УДК 341.4

Формы противодействия киберпреступности

Розенцвайг А.И.
Кандидат юридических наук, доцент кафедры
теории и истории государства и права и международного права
Самарского национального исследовательского
университета им. академика С.П. Королева

Чертилин В.С.
Студент юридического факультета
Самарского национального исследовательского
университета им. академика С.П. Королева

Проанализировано развитие киберпреступности под влиянием современных технологий, охватывающих различные аспекты жизнедеятельности. Сделан вывод о повышенной латентности киберпреступлений, транснациональном характере, а также отсутствии эффективных форм противодействия им, что указывает на необходимость диффузии норм и перехода от формально-юридического подхода к юридически-технологическому.

Ключевые слова: киберпространство, киберпреступность, кибертерроризм, киберпреследование, противодействие киберпреступлениям.

Современные общественные отношения давно уже вышли за рамки «реального» мира, подверглись «оцифровке» и перешли в виртуальную плоскость. С помощью компьютерных автоматизированных систем люди собирают и хранят персональные данные, осуществляют юридически значимые действия, проводят исследования, общаются друг с другом и обмениваются информацией.

Одним из негативных последствий развития информационных технологий является то, что глобальная сеть (в частности, информационно-телекоммуникационная сеть «Интернет») предоставляет неограниченные возможности для воздействия, в том числе и негативного, на личность отдельного индивида и общества в целом [1].

Развитие информационных технологий и их нецелевое использование послужили толчком к появлению и развитию нового вида преступности, получившей в доктрине наименование «киберпреступность».

По мнению профессора В.А. Номоконова и Т.Л. Тропиной, киберпреступность – это «совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, и против компьютерных систем, компьютерных сетей и компьютерных данных» [2].

Под киберпространством в науке понимается «виртуальное пространство» – второй мир, как внутри компьютеров, так и внутри компьютерных систем [3]. При этом компьютерная система – это одно или несколько взаимосвязанных устройств, которые, в соответствии с программой, осуществляют автоматизированную обработку данных, а компьютерная сеть – это система, обеспечивающая обмен данными между вычислительными устройствами.

Таким образом, из данного выше определения следует, что киберпреступность – это противоправные действия, связанные с изменением виртуального пространства при помощи технических средств – компьютерных систем и компьютерных сетей.

В свою очередь, Д.Н. Карпова отмечает, что киберпреступление – это «акт социальной девиации с целью нанесения ущерба индивиду, организации или государству посредством технического средства с доступом в сеть Интернет» [4].

Можно заметить, что второе определение несколько уже, чем первое, поскольку затрагивает правоотношения исключительно в сфере сети Интернет, которая в полной мере не охватывает понятие киберпространства. Тем не менее, автор выделяет важный критерий для отнесения того или иного киберявления к противоправному – это наличие ущерба, выраженного в той или иной форме.

Уголовный кодекс Российской Федерации не дает определения киберпресупности, поэтому, основываясь на доктрине уголовного права, можно отграничить некриминальные правонарушения от противоправных деяний, за которые установлена уголовная ответственность. Исходя из этого, можно предложить следующее определение киберпреступности.

Киберпреступность – это совокупность запрещенных уголовным законом противоправных деяний, совершаемых в цифровой среде с использованием электронно-вычислительной техники, причинивших ущерб, иные тяжкие последствия, нарушающих общественный порядок и общественную безопасность.

Учитывая, что киберпреступность развивается параллельно с процессами внедрения новых технологий и глобализацией общественных отношений, можно выделить несколько видов киберпреступлений.

Во-первых, это – финансовые преступления. Они являются наиболее распространенными, как в реальном пространстве, так и в виртуальной реальности. К ним относятся мошенничество с банковскими картами, хищение денежных средств во время совершения банковских операций, кибермошенничество и хищение денежных средств из электронных кошельков и вкладов.

Во-вторых, явление, получившее название фишинг. Суть данного преступления заключается в незаконном получении персональных данных граждан, необходимых для совершения от их имени юридически-значимых действий.

В-третьих, к киберпреступлениям относится интернет-торговля объектами, выведенными из гражданско-правового оборота. Это – торговля наркотическими и иными запрещенными веществами, оружием, красно-книжными животными, продуктами, ввоз которых запрещен на территорию государства.

В-четвертых, кибертерроризм. Посредством современных технологий совершается вербовка в террористические организации, распространение запрещенной литературы, инструктаж террористов и планирование преступлений.

В-пятых, определенное место в системе киберпреступлений занимает киберпорнография. Она включает в себя распространение порнографических материалов, ведение сайтов, содержащих детскую порнографию, вовлечение несовершеннолетних в занятие проституцией (в том числе и киберпроституцией).

Отдельно можно выделить такие виды преступлений, как киберпреследование (то есть слежка с помощью геолокации и детализации) и проведение азартных игр и пари в сети «Интернет».

Стоит так же отметить, что электронно-вычислительная техника и информационно-коммуникационная сеть Интернет выступают в качестве новых «инструментов» для совершения преступлений, которые были известны и ранее. Например, с помощью Интернета злоумышленники склоняют несовершеннолетних к совершению самоубийств, мошенники продают заведомо неэффективные видеокурсы, а сектанты вербуют себе участников.

Из этого можно сделать вывод, что развитие технологий не только порождает новые виды и формы преступлений, но и упрощает совершение существующих преступлений. В связи с этим необходимо уделять особое внимание формам противодействия киберпреступности.

Сложность в такой борьбе представляет транснациональный характер правоотношений. Зачастую преступник и жертва могут быть гражданами разных государств, не знать друг друга лично и не осознавать истинных намерений друг друга.

Данная проблема носит не только межгосударственный, но и галактический характер. Так, летом 2019 г., было совершено первое преступление в космосе. «Гражданка США астронавт Энн Маклейн незаконно завладела персональными данными своей супруги и получила неправомерный доступ к ее банковским счетам, использовав при этом бортовой компьютер Международной космической станции» [3].

Помимо транснационального характера киберпреступности важной проблемой является ее повышенная латентность. Технологии позволяют оставаться анонимными, менять геолокации, «взламывать» чужие аккаунты, тем самым запутывая информационные следы и делая такие преступления трудно раскрываемыми.

На сегодняшний день не существует детальной статистики киберпреступлений, однако специалисты отмечают, что доход преступников в цифровой среде в разы превышает доходы от иных преступлений.

Цифровая безопасность может быть достигнута лишь при условии объединении усилий значительного числа субъектов и в большинстве государств является одной из приоритетных задач.

В Российской Федерации вопросами раскрытия киберпреступлений занимается специальный отдел «К», созданный на базе ГУ МВД России. В его задачи входит пресечение и раскрытие преступлений в сфере компьютерной информации, преступле-

ний, совершаемых с использованием информационно-телекоммуникационных сетей (включая сеть Интернет) и направленных против здоровья несовершеннолетних и общественной нравственности, преступлений, связанных с незаконным оборотом специальных технических средств, предназначенных для негласного получения информации и преступлений, связанных с незаконным использованием объектов авторского права или смежных прав [1].

Можно выделить две основные формы противодействия киберпреступлениям.

Во-первых, совершенствование правового регулирования общественных отношений в цифровой среде. В рамках этого вносятся существенные изменения в законодательные акты о связи, информационных технологиях, СМИ, вносятся изменения в Уголовный Кодекс РФ, блокируются судами и органами исполнительной власти информационные ресурсы, распространяющие запрещенную в России информацию, обсуждаются проекты введения в Уголовный Кодекс РФ новой главы, посвященной киберпреступлениям.

Критики данной формы противодействия киберпреступлениям отмечают, что государственное регулирование цифровых вопросов находится на грани с цензурой и необоснованно вторгается в личное пространство добросовестных граждан.

Во-вторых, разработка технических средств и инструментов, позволяющих эффективно препятствовать совершению преступлений, защищать цифровые данные и раскрывать преступления.

На наш взгляд, наиболее эффективным способом противодействия киберпреступлениям будет являться совмещение двух форм, поскольку правовые институты не смогут «работать» эффективно без обеспечения их технологическим инструментарием, а новые технологии защиты информации не смогут функциоировать без надлежащей правовой регламентации.

Видится необходимым подкрепление законодательного запрета на обход идентификационных программ при помощи прокси установлением технической блокировки соответствующих программ. Это сделает невозможным для злоумышленников смену IP-адресов, а, следовательно, повысит раскрываемость киберпреступлений.

Представляется возможным по примеру Китайской Народной Республики установить на законодательном уровне обязанность граждан проходить процедуру удостоверения личности при регистрации в социальных сетях. Это реализуемо по примеру регистрации на портале Госуслуги и удостоверения личности в офисах интернет-провайдеров или самими социальными сетями.

Помимо вышеизложенного, представляется важным выстраивание механизмов противодействия международным киберпреступлениям. Для этого требуется осознание существующих угроз всеми участниками международно-правовых отношений. Необходимо также установление «кибергражданства» – государственной «приписки» индивидов и организаций, осуществляющих деятельность в сети Интернет, посредством регистрации и лицензирования их деятельности и необходимости подчиняться законам государства-приписки. Это позволит навести правовой порядок в киберпространстве, избежать коллизий, установить государственный контроль за цифровой деятельностью.

Целесообразно не допускать вмешательства в личные дела граждан. Государственные органы не должны иметь доступ к личным данным и переписке пользователей социальных сетей. При этом обмен информацией может находиться под контролем искусственного интеллекта. Подозрительные действия должны блокироваться автоматически системными программами, а не органами служб безопасности.

Исходя из вышеизложенного, можно сделать вывод о том, что киберпреступность развивается вместе с современными технологиями, охватывает многие стороны человеческой жизни, носит латентный, транснациональный характер. Существующие формы борьбы с ней являются недостаточно эффективными, что свидетельствует о необходимости диффузии этих норм и перехода от формально-юридического подхода к юридико-технологическому. Эффективное противодействие киберпреступности возможно исключительно при условии взаимодействия юристов и программистов, создания новых правовых институтов и технологических инструментов, консолидации сил всего мирового сообщества.

Согласно индексу кибербезопасности, составленному Международным союзом электросвязи, Россия занимает 28 место [6]. В рейтинге учитываются технические и организационные мероприятия, законодательная база, деятельность в международной сфере и создание потенциала для усиления кибербезопасности. Учитывая, что ещё год назад, Россия занимала 10 строку в рейтинге, можно сделать вывод о том, что деятельность в рассматриваемом направлении является не достаточно эффективной и для прогресса необходимо более тщательное правовое регулирование и использование положительного опыта иностранных государств в данной сфере.

Литература:

1. Герасименко Ю.В., Осташевская В.О. К вопросу об эффективной борьбе с киберпреступностью // Цифровизация экономики и общества: проблемы, перспективы, безопасность. – М., 2019. – С. 37-42.
2. Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. – 2012. – № 24. – С. 45-55.
3. Книжникова С.В., Гребёнкина Ю.В. Риск вовлечения детей и молодежи в преступления через медиасреду // Научно-методический электронный журнал «Концепт». – 2016. – Т. 24. – С. 88-93.
4. Карпова Д.Н. Киберпреступность: глобальная проблема и ее решение // Власть. – 2014. – № 8. – С. 46-50.
5. Первое преступление в космосе: в чем обвиняют астронавта. – URL: https://www.gazeta.ru/social/2019/08/25/12600943.shtml (дата обращения: 05.11.2019).
6. Global Cybersecurity Index. – URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx (дата обращения: 05.11.2019).

Forms of counteraction to cybercrimes

Rozentsvaig A.I., Chertilin V.S.
Samara National Research University

The article deals with the development of cybercrimes under the influence of modern technologies covering various aspects of life. The conclusion is made about the increased latency of cybercrimes, their transnational nature, as well as the lack of effective forms of countering them, that indicates the need for diffusion of norms and the transition from the formal legal approach to the legal and technological one.

Key words: cyberspace, cybercrime, cyberterrorism, counteraction to cybercrimes.