S. Fighting cybercrime: joint effort / S. Boes, E.R. Leukfeldt // Ciber-Physical Security: Protecting Critical Infrastructure at the State and Local Level. — Cincinnati : Springer, 2016. — P. 185–205.

6. Бегишев И.Р. Преступления в сфере цифровой информации / И.Р. Бегишев // Информационное право. — 2010. — № 2. — С. 18–21.

7. Степанов-Егиянц В.Г. Преступления в сфере безопасности обращения компьютерной информации: сравнительный анализ : дис. ... канд. юрид. наук : 12.00.08 / В.Г. Степанов-Егиянц. — М., 2005. — 168 с.

8. Hajli N. Social commerce and new development in e-commerce technologies / N. Hajli, M.S. Featherman // International Journal of Information Management. — 2017. — № 37. — P. 177–178.

9. 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.

10. Leukfeldt E.R. Organised cybercrime and social opportunity structures: a proposal for future research directions / E.R. Leukfeldt // The European Review of Organised Crime. — 2015. — № 2. — P. 91–103.

11. Trust in Electronic Commerce / C. Prins et al. — Norwell : Kluwer Law International, 2002. — 321 p.

12. Gercke M. Understanding Cybercrime: Phenomena, Challenges and Legal Response / M. Gercke. — Geneva : Telecommunication Development Sector, 2012. — 356 p.

13. Okamura H. Liability of Internet Service Provider [Electronic resource] / H. Okamura. — Mode of access: http://www.softic.or.jp/symposium/open_materials/10th/en/okamura-en.pdf.

14. Weber R.H. Internet Service Provider Liability. The Swiss Perspective [Electronic resource] / R.H. Weber. — Mode of access: http://www.jipitec.eu/issues/jipitec-1-3-2010/2793/Weber_ISP_Ch.pdf.

15. Филимонов С.А. Проблемы борьбы с компьютерным мошенничеством как потенциальной угрозой информационному сообществу / С.А. Филимонов // Современное право. — 2014. — № 9. — С. 123–127.

16. Osborne G. Chancellor's Speech to GCHQ on Cyber Security, 2015 [Electronic resource] / G. Osborne. — Mode of access: https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security.

17. Andelin P. ISP Level Malware Filtering: An Extended Clean Feed? [Electronic resource] / P. Andelin. — Mode of access: http://www.lavasoft.com/support/spywareeducationcenter/wp_ispmalwarefiltering.php.

18. Cyber Security Breaches Survey 2016: Main Report / R. Klahr et al. — London, 2016. — 49 p.

19. Barlow J.P. A Declaration of Independence of Cyberspace [Electronic resource] / J.P. Barlow. — Mode of access: www.eff.org/-barlow/Declaration-Final.html.

20. Наумов В.Б. Право и Интернет: очерки теории и практики / В.Б. Наумов. — М. : Кн. дом «Университет», 2002. — 432 с.

21. Wilske S. International Jurisdiction in Cyberspace: Which States May Regulate the Internet? [Electronic resource] / S. Wilske, T. Schiller. — Mode of access: www.law.indiana.edu/fclj/pubs/v50.

REFERENCES

1. Fat'yanov A.A. Topical problems of information security in the virtual reality of the Internet. *Referativnyi zhurnal VINITY = Digest Journal of Russian Institute for Scientific and Technical Information (VINITY RAS)*, 2001, no. 10, pp. 6–8. (In Russian).
2. Rassolov I.M. *Internet-pravo* [Internet law]. Moscow, Zakon i pravo Publ., 2012. 143 p.
3. Menthe D. Jurisdiction in cyberspace: A theory of international spaces. *Michigan Telecommunications and Technology Law Review*, 1998, vol. 4, iss. 1, pp. 103.
4. Wang F.F. *Internet Jurisdiction and Choice of Law: Legal Practices in the EU, US and China*. Cambridge, 2010. 276 p.
5. Boes S., Leukfeldt E.R. Fighting cybercrime: joint effort. *Ciber-Physical Security: Protecting Critical Infrastructure at the State and Local Level.* Cincinnati, Springer, 2016, pp. 185–205.
6. Begishev I.R. Crimes in the sphere of digital information. *Informatcionnoe pravo = Information Law,* 2010, no. 2, pp. 18–21. (In Russian).
7. Stepanov-Egiants V.G. *Prestupleniya v sfere bezopasnosti obrashcheniya komp'yuternoi informatsii: sravnitel'nyi analiz. Kand. Diss.* [Crimes in the sphere of computer information security: a comparative analysis. Cand. Diss.]. Moscow, 2005. 168 p.
8. Hajli N., Featherman M.S. Social commerce and new development in e-commerce technologies. *International Journal of Information Management,* 2017, no. 37, pp. 177–178.
9. 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.
10. Leukfeldt E.R. Organised Cybercrime and social opportunity structures: a proposal for future research directions. *The European Review of Organised Crime,* 2015, no. 2, pp. 91–103.
11. Prins C. et al. *Trust in Electronic Commerce*. Norwell, Kluwer Law International, 2002. 321 p.
12. Gercke M. *Understanding Cybercrime: Phenomena, Challenges and Legal Response*. Geneva, Telecommunication Development Sector, 2012. 356 p.
13. Okamura H. *Liability of Internet Service Providers*. Available at: http://www.softic.or.jp/symposium/open_materials/10th/en/okamura-en.pdf.
14. Weber R.H. *Internet Service Provider Liability. The Swiss Perspective*. Available at: http://www.jipitec.eu/issues/jipitec-1-3-2010/2793/Weber_ISP_Ch. pdf.
15. Filimonov S.A. Problems of fight against computer fraud as the potential threat to the information community. *Sovremennoe pravo = Modern Law*, 2014, no. 9, pp. 123–127. (In Russian).
16. Osborne G. *Chancellor's Speech to GCHQ on Cyber Security*, 2015. Available at: https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security.
17. Andelin P. *ISP Level Malware Filtering: An Extended Clean Feed?* Available at: http://www.lavasoft.com/support/spyware-educationcenter/ wp_ispmalwarefiltering.php.
18. Klahr R. et al. *Cyber Security Breaches Survey 2016: Main Report*. London, 2016. 49 p.
19. Barlow J.P. *A Declaration of Independence of Cyberspace*. Available at: www.eff.org/-barlow/Declaration-Final.html.
20. Naumov V.B. *Pravo i Internet: ocherki teorii i praktiki* [Law and the Internet: essays on the theory and practice]. Moscow, Universitet Publ., 2002. 432 p.
21. Wilske S., Schiller T. *International Jurisdiction in Cyberspace: Which States May Regulate the Internet?* Available at: www.law.indiana.edu/fclj/pubs/v50.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Суходолов Александр Петрович — ректор Байкальского государственного университета, доктор экономических наук, профессор, заслуженный экономист Российской Федерации, г. Иркутск, Российская Федерация; e-mail: rector@bgu.ru.

Колпакова Людмила Алексеевна — заместитель начальника кафедры уголовного процесса, криминалистики и оперативно-розыскной деятельности Вологодского института права и экономики Федеральной службы исполнения наказаний, кандидат юридических наук, доцент, г. Вологда, Российская Федерация; e-mail: upkiord@yandex.ru.

Спасенников Борис Аристархович — главный научный сотрудник Научно-исследовательского института Федеральной службы исполнения наказаний, доктор юридических наук, доктор медицинских наук, профессор, г. Москва, Российская Федерация; e-mail: borisspasennikov@yandex.ru.

БИБЛИОГРАФИЧЕСКОЕ ОПИСАНИЕ СТАТЬИ

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

INFORMATION ABOUT THE AUTHORS

Sukhodolov, Alexander P. — Rector, Baikal State University, Doctor of Economics, Professor, Honored Economist of the Russian Federation, Irkutsk, the Russian Federation; e-mail: rector@bgu.ru.

Kolpakova, Ludmila A. — Deputy Head, Chair of Criminal Process, Criminalistics and Investigative Activities, Vologda Institute of Law and Economics, Federal Penitentiary Service of Russia, Ph.D. in Law, Ass. Professor, Vologda, the Russian Federation; e-mail: upkiord@yandex.ru.

Spasennikov, Boris A. — Chief Researcher, Research Institute of Federal Penitentiary Service of Russia, Doctor of Law, Doctor of Medicine, Professor, Moscow, the Russian Federation; e-mail: borisspasennikov@yandex.ru.

BIBLIOGRAPHIC DESCRIPTION

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).