УДК: 343
DOI: 10.24411/2312-3184-2019-10005

Урбан Вячеслав Владимирович
старший научный сотрудник
научно-исследовательского
центра Академии управления
МВД России
кандидат юридических наук
E-mail: policaj@mail.ru

Urban Vyacheslav Vladimirovich
senior researcher of Research Center
Management Academy of the Ministry
of the Interior of Russia
Candidate of Law
E-mail: policaj@mail.ru

ПРЕСТУПЛЕНИЯ, СОВЕРШАЕМЫЕ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ: ОБЩАЯ ХАРАКТЕРИСТИКА И УГОЛОВНО-ПРОЦЕССУАЛЬНЫЕ МЕРЫ ПО ИХ ПРОТИВОДЕЙСТВИЮ

Введение: в связи с широким распространением информационно-коммуникационных технологий меняется характер преступности. В настоящее время все больше преступлений совершаются с помощью компьютерной техники и сети Интернет. Целью данной статьи является анализ составов преступлений, которые совершаются с использованием сети Интернет, а также выработка системы мер противодействия таким преступлениям.

Материалы и методы: нормативную основу исследования образуют Конституция Российской Федерации, уголовное и уголовно-процессуальное законодательство. Использованы современные общенаучные методы познания социальных явлений и процессов. Представлен анализ действующего российского уголовного законодательства в сфере противодействия преступлениям, связанным с компьютерной информацией, рассмотрены иные составы преступлений, способом (орудием) совершения которых могут выступать информационно-телекоммуникационные сети.

Результаты исследования: в результате исследования предложены основные направления повышения эффективности уголовно-процессуального противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей, в том числе связанные с развитием международного сотрудничества в сфере уголовного процесса.

Выводы и заключения: полученные данные могут быть использованы для предотвращения и эффективного противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей.

Ключевые слова: правоохранительная деятельность, уголовный процесс, информационно-телекоммуникационные сети, сеть Интернет, преступления, совершаемые с использованием информационно-телекоммуникационных сетей, незаконный оборот наркотиков, группы смерти, киберпреступность.

CRIMES COMMITTED WITH THE USE OF INFORMATION AND TELECOMMUNICATION NETWORKS: GENERAL CHARACTERISTICS AND CRIMINAL PROCEDURAL MEASURES TO COUNTER THEM

Introduction. Due to the wide spread of information and communication technologies, the nature of crime is changing. Currently, more and more crimes are committed using computer equipment and the Internet. The purpose of this article is to analyze the composition of crimes that are committed using the Internet, as well as to develop a system of measures to counter such crimes.

Materials and methods. The regulatory framework of the study is formed by the Constitution of the Russian Federation, criminal and criminal procedure legislation. Used modern general scientific methods of cognition of social phenomena and processes. The analysis of the current Russian criminal legislation in the field of countering crimes related to computer information is presented, other corpus delicti are considered, the informational telecommunication networks can act as an instrument (instrument) of which.

Results. As a result of the study, the main directions of improving the efficiency of criminal procedure to counter crimes committed using information and telecommunication networks, including those related to the development of international cooperation in the criminal process, have been proposed.

Conclusions and conclusions. The obtained data can be used to prevent and effectively counter crimes committed using information and telecommunication networks.

Key words: Law enforcement activities; criminal process; information and telecommunication networks; Internet; crimes committed with the use of information and telecommunication networks; drug trafficking; death groups; cybercrime.

Одной из ключевых функций государства является правоохранительная, которая призвана обеспечивать выживание, сохранение и развитие общества как целостной системы. В основе данной функции лежит деятельность по защите прав и свобод личности, организаций и в целом общества и государства. Основ-

ной формой реализации рассматриваемой функции является правоохранительная деятельность, которая включает в себя такие направления, как обеспечение общественной безопасности, охрану общественного порядка, деятельность по выявлению и расследованию преступлений, осуществление правосудия, уголовно-исполнительную деятельность и др.

В рамках настоящей работы ограничим круг исследования уголовно-процессуальной деятельностью правоохранительных органов в части организации противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей (далее – ИТС).

Количество пользователей сети Интернет в России непрерывно растет. Так, только в российском сегменте сети Интернет в 2016 г. было более 80 млн человек. Например, в 2015 г. оборот товаров и услуг с использованием сети Интернет составил 2,3 % валового внутреннего продукта и в настоящее время сохраняет тенденцию к росту [2]. Ресурсы сети Интернет весьма разнообразны – электронные средства массовой информации, веб-сайты органов исполнительной власти, сайты подачи онлайн-объявлений, социальные сети и т.д. Соответственно, у человека появляется возможность осуществлять в сети Интернет посредством имеющихся там ресурсов практически те же действия, что и в реальной жизни. При этом виртуальное пространство находится под гораздо более слабым контролем со стороны государства, нежели реальная среда.

В связи с широким распространением информационно-коммуникационных технологий меняется характер преступности. В настоящее время все больше преступлений совершаются с помощью компьютерной техники и ИТС. Интернет-преступность растет быстрыми темпами. Информационная инфраструктура позволяет преступникам действовать скрытно, не оставляя своих координат, совершать преступные действия с территории любого государства (где имеются технические возможности), а также действовать с соисполнителями на международном уровне.

По подсчетам, произведенным компанией Symantec, совокупные доходы киберпреступников составляют более 110 млрд долларов в год. При этом побочные убытки, возникающие в результате совершения данных преступлений (затраты времени на восстановление работоспособности, простой оборудования и пр.), можно дополнительно оценить еще в 274 млрд долларов. Соответственно, общий ущерб от киберпреступности в мировом масштабе составляет около 388 млрд долларов в год. При этом глобальный мировой оборот марихуаны, кокаина и героина, составляет порядка $288 млрд, что на 26 % ниже [9, с. 38].

В последние годы на страницах юридической печати стало все больше внимания уделяться вопросам использования ИТС для совершения различных преступлений. Так, диссертационные исследования по указанной проблематике проводились У.В. Зининой (Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве), А.Н. Копырюлиным (Преступления

в сфере компьютерной информации: уголовно-правовой и криминологический аспекты), Г.И. Узембаевой (Преступления экстремистской направленности, совершаемые с использованием средств массовой информации либо информационно-телекоммуникационных сетей: уголовно-правовая и криминологическая характеристика), З.И. Хисамовой (Уголовно-правовые меры противодействия преступлениям, совершаемым в финансовой сфере с использованием информационно-телекоммуникационных технологий) и др. Отдельные аспекты проблемы предупреждения преступлений, совершаемых с использованием компьютерных и информационных технологий, нашли отражение в работах Ю.В. Гаврилина, В.П. Коняхина, В.П. Котина, И.Л. В.Д. Ларичева, Ю.И. Ляпунова, И.Г. Чекунова, А.Ю. Чупровой, Н.Г. Шурухнова.

Однако проводимые научные исследования в указанной области, как правило, имеют узкую направленность, тогда как обозначенная в статье проблема отличается комплексным характером и требует системного подхода к решению.

Нормативную основу исследования образуют Конституция Российской Федерации, уголовное, уголовно-процессуальное законодательство и иные нормативные правовые акты, касающиеся регламентации вопросов в рассматриваемой области.

Методологической основой исследования является прежде всего диалектический метод познания, позволивший всесторонне и объективно рассмотреть поставленные вопросы.

Теоретическую основу исследования составили научные труды, посвященные вопросам борьбы с преступлениями, совершаемыми с использованием ИТС.

Современное российское уголовное законодательство предусматривает санкции лишь за деяния, связанные с нарушением сохранности компьютерной информации, т. е. преступления, в которых объектом выступают общественные отношения, возникающие в сфере компьютерной информации или обеспечивающие безопасность компьютерной информации [10, с. 54].

При этом в настоящее время с использованием информационно-коммуникационных технологий совершаются не только преступления, связанные с компьютерной информацией. Практически по всем преступлениям современные виды компьютерных программ или программно-технические средства могут использоваться в качестве средства или орудия совершения.

По справедливому мнению И.М. Рассолова, компьютерная преступность представляет собой криминальную отрасль, в которой действуют мошенники, хакеры, вымогатели, педофилы, сутенеры, процветает торговля людьми и наркотиками, а также многие другие правонарушения [6].

Так, ряд преступлений в сфере экономики совершается с использованием информационно-коммуникационных технологий. К таковым можно отнести мошеннические действия, связанные со взломом профилей пользователей в социальных сетях и последующей рассылкой сообщений «друзьям» жертвы взлома с

просьбой о переводе денежных средств под различными предлогами. В эту же группу можно отнести заведомо фиктивную продажу товаров (услуг).

Основным средством совершения таких преступлений, как неправомерный оборот средств платежей, незаконная банковская деятельность, также являются информационно-коммуникационные технологии. Так, совершение данных преступлений предполагает проведение банковских операций по переводу денежных средств. При этом платежные поручения направляются в основном посредством сети Интернет, что значительно ускоряет и упрощает преступную деятельность, а также создает определенные препятствия по уголовно-процессуальному документированию данной деятельности.

Постоянно увеличивается число фактов совершения преступлений против половой свободы и половой неприкосновенности, в частности в отношении несовершеннолетних. Так, в Российской Федерации есть только один вступивший в законную силу обвинительный приговор за совершение действий сексуального характера (ст. 132 УК РФ) с использованием сети Интернет в отношении потерпевшей, не достигшей четырнадцатилетнего возраста [5, с. 44]. Мужчина посредством социальной сети «ВКонтакте», познакомившись с девочкой, не достигшей 14-летнего возраста, стал демонстрировать фотографии обнаженных мужских половых органов, сопровождая их текстовыми сообщениями с предложениями о совершении действий сексуального характера за денежное вознаграждение.

Кроме того, в сети функционируют сайты, содержащие порнографические материалы с участием несовершеннолетних.

На протяжении последних нескольких лет в сети Интернет стали активно развиваться «группы смерти», созданные с целью склонения детей и подростков к суицидам. Для того, чтобы вступить в группу, необходимо выполнять определенные задания, связанные с фотографированием себя в опасных местах, например, на краю крыш высотных зданий, на железнодорожных рельсах и т.д. Кроме того, членам группы внушается, что они никому не нужны, что есть другой, более счастливый мир, куда надо стремиться. Психологическое воздействие на членов групп заключается в основном в эксплуатации потребности принадлежать к значимой тайной группе, ощущать свою избранность и уникальность [3].

Члены различных деструктивных организаций активно пользуются возможностями ИТС в целях распространения материалов экстремистского характера, вербовки в свои ряды новых членов, а также координации противоправной деятельности. Кроме того, ИТС активно используются в качестве средства связи, дистанционного руководства, а также обучения террористической деятельности, поиска дополнительных источников финансирования.

По различным данным в настоящее время в мире действуют около 5 тыс. Интернет-сайтов, содержащих экстремистский (террористический) контент. Что касается русскоязычных сайтов экстремистской направленности, то более 90 %

из них находятся за пределами российского правового поля. Для достижения своих целей представители экстремистских и террористических организаций используют возможности социальных сетей (ВКонтакте, Фейсбук, Твиттер, Одноклассники), в которых ведется активная пропагандистская работа. В настоящее время преобладает и имеет устойчивую тенденцию к росту количество преступлений, которые совершаются с использованием сети Интернет. В структуре экстремистской преступности удельный вес таких деяний составляет практически две трети [8, с. 17].

Коммуникационные возможности ИТС также активно используются для совершения преступлений, связанных с незаконным оборотом наркотиков. В настоящее время наиболее распространен бесконтактный сбыт наркотиков. Так, установление контакта потребителя со сбытчиком происходит посредством переписки или звонков через социальные сети и мессенджеры (например, Skype, Viber, WhatsApp и т.п.). Затем производится оплата посредством различных платежных систем. После оплаты сбытчики сообщают места так называемых закладок с наркотическим веществом. Вещество в место закладки помещается обычно таким образом, чтобы максимально снизить возможность его обнаружения посторонними лицами [7, с. 85].

На территории Российской Федерации законодательно запрещено осуществление деятельности, связанной с организацией и проведением азартных игр с использованием ИТС. Игорные заведения могут функционировать лишь в специально отведенных игорных зонах [1]. Но многие предприниматели в обход российского законодательства регистрируются и осуществляют организацию азартных игр с территории иностранных государств. Для доказывания факта организации незаконной игорной деятельности необходимо иметь доступ к соответствующим серверам, которые, как отмечено выше, в основном располагаются на территории иностранных государств. В связи с этим доказать факт преступной деятельности представляется достаточно проблематичным.

Таким образом, в настоящее время четко прослеживается тенденция увеличения количества преступлений, совершаемых с использованием ИТС и в ближайшей перспективе изменения данной тенденции не предвидится.

Специфика преступлений определяется использованием при их совершении высоких технологий, необходимостью обладания определенным уровнем специальных познаний и наличием специального инструментария для их совершения. Данные обстоятельства обусловливают высокую латентность этих преступлений, что существенно затрудняет их выявление и документирование, а также организацию уголовно-процессуального противодействия им.

Основными особенностями преступлений, совершаемых с использованием ИТС, являются иные механизмы следообразования, и, соответственно перед правоохранительными органами ставится проблема их выявления и фиксации.

Также особенностью является отсутствие привязки совершения активных преступных действий к месту наступления последствий, т.е. дистанционный характер совершения преступлений.

Исходя из этого, представляется целесообразным разрабатывать новые способы противодействия такой категории преступлений.

Способы противодействия можно условно разделить на внутригосударственные и межгосударственные. К внутригосударственным способам противодействия можно отнести совершенствование криминалистических тактик и методик расследования, а также выработку новых требований к сбору, проверке и оценке доказательств при расследовании преступлений, совершенных с использованием ИТС.

Применительно к Российской Федерации представляется целесообразным значительное внимание уделять разработке тактики проведения таких следственных действий, как осмотр места происшествия, обыск (выемка) контроль телефонных и иных переговоров, допрос.

Специфика проведения осмотра места происшествия, а также обыска или выемки предполагает тщательную предварительную подготовку к нему, привлечение специалистов соответствующего профиля, использование, кроме стандартных технико-криминалистических средств, также специальных технических устройств и программного обеспечения, принятия мер, направленных на обеспечение сохранности компьютерной информации [4].

Также необходима выработка рекомендаций по изъятию, упаковке и транспортировке компьютерной техники и иных носителей информации, обнаруженных в ходе данных следственных действий.

Проведение такого следственного действия, как контроль телефонных и иных переговоров по уголовным делам может способствовать выявлению мест нахождения используемой компьютерной техники, иных незаконных предметов, документов (в частности электронных).

При проведении допроса значительное внимание необходимо уделять вопросам использования в преступных целях ИТС.

Учитывая, что к ИТС практически неприменим принцип территориальности, то расследование такого рода преступлений лишь на национальном уровне малоэффективно. В связи с тем, что во многих случаях поставщики информационно-телекоммуникационных услуг зарегистрированы, как отмечено выше, на территории иностранных государств, одним из важнейших вопросов в сфере противодействия преступлениям, совершаемым с использованием ИТС, является необходимость совершенствования международного сотрудничества, в том числе в сфере уголовного процесса.

В настоящее время основной формой международного сотрудничества в уголовно-процессуальной сфере является направление запросов о правовой помощи. Порядок взаимодействия российских судов, прокуроров, следователей и орга-

нов дознания с соответствующими компетентными органами и должностными лицами иностранных государств регламентирован главами 53, 54 и 55 УПК РФ.

Международная правовая помощь по уголовным делам может оказываться в случаях, когда возникает необходимость производства на территории иностранного государства таких следственных действий, как осмотр, обыск (выемка), допрос, экспертиза либо иных процессуальных действий. В частности, когда обвиняемый (подозреваемый) скрывается на территории другого государства, либо в случаях, когда свидетели, потерпевшие или иные участники уголовного судопроизводства, а также документы, необходимые для расследования, находятся на территории другого государства.

Представляется необходимым развивать международное сотрудничество в уголовно-процессуальной сфере, в особенности по преступлениям, совершаемым с использованием ИТС. Так, целесообразно предусмотреть упрощенный порядок трансграничного взаимодействия с поставщиками информационно-телекоммуникационных услуг с целью получения от них данных об абонентах, траффике и контенте коммуникаций. Основной целью выработки упрощенных порядков должна выступать оперативность исполнения запроса о правовой помощи, т. е. получение запрашиваемой информации должно осуществляться в максимально короткие сроки, что напрямую влияет на эффективность расследования вышеуказанных преступных проявлений.

Проведенное исследование позволило сформулировать вывод о том, что с целью эффективной реализации правоохранительной функции государства в сфере борьбы с преступлениями, совершаемыми с использованием информационно-телекоммуникационных сетей (в том числе сети Интернет), необходимо совершенствование криминалистических тактик и методик их расследования, выработка новых требований к сбору, проверке и оценке доказательств по уголовным делам указанной категории, а также дальнейшее развитие международного сотрудничества, в том числе в области уголовного процесса.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ

1. О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации: федеральный закон от 29.12.2006 № 244-ФЗ (ред. от 28.03.2017) // Рос. газ. – 2006. – № 297. – 31 дек.

2. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: указ Президента РФ от 09.05.2017 № 203 // СЗ РФ. – 2017. – № 20. – Ст. 2901.

3. О направлении методических материалов: письмо Минобрнауки России от 31.03.2017 № ВК-1065/07 // СПС «КонсультантПлюс».

4. Давыдов В.О. Информационное обеспечение раскрытия и расследования преступлений экстремистской направленности, совершенных с использованием компьютерных сетей: автореф. дис. … канд. юрид. наук. – Ростов н/Д., 2013. – 26 с.

5. Попова Л.В., Михайлов В.В. Уголовная ответственность за совершение действий сексуального характера с использованием сети Интернет // Законность. – 2016. – № 2. – С. 44–48.

6. Рассолов И.М. Киберпреступность: понятие, основные черты, формы проявления // Юридический мир. – 2008. – № 2. – С. 44–46.

7. Торговченков В.И., Иванов С.А. Особенности предупреждения бесконтактных способов сбыта наркотических веществ в Российской Федерации // Законы России: опыт, анализ, практика. – 2016. – № 12. – С. 84–88.

8. Хохлов Ю.П. Этот опасный Интернет. Генеральная прокуратура Российской Федерации реализует комплекс мер, направленных на обеспечение профилактики экстремизма и терроризма // Прокурор. – 2015. – № 3. – С. 15–19.

9. Чекунов И.Г. Киберпреступность: Понятие и классификация // Рос. следователь. – 2012. – № 2. – С. 37–44.

10. Чекунов И.Г. Понятие и отличительные особенности киберпреступности // Там же. – 2014. – № 18. – С. 53–56.

BIBLIOGRAPHIC REFERENCES

1. Federal Law of 29.12.2006 No. 244-ФЗ (ed. Dated 28.03.2017) “On state regulation of the organization and conduct of gambling and on amendments to some legislative acts of the Russian Federation” // Rossiyskaya gazeta, No. 297, December 31, 2006.

2. Presidential Decree of 09.05.2017 No. 203 “On the Strategy for the Development of the Information Society in the Russian Federation for 2017–2030” // “Collection of Legislation of the Russian Federation”, 05.15.2017, No. 20, Art. 2901.

3. Letter of the Ministry of Education and Science of Russia No. VK-1065/07 dated March 31, 2017, “On the Direction of Methodological Materials” // SPS Consultant Plus.

4. Davydov V.O. Information support for the disclosure and investigation of extremist crimes committed using computer networks: author. dis. ... Cand. legal sciences. – Rostov-on-Don, – 2013. – P. 26.

5. Popova L.V., Mikhailov V.V. Criminal liability for committing acts of a sexual nature using the Internet // Legality. – 2016. – No. 2. – P. 44–48.

6. Rassolov I.M. Cybercrime: concept, main features, forms of manifestation // Legal World. – 2008. – № 2. – P. 44–46.

7. Merchant V.I., Ivanov S.A. Features of prevention of contactless methods of selling drugs in the Russian Federation // Laws of Russia: experience, analysis, practice. – 2016. – No. 12. – P. 84–88.

8. Khokhlov Yu.P. This dangerous internet. The Prosecutor General's Office of the Russian Federation implements a set of measures aimed at ensuring the prevention of extremism and terrorism // Prosecutor. – 2015. – № 3. – P. 15–19.

9. Chekunov I.G. Cybercrime: The concept and classification // Russian investigator. – 2012. – № 2. – P. 37–44.

10. Chekunov I.G. The concept and distinctive features of cybercrime // Russian investigator. – 2014. – No. 18. – P. 53–56.