УДК 343.9

И.П. Родивилин

СОВРЕМЕННАЯ СПЕЦИФИКА ДЕТЕРМИНАЦИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ ОБРАЩЕНИЯ ОХРАНЯЕМОЙ ЗАКОНОМ ИНФОРМАЦИИ

Статья посвящена исследованию детерминантов девиантного поведения, связанного с совершением преступлений в сфере обращения охраняемой законом информации. Делается вывод о том, что детерминанты указанных преступлений имеют многофакторный характер, к которым относятся факторы правового характера, технические, организационные, виктимологические. Анализ судебно-следственной практики показывает, что ситуации, способствующие совершению преступлений, часто создают сами потерпевшие. Неосмотрительное поведение потерпевших часто выступает основным виктимологическим фактором при их виктимизации от указанных преступлений. Такое поведение наиболее часто проявляется в несоблюдении элементарных правил безопасности, известных потерпевшему, либо в незнании таких правил. Такое положение свидетельствует о низкой культуре информационной безопасности граждан нашей страны. В ходе проведенных автором исследований было выявлено, что потерпевшие сами создают условия для совершения преступлений в сфере обращения охраняемой законом информации и их можно было бы не допустить при должной осмотрительности со стороны потерпевших. Также делается вывод о том, что основное внимание в предупреждении преступлений в сфере обращения охраняемой законом информации должно уделяться виктимологической профилактике, заключающейся в обеспечении надежной защиты информации.

Ключевые слова: преступления в сфере компьютерной информации, факторы преступности, ddos-атака, кибератака, информационная безопасность.

DOI: 10.35634/2412-9593-2021-31-2-305-311

В криминологии существует значительное количество научных подходов, раскрывающих детерминанты преступности. Обобщив большой объём данных, приходим к выводу, что они являются закономерным следствием тех социальных явлений, которые и порождают преступность[1].

Со стороны государства проблеме противодействия преступлениям в сфере обращения охраняемой законом информации уделяется внимание, о чем свидетельствует включение этой проблемы в основные цели Концепции общественной безопасности Российской Федерации. Однако принимаемых мер в настоящий момент недостаточно.

В ходе проведенного автором исследования выявлены криминогенные факторы совершения преступлений в сфере обращения охраняемой законом информации, которые можно разделить по следующим основаниям.

Факторы правового характера. Одной из причин компьютерной преступности является слабость норм. Е.П. Ищенко одним из условий, способствующих криминализации киберпространства, а значит, и влияющих на рост преступлений в сфере обращения охраняемой законом информации, считает отставание законодательного регулирования от возможностей противоправного использования информационно-коммуникационных технологий, темпов информатизации всех сфер общественной жизни[2]. Борьбу с преступлениями в сфере обращения охраняемой законом информации затрудняет отсутствие некоторых специальных норм в УК РФ, например, предусматривающих ответственность за блокировку интернет-ресурсов посредством DdoS-атак.

Рассматривая DdoS-атаку с технической точки зрения, правоприменителю понятна и ясна схема ее совершения, однако с позиции уголовно-правового понимания этого явления возникает ряд трудностей. По сложившейся практике DdoS-атака квалифицируется по совокупности двух статей УК РФ: ст. 272 (неправомерный доступ к компьютерной информации) и ст. 273 (создание, использование и распространение вредоносных компьютерных программ).

---

[1] Криминология: учебник / под ред. Н.Ф. Кузнецовой и Г.М Миньковского. М.: БЕК, 1998. С. 163; Криминология: учебное пособие / под ред. В.Э. Эминова. М.: Юность, 1997. С. 80.

[2] Ищенко Е.П. Киберпреступность: криминалистический аспект проблемы // Библиотека криминалиста. 2013. № 5. С. 189.

Под неправомерным доступом к охраняемой законом информации понимается незаконное (либо неразрешенное владельцем данной информации) использование возможности получения информации[3]. Закон определяет под доступом к информации возможность получения информации и ее использования. Другими словами, доступ к информации можно считать осуществленным с момента, когда пользователь выполнил некоторые действия, в результате которых стало возможным получать и использовать информацию, ранее для пользователя недоступную. Также под доступом понимается проникновение в ее источник с использованием средств (вещественных и интеллектуальных) компьютерной техники, позволяющее использовать полученную информацию (копировать, модифицировать, блокировать либо уничтожать ее). Если же речь идет о DdoS-атаке на интернет-ресурс, то проникновения в ее источник не происходит. Другими словами, злоумышленник не получает доступ к управлению сайтом и не может использовать администраторские права для блокировки доступа к информации, находящейся на сервере. Таким образом, в данном случае неправомерного доступа с точки зрения уголовного права не происходит.

При совершении ddos-атаки на сайт в сети Интернет пользователи санкционированно обращаются на сайт, и хотя и владельцы компьютерной техники этого не осознают, сайт фактически для этого и создан, чтобы на него заходили пользователи.

Другой пример, если злоумышленник специально приобрел несколько тысяч компьютеров для того, чтобы они совершали аномальное количество обращений на определенный сайт в сети Интернет, с целью совершить ddos-атаку, то привлечь его к уголовной ответственности в настоящий момент не получится из-за отсутствия соответствующей нормы в Уголовном кодексе РФ. Однако право граждан на доступ к информации, закрепленное в Конституции РФ, будет нарушено, а собственник информационного ресурса не сможет распространять свои услуги или информацию. Вся информационная безопасность государства подвергается опасности, если ddos-атаки будут совершаться на сайты государственных органов и компаний. Под незаконным ограничением доступа к информации, находящейся в телекоммуникационных сетях, следует понимать нарушение права граждан на получение информации, свободу распространения информации законным способом.

В связи с вышеизложенным предлагается дополнить УК РФ ст. 274.2 следующего содержания:

«Статья 274.2 Незаконное ограничение доступа к информации.

4. Незаконное ограничение доступа к информации, находящейся в телекоммуникационных сетях, –

5. Деяния, предусмотренные частью первой настоящей статьи, совершенные группой лиц по предварительному сговору, организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или из корыстной заинтересованности, –

6. Деяния, предусмотренные частями первой или второй настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, – ».

Представляется, что совершение указанных действий, если они не повлекли тяжких последствий и не причинили моральный или материальный вред, не соотносится с принципом справедливости, согласно которому наказание и иные меры уголовно-правового характера, применяемые к лицу, совершившему преступление, должны соответствовать характеру и степени общественной опасности преступления, обстоятельствам его совершения. Последствия, прописанные в ст. 272-274.1 УК РФ, в виде копирования, блокирования, модификации и уничтожения информации не дифференцируют вред, причиненный преступлением. Например, при удалении электронного письма, в котором ведется переписка с друзьями о погоде, текущем состоянии дел и т.п. не приносит ее обладателю никакого вреда (ни морального, ни материального). А вот копирование идентификатора учетной записи и пароля для электронных платёжных систем с целью похищения денежных средств может нанести владельцу указанной информации материальный ущерб (возможно, даже в крупном размере). Или, например, копирование информации врачебного диагноза может причинить гражданину страдания, вплоть до совершения им самоубийства.

Таким образом, необходимо отграничивать преступления в сфере обращения охраняемой законом информации от административного правонарушения. В.Г. Степанов-Егиянц считает необходимым введение административной ответственности за неправомерный доступ к компьютерной инфор-

[3] Репецкая А.Л., Родивилин И.П. Незаконное ограничение доступа к компьютерной информации в сети Интернет: уголовно-правовой аспект // Библиотека уголовного права и криминологии. № 3 (15). 2016. С. 82;

мации без наступления последствий, указанных в ст. 272 УК РФ[4]. Согласимся с этим мнением, но с некоторыми поправками. Во-первых, считаем целесообразным привлекать к административной ответственности не только за неправомерный доступ к охраняемой законом информации без наступления последствий в виде копирования, блокирования, модификации, но и при наступлении таковых последствий, если эти действия не причинили моральные страдания или не совершены из корыстной заинтересованности либо мести. Несомненно, подобные нововведения усложнят процедуру привлечения к уголовной ответственности. Однако это будет способствовать повышению уровня доверия к правоохранительной системе, так как прекратится поток бессмысленных приговоров в отношении лиц, к которым в силу малозначительности совершенного ими деяния возможно применить иные меры воздействия.

А также внести в Кодекс Российской Федерации об административных правонарушениях следующие изменения:

1) Дополнить статьей 13.14.1 следующего содержания:

«Статья 13.14.1 «Неправомерный доступ к информации, которая ограничена федеральным законом, повлекший копирование блокирование, уничтожение, ознакомление (за исключением случаев, если разглашение такой информации влечет уголовную ответственность)».

Ввиду того, что пользовательская информация стала разновидностью информации ограниченного доступа, необходимо включить ее в ФЗ № 152-ФЗ. К пользовательской информации следует относить фотографии, ФИО, дату рождения, адрес проживания, телефон, интересы, поисковые запросы.

Отсутствие единого понятийного аппарата, регламентирующего преступления в сфере оборота охраняемой законом информации, информатизация всех сфер общественной жизни, отсутствие уголовной ответственности за ограничение доступа к охраняемой законом информации и другие проблемы уголовно-правового характера также влияют на развитие и рост преступлений в сфере обращения охраняемой законом информации.

Подобные меры противодействия преступлениям в сфере оборота охраняемой законом информации помогут снизить их рост, оперативнее выявлять виновных лиц, совершающих преступления подобной категории.

Организационные факторы. Нарушение правил работы с охраняемой законом информацией, в том числе в силу цифрового неравенства, усиление цифрового неравенства между странами запада и России является причинами появления преступлений в сфере компьютерной информации. Под цифровым неравенством понимается, с одной стороны, «различие в уровнях развития информационных коммуникаций между различными странами и регионами, внутри страны, возрастными и социальными группами, различными государственными учреждениями, между институтами гражданского общества»[5]; с другой – разрыв в возможностях доступа к информации между богатыми и бедными (в том числе качественные различия), что характерно и для развитых стран[6].

Усиление цифрового неравенства между странами запада и России также является одной из причин появления преступности в сфере обращения охраняемой законом информации. Так, например, лицензионное программное обеспечение в России стоит относительно дорого, поэтому для подавляющего большинства российских пользователей не является проблемой использование контрафактных программ. По рыночным законам спрос рождает предложение, что обусловливает появление создателей специфического вида программного обеспечения под названием «Варез» или «Warez» (от английского «software» – «программное обеспечение»).

Также следует обратить внимание на то обстоятельство, что в контрафактном программном обеспечении в большинстве случаев присутствуют вредоносные компьютерные программы.

Еще один аспект цифрового неравенства между Россией и странами Запада заключается в отсутствии в России средств массовой информации, способных донести позицию Российской Федерации до жителей иностранных государств, а иногда и до граждан собственной страны. Так, например, почти в каждом смартфоне с операционной системой «Android» установлено приложение «Google», в

[4] Степанов-Егиянц В.Г. Объективная сторона неправомерного доступа к компьютерной информации по уголовному кодексу РФ // Библиотека криминалиста. 2013. № 5 (10). С. 47.

[5] Гиляревский Р.С. Информатика как наука об информации: информационный, документальный, технологический, экономический, социальный и организационный аспекты. М.: Фаир-Пресс, 2006. С. 304.

[6] Вальвачев В.В. Динамика цифрового неравенства в современном мире // Научные проблемы гуманитарных исследований. 2010. №7. URL: http://cyberleninka.ru/article/n/dinamika-tsifrovogo-neravenstva-v-sovremennom-mire.

котором, среди прочего, присутствует новостная лента (Google Now), которая ориентирована на новости оппозиционных СМИ.

Сокращение цифрового неравенства остается приоритетным направлением деятельности правительства Российской Федерации. Сокращение информационного разрыва решит несколько проблем современного российского общества: во-первых, уменьшится оборот нелицензионного программного обеспечения, что снизит уровень преступности в сфере обращения охраняемой законом информации, сократится число «зараженных» устройств, используемых в сетях «Ботнет»; во-вторых, разработка собственного программного обеспечения позволит минимизировать риск получения информации иностранными спецслужбами.

Следует обратить внимание на то обстоятельство, что дать отпор преступлениям в сфере обращения охраняемой законом информации в частности и киберпреступлениям в целом невозможно без международного сотрудничества и принятия международных соглашений в области противодействия преступлениям в сфере обращения охраняемой законом информации. С.В. Воронцова считает, что «отдельная страна не может самостоятельно вести борьбу с киберпреступностью, и только международное сообщество способно противостоять данному виду преступности»[7]. Решить проблему могло бы тесное взаимодействие следователей и оперативных работников, занимающихся выявлением, раскрытием преступлений в этой сфере. Тем не менее большинство стран неохотно раскрывают сведения о банковских счетах своих граждан, например, США и страны Европейского Союза. Сложившаяся международная обстановка также способствует изоляции России от внешнего мира. Это совершенно неоправданно, так как субъектами совершения преступления в большинстве случаев являются российские граждане, а потерпевшими иностранцы – жертвы российских хакеров. Поэтому непредоставление информации российским правоохранительным органам наносит вред именно их безопасности.

Однако несмотря на то, что уже несколько лет назад вступило в законную силу Постановление Правительства РФ № 758, механизм реализации его мер на практике так и не установлен. Более того, многие владельцы коллективных точек доступа в сеть Интернет до сих пор не знакомы с разъяснениями Министерства связи и массовых коммуникаций Российской Федерации.

В изменениях в Правилах оказания услуг связи Постановлением Правительства РФ № 758 не сказано, что идентификация пользователей коллективных точек доступа Wi-Fi обязательно должна происходить только через мобильные номера российского оператора. Запрета нет, это очевидно. Но иностранные сотовые операторы информацию о владельце номера телефона могут и не дать. На сайте государственных услуг иностранные граждане тоже не зарегистрированы. Для удостоверения личности иностранец может предъявить паспорт администрации общественного места, где установлена точка доступа к Wi-Fi, оформить сим-карту российского оператора связи и авторизоваться с ее помощью.

С технической точки зрения организовать доступ к сети Интернет в общественных местах по документу, удостоверяющему личность, или с привязкой к телефонному номеру несложно. Для этого следует организовать так называемый гостевой доступ, для получения которого на специальной вебстранице заполнить специальную форму.

Если для пользования пунктами коллективного доступа по Wi-Fi в общественных местах законодательная база есть, хотя и механизм четко не проработан, то интернет-кафе остается привлекательным местом для киберпреступников. Во многих странах действуют жесткие меры идентификации лиц, пользующихся подобного рода услугами. Так, например, в Китае посетителей интернет-кафе обязали предоставлять администрации паспорт или удостоверение личности.

Владельцы интернет-клубов в Белоруссии несут ответственность за переданные через сеть Интернет сообщения посетителей. Если IP-адрес, который выделялся при совершении какого-либо противоправного деяния, ведет в интернет-кафе, существует возможность привлечь к ответственности его владельца. Таким образом, владелец пункта доступа к сети Интернет по Wi-Fi становится первым, кто заинтересован в том, чтобы в клубе были видеокамеры, учет пользователей, логирование посещений.

Власти Италии приняли закон, согласно которому владельцы точек публичного доступа в сеть Интернет обязаны копировать паспорта клиентов и отслеживать сайты, которые они посещают, а также устанавливать специальные программы для слежения за активностью клиентов. Генерируемые программой отчеты регулярно должны направляться в полицию. Также отмечается, что перлюстра-

[7] Воронцова С.В. Киберпреступность: проблемы квалификации преступных деяний // Российская юстиция. 2011. №2. С. 14-15.

ции переписки подвергаются только те лица, которые находятся в «черных списках» правоохранительных органов.

Обязательно осуществление координации деятельности правоохранительных органов и иных органов и организаций в целях профилактики борьбы с преступлениями в сфере обращения охраняемой законом информации. В частности, нуждается в укреплении взаимодействие правоохранительных органов и операторов связи для оперативного получения у них информации об абонентах и оказанных им услугах связи. Нужно сформировать рабочие группы, состоящие из представителей органов местного самоуправления, студентов, лиц, занимающих информационной безопасностью и возложить на них обязанность по мониторингу сети Интернет с целью отыскания потерпевших от преступлений в сфере обращения охраняемой законом информации, а также о лицах, осуществляющих подобного рода деятельность.

Также необходимо повышать эффективность работы правоохранительных органов, организовывать межрегиональное сотрудничество на территории Российской Федерации, а также межгосударственное взаимодействие. Снижению уровня латентности преступлений в сфере обращения охраняемой законом информации, на наш взгляд, способствует подготовка компетентных сотрудников с достаточным уровнем знаний в сфере информационных технологий, а также взаимодействие со средствами массовой информации.

Следует проводить индивидуальное предупреждение, которое включает в себя работу с лицами, склонными к совершению преступлений в сфере обращения охраняемой законом информации, в целях предотвращения их криминальной самореализации.

По этой причине противодействие преступлениям в сфере обращения охраняемой законом информации должно включать в себя следующие направления:

1) осуществление постоянного мониторинга лиц, склонных к совершению преступлений в сфере обращения охраняемой законом информации, которое необходимо возложить на специальные подразделения органов внутренних дел. Следует обратить внимание на то, что эта деятельность в основном должна проводиться в виртуальной среде;

2) осуществление надзора за лицами, которые были осуждены за преступления в сфере обращения охраняемой законом информации.

Социально-экономические факторы. Огромные финансовые потоки в нелегальных видах интернет-бизнеса скрыты от государства, это приводит к тому, что все они остаются «в тени» без правового и социального контроля, тем самым уменьшая риск быть пойманными. На наш взгляд, данное обстоятельство формирует в киберпространстве условия, при которых появляется возможность получения преступным путем сверхприбыли при минимальных затратах и рисках, что является объективным детерминантом преступности в сфере оборота охраняемой законом информации, поскольку побуждает виновных их совершать. Данную проблему, на наш взгляд, можно решить профилактикой киберпреступности среди населения и популяризацией легальных способов получения крупных доходов в сети Интернет.

Виктимологические факторы. Ежегодно из-за утечек персональной информации в сеть Интернет попадают миллионы паролей пользователей. Компания SplashData каждый год составляет список самых простых паролей. Обычно в их отчете оказываются пароли вроде 123456, но каждый год в этом списке появляются и новые позиции – например, в 2018 г. туда попал donald[8]. Между тем пользователи информации пренебрегают сменой пароля от своих учетных записей при разводе, увольнении, потере телефона или записной книжки, тем самым подвергая свою информацию ограниченного доступа опасности неправомерного использования со стороны бывшего супруга, коллеги и т.п. Подобные факты присутствуют в судебно-следственной практике.

В связи с этим необходимо разработать систему максимально полного информирования правоохранительными органами граждан, в том числе и посредством подготовки информационных материалов по проблемам преступлений, посягающих на охраняемую законом информацию.

Из-за отсутствия в российском законодательстве четких правил по защите персональных и пользовательских данных и из-за невключения цифровых прав человека в Конституцию РФ пользователи сети Интернет в настоящий момент должны сами позаботиться о своей безопасности в сети Интернет и предпринять меры по защите своей личной информации:

[8] URL: https://www.teamsid.com/splashdatas-top-100-worst-passwords-of-2018.

1) шифрование всех данных. Даже если компьютерная система защищена паролем, злоумышленник сможет легко сбросить его, загрузившись с внешнего диска. Сбрасывать пароль также не нужно – любой Live-дистрибутив Linux может легко прочитать и скопировать данные. Поэтому нужно предпринять меры по шифрованию информации;

2) использование менеджера паролей, который генерирует каждый раз новые случайные пароли для любого создаваемого аккаунта в сети Интернет.

Абсолютная приватность в сети Интернет недостижима в принципе. Но перечисленные приёмы смогут защитить пользователей сети Интернет от кражи конфиденциальных данных мошенниками, от любопытства коллег, сидящих за одним столом, от назойливого внимания маркетологов Google и Microsoft.

Внимание к данной проблеме и активная работа в обозначенных направлениях являются, на наш взгляд, важным шагом на пути эффективного выявления и предупреждения преступлений в сфере обращения охраняемой законом информации.

На основании вышеизложенного можно сделать вывод, что существование преступности в сфере оборота охраняемой законом информации определяется несколькими специфическими факторами, которые не совпадают с факторами, порождающими преступность в целом. К таким факторам можно отнести:

1) факторы правового характера (отсутствие единого понятийного аппарата, регламентирующего преступления в сфере обращения охраняемой законом информации, отсутствие уголовной ответственности за ограничение доступа к охраняемой законом информации);

2) технические факторы (увеличение количества компьютерной техники и объемов информации, недостаточность защиты самих технических средств защиты компьютерной техники);

3) организационные факторы (усиление цифрового неравенства в России).

Проведенный анализ уголовных дел о преступлениях в сфере обращения охраняемой законом информации, исследование особенностей их совершения, данные о личности преступника и потерпевшего позволили выделить ряд задач, решение которых качественно улучшит профилактическую работу правоохранительных органов по борьбе с преступлениями в сфере обращения охраняемой законом информации.

Во-первых, необходимо включить сайты, на которых происходит общение лиц, интересующихся преступлениями в сфере обращения охраняемой законом информации в реестр запрещённых сайтов, наряду с порнографическими сайтами, сайтами по пропаганде наркотиков и т.д. При этом не нужно забывать о том, что предупреждение – это «машина», включающая в себя большое количество «механизмов», среди которых уголовно-правовые средства должны стоять не на первом месте исходя из идеи, что совершение деяния должно быть предупреждено, а не наказано. Если какому-либо пользователю сети Интернет удалось обойти блокировку сайта, то необходимо, не дожидаясь от него конкретных реальных действий, воплощающих его умысел, проводить профилактическую беседу. Таким образом, блокировка подобного рода сайтов и контроль их посетителей будет является эффективным способом предупреждения преступлений в сфере обращения охраняемой законом информации.

В частности, речь идет о принятии Федерального закона «Об основах системы профилактики киберпреступлений», в котором можно было бы сконцентрировать все нормы, регулирующие общественные отношения, связанные с сетью Интернет, электронной информацией, закрепленные в настоящий момент в различный подзаконных актах, а иногда в локальных актах коммерческих организаций. В некоторых из них содержатся нормы, применение которых позволило бы сократить риск совершения преступлений в сфере обращения охраняемой законом информации и облегчить поиск злоумышленников.

Поступила в редакцию 21.12.2020

Родивилин Иван Петрович, старший оперуполномоченный по ОВД
отдела «К» (по борьбе с правонарушениями в сфере информационных технологий)
Главного Управления МВД России по Иркутской области
664003, Россия, г. Иркутск, ул. Литвинова, 15
E-mail:377a@bk.ru

I.P. Rodivilin

MODERN SPECIFICITY OF CRIME DETERMINATION IN THE SPHERE OF CIRCULATION OF INFORMATION PROTECTED BY LAW

DOI: 10.35634/2412-9593-2021-31-2-305-311

The article is devoted to the study of the determinants of deviant behavior associated with the commission of crimes in the field of circulation of information protected by law. It is concluded that the determinants of these crimes are multifactorial in nature, they include: factors of a legal nature, technical, organizational, victimological. An analysis of forensic practice shows that situations conducive to the commission of crimes are often created by the victims themselves. The imprudent behavior of victims is often the main victimological factor in their victimization from these crimes. This behavior most often manifests itself in non-observance of elementary safety rules known to the victim, or in ignorance of such rules. This situation testifies to the low culture of information security of the citizens of our country. Based on the research conducted by the author, during which it was revealed that victims themselves create conditions for committing crimes in the field of circulation of information protected by law, and they could have been prevented with due diligence on the part of the victims. It is also concluded that the main attention in the prevention of crimes in the sphere of circulation of information protected by law should be given to victimological prevention, which consists in ensuring reliable protection of information.

Keywords: crimes in the field of computer information, crime factors, DDOS attack, cyber attack, information security.

Received 21.12.2020

Rodivilin I.P., senior operative for the internal affairs department
of the “K” department (for the fight against offenses in the field of information technology)
Main Directorate of the Ministry of Internal Affairs of Russia for the Irkutsk Region
Litvinova st., 15, Irkutsk, Russia, 664003
E-mail: 377a@bk.ru