А. А. Ходусов,
кандидат юридических наук, доцент,
Международный юридический институт

К ВОПРОСУ О СОВЕРШЕНСТВОВАНИИ ЗАКОНОДАТЕЛЬСТВА ОБ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА СОВЕРШЕНИЕ ПРЕСТУПЛЕНИЙ В СФЕРЕ ОБРАЩЕНИЯ ЦИФРОВОЙ ИНФОРМАЦИИ

Аннотация. В данной работе проведен анализ проблем и путей совершенствования законодательства об уголовной ответственности за совершение преступлений в сфере обращения цифровой информации. Проведен анализ статьи 272 УК РФ – неправомерный доступ к компьютерной информации, ее объект и предмет, судебная практика и ее основные проблемы в системе уголовного права, также автор рассмотрит вопросы квалификации данного преступления в зарубежной практике.

Ключевые слова: Уголовный кодекс РФ, компьютерная информация, квалификация, проблемы, обращение цифровой информации

ON THE ISSUE OF IMPROVING THE LEGISLATION ON CRIMINAL LIABILITY FOR CRIMES IN THE FIELD OF DIGITAL INFORMATION CIRCULATION

Abstract. This paper analyzes the problems and ways to improve the legislation on criminal liability for crimes in the field of digital information circulation. The analysis of Article 272 of the Criminal Code of the Russian Federation – illegal access to computer information, its object and subject, judicial practice and its main problems in the criminal law system, the author will also consider the issues of qualification of this crime in foreign practice.

Keywords: Criminal Code of the Russian Federation, Computer information, Qualification, Problems, Circulation of digital information

С развитием технологий, возможности человека, у которого есть персональный компьютер, становятся гигантскими, начиная от покупки вещей в сети Интернет и заканчивая ведением бизнеса через интернет.

При этом человек так же, как и в обычном пространстве подвергается постоянной опасности совершения в отношении его преступного посягательства, а именно, у него в любой момент могут завладеть личной информацией, которая хранится в компьютере. В связи с этим необходимо разобрать актуальные проблемы уголовного законодательства относительно данной статьи, что может послужить улучшению методов борьбы с злоумышленниками, пытающимися завладеть чужой компьютерной информацией [4].

Следующие составы, по мнению МВД России, относятся к уголовным делам в сфере информационных технологий следующие составы преступлений: ст. 158, 159, 159.3, 159.6 УК РФ (кражи и мошенничества при использовании технологий в сфере компьютерной информации), 171.2, 205.2, 228.1 242, 242.1, 242.2, 280 УК РФ; преступления в сфере компьютерной информации, предусмотренные главой 28 УК РФ (ст. 272–274.1 УК РФ).

По мнению некоторых авторов, преступления в сфере компьютерной информации не ограничиваются главой 28 УК РФ, к данной категории возможно отнести любое преступление, совершенное с использованием телекоммуникационных и компьютерных технологий, в частности преступления в кредитно-финансовой деятельности (преступная банковская деятельность, отмывание и т. п.).

При установлении понятия категории преступлений необходимо установить такие понятия, как «информационно-телекоммуникационные технологии» и «компьютерная информация».

Первым этапом в процессе доказывания является установление факта совершения преступления.

Установление факта совершения преступления необходимо при принятии решении о возбуждении уголовного дела, если не установлен факт совершения преступления, то нет оснований для возбуждения дела.

Выделяют способы совершения преступлений в сфере информационных технологий: способ непосредственного воздействия на компьютерную и иную информацию; способ опосредованного (удаленного) воздействия на компьютерную информацию: удаленное проникновение в информационно-телекоммуникационные сети [5].

В ходе анализа положений УПК РФ ст. 64 Закона № 126-ФЗ установлено, что законодательство РФ не устанавливает понятие лог-файлов, не регулирует отдельно порядок их предоставления следователю. Следователь таких прав не имеет, поскольку он собирает доказательства в рамках следственных действий. Согласно ч. 5 ст. 64 Закона № 126-ФЗ операторы не передают информацию следователю, а оказывают содействие в рамках следственных действий. В связи с этим возникает проблема, такого следственного действия как получение компьютерной информации не существует, а действующие следственные действия не позволяют получать информацию с технических каналов связи в ходе доследственной проверки.

При доказывании необходимо устанавливать и иные обстоятельства, указанные в ст. 73 УПК РФ. На основе анализа процессуальных действий, проводимых в ходе проверки сообщения о преступлении, установлено, что Конституционный суд Российской Федерации в Определении от 22.12.2015 № 2885-О установил, что истребование документов возможно в рамках досудебной проверки, только при наличии согласия на их передачу.

В данной ситуации необходимо установить, что истребование должно осуществляться на основании ч. 4 ст. 21 УПК РФ. Истребование документов необходимо для целей возбуждения уголовного дела в проведения обыска у подозреваемого. Тактика субъекта доказывания не должна быть направлена на раскрытие информации о проверке сообщения о преступлении, поскольку, если преступник узнает, что в отношении него проводится проверка, он попытается уничтожить следы.

В ходе анализа ст. 145.1 УПК РФ сделан вывод, что необходимо обязательно изымать электронные носители по делам в сфере информационных технологий, что следует из анализа ст. 145.1 УПК РФ, за исключением ограничений, установленных статьей.

Статьи УК РФ иногда сгруппированы таким образом, что дают некоторым толкователям возможность подменять значение признаков состава преступления

и придавать слишком большое значение информации, относя ее к предмету посягательства, например, в преступлениях, предусмотренных ст. 325 и ст. 327 УК РФ.

Документы (даже официальные) не представляют социальной ценности сами по себе, но важны, потому что содержат юридически значимые факты или статусы, которые удостоверяют. Причем ценность указанных предметов проявляется только в возможности их использования в свою пользу или против чужих интересов [3].

Документ – лишь материальный носитель этой знаковой информации. Реальная общественная опасность незаконных манипуляций с ними возникает именно тогда, когда этой информацией, зафиксированной документально, начинают пользоваться вопреки правилам и причиняют вред. До этого момента нет воздействия на конкретный вид социально-значимого блага, которое бы могло олицетворять объект преступления.

Примером аналогичного заблуждения относительно места признака в системе состава преступления могут служить объекты интеллектуальной собственности. Настоящую социальную (а не персонифицированную в авторском праве ценность) они обретают только на уровне предметов, участвующих в экономическом обороте (ст. 146 и ст. 147 УК РФ предполагают наступление имущественного ущерба для правообладателей). То есть незаконное использование экономически невостребованного объекта интеллектуальной собственности не может создать общественно опасного деяния. Деяния, запрещенные некоторыми статьями УК РФ, посвященными «нарушению специальных правил» (например, в сфере экологии), иногда тоже относятся в юридической литературе к преступлениям, где предметом выступают сами эти правила [6].

В такой «транскрипции», когда признак предмета преступления выходит за рамки классической концепции: вещи материального мира, воздействуя на которые виновный причиняет вред объекту уголовно-правовой охраны», он смешивается с категорией средств совершения преступления.

Именно в этот момент во многих составах преступлений, закрепленных в уголовном законе, происходит преувеличение значения информации – вместо средства ее начинают считать самоцелью посягательства. Нарушение правил оборота государственной тайны причиняет вред не этому обороту, а общественным отношениям по поводу государственной безопасности. Разглашение тайны усыновления нарушает личные границы, и вред причиняется личности, а не обороту актов гражданского состояния. Исключением может служить, пожалуй, информация, предоставляемая в процессе судопроизводства и предварительного следствия.

Так как правосудие основано на поиске истины, которая может выявляться только при условии достоверности данных, то любое искажение информации влияет на итог, а значит на объект уголовно-правовой охраны. Искажение данных в официальных документах в результате приведет к нарушению отдельных видов прав субъектов общественных отношений в какой-либо сфере жизни (экономической, семейной, трудовой или др.). В этом случае следовало бы квалифицировать содеянное, исходя из вида пострадавшего объекта.

Аналогичная ситуация прослеживается при ближайшем рассмотрении посягательств, предусмотренных ст. 272–274.1 УК РФ. Компьютерная (цифровая) ин-

формация – это не столько вид информации (она может относиться к любой сфере жизнедеятельности социума и его участников), сколько форма ее существования. Подход, согласно которому глава 28 не должна выделяться в УК РФ в качестве самостоятельной, так как не имеет собственного объекта уголовно-правовой охраны, также присутствует в теории отечественного уголовного права.

В силу специфики (исключительно физической) хранения и передачи такой информации, реальная опасность ее утраты ничем не отличается от утраты сведений на других, не компьютеризированных носителях. Сам факт существования цифровых данных не делает из них иные сведения, и отличие от любой другой информации заключается здесь только в способе фиксации и хранения, т. е. в форме. Сложившаяся тенденция по усилению уголовной ответственности за совершение преступлений (в частности, вербальных) посредством информационно-коммуникационных сетей в ст. 110.2, 137, 205.2, 230, 280, 280.1 УК РФ, на наш взгляд, преувеличивает объемы необходимой репрессии за использование цифровой среды и цифровой информации в рамках криминального поведения.

Несанкционированное копирование компьютерной информации, криминализированное ст. 272 УК РФ, например, явно не охватывает такие способы тиражирования, как фотографирование экрана или переписывание вручную сведений [5. С. 529].

Хотя в зависимости от последствий, выделенные способы все равно могут нарушать тайну переписки или даже государственную тайну, быть приготовлением или покушением к иным видам преступлений, т. е. обладать общественной опасностью в рамках традиционных объектов посягательств.

Вопрос о нарушениях и злоупотреблениях компьютерной информацией, относящейся к программному обеспечению (например, вредоносные программы), на наш взгляд, может также решаться через призму причиненного вреда правообладателям легального контента. Распространенные в настоящее время «компьютерное хулиганство», «компьютерное мошенничество» и др. т. п. деяния вполне можно квалифицировать по имеющимся в УК РФ статьям вне пределов главы 28, если признать, что компьютерная (цифровая) информация – не само ценность, а форма существования сведений.

Иными словами, считаем, что выделять самостоятельный объект уголовно-правовой охраны в виде отношений по поводу оборота компьютерной информации – неоправданное расширение уголовной репрессии.

Важно определить объект и предмет ст. 272 УК РФ. Некоторые авторы считают, что у нормы статьи, объект и предмет тождественны, однако, как пишет законодатель, предмет не находится в ограниченной связи с объектом данного преступления [1].

Как и в большинстве норм уголовного кодекса, связанных с имуществом, объектом данного преступления принято считать не завладения определенной компьютерной информацией, а общественные отношения, которые обеспечивают конфиденциальность и сохранность компьютерной информации.

Предметом же будет являться охраняемая законом компьютерная информация.

Таким образом, можно заметить, что объект отвечает за конкретные действия, направленные на законное хранение и оборот информации, хранящейся на компьютере [2].

На сегодняшний день проблема возбуждений уголовных дел по ст. 272 УК РФ является неоднозначной.

Интернет не ограничивается одним городом или страной, он связан со всем миром, в этом же и проявляется немаловажная проблема, она заключается в том, что если похищение злоумышленником данных происходит в конкретной стране и в конкретном городе, то это возможно пресечь, однако, если хищение данных исходит из других стран, то тут уже не физически не юридически невозможно воздействовать на злоумышленника. Единственное, что необходимо в данном случае это обезопасить информацию, хранящуюся на компьютере при помощи различных антивирусных программ и не скачивать подозрительные программы, которые могут поспособствовать хищению данных [5].

Существует проблема и квалифицирующего характера, она связана с тем, что преступным деянием является именно неправомерный доступ к информации, которая содержится на компьютере, а не на каком-либо носителе данной информации. В этом случае такое деяние может быть квалифицированно как умышленное уничтожение или повреждение имущества (ст. 167 УК РФ).

Проблема заключается в том, что при уничтожении носителя данной информации санкция предусмотрена более мягкая мера наказания, чем в ст. 272 УК РФ.

Также существует проблема доказательства удаления ценной информации, это необходимо для квалификации ч. 2 ст. 272 УК РФ (причинившее крупный ущерб), ведь уничтожение компьютерной информации предполагает ее исчезновение без возможности восстановления, что может повлечь затруднения в уголовном процессе.

Важной деталью является то, что законодатель делает акцент на тех сведениях, по которым неправомерный доступ может причинить огромный ущерб, законодательство Российской Федерации выделяет следующие сведения:

– Тайна следствия и судопроизводства.

– Факты и события частной жизни гражданина, идентифицирующие его личность.

– Служебные сведения (в соответствии с ГК).

– Тайна профессиональной деятельности (пример: адвокатская тайна).

– Тайна коммерческой деятельности.

– Интеллектуальная тайна (пример: еще неопубликованные изобретения).

Рассмотрев данные сведения, важно заметить, что законодатель понимает уязвимые стороны различных областей страны, однако, как и говорилось ранее, методы предотвращения хищений данных сведений через электронные системы слабо развиты, именно поэтому, когда во всем мире происходит процесс переноса данных на виртуальные носители, государству также необходимо задуматься о надежной защите этих данных, не только посредством введения уголовно наказуемых норм в Уголовный кодекс РФ, но и разработкой методов предотвращения данных преступлений.

На данный момент ситуация со ст. 272 УК РФ не однозначна. С одной стороны, наше законодательство не только дает понимание о противоправности деяний, связанных с неправомерным завладением информацией, но и в отличие от законодательств других стран разделяет по способу ее совершения [6].

С другой стороны, до конца непонятна сама необходимость данного разделение, ведь оно может порождать проблемы в правоохранительной системе, что и наблюдается на сегодняшний день.

Наконец нужно отметить, что российскому законодательству в данном вопросе еще предстоит множество изменений и дополнений, прежде всего уже на сегодняшнем этапе необходимо выделить наиболее действенные методы противодействия незаконному получению компьютерной информации, а также необходимо повышать квалификацию правоохранительных органов в сфере компьютерной безопасности, хотя как вариант можно использовать привлечение специалистов для разработки более действенных программ, отслеживающих следы компьютерных преступлений [3. С. 60].

Таким образом, повышение интереса правоохранительных органов к компьютерной безопасности сделает отличную базу для безопасного перехода Российской Федерации к информационному прогрессу.

Ознакомившись с архивами судебных решений за исследуемый период, можно сделать следующие выводы, что по ст. 273 УК РФ в настоящий момент существует множество неоднозначных вопросов по проблеме применения рассматриваемой статьи, споры о правильном решении которых, в научной среде ведется до сих пор.

Получение информации, путем хищения с электронного носителя, на законодательном уровне называется мошенничеством и его классическое понятие имело закрепление в ст. 159 УК РФ. Но в ходе изменений УК РФ, рассматриваемый нами объект посягательства, получил свое закрепление в ст. 159.6 УК РФ «мошенничество в сфере компьютерной информации», что и будет исследовано нами далее.

В ней рассматривается мошенничество, т. е. хищение чужого имущества путем кражи электронного носителя, но виды мошенничества очень разнообразны, даже в сфере IT-технологий вариантов совершения подобных преступлений очень много [7].

Неоднократно А. А. Чугунов утверждал, что: «мошенничество предполагает наличие потерпевшего, которого можно обмануть или чьим доверием можно злоупотребить, что является ключевым фактором для отнесения общественно опасного деяния к данному виду преступления».

С подобным высказыванием невозможно не согласиться, но получается, что ст. 159.6 УК РФ не имеет весь спектр, относящийся к мошенничеству, именно если оно касается IT-технологий, ведь в большинстве случаев потерпевшие даже не подозревают о наличии злоумышленника в их электронном носителе. В любом случае на техническое средство невозможно воздействовать как на человека, с точки зрения эмоций, чувств или же путем злоупотребления доверия. Из этого следует, что данная статья в УК РФ не совсем точно определяет объективную сторону состава рассматриваемого преступления. На наш взгляд, было бы более правильно откорректировать объективные признаки состава преступления в сфере мошенничества.

Если же для мошенника основной целью является хищение денежных средств или информации, путем подбора паролей, входа с чужой учетной записи или подбора пин-кода, то в подобной ситуации правильнее утверждать о тайном хищении чужой информации или имущества, путем использования компьютерных технологий.

Так в своей статье А. Н. Харитонов и Е. В. Никульченкова утверждают, что: «одним из путей решения данной проблемы видится исключение ст. 159.6 УК РФ из уголовного закона с последующим внесением изменения в виде квалифицирующего признака в ст. 158 УК РФ: кража, совершенная с использованием компьютерных технологий».

Таким образом, мнения по рассматриваемой проблеме поделились, некоторые считают, что правильнее будет проработать ст. 159.6 УК РФ, а другие придерживаются мнения исключения подобной статьи из УК РФ и внесения данных объективных признаков в ст. 158 УК РФ в качестве квалифицирующего признака.

В любом случае по опыту применения данной статьи можно сделать вывод, что она является до конца не проработанной, а, значит, в судебно-следственной практике будет иметься большое количество недочетов и ошибок.

В них говорится о сознательном уничтожении информации, блокировке, копировании данных, хранении, передаче данных, при помощи вирусных программ, программ-шпионов или иных вредоносных систем. Даже в случае, если преступнику в сфере компьютерной информации не удастся до конца заполучить данными или применить их в своих корыстных целях, он все равно будет привлечен к уголовной ответственности, так как перечисленные составы имеют вид формальных.

Примером может послужить дело, в котором гражданин В., самостоятельно разработал вирусную программу – спам для получения личной информации законопослушных граждан через социальные сети.

После того как люди стали переходить по его ссылке, заранее отправленной в социальной сети, часть информации, а зачастую и логины с паролями переходили на личный компьютер гражданина В. В последующем он был привлечен к уголовной ответственности по ст. 273 УК РФ [8].

Таким образом, преступник, применивший в отношении законопослушного гражданина неправомерное деяние, будет нести ответственность за любой вред, причиненный с его стороны, но ответственность по статье «Мошенничество в сфере компьютерной информации» не наступит в связи с тем, что сам носитель информации будет находиться у потерпевшего.

На наш взгляд, глава 28 УК РФ достаточно подробно описывает компьютерные преступления. Однако в ней не рассматривается специфика мошенничества в целом, а значит, эта глава также может быть существенно изменена.

Список литературы

1. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // Собрание законодательства Российской Федерации от 17 июня 1996 г. № 25 ст. 2954 (в ред. 14.07.2022). URL: https://normativ.kontur.ru/document?moduleId=1&documentId=427835 (дата обращения: 19.08.2022).

2. Абов А. И. Преступления в сфере компьютерной информации: неправомерный доступ к компьютерной информации. URL: https://search.rsl.ru/ru/record/01002559391 (дата обращения: 19.08.2022)

3. Анисимова И. А. Уголовно-правовое значение преступного вреда: Дисс. … канд. юрид. наук. Томск, 2008. 232 с.

4. Бражник С. Д. Преступления в сфере компьютерной информации: проблемы законодательной техники: дисс. … канд. юрид. наук. Ижевск. 2002. 189 с.

5. Евдокимов К. Н. Особенности личности преступника, совершающего неправомерный доступ к компьютерной информации (на примере Иркутской области). URL: https://cyberleninka.ru/article/n/osobennosti-lichnosti-prestupnika-sovershayuschego-nepravomernyy-dostup-k-kompyuternoy-informatsii-na-primere-irkutskoy-oblasti (дата обращения: 19.08.2022).

6. Пелевина А. В. Криминообразующие признаки диспозиции статьи 272 УК РФ // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2015. № 4 (32). С. 261–267.

7. Старичков М. В. Понятие «Компьютерная информация» в российском уголовном праве. URL: https://www.elibrary.ru/item.asp?id=21342806 (дата обращения: 19.08.2022).

8. Табаков А. В. Уголовное наказание за неправомерный доступ к охраняемой законом компьютерной информации: толкование текста статьи 272 УК РФ и обоснование необходимости внесения в нее изменений. URL: https://cyberleninka.ru/article/n/ugolovnoe-nakazanie-za-nepravomernyy-dostup-k-ohranyaemoy-zakonom-kompyuternoy-informatsii-tolkovanie-teksta-stati-272-uk-rf-i (дата обращения: 19.08.2022).

Е. А. Черкасова,
кандидат юридических наук,
Белгородский государственный национальный
исследовательский университет

ЦИФРОВЫЕ ТЕХНОЛОГИИ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ: СОВРЕМЕННОЕ СОСТОЯНИЕ И ПЕРСПЕКТИВЫ

Аннотация. Целью статьи является исследование современного состояния применения цифровых технологий в уголовном процессе, а также перспектив перехода к электронному уголовному судопроизводству. В статье исследованы позиции ряда ученых-процессуалистов о перспективах расширения информационных технологий в уголовном процессе. Высказана точка зрения об основных этапах перехода к новым цифровым технологиям в уголовном судопроизводстве.

Ключевые слова: уголовно-процессуальное законодательство, цифровизация, цифровые технологии, электронное уголовное дело, электронные документы, электронные носители информации, электронное производство по уголовным делам

DIGITAL TECHNOLOGIES IN CRIMINAL PROCEEDINGS: CURRENT STATUS AND PERSPECTIVES

Abstract. The purpose of this article is to study the current state of the use of digital technologies in criminal proceedings, as well as the prospects for the transition to electronic criminal justice. The article examines the positions of a number of procedural scientists on the introduction of information technology in the criminal process. A point