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

Вопросы предупреждения преступлений в сфере цифровой экономики

В статье сформулированы современные проблемы противодействия преступности в сфере экономики, связанной с особенностями совершения соответствующих уголовно наказуемых деяний с использованием возможностей информационно-телекоммуникационных сетей.

Ключевые слова: *Цифровая экономика, киберпреступность, криминология, предупреждение преступлений в сфере экономики.*

На XIII конгрессе ООН по предупреждению преступности и уголовному правосудию, состоявшемуся в 2015 г., преимущественно посвящённом противодействию транснациональному криминалитету, в частности была подчёркнута необходимость обеспечения использования экономических, социальных и технологических благ в качестве положительной силы, укрепляющей усилия сотрудничающих стран, направленные на предупреждение новых и возникающих форм преступности и борьбу с ними. Для этого предлагается разрабатывать и осуществлять всеобъемлющие меры реагирования в области предупреждения преступности и уголовного правосудия, в том числе принимать необходимые законодательные и административные меры для эффективного предупреждения новых, появляющихся и видоизменяющихся форм преступности и борьбы с ними на национальном, региональном и международном уровнях [1, с. 375–380; 3, с. 125–128].

Применительно к киберпреступности было предложено опробовать конкретные меры по созданию защищенной и устойчивой киберсреды, предупреждать и пресекать преступную деятельность, осуществляемую с использованием сети «Интернет», укреплять сотрудничество между правоохранительными органами на национальном и международном уровнях, повышать защищенность компьютерных сетей и обеспечивать защиту соответствующей инфраструктуры и стараться оказывать долгосрочную техническую помощь и содействие наращиванию потенциала для укрепления способности национальных ведомств противодействовать киберпреступности, в

том числе посредством профилактики, выявления, расследования и уголовного преследования таких преступлений во всех их формах [2, с. 256–263].

В Стратегии национальной безопасности Российской Федерации к числу главных стратегических угроз национальной безопасности в области экономики, в частности, отнесены незащищенность национальной финансовой системы от действий нерезидентов, уязвимость ее информационной инфраструктуры, сохранение значительной доли теневой экономики и условий для криминализации хозяйственно-финансовых отношений. При этом отмечается появление новых форм противоправной деятельности с использованием информационных, коммуникационных и высоких технологий [7, с. 495–502].

В Доктрине информационной безопасности указано, что информационные технологии с течением времени приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятельности личности, общества и государства. Поэтому их эффективное применение следует рассматривать как фактор ускорения экономического развития государства и формирования информационного общества. Вместе с тем, как подчёркивается в данном документе, наблюдается рост компьютерной преступности, прежде всего в кредитно-финансовой сфере, причём способы и средства совершения таких преступлений становятся все изощрённее.

Отметим, что в последние годы российские учёные стали обращать пристальное внимание на активизацию использования информационно-телекоммуникационных сетей для совершения различных преступлений, в том числе относящихся к числу экономических, террористических и экстремистских уголовно наказуемых деяний [6, с. 258–267]. Вместе с тем специализированные научные исследования в данной области проводятся редко и, как правило, имеют узкую направленность, тогда как выделенная проблема имеет комплексный характер и требует системного подхода к её решению. Национальный законодатель также с запозданием реагирует на видоизменения преступности, в том числе на новые способы совершения преступлений в сфере экономики, обусловленные развитием информационных технологий [5, с. 13–21].

Анализ норм раздела VIII Уголовного кодекса Российской Федерации (далее – УК РФ) «Преступления в сфере экономики» и практики их применения показал существенное расхождение между юридически закреплёнными и фактическими видами преступлений в сфере экономики, совершаемыми с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет».

Так, в указанном разделе Особенной части УК РФ содержится только две статьи, в которых упоминаются информационно-телекоммуникационные сети: 1) ст. 159^6 «Мошенничество в сфере компьютерной информации» и 2) ст. 171^2 «Незаконные организация и проведение азартных игр». Первая уголовно-правовая норма была введена Федеральным законом от 29 ноября 2012 г. № 207-ФЗ, а вторая – Федеральным законом от 20 июля 2011 г. № 250-ФЗ [4].

Информационно-телекоммуникационные сети могут использоваться и для совершения экономических преступлений, связанных с приобретением и сбытом определённых предметов, в том числе поддельных денег, ценных бумаг, банковских карт, а также данных действующих банковских карт. Однако в данном случае использование сети «Интернет» или других информационно-телекоммуникационных сетей является одним из возможных способов совершения соответствующих преступлений и, как правило, не придаёт им какую-либо специфику, то есть выступает в качестве их факультативного признака. Например, данные действующих банковских карт позволяют совершать покупки в Интернет-магазинах без использования специального ПИН-кода. В Интернете к продаже активно предлагаются двухсторонние изображения банковских карт, а также их ПИН-коды, при наличии которых можно изготовить поддельный аналог таких карт и

использовать его для оплаты товаров в обычных магазинах. Также через ресурсы сети «Интернет» продаются и покупаются скиммеры (приборы, устанавливаемые на банкоматах, позволяющие считать данные используемой банковской карты. Вне связи с конкретным преступлением многие из таких действий (например, предоставление данных действующей банковской карты или продажа скиммера) не являются уголовно наказуемыми, что является пробелом в праве.

Опрос и изучение уголовных дел показали, что информационно-телекоммуникационные сети, хотя и не используются при выполнении объективной стороны других преступлений в сфере экономики, однако задействуются в процессе приготовления к ним, в том числе для поиска необходимой информации, обмена сведениями, приобретения необходимых орудий и средств, подыскания соучастников преступления и сговор с ними на совместное совершение последнего. То есть использование информационно-телекоммуникационных сетей в настоящее время является одним из обязательных либо факультативных объективных признаков ряда составов преступлений в сфере экономики, кроме того, такие сети фактически выступают средством, которое может использоваться в ходе приготовления к любым уголовно наказуемым деяниям экономической направленности.

В результате изучения материалов 120 уголовных дел (44 дел о мошенничестве в сфере компьютерной информации, 31 дела об организации азартных игр, 15 дел о причинении имущественного ущерба путём обмана или злоупотребления доверием, 11 дел о незаконных получении и разглашении сведений, составляющих коммерческую, налоговую или банковскую тайну, и 19 дел об иных преступлениях в сфере экономики) и опроса указанных выше респондентов мы пришли к выводу, что использование информационно-телекоммуникационных сетей для приготовления и (или) последующего совершения таких преступлений, как правило, придаёт соответствующей криминальной деятельности усложнённый, профессиональный характер, предполагающий использование виновными знаний, умений и навыков в области информационных технологий, превышающих уровень обычных компьютерных пользователей; планирование своего преступного поведения и дальнейшего сокрытия его следов, а также направлений использования и легализации преступно полученного имущества; использование возможностей и преимуществ удалённого совершения преступления; увеличение размера и расширение спектра причиняемых общественно опасных последствий. Помимо этого, 23% опрошенных сотрудников правоохранительных органов отметили, что в ходе оперативно-розыскного сопровождения уголовных дел о таких преступлениях ими были выявлены сведения об организованном и транснациональном характере данной преступной деятельности. Эти обстоятельства также отмечаются в теоретических исследованиях [4].

Выделенные особенности таких преступлений осложняют деятельность по их предупреждению, и вызывают необходимость выработки комплекса научно-обоснованных рекомендаций, направленных на повышение эффективности соответствующей превентивной деятельности, в том числе на придание ей системного характера. Предупреждение таких преступлений должно строится с учётом общих принципов и устоявшегося содержания такой деятельности и одновременно учитывать особенности рассматриваемых уголовно наказуемых деяний и лиц, их совершающих, современное состояние законодательства и правоохранительной деятельности в данной области [7, с. 495–50].

Нами также были изучены уголовные дела о причинении имущественного ущерба путём обмана или злоупотреблении доверием (ст. 165 УК РФ), которое также может совершаться с использованием информационно-телекоммуникационных сетей (по 11 из 15 изученных уголовных дел). Данное преступление наиболее сходно

с мошенничеством и, по нашему мнению, обладает не меньшей общественной опасностью, однако законодатель в 2011 г. включил в число обязательных признаков состава рассматриваемого преступления крупный размер причиняемого ущерба, что оставило вне сферы уголовной ответственности подавляющее большинство деяний, ранее подпадавших под действие ст. 165 УК РФ. Данное законодательное изменение мы находим необоснованным, с чем согласились 70,6% опрошенных сотрудников правоохранительных органов, 92,6% судей и 77,9% научно-педагогических работников. Также респонденты поддержали наше предложение о дополнении статей 165 и 183 УК РФ квалифицирующим признаком в виде совершение преступление с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет» - 50,8%, 43,6% и 81,1% опрошенных соответственно.

Анализ материалов уголовных дел и опрос представителей практики позволили нам сделать вывод о необходимости совершенствования и других нормативных правовых актов, направленных на предупреждение преступности.

Прежде всего, это Федеральный закон от 23 июня 2016 г. № 182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации», в котором отсутствуют положения, учитывающие специфику предупреждения преступлений, совершаемых с использованием информационно-телекоммуникационных сетей [7, с. 495–50].

Полагаем, что сотрудничающие государства должны стремиться к укреплению и расширению взаимодействия в области противодействия преступности, в том числе преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей. Принятие двухсторонних и многосторонних договоров в этой области будет способствовать унификации правовых средств, направленных на предупреждение, выявление, раскрытие и доказывание таких преступлений.

В заключение отметим, что предупреждение рассматриваемых уголовно наказуемых деяний должно быть встроено в общую систему предупреждения преступлений, совершаемых с использованием информационно-телекоммуникационных сетей. Элементы современной преступности тесно переплетены и взаимосвязаны, поэтому превентивные меры также должны иметь согласованный, дополняющий друг друга характер и в своей совокупности представлять единую систему противодействия преступности, ориентированную на эффективную защиту личности, общества и государства от общественно опасных посягательств.

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.

© Богачева Н.С, Спасенников Б.А.,2017