СЕКЦИЯ ПРАВОВОЕ РЕГУЛИРОВАНИЕ И КРИМИНАЛИСТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДОСУДЕБНОГО И СУДЕБНОГО ПРОИЗВОДСТВА ПО УГОЛОВНЫМ ДЕЛАМ

Калугин А.Г.,

кандидат юридических наук, доцент
Сибирский юридический институт МВД России (г. Красноярск)

О НЕОБХОДИМОСТИ РАЗРАБОТКИ КОНЦЕПЦИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная безопасность – понятие емкое и многогранное. Поэтому следует сразу оговориться, что в данной работе речь пойдет лишь об одном из аспектов обеспечения информационной безопасности, а именно – о проблемах противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий (далее – ИКТ), о борьбе с так называемой киберпреступностью.

На нынешнем этапе развития науки и техники в нашу жизнь как неотъемлемая часть вошли цифровые технологии Невозможно представить себе жизнь современного человека без мобильной связи, Интернета, электронных платежных систем и т.д. На наших глазах произошла стремительная виртуализация социальной жизни; интернет-сайты и блоги стали для большинства граждан моложе 40 лет не только основным средством массовой информации, но и вообще основным источником информации об окружающем мире.

Однако достижениями научно-технического прогресса активно пользуются и представители преступного мира. Наряду с совершением в интернет-сети традиционных видов преступных посягательств – краж денежных средств из электронных кошельков, банкоматов, с телефонных и банковских счетов, мошенничеств, в том числе так называемых телефонных, а также совершаемых с использованием банковских карт и фальшивых сайтов-однодневок, сбора и продажи конфиденциальной информации, вымогательства, постоянно возрастают масштабы распространения через Интернет предметов и услуг, исключенных из легального оборота (наркотических средств, детской порнографии).

По данным Центробанка России, за первые три квартала 2016 г. со счетов в российских банках было похищено более 2 млрд. рублей.[1]

Во время панельной сессии «Киберпреступность – одна из ключевых угроз роста мировой экономики. Готова ли Россия к новым вызовам?», которая состоялась на международном инвестиционном форуме «Сочи-2016», было отмечено, что в 2015 г. киберпреступники нанесли ущерб мировому бизнесу в размере 400 млрд. долларов. По оценкам российских экспертов, количество киберпреступлений в России к 2018 г. может вырасти примерно в четыре раза, а общие потери нашей страны от них – превысить 2 трлн. Рублей.[2]

Следует отметить, что ИКТ активно используются не только для хищения, но и для «отмывания» денежных средств,

полученных в результате преступной деятельности.

Высок уровень присутствия в социальных сетях, а также в распространяемых через Интернет компьютерных играх образцов и примеров насилия, агрессии, создания виртуальных образов вседозволенности для лиц, допускающих подобное поведение, формирования их привлекательности для молодежной аудитории. Следствием этого является возрастание агрессии в подростковой среде[3], совершение преступлений против жизни и здоровья с особой жестокостью и цинизмом, с последующим выкладыванием либо прямой трансляцией своих «подвигов» в Интернете.

Относительно новой негативной тенденцией насильственной преступности стало распространенное в социальных сетях провоцирование суицидального поведения подростков.

Одним из самых опасных видов современной интернет-преступности стало использование социальных сетей и других интернет-ресурсов для распространения экстремистских призывов, организации массовых беспорядков, акций неповиновения властям, в том числе направленных на свержение правительств, изменение конституционного строя. По данным ГИАЦ МВД России, в 2016 г. зарегистрированы 950 преступлений экстремистской направленности, совершенных на территории Российской Федерации с использованием сети Интернет (+28,9% к уровню 2015 г.).

Наконец, на данном этапе развития человечества Интернет стал ключевым инструментом в руках международных террористических организаций, используемым для распространения и пропаганды идеологии терроризма, культивирования жестокости, радикализации религиозных и националистических течений, рекрутирования в террористические группировки новых членов, координации террористической деятельности. По данным ГИАЦ МВД России, в 2016 г. на территории Российской Федерации были зарегистрированы 186 преступлений террористического характера, совершенных с использованием сети Интернет (+39,8% в сравнении с 2015 г.)[4].

Следует отметить психологически грамотную работу «идеологов» международных террористических группировок, иностранных разведок и контролируемых ими деструктивных организаций внутри России, проводимую в отношении как наиболее уязвимых групп населения, так и целенаправленно в отношении молодежи и подростков.[5]

По данным Роскомнадзора, за годы работы с экстремистским контентом были заблокированы более 23 тысяч ресурсов, пропагандирующих только одну запрещенную в России организацию – ИГИЛ (ДАИШ). В ИГИЛ созданы русскоязычные редакции, которые выпускают распространяемые через Интернет фильмы и электронные журналы. Больше всего экстремистского контента – в сумме почти треть от общего числа – обнаружено в социальной сети «ВКонтакте» и на видеохостинге YouTube. Обе эти площадки исправно удаляют подобные материалы или ограничивают доступ к ним с территории России. Только за 2015 г. Роскомнадзор заблокировал более 900 сайтов, содержащих информацию экстремистского характера, распространение которой запрещено российским законодательством[6].

Характерными особенностями преступлений, совершаемых с использованием ИКТ, являются:

1) глобализация, транснациональный и трансграничный характер совершаемых преступлений; размещение большей части криминальных интернет-ресурсов (пропагандирующих терроризм, наркопотребление, распространяющих наркотические средства, предоставляющих финансовые услуги, в том числе по выводу денег, полученных от незаконного оборота наркотиков, за рубеж) на территории иностранных государств, что не позволяет в полной мере пресекать их деятельность и привлекать к ответственности ее организаторов;

2) высокий уровень конспирации, жесткое распределение ролей между участниками криминальных интернет-сообществ, использование для продажи наркотиков и легализации криминальных доходов закрытых (анонимных) интернет-площадок («темной сети») и

шифрованных цифровых каналов связи, что, в свою очередь, влечет высокий уровень латентности этого сегмента преступности.

Существующие в реальности тенденции бурного роста упомянутых выше видов преступлений, совершаемых с использованием ИКТ, практически не находят отражения в уголовной статистике.

Так, в 2015 г. в Российской Федерации были зарегистрированы 2382 преступления в сфере компьютерной информации (имеются в виду составы, включенные в главу 28 УК РФ). В то же время в результате исследования, проведенного специалистами АО «Лаборатория Касперского» с помощью своего антивирусного программного обеспечения, установленного на компьютерах 18,7 тыс. пользователей, в 2015 г. были зафиксированы не менее 291 млн., а в 2013 г. – не менее 1 млрд. фактов использования вредоносных компьютерных программ либо попыток неправомерного доступа к компьютерной информации. По формальным признакам каждый такой случай должен как минимум получать квалификацию по ст. 272 или 273 УК РФ. С учетом хотя бы единичных случаев обнаружения вредоносного программного обеспечения с уникальным вердиктом на каждом отдельном устройстве, что само по себе указывает на создание и использование новой вредоносной компьютерной программы (ст. 273 УК РФ), можно говорить о том, что в мире ежегодно создается от 8 до 12 млн. новых вредоносных компьютерных программ. При этом нельзя забывать, что в большинстве случаев вредоносные компьютерные программы используются лишь как средство совершения других преступлений; чаще всего – различных преступлений против собственности. Приведенные данные позволяют говорить о киберпреступлениях как не просто о высоколатентных, а о сверхвысоколатентных.[7]

Среди основных причин высокой латентности этой категории преступлений можно выделить следующие:

1) повсеместная доступность ИКТ. Сегодня практически любой гражданин может получить доступ к сети Интернет за сравнительно небольшую оплату и без географической привязки к месту проживания или работы. Кроме того, многие общественные места оснащены беспроводной сетью Wi-Fi, при этом доступ к сети Интернет можно получить на безвозмездной основе;

2) возможность действовать в сети Интернет анонимно, по крайней мере, в ее русскоязычном сегменте;

3) постоянное увеличение в общей массе пользователей Интернета доли граждан молодого, социально активного возраста, свободно владеющих информационными технологиями, но не нашедших себе применения на рынке труда либо не желающих трудиться, со сформировавшейся психологией потребления;

4) сложность выявления и доказывания киберпреступлений «традиционными» методами и средствами оперативно-розыскной и уголовно-процессуальной деятельности;

5) отсутствие в Российской Федерации государственной стратегии и единого координирующего центра в области обеспечения компьютерной безопасности;

6) отсутствие широкомасштабной подготовки специалистов для правоохранительной и судебной систем, способных к полноценной работе по выявлению, раскрытию, расследованию и рассмотрению в судах уголовных дел о преступлениях, совершаемых с использованием ИКТ.

Приходится также констатировать отсутствие в законодательстве Российской Федерации правового механизма реагирования на хищения денежных средств в небольшом размере, совершаемые неустановленными лицами. В частности, широко распространены случаи похищения денежных средств с банковских счетов и платежных карт путем кражи или мошенничества на относительно небольшие суммы. Если размер ущерба в результате одной незаконной транзакции составляет менее 2500 рублей, содеянное подпадает под признаки мелкого хищения (ст. 7.27 КоАП РФ), если менее 5000 рублей – под признаки

простого (неквалифицированного) хищения (ч. 1 ст. 158 (кража), ч. 1 ст. 159.3 (мошенничество с использованием платежных карт) или ч. 1 ст. 159.6 (мошенничество в сфере компьютерной информации) УК РФ), то есть преступления, предварительное следствие по которому необязательно.

Для раскрытия таких хищений необходим комплекс оперативно-розыскных мероприятий, в том числе ограничивающих конституционные права человека и гражданина на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи (включая получение компьютерной информации), а также право на неприкосновенность жилища. В силу ст. 8 Федерального закона «Об оперативно-розыскной деятельности» проведение таких ОРМ допускается по судебному решению и при наличии информации о признаках подготавливаемого, совершаемого или совершенного противоправного деяния, по которому производство предварительного следствия обязательно, либо о событиях или действиях (бездействии), создающих угрозу государственной, военной, экономической, информационной или экологической безопасности Российской Федерации. Таким образом, по описанным выше фактам осуществление оперативно-розыскной деятельности не разрешается.

Как следствие следует в ближайшей перспективе ожидать дальнейшего увеличения в структуре преступности количества таких преступлений, как:

– «интеллектуальные» мошенничества, связанные с использованием ИКТ, средств сотовой связи, дистанционного банковского обслуживания;

– кражи денежных средств с банковских счетов, карт и электронных кошельков;

– совершенный бесконтактным способом сбыт наркотических средств и психотропных веществ, а также их пересылка и контрабанда с последующим обналичиванием или легализацией денежных средств посредством ИКТ. Так, только за первые два месяца 2017 г. МВД России проинформировало Роскомнадзор о необходимости блокировки более чем 1200 сайтов, содержащих информацию о продаже наркотиков или о способах их изготовления.

Изложенное свидетельствует о необходимости комплексного подхода к выработке мер по противодействию киберпреступности в рамках национальной Концепции информационной безопасности.

В настоящее время подобных документов по данному направлению в нашей стране нет за исключением Концепции информационной безопасности детей, утвержденной распоряжением Правительства Российской Федерации от 2 декабря 2015 г. № 2471-р.

Помимо других аспектов (защиты персональных данных, сведений, составляющих государственную тайну и иные виды охраняемой законом тайны, защиты авторских прав и т.д.) предлагаемая Концепция информационной безопасности должна включать несколько блоков мер, направленных на противодействие преступности.

1. В области совершенствования законодательства:

а) уголовного – в части усиления ответственности за преступления, совершаемые с использованием ИКТ;

б) уголовно-процессуального – в части установления порядка получения, фиксации и исследования доказательственной информации, циркулирующей в виртуальном пространстве;

в) административного – в части формирования эффективной системы ограничений, запретов и ответственности за их нарушение для интернет-провайдеров и субъектов, работающих на рынке финансовых услуг;

г) информационного – в части установления правил регистрации в сети Интернет при условии возможности идентификации пользователя, а также предоставления надзорному органу государства блокировать анонимный трафик (как это предусмотрено законодательством Китая, Сирии, Таиланда, Ирана и ряда других стран);

д) законодательства о военном и чрезвычайном положении – в части предоставления федеральным органам ис-

полнительной власти полномочий при объявлении данных режимов осуществлять редактирование и (или) блокирование компьютерной информации, размещенной в сети Интернет, а также устанавливать иные ограничения доступа к сети Интернет[8].

2. В области организации деятельности правоохранительных и контролирующих органов:

а) существенное расширение, кадровое и материально-техническое укрепление подразделений ФСБ России, МВД России, осуществляющих мониторинг интернет-пространства, выявление террористических, экстремистских и иных криминальных интернет-ресурсов и документирование противоправной деятельности в сети Интернет;

б) совершенствование порядка взаимодействия органов, осуществляющих оперативно-розыскную деятельность, с Роскомнадзором, с интернет-провайдерами:

по выявлению в сети Интернет и «маркировке» криминального контента с целью его последующего удаления или блокирования соответствующих интернет-ресурсов;

по геолокации преступников с целью документирования и пресечения их преступной деятельности.

в) организация подготовки, переподготовки и повышения квалификации кадров для оперативных, следственных и экспертно-криминалистических подразделений, специализирующихся в области борьбы с киберпреступностью.

3. В области предупреждения преступлений, совершаемых с использованием ИКТ:

а) разработка и внедрение программного обеспечения для защиты от возможных опасностей, связанных с использованием сети Интернет (защищенные протоколы связи, криптографические методы защиты информации и другие), и предупреждения пользователей о возможных опасностях[9];

б) организация последовательных и регулярных мероприятий органов государственной власти, общественных организаций, средств массовой информации, направленных на выработку у населения, в первую очередь у детей, навыков безопасного существования в современном информационном пространстве (формирование культуры пользования информационными и коммуникационными ресурсами, способности критической оценки получаемых сведений). В частности, речь идет о разработке и внедрении специальных образовательных и просветительских программ, содержащих сведения об информационных угрозах, о правилах безопасного пользования сетью Интернет, о средствах защиты несовершеннолетних от доступа к информации, наносящей вред их здоровью, нравственному и духовному развитию. Такие программы могут предназначаться для родителей, работников системы образования, детских и юношеских библиотек и других специалистов, занятых обучением и воспитанием несовершеннолетних, организацией их досуга.

---

[1] Официальный сайт информационного агентства РИА-Новости. URL: https://ria.ru/economy /20161202/1482748772.html (дата обращения: 10.04.2017).

[2] Официальный сайт «Российской газеты». URL: https:// rg.ru/2016/10/01/reg-ufo/poteri-kiberprestuplenij-prevysiat-2-trln.html (дата обращения: 10.04.2017).

[3] Комплексный анализ состояния преступности в Российской Федерации по итогам 2016 года и ожидаемые тенденции ее развития : аналитический обзор. М.: ФГКУ «ВНИИ МВД России», 2017. С. 5.

[4] Угрозы современного терроризма. Обзорная информация. Зарубежный опыт. Вып. 1. М.: ФКУ «ГИАЦ МВД России», 2017. С. 12.

[5] Комплексный анализ состояния преступности в Российской Федерации по итогам 2016 года и ожидаемые тенденции ее развития… С. 29.

[6] Данные с официального сайта Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций. URL: http://rkn.gov.ru/press/publications /news43699.htm (дата обращения: 10.04.2017).

[7] Чекунов И.Г., Шумов Р.Н. Современное состояние киберпреступности в Российской Федерации // Российский следователь. 2016. № 10. С. 44-47.

[8] Струков К.В. Контрольная деятельность Российского государства за информационными отношениями в сети Интернет // Журнал российского права. 2016. № 7.

[9] Микаева А.С. Проблемы правового регулирования в сети Интернет и их причины // Актуальные проблемы российского права. 2016. № 9.