Уголовное право и информатизация

РУССКЕВИЧ Евгений Александрович, старший преподаватель кафедры уголовного права Московского университета МВД России им. В. Я. Кикотя, кандидат юридических наук
117437, Россия, г. Москва, ул. Академика Волгина, 12
E-mail: russkevich@mail.ru

Построение информационно-коммуникационной инфраструктуры закономерно вызвало появление новой формы общественно опасного поведения личности — компьютерной преступности. Другим следствием глобальной информатизации явилось изменение облика преступности в целом, которая в связи с использованием информационно-коммуникационных технологий приобрела несвойственные ей ранее признаки. Процесс проникновения кибернетических методов, а также инструментария информационно-коммуникационных технологий в механизм преступления (информатизация преступности) актуализирует необходимость научного осмысления состояния и перспектив развития отечественного уголовного права.

Цель исследования состоит в разработке теоретических рекомендаций и предложений по преодолению проблем, возникающих в связи с уголовно-правовым противодействием преступлениям, совершаемым с использованием информационно-коммуникационных технологий. Реализация указанной цели достигалась путем оценки состояния отечественного уголовного законодательства, классификации преступлений, совершаемых с использованием информационно-коммуникационных технологий, определения основных направлений и условий эффективной модернизации Уголовного кодекса Российской Федерации.

Исследование основано на применении общенаучных и специальных методов (анализ, синтез, индукция, формально-юридический, абстрактно-логический и др.).

Реформирование отечественного уголовного законодательства должно осуществляться по трем основным направлениям: 1) расширение перечня преступлений, посягающих на информационную безопасность; 2) криминализация новых высокотехнологичных форм посягательств на традиционно охраняемые уголовным законом общественные отношения; 3) модернизация действующих составов преступлений путем детализации их совершения специфическим способом — с использованием информационно-коммуникационных технологий. Несмотря на масштаб и сложность проблемы эффективного противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий, изменение Уголовного кодекса Российской Федерации должно осуществляться по принципу минимизации вносимых поправок.

Ключевые слова: уголовное право, уголовная политика, информатизация, информационно-коммуникационные технологии, информационная безопасность, компьютерные преступления.

Criminal Law and Informatization

E. A. RUSSKEVICH, senior lecturer at the Department of criminal law of the Kikot Moscow University of the Ministry of Internal Affairs of the Russian Federation
12, Akademik Volgin st., Moscow, Russia, 117437
E-mail: russkevich@mail.ru

The construction of information and communication infrastructure naturally caused the emergence of a new form of socially dangerous behavior of a person — computer crime. Another consequence of global informatization was the change in the appearance of crime in general, which, due to the use of information and communication technologies, acquired features that were not characteristic of it before. The process of penetration of cybernetic methods, as well as tools of information and communication technologies in the mechanism of crime (informatization of crime), actualizes the need for scientific understanding of the state and prospects for the development of domestic criminal law.

The research objective is to develop theoretical recommendations and proposals for overcoming the problems arising in connection with criminal legal counteraction to crimes committed using information and communication technologies. The implementation of this goal was achieved by assessing the

state of domestic criminal legislation, the classification of crimes committed using information and communication technologies, determining the main directions and conditions for effective modernization of the Criminal Code of the Russian Federation.

The study is based on the application of general scientific and special methods (analysis, synthesis, induction, formal-legal, abstract-logical, etc.)

Reforming of domestic criminal legislation should be carried out in three main areas: 1) expanding the list of crimes that encroach on information security; 2) the criminalization of new high-tech forms of encroachment on the social relations traditionally protected by criminal law; 3) modernization of existing crime patterns by detailing their commission in a specific way — using information and communication technologies. Despite the scale and complexity of the problem of effective counteraction to crimes committed with using information and communication technologies, the amendment of the Criminal Code of the Russian Federation should be carried out on the principle of minimizing the introduced changes.

Keywords: criminal law, criminal policy, computerization, information and communication technology, information security, computer crime.

DOI: 10.12737/article_597714e7c1b439.52593067

Научно-технический прогресс, совершенствование производства и, как следствие, удешевление компьютерной техники, программного обеспечения и услуг связи обусловили процесс непрерывного роста использования информационно-коммуникационных технологий (далее — ИКТ) во всех сферах жизни общества. Можно с уверенностью утверждать, что продолжается он и до настоящего времени. На этой основе сформировалась новая модель социального взаимодействия, основанная в большей мере не на личном, а на интерактивном (дистанционном и нередко анонимном) общении.

Увеличение числа пользователей современными электронными средствами связи («виртуализация» жизнедеятельности¹) открыло новые возможности не только для политики, экономики и культуры, но и для преступной деятельности. Построение информационно-коммуникационной инфраструктуры закономерно вызвало появление новых форм общественно опасного поведения личности — компьютерной преступности (computer crime).

¹ См.: Гилинский Я. И. Криминологические основы уголовного права в эпоху постмодерна // Криминологические основы уголовного права: матер. X Российского конгресса уголовного права, состоявшегося 26—27 мая 2016 г. / отв. ред. В. С. Комиссаров. М., 2016. С. 296.

Другим следствием глобальной информатизации явилось изменение облика преступности в целом, которая в связи с использованием ИКТ приобрела несвойственные ей ранее признаки. Следует отметить, что в отечественной теории уголовного права нет общепринятой дефиниции подобного рода «гибридных» преступлений. Используются различные категории: информационные преступления², киберпреступления³, преступления в сфере высоких технологий⁴, интернет-преступления⁵. В зарубежной литературе распространение получили два поня-

² См.: Букалерева Л. А. Информационные преступления в сфере государственного и муниципального управления: законотворческие и правоприменительные проблемы: дис. ... д-ра юрид. наук. М., 2007; Крылов В. В. Информационные компьютерные преступления. М., 1997.

³ См.: Тропина Т. Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. ... канд. юрид. наук. Владивосток, 2005; Чекунов И. Г. Криминологическое и уголовно-правовое обеспечение предупреждения киберпреступности: автореф. дис. ... канд. юрид. наук. М., 2013.

⁴ См.: Козаев Н. Ш. Современные технологии и проблемы уголовного права (анализ зарубежного и российского законодательства): монография. М., 2015.

⁵ См.: Гузеева О. С. Преступления, совершаемые в российском сегменте сети Интернет: монография. М., 2015.

тия: cyber crime и computer-related crime⁶.

На наш взгляд, указанные явления представляют собой результат информатизации преступности — процесса проникновения кибернетических методов, а также инструментария ИКТ в механизм преступления.

В связи с этим современное общество столкнулось с необходимостью решения двух взаимосвязанных уголовно-политических задач:

1) построение эффективной системы защиты информации и информационно-коммуникационной инфраструктуры;

2) приведение в соответствие сложившихся положений уголовного права с последствиями глобальной информатизации преступности.

Очевидно, что решение первой задачи требует определения круга деяний, посягающих на информационную безопасность, противодействие которым необходимо эффективно осуществлять посредством уголовно-правовых предписаний.

Значительно более сложной видится вторая задача. Информатизация преступности рождает ряд непростых вопросов модификации уголовного закона: 1) пригодны ли классические положения института соучастия к случаям виртуального преступного взаимодействия, являющегося дистанционным и, как правило, анонимным; 2) каким должно быть оптимальное количество составов преступлений, посягающих на информацию и элементы информационно-коммуникационной инфраструктуры; 3) есть ли необходимость и насколько обширно следует изменить диспозиции традиционных

составов преступлений путем детализации их совершения специфическим способом — с использованием ИКТ; 4) будет ли модернизация традиционных составов преступлений достаточной для противодействия современным криминальным угрозам и не потребуются ли определение ряда специальных норм; 5) какую роль использование ИКТ должно занять в сложившейся системе дифференциации уголовной ответственности?

Хотя накопившиеся проблемы сделали перемены не только насущно необходимыми, но и уже серьезно запоздалыми, до настоящего времени, пожалуй, нет четкого понимания относительно того, насколько современное уголовное право должно измениться, адаптируясь к условиям информационного общества. Во многом это объясняется таким обстоятельством, как нехватка или недостоверность криминологического знания⁷. На уровне профессиональных субъектов уголовной политики нет не только стратегически выверенного плана модернизации уголовного законодательства, но и относительно внятного представления о специфике и масштабах проблемы. Опыт криминализации мошенничества в сфере компьютерной информации (ст. 159⁶ УК РФ) является, пожалуй, наглядным тому подтверждением⁸.

⁷ См.: Бабаев М. М., Пудовочкин Ю. Е. Проблемы российской уголовной политики. М., 2014. С. 93.

⁸ Благое намерение Верховного Суда РФ облегчить жизнь правоприменителя и упорядочить судебно-следственную практику, пожалуй, так и осталось нереализованным. Появление специальной нормы о мошенничестве в сфере компьютерной информации имело, по сути, обратный эффект, поскольку вызвало еще больше проблемных вопросов. См., например: Кауфман М. А. Проблемность, неопределенность, избыточность уголовного законодательства как криминогенные факторы // Криминологические основы уголовного права: матер. X Российского

⁶ См.: Dana L. Bazelon, Yun Jung Choi, Jason F. Conaty. Computer Crimes. Am. Crim. L. Rev. 2006; Douglas H. Hancock. To What Extent Should Computer Related Crimes be the Subject of Specific Legislative Attention? Alb. L. J. Sci. & Tech. 2001; Stephen P. Heymann. Legislating Computer Crime. Harv. J. On Legis. 1997.

В связи с этим на первоначальном этапе необходимо добиться смысловой определенности проблемы, ясно-го понимания ее сущности. Для достижения этой цели прежде всего требуется тщательно проработать вопрос о типологизации преступлений, совершаемых с использованием ИКТ, что позволит выявить и лучше уяснить содержание данного явления.

Не вызывает сомнений, что самостоятельным видом преступлений, совершаемых с использованием ИКТ, являются компьютерные преступления, т. е. деяния, посягающие на охраняемую законом информацию и безопасность информационно-коммуникационной инфраструктуры. Природа данных преступлений специфична в том смысле, что само их происхождение, существование и, следовательно, совершение немислимы без информационной среды.

В этом аспекте отечественное уголовное законодательство, а именно гл. 28 УК РФ, требует серьезной доработки. Научному сообществу и законодателю еще потребуются оценить необходимость криминализации DDoS-атаки⁹, спаминга, фишинга и др. Этому должна сопутствовать реалистичная оценка текущих и перспективных возможностей государства, включая материальные, организационные и технические.

Близкую по природе, но качественно иную группу деяний образу-

ют новые формы общественно опасных посягательств на традиционно охраняемые уголовным законом общественные отношения, совершаемые в информационной среде. Ярким представителем данного вида является хищение денежных средств потерпевшего в результате автоматического срабатывания информационной системы (распространенное хищение денежных средств с банковского счета посредством использования сервисов дистанционного банковского обслуживания). Деяние, которое неоправданно было оценено законодателем как мошенничество, в действительности представляет совершенно новую (седьмую¹⁰) форму хищения.

Примером, пожалуй, также выступают деяния, связанные с требованием о передаче имущества в качестве условия разблокировки программного обеспечения компьютера, возобновления доступа к электронной почте или аккаунту в социальной сети, восстановления модифицированной информации и т. п.

Как представляется, значительный потенциал расширения преступлений данного вида содержится в регламентации средств уголовно-правового противодействия посягательствам на объекты «виртуальной собственности». Следует отметить, что правовая природа подобного рода объектов до настоящего времени четко в науке не определена. Юристы спорят, могут ли такие объекты, как электронные книги, библиотеки iTunes, аккаунт в социальной сети или многопользовательской игре, переходить в порядке наследования, а равно возможно ли возложить на подобное цифровое имущество обременение или использовать его в порядке исполнительного производства¹¹. Разумеется, в решении

конгресса уголовного права, состоявшегося 26—27 мая 2016 г. / отв. ред. В. С. Комиссаров. М., 2016; Третьяк М. И. Проблемы понимания способа компьютерного мошенничества в судебной практике // Уголовное право. 2015. № 5; Чупрова А. Ю. Проблемы квалификации мошенничества с использованием информационных технологий // Уголовное право. 2015. № 5.

⁹ Атаки на вычислительную систему (сайт) в целях создания условий, при которых добросовестные пользователи системы не смогут получить доступ к предоставляемым системным ресурсам (серверам) либо этот доступ будет затруднен.

¹⁰ См.: Шумихин В. Г. Седьмая форма хищения чужого имущества // Вестник Пермского университета. 2014. № 2. С. 229.

¹¹ См., например: Архипов В. В. Виртуальное право: основные проблемы ново-

этого вопроса доктрина уголовно-го права зависит от развития науки цивилистической, которая, думается, должна выделить такие объекты в качестве особой категории объектов гражданских прав с использованием отдельных элементов правового режима вещей, как это сделано, например, в отношении бездокументарных ценных бумаг.

И, наконец, значительно большую группу образуют традиционные преступления, объективная сторона которых может быть выполнена посредством программно-технических средств обработки информации. Особенностью данных преступлений является то, что в целом они не предполагают обязательного использования методов или процессов обработки информации, однако их совершение с использованием ИКТ является не только возможным, но и нередко встречающимся на практике. Так, использование «сайта-двойника» или электронной торговой площадки, смс-рассылка по типу «Мама, отправь 1000 рублей на этот номер! Позже все объясню!» являются лишь новыми формами обмана как традиционного способа мошенничества.

Несмотря на масштаб и сложность проблемы эффективного противодействия преступлениям, совершаемым с использованием ИКТ, полагаем, что модернизация уголовного закона должна осуществляться крайне осторожно, по принципу минимизации вносимых поправок. Нет никакой необходимости сплошного «насыщения» диспозиций уго-

ловно-правовых норм указанием на возможность их совершения посредством ИКТ. Такие оговорки должны иметь место только в случаях пробельности уголовного закона, его очевидного несоответствия современным угрозам. Например, действующая уголовно-правовая норма об ответственности за вымогательство не позволяет должным образом оценить встречающиеся на практике случаи требования передачи денежных средств или иного имущества под угрозой совершения DDoS-атаки. В связи с этим, думается, что ст. 163 УК РФ нуждается в изменениях.

Пожалуй, в качестве примера успешной модернизации уголовного закона к условиям информатизации преступности можно привести дополнение диспозиции ст. 187 УК РФ такой альтернативной формой совершения преступления, как изготовление, приобретение, хранение, транспортировка в целях использования или сбыта, а равно сбыт компьютерных программ, предназначенных для неправомерного осуществления приема, выдачи или перевода денежных средств.

Выборочным, социально и криминологически обоснованным должно быть также признание использования ИКТ квалифицирующим признаком преступления. Очевидно, далеко не всякое применение информационных технологий (например, Интернет) влияет на степень общественной опасности деяния. Так, не имеет принципиального значения, состоялось ли разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну, путем передачи документов либо посредством отправки письма по электронной почте. Мошенник, обманывающий потерпевших через Skype, вымогатель, отправляющий свои угрозы посредством сервиса WhatsApp, вряд ли совершает более тяжкое преступление по сравнению с классическими его формами. Таким образом, использование ИКТ имеет неравнозначный

го направления юридических исследований // Известия высших учебных заведений. Правоведение. 2013. № 2; Дюранске Б. Т., Кейн Ш. Ф. Виртуальные миры, реальные проблемы // Известия высших учебных заведений. Правоведение. 2013. № 2; Семенюта Б. Онлайн-игры: правовая природа отношений // Интеллектуальная собственность. Авторское право и смежные права. 2014. № 8.; Лисаченко А. В. Право виртуальных миров: новые объекты гражданских прав // Российский юридический журнал. 2014. № 2.

характер с точки зрения влияния на характер и степень общественной опасности преступления. Данный факт является настолько очевидным, насколько теоретически непроработанным. Специалисты обходят стороной эту проблему, не опираясь на какие-либо критерии, нередко почти интуитивно предлагают предусмотреть использование ИКТ квалифицирующим признаком того или иного преступления.

Включение квалифицирующего признака в состав преступления необходимо в случаях, когда он объективно повышает вероятность наступления вредных последствий, что является важнейшим показателем опасности действия. Как справедливо писал по этому поводу В. Н. Кудрявцев, «опасность действия заключается в том, что оно может вызвать определенные вредные последствия. Однако эти последствия наступают не во всех случаях. Естественно, что действия будут сравнительно тем опаснее, чем выше степень вероятности наступления вредных последствий»¹².

Например, Федеральным законом от 1 марта 2012 г. № 18-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» система квалифицирующих признаков сбыта наркотических средств, психотропных веществ или их аналогов была обоснованно дополнена указанием на использование электронных или информационно-телекоммуникационных сетей (включая сеть Интернет). Дело здесь не только в том, что использование информационно-телекоммуникационных сетей существенно осложняет выявление и раскрытие сбыта наркотических средств, но, что более важно, оно существенно облегчает его совершение (предоставляет неограниченные возможности для формирования клиентской базы, гарантирует анонимность, упрощает расчеты и т. д.).

¹² Кудрявцев В. Н. Объективная сторона преступления. М., 1960. С. 102.

Соглашаясь с приведенным решением, закономерно возникает вопрос о последовательной реализации уголовно-политического курса и распространении такого подхода к дифференциации ответственности за сбыт оружия (ст. 223 УК РФ), незаконный оборот сильнодействующих или ядовитых веществ (ст. 234 УК РФ), новых потенциально опасных психоактивных веществ (ст. 234¹ УК РФ), недоброкачественных лекарственных средств или медицинских изделий (ст. 238¹ УК РФ) и др. Очевидно, что для упорядочения и унификации в этой области недостаточно только устранения погрешностей в отдельных статьях и даже главах уголовного закона, для этого потребуются ревизия всего Уголовного кодекса РФ.

Руководствуясь приведенным выше критерием оценки опасности действия в зависимости от вероятности наступления общественно опасных последствий, следует сделать вывод, что использование ИКТ должно признаваться квалифицирующим признаком составов преступлений, объективная сторона которых связана с распространением деструктивной информации: ст. 230 «Склонение к потреблению наркотических средств, психотропных веществ или их аналогов», ст. 354 «Публичные призывы к развязыванию агрессивной войны», ст. 354¹ «Реабилитация нацизма» УК РФ и др.

Использование ИКТ является нередкой практикой по делам о распространении клеветнических сведений в отношении судьи, работников прокуратуры или следователей (ст. 298¹ УК РФ).

М. был осужден по ч. 1 ст. 298¹ УК РФ. Согласно приговору суда М., заведомо зная о том, что А. и Д. к уголовной и административной ответственности не привлекались, являются не судимыми, используя персональный компьютер, подключенный к сети Интернет, осознавая противоправный и общественно опасный характер своих действий и желая наступления общественно опасных

последствий в виде сообщения заведомо ложной, клеветнической информации, действуя с прямым умыслом, разместил в видеохостинге сети Интернет свое видеообращение в отношении А. и Д., озаглавленное «В Верховный Суд РФ», в котором сообщил заведомо ложные сведения о том, что заместитель Председателя Верховного суда Республики Мордовия А., используя свое служебное положение, творит правовой беспредел, принимает решения по своему усмотрению, без оглядки на закон, совершил коррупционное правонарушение, т. е. использовал свое служебное положение вопреки интересам службы, занимается фабрикацией материалов и фальсификацией доказательств, совершил должностное преступление, является преступником. В том же обращении в адрес неопределенного круга лиц М. сообщил заведомо ложные сведения о том, что судья Верховного суда Республики Мордовия Д. грубейшим образом нарушает действующее законодательство, попирает права и законные интересы граждан, совершила преступление против правосудия, является преступницей. Указанные преступные действия М., выразившиеся в распространении заведомо ложных сведений, размещенных им в открытом доступе для неограниченного круга пользователей сети, опорочили честь, достоинство А. и Д., а также подорвали их деловую репутацию, что стало известно не менее чем 300 пользователям видеохостинга сети Интернет¹³.

При решении вопроса о закреплении использования ИКТ в качестве квалифицирующего признака необходимо также учитывать степень его распространенности. При этом требуется не только оценка фактиче-

ской распространенности, но и анализ реальной опасности эскалации такого поведения в случае непринятия уголовно-политического решения. Так, отмечая, что современное медицинское оборудование нередко имеет беспроводной интерфейс доступа, специалисты обсуждают угрозу совершения убийства посредством дистанционного управления имплантируемым электрокардиостимулятором или дефибриллятором-кардиовертером¹⁴. Нельзя не признать основательность таких угроз, возможность их реального воплощения в будущем. Вместе с тем вряд ли следует утверждать, что такие формы посягательства на жизнь человека будут иметь типичный характер и потребуют определения в ряду квалифицирующих признаков убийства.

В качестве вывода отметим, что правовые проблемы, связанные с преступлениями, совершаемыми с использованием ИКТ, со временем будут лишь актуализироваться. Стремительно развивающаяся информационно-коммуникационная инфраструктура содержит большой методологический потенциал для юриспруденции, что является залогом последующего интереса к этой теме, в том числе в аспекте науки уголовного права.

¹⁴ На конференции по безопасности Breakpoint в Мельбурне (17.10.2012 г.) исследователь Барнаби Джек выступил с заявлением, что из-за недоработок в программном обеспечении имплантируемые кардиостимуляторы можно заставить нанести смертоносный удар током напряжением 830 вольт путем отправки команды с ноутбука, находящегося на расстоянии до 15 м. URL: <http://hitech.newsru.com/article/17Oct2012/cardio> (дата обращения: 08.08.2016).

¹³ См.: Дело № 1-6/2015 // Архив Ленинского районного суда г. Пензы.

Библиографический список

- Dana L. Bazelon, Yun Jung Choi, Jason F. Conaty. Computer Crimes. Am. Crim. L. Rev. 2006.
Douglas H. Hancock. To What Extent Should Computer Related Crimes be the Subject of Specific Legislative Attention? Alb. L. J. Sci. & Tech. 2001.
Stephen P. Heymann. Legislating Computer Crime. Harv. J. On Legis. 1997.
Архипов В. В. Виртуальное право: основные проблемы нового направления юридических исследований // Известия высших учебных заведений. Правоведение. 2013. № 2.

- Бабаев М. М., Пудовочкин Ю. Е. Проблемы российской уголовной политики. М., 2014.
- Букалерова Л. А. Информационные преступления в сфере государственного и муниципального управления: законотворческие и правоприменительные проблемы: дис. ... д-ра юрид. наук. М., 2007.
- Гилинский Я. И. Криминологические основы уголовного права в эпоху постмодерна // Криминологические основы уголовного права: матер. X Российского конгресса уголовного права, состоявшегося 26—27 мая 2016 г. / отв. ред. В. С. Комиссаров. М., 2016.
- Гузеева О. С. Преступления, совершаемые в российском сегменте сети Интернет: монография. М., 2015.
- Дюранске Б. Т., Кейн Ш. Ф. Виртуальные миры, реальные проблемы // Известия высших учебных заведений. Правоведение. 2013. № 2.
- Кауфман М. А. Пробельность, неопределенность, избыточность уголовного законодательства как криминогенные факторы // Криминологические основы уголовного права: матер. X Российского конгресса уголовного права, состоявшегося 26—27 мая 2016 г. / отв. ред. В. С. Комиссаров. М., 2016.
- Козаев Н. Ш. Современные технологии и проблемы уголовного права (анализ зарубежного и российского законодательства): монография. М., 2015.
- Крылов В. В. Информационные компьютерные преступления. М., 1997.
- Кудрявцев В. Н. Объективная сторона преступления. М., 1960.
- Лисаченко А. В. Право виртуальных миров: новые объекты гражданских прав // Российский юридический журнал. 2014. № 2.
- Семенюта Б. Онлайн-игры: правовая природа отношений // Интеллектуальная собственность. Авторское право и смежные права. 2014. № 8.
- Третьяк М. И. Проблемы понимания способа компьютерного мошенничества в судебной практике // Уголовное право. 2015. № 5.
- Тропина Т. Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. ... канд. юрид. наук. Владивосток, 2005.
- Чекунов И. Г. Криминологическое и уголовно-правовое обеспечение предупреждения киберпреступности: автореф. дис. ... канд. юрид. наук. М., 2013.
- Чупрова А. Ю. Проблемы квалификации мошенничества с использованием информационных технологий // Уголовное право. 2015. № 5.
- Шумихин В. Г. Седьмая форма хищения чужого имущества // Вестник Пермского университета. 2014. № 2.
-
-