Н.С. Богачева

Магистрант ЧОУ ВО «Институт управления», г. Архангельск

Б.А. Спасенников

Доктор юридических наук, профессор, главный научный сотрудник, Научно-исследовательский институт Федеральной службы исполнения наказаний, г. Москва

Криминальные угрозы в сфере цифровой экономики

Цель исследования состоит в формировании научно обоснованных предложений по совершенствованию системы мер противодействия преступности в сфере цифровой экономики.

Ключевые слова: цифровая экономика, информационная безопасность, противодействие преступности, киберпреступность.

Концепция электронной («цифровой») экономики, которая появилась в конце XX века и стремительно обретающей новые формы, в настоящее время влечет поистине революционные изменения в классической модели хозяйствования и бизнес-сфере. В силу переноса экономических отношений в Интернет-пространство (виртуальную среду, киберпространство) 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 (BCG) тройку лидеров с наиболее развитой «цифровой экономикой» составляют Великобритания (12,4 % от ВВП), Южная Корея (8 %) и Китай (6,9 %). 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, конфиденциальности защиты интеллектуальной собственности говорится и в Канкунской декларации ОЭСР 2016 г. [1, с. 375–380].

Понятие «цифровой экономики» в узком смысле сводится к так называемой электронной коммерции, осуществляемой посредством информационных и коммуникационных технологий. 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 – «Интернет», вместо физического обмена. Аналитический центр при Правительстве РФ в период с 12 по 25 января 2017 года провел опрос, в рамках которого 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. Таким образом, рассматриваемое явление нельзя сводить к чистой коммерции. Оно имеет также значительный социальный и культурный потенциал. Оценка влияния «цифровой экономики» на национальную и глобальную экономику, а также неизбежно на всю социальную сферу весьма важна ввиду нарастающих проблем преступности, также модернизирующейся благодаря электронизации и цифровизации общества. В специальной литературе отмечается, что кибер–преступность может быть ассоциирована не только с проблемами информационной безопасности, но и с угрозами государственности, военно–промышленному и производственному комплексам, инфраструктуре жизнеобеспечения [3, с. 125–128].

Сегодня, говоря о преступлениях в сфере экономики, целесообразно выделять в отдельную категорию для изучения 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 2572. Однако заметим, что эта цифра не характеризует в полном объеме размах исследуемого явления во многом благодаря высокой латентности, проистекающей главным образом от 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 и 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 статьи 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 главами 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, за создание, использование и распространение которых ответственность предусмотрена ст. 273 УК РФ, преступники могут применять программное обеспечение иного рода, например, предназначенное для дешифрования информации, подбора паролей, а также различные электронные приспособления, такие как сканеры портов и прочее. В условиях запрета применения 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, что поможет снять ряд вопросов с квалификацией соответствующих деяний [2, с. 256–263].

Проникновение информационных и телекоммуникационных технологий в экономику обострило проблемы охраны персональных данных, коммерческой, корпоративной и банковской тайн. 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, к примеру, 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. все чаще используются в мошеннических целях [4].

В структуре преступлений экономической направленности значительно превалируют деяния в финансово–кредитной сфере (28884 из 108754 выявленных преступлений за 2016 г.). 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 лежит 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 % – государственные финансовые институты. Материалы изученных уголовных дел также 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 кибер-атак.

Так, в феврале 2017 года 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 помощью которых получала доступ к управлению банковскими счетами юридических лиц и совершила хищения денежных средств на общую сумму 100 млн. рублей. Уголовное дело возбуждено по ч. 1 ст. 273 и ч. 3 ст. 159.6 УК РФ [7, с. 495–502].

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», с использованием вредоносной программы и путем использования похищенных аутентификационных данных (электронно-цифровой подписи) получали незаконный доступ к счетам агентов систем электронных платежей, перечисляли с них средства на лицевые счета абонентских номеров телефонов, а после обналичивания, перечисляли 25 % от похищенной суммы на неустановленный кошелек электронной платежной системы «WebMoney Transfer», предоставленный неустановленным соучастником. В течение 2 часов ими было совершено более 130 незаконных операций по переводу денежных средств на общую сумму 1.597.600 руб. В эти же и следующие сутки таким же способом было осуществлено хищение еще 1.480.000 руб. 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 [6, с. 258–267].

Цифровые технологии в руках даже одного человека, не говоря уже о действии организованных преступных групп, 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-ритейлеров и манипулировать 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 которому приходит более эфемерная форма взаимодействия – криминальные макро–сети, их участниками становятся посетители форумов, чатов, закрытых онлайн–сообществ. Однако, чтобы стать вхожим в данные круги, требуется заслужить определенное доверие, иметь определенный статус и репутацию, поэтому остается открытым вопрос, является ли подобное взаимодействие менее устойчивым, нежели общение в преступной группе традиционной формы [5, с. 13–21].

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 Управлением «К» МВД России информация о выявленных фактах преступлений, в целом сходных по криминообразующим признакам, на «Интернет»-портале МВД РФ, 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 большим 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 это вопрос выносится за рамки уголовной юрисдикции в порядке более точного определения суммы гражданского иска, но именно этот 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 требуется 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.

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 требует серьезной разъяснительной работы с населением в рамках общей виктимологической профилактики. Обязанности по ее осуществлению следует возложить, прежде всего, на субъектов, предоставляющих соответствующие услуги. Так, например, банковский работник, оформляя клиенту платежную карту и подключая услугу «Мобильный банк», обязан разъяснить, от каких действий следует 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.

Общность проблем противодействия преступности в сфере «цифровой экономики» за рубежом и в России позволяет сделать вывод о необходимости аккумулирования и анализа положительного опыта таких стран как Швейцария, Великобритания, Норвегия, Дания [8; 9, с. 185-205], которые не только преуспели в продвижении инноваций в экономике, но и в сфере противодействия противозаконному их использованию.

Библиографический список:

1. Иванцов С.В. Организованная преступность в системе криминально-экономических отношений // Российский криминологический взгляд. 2012. № 1. С. 375–380.
2. Иванцов С.В. Средства массового информационного ресурса и противодействие преступности // Современные проблемы уголовной политики V Международная научно-практическая конференция. Под редакцией А.Н. Ильяшенко. 2014. С. 256–263.
3. Иванцов С.В. Теоретические предпосылки развития системного подхода в криминологических исследованиях преступности // Вестник Московского университета МВД России. 2014. № 11. С. 125–128.
4. Иванцов С.В., Новиков С.В. Преступления на рынке ценных бумаг. Криминологическая характеристика и предупреждение: монография. М., 2012.
5. Суходолов А.П., Иванцов С.В., Борисов С.В., Спасенников Б.А. Актуальные проблемы предупреждения преступлений в сфере экономики, совершаемых с использованием информационно-телекоммуникационных сетей // Всероссийский криминологический журнал. 2017. Т. 11. № 1. С. 13–21.

6. Суходолов А.П., Колпакова Л.А., Спасенников Б.А. Проблемы противодействия преступности в сфере «цифровой экономики» // Всероссийский криминологический журнал. 2017. Т. 11. № 2. С. 258–267.
7. Суходолов А.П., Спасенников Б.А., Швырев Б.А. Цифровая экономика: электронный мониторинг правонарушителей и оценка его экономической эффективности // Всероссийский криминологический журнал. 2017. Т. 11. № 3. С. 495–502.
8. Wang F.F. Internet Jurisdiction and Choice of Law: Legal Practices in the EU, US and China. Cambridge, 2010.
9. Boes S., Leukfeldt E.R. Fighting Cybercrime: Joint Effort // Ciber-Physical Security: Protecting Critical Infrastructure at the State and Local Level. Cincinnati: Springer. 2016. P. 185-205.