DOI dx.doi.org/10.24866/VVSU/2073-3984/2020-2/103-117

УДК 341.9 + 343.1+343.2/.7

А. В. Верещагина

Владивостокский государственный университет экономики и сервиса
Владивосток. Россия

К вопросу о предмете неправомерного доступа к компьютерной информации

Цифровая революция детерминировала перевод значительной части общественных отношений в виртуальное пространство. Означенная ситуация не могла не породить рост числа компьютерных правонарушений, одним из средств противодействия которым является установление уголовно-правовых запретов.

Цель исследования – выявление проблемных аспектов регламентации предмета преступления – неправомерного доступа к охраняемой законом компьютерной информации.

Предмет исследования составляют нормы, регулирующие родовое и уголовно-правовое понятие информации.

Методы проведения работы. При проведении исследования автор, опираясь на принципы научного познания, использовал статистический, логико-догматический и сравнительно-правовой методы.

Теоретическая, нормативная и эмпирическая основа исследования. При изучении проблемных аспектов предмета преступления, предусмотренного ст. 272 УК РФ, автор тщательно проработал научные публикации по теме исследования, проанализировал регламентацию понятия «неправомерный доступ к охраняемой законом компьютерной информации» в российском уголовном законе, а также уголовном законодательстве государств постсоветского пространства. Эмпирической основой исследования являются решения судов разных регионов России.

Регламентация в уголовном законе России предмета преступления, предусмотренного ст. 272 УК РФ, несмотря на имевшиеся позитивные изменения, нуждается в корректировке. В легальном определении компьютерной информации следует отказаться от использования технических терминов и указания на то, что защите подлежит только охраняемая законом информация. Означенные изменения уголовного закона будут способствовать оптимизации правоприменения.

Ключевые слова и словосочетания: уголовное право, компьютерное преступление, объект преступления, предмет преступления, компьютерная информация, неправомерный доступ, охраняемая законом компьютерная информация.

Верещагина Алла Васильевна – канд. юрид. наук, доцент, зав. кафедрой уголовно-правовых дисциплин Института права; e-mail: vereschagina_alla@mail.ru

A.V. Vereschagina

Vladivostok State University of Economics and Service
Vladivostok. Russia

On the subject of unauthorized access to computer information

The digital revolution determined the translation of a significant part of social relations to the virtual space. The above-mentioned situation could not but give rise to an in-crease in the num-ber of computer offenses, one of the means of countering which is the establishment of criminal law prohibitions, for violation of which a person can be brought to criminal responsibility.
The purpose of the study is to identify problematic aspects of regulating the subject of the crime: "illegal access to computer-protected information protected by law".
The subject of the research is the norms regulating generic and criminal concept of in-formation.
Methods. The author, based on the principles of scientific knowledge, used statistical, logi-cal-dogmatic and comparative-legal methods.
Theoretical, normative and empirical research bases. The author carefully studied scientific publications on the topic under study, analyzed the concept of "illegal access to com-puter-protected information protected by law" in Russian criminal law, as well as in the criminal codes of the post-Soviet states. The empirical basis of the research is the decisions of courts in diffrent re-gions of Russia.
The regulation of the subject of the crime under article 272 of the criminal code of the Rus-sian Federation, despite positive changes, needs to be adjusted. In the legal definition of computer information, the use of technical terms and the indication that only legally protected information is subject to defense should be avoided. The above-mentioned amendments to the criminal law will help optimize the work of law enforcement agencies.

Keywords: criminal law, computer crime, object of crime, subject of crime, computer information, unauthorized access, computer information protected by law.

Введение. Перевод взаимоотношений общества, государства, личности в виртуальную среду не мог не породить противоправных явлений, направленных на неправомерный доступ к компьютерной информации. Государство пытается вырабатывать приёмы, ограждающие личность и общество от совершения компьютерных правонарушений, в том числе введением уголовно-правовых запретов (глава 28 «Преступления в сфере компьютерной информации» УК РФ) [33]. Несмотря на всё большую цифровизацию всех сторон жизни, что является объективной предпосылкой роста компьютерных правонарушений, число лиц, осуждённых за совершение преступлений, предусмотренных главой 28 УК РФ, крайне незначительно и варьируется за период с 2009 по 2019 г. от 0,02 до 0,04% (рис. 1) [23].

Причины незначительного количества осуждённых за совершение компьютерных преступлений могут быть различными. По нашему мнению, одной из основных является сложность доказывания преступлений, совершаемых с применением информационных технологий и компьютерных преступлений, что демонстрирует приговор в отношении А. Ю. Хрусталёва, осуждённого за совершение нескольких преступлений, предусмотренных ч. 2 ст. 272 УК РФ. Органы, осуществлявшие предварительное расследование, и суд не смогли установить в полном объёме объективную сторону неправомерных доступов к охраняемой

законом компьютерной информации, инкриминированных А. Ю. Хрусталёву [45]. В пользу утверждения о сложности доказывания компьютерных преступлений также свидетельствует длительность расследования и рассмотрения уголовных дел о компьютерных преступлениях. Приведём лишь один пример. Уголовное дело в отношении Д. В. Новикова, которому вменялся один эпизод, квалифицированный по ч. 1 ст. 272 УК РФ, расследовалось в течение 3 лет 3 месяцев и 2 дней, в суде дело рассматривалось 9 месяцев, общая продолжительность производства по делу составила 4 года и 2 дня [35].

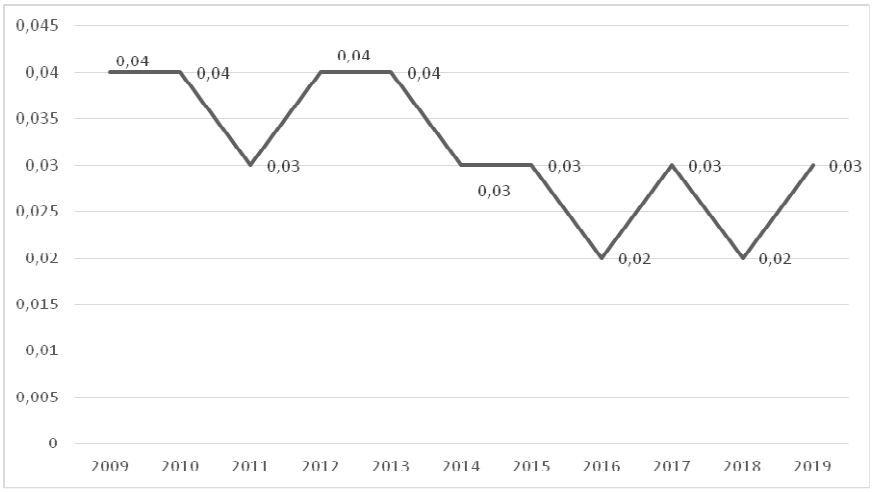

Рис. 1. Удельный вес осужденных за совершение преступлений, предусмотренных главой 28 УК РФ (% от общего числа осуждённых по всем статьям УК РФ)

Обоснованность тезиса о проблемах доказывания также подтверждается высоким удельным весом прекращаемых судами уголовных дел, возбуждённых по фактам совершения преступлений, предусмотренных гл. 28 УК РФ (рис. 2).

Удельный вес лиц, в отношении которых суд прекратил производство по уголовным делам по различным основаниям по всем составам УК РФ в период с 2009 до 2019 г., колеблется от 21,11 до 23,85%, а в отношении лиц, которым инкриминировали составы гл. 28 УК РФ, от 31,77 до 45,41%. Иными словами, удельный вес прекращений в отношении лиц, которым вменялось совершение компьютерных преступлений (гл. 28 УК РФ), в разные годы превышает удельный вес прекращений по всем инкриминированным составам на 10,66 и более процентов. С учётом того, что российский правоприменитель традиционно прекращение производства по уголовному делу увязывает не с наличием законных оснований, позволяющих прекратить уголовное преследование, а со слабостью доказательственной базы, т.е. как вынужденный шаг, вуалирующий бессилие органов, осуществляющих уголовное преследование, как некий брак в работе, то приведённая статистика есть не что иное, как безусловное следствие сложности доказывания по этой категории уголовных дел.

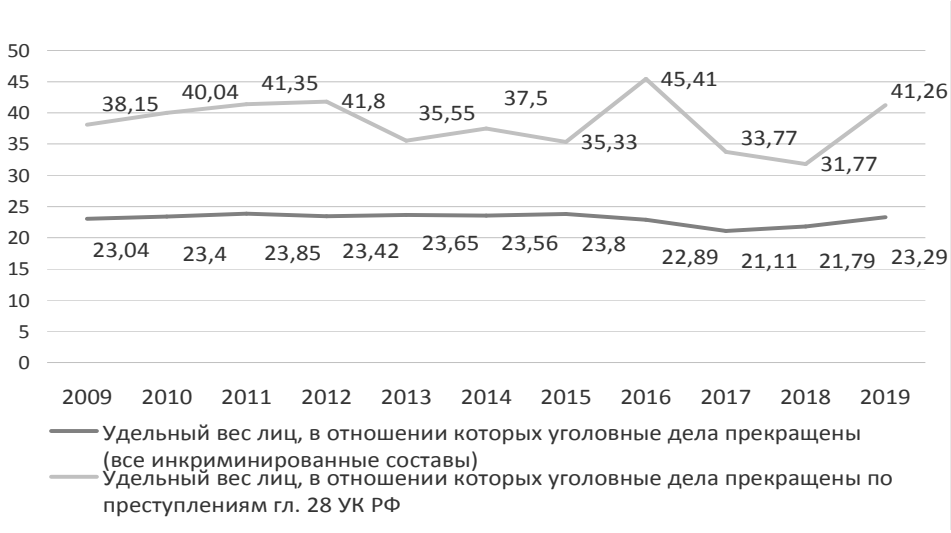

Рис. 2. Удельный вес лиц, в отношении которых судом производство по уголовному делу прекращено (%)

Проблемность доказывания компьютерных преступлений подтверждается ещё одним показателем – раскрываемость преступлений, совершаемых с применением информационных технологий. За 2019 г. удельный вес зарегистрированных преступлений, совершаемых с применением информационных технологий, составил 14,54% от общего числа зарегистрированных преступлений в России, а раскрываемость этих преступлений – 29,52%. Если обратиться к крайним значениям раскрываемости, то в Ленинградской области она составила 12,85%, а в Республике Дагестан – 57,4%. Допускаем, что столь высокая относительно других субъектов РФ раскрываемость в Республике Дагестан объяснима незначительным удельным весом преступлений, совершённых с применением информационных технологий, – 3,5% от общего количества зарегистрированных.

Косвенно на значимость противодействия совершению преступлений с применением компьютерных технологий и о наличии проблемы с выявлением, раскрытием, доказыванием рассматриваемой категории преступлений указывает тот факт, что в отчёте МВД РФ о состоянии преступности за 2019 г. впервые появился самостоятельный раздел, посвящённый преступлениям, совершённым с применением информационных технологий [18].

В связи с изложенным не случайна активность исследователей, занимающихся различными аспектами компьютерной преступности [4; 8; 11].

В предлагаемой публикации мы коснёмся только некоторых моментов, связанных с понятием предмета неправомерного доступа к компьютерной информации.

При проведении исследования автор руководствовался принципами научного познания (всесторонности, объективности, полноты, плюрализма и др.) и применял статистический, логико-догматический и сравнительно-правовой методы.

Основная часть. В системе регистрируемых преступлений, предусмотренных гл. 28 УК РФ, подавляющее большинство составляет неправомерный доступ к компьютерной информации (ст. 272 УК РФ) – 83,94% в 2019 г. [18]. Важным для эффективного уголовного преследования лиц, которым инкриминируется неправомерный доступ к компьютерной информации, является чёткое понимание того, что такое охраняемая законом компьютерная информация, неправомерный доступ к которой уголовно наказуем.

В уголовно-правовой теории преступление – это единство четырёх элементов: 1) объект, 2) объективная сторона, 3) субъект и 4) субъективная сторона. Данный подход получил легальное закрепление в ст. 8 УК РФ, в соответствии с которым лицо может быть привлечено к уголовной ответственности, если совершило деяние, содержащее «…все признаки состава преступления», т.е., повторимся, в наличии объект и субъект, объективная и субъективная стороны. Однако указанная точка зрения не единственная [13, с. 51-56]. По мнению В.Я. Тация, всё многообразие трактовок предмета преступления можно разделить на две группы: 1) предмет как правовой феномен не находится в органической связи с объектом преступления и 2) предмет и объект преступления тождественны [13, с. 52]. Означенный автор определяет предмет преступления как любую вещь материального мира, со свойствами которой закон связывает наличие в действиях лица признаков состава преступления [13, с. 55]. Сходная дефиниция даётся Б. В. Епифановым [7, с. 71]. Некоторые исследователи (например, В. Ю. Шевченко) помимо четырёх элементов состава преступления выделяют факультативные признаки, к которым относят предмет преступления [14, с. 20]. Ряд учёных, в частности В. Н. Винокуров, И. В. Кузнецов, с учётом современных реалий уточняют, что предмет преступления – это не только предметы внешнего мира, но и информация, существующая до совершения преступления и удовлетворяющая потребности людей, «…энергия и объекты экологии, доступные для восприятия и способные подвергаться воздействию …» [3, с. 62; 9, с. 142–143]. По мнению В.Н. Винокурова, служебная роль понятия «предмет преступления» заключается в конкретизации общественных отношений как объекта преступления [3, с. 60]. Вне зависимости от особенностей изложенных суждений все перечисленные выше авторы едины в том, что предмет преступления – это нечто, имеющее значение для установления состава преступления и как следствие для обоснованности уголовного преследования конкретного субъекта.

Объектом преступлений, предусмотренных гл. 28 УК РФ, являются «общественные отношения, связанные с посягательствами на компьютерную информацию» [2, с. 37], а предметом – охраняемая законом компьютерная информация. Ясная, логичная уголовно-правовая регламентация – это предпосылка правильной квалификации, в основе которой лежит верное определение объекта и предмета преступного посягательства. Иными словами, правоприменитель, опираясь на уголовный закон, должен грамотно определить объект и предмет компьютерных преступлений, чтобы избегать ситуаций, подобных по делу А.Н. Велигодского, которому одно деяние квалифицировали одновременно по ч. 1 ст. 159 и ч. 1 ст. 272 УК РФ (мошенничество и неправомерный доступ к ком-

пьютерной информации соответственно), вместо ч. 1 ст. 159.6 УК РФ (мошенничество в сфере компьютерной информации) [42].

Родовое понятие информации содержится в ст. 2 ФЗ «Об информации, информационных технологиях и о защите информации» (далее – ФЗ «Об информации»). «Информация – сведения (сообщения, данные) независимо от формы их представления» [20]. Понятие компьютерной информации фиксируется в примечании 1 к ст. 272 УК РФ: «под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи». Имеющееся в уголовном законе определение компьютерной информации фактически носит бланкетный характер и существенно отличается от предыдущей редакции нормы примечания 1 ст. 272 УК РФ, в которой законодатель пытался конкретизировать возможные средства хранения, обработки и передачи компьютерной информации: машинные носители, электронно-вычислительные машины (ЭВМ), системы ЭВМ или их сети. Отказ от конкретизации в нормах ст. 272 УК РФ средств хранения, обработки и передачи компьютерной информации имеет практическое значение, поскольку позволяет противостоять словесной эквилибристике при рассмотрении уголовного дела. К примеру, П. О. Врублевский, обжалуя приговор суда, заявил, что в его действиях нет состава преступления, т.к. новая редакция норм ст. 272 УК РФ не содержит последствия «блокирование работы системы ЭВМ и их сети». Суд, аргументируя свою позицию, опирался на грамотное понимание объекта и предмета преступления и обновленную редакцию легального понятия компьютерной информации, что позволило без труда опровергнуть доводы стороны защиты [38]. Помимо этого, как справедливо указывают В. Быков и В. Черкасов, развитие науки и техники предполагает появление новых средств хранения, обработки и передачи информации, что делает неизбежной постоянную корректировку закона [2, с. 38]. Кроме того, конкретизация в законе средств хранения, обработки и передачи информации может негативно влиять на правоприменение из-за недопустимости расширительного толкования уголовного закона и диссонанса между темпами развития научно-технической мысли, длительности приведения закона в соответствие с научно-техническими реалиями и жёсткими сроками принятия решений по уголовному делу, не дающими возможность дождаться уточнения закона.

Отмеченное выше положительное изменение легальной дефиниции «компьютерная информация» всё-таки, по нашему мнению, не совсем последовательно. Обновлённая нормативная регламентация позволяет расширить сферу применения уголовно-правового запрета, который направлен на охрану не только зафиксированной на каком-либо носителе информации, но и информации, находящейся в процессе передачи [6, с. 3]. Однако использование в законе термина «электрический сигнал» влечёт за собой как минимум две проблемы:

1. Законодатель не совсем корректно указал, что компьютерная информация представляется в форме электрических сигналов независимо от средств их хранения, обработки и передачи. Сигнал – это изменяющаяся физическая величина, отображающая сообщение [15; 17]. Информацию можно передавать с помощью

сигналов разной мощности, т.е. изменение их состояния, а не само состояние являются признаком наличия информации. Однако в таком случае говорить о хранении сигналов, представляющих собой изменение величин, нелогично. Возможно, законодатель, закрепляя в примечании 1 ст. 272 УК РФ понятие компьютерной информации, подразумевал способы хранения самой информации, а не электрических сигналов. В любом случае вне зависимости от целеполагания разработчиков нормы примечания 1 ст. 272 УК РФ означенный дефект желательно устранить.

2. Законодатель не учёл, что информация может передаваться не только посредством электрических сигналов. По физической природе носители информации могут быть электромагнитными, оптическими, акустическими, что не тождественно электрическим сигналам, и с формально-юридической точки зрения не охраняются уголовным законом. Кроме того, понятие компьютерной информации не охватывает посягательство на информацию, содержащуюся на некоторых видах носителей информации, таких, как оптические диски, флэш-память [5, с. 527–532].

В связи с изложенным предпочтительнее выглядит определение, содержащееся в УК Азербайджанской Республики: «Под «компьютерной информацией» подразумевается любая информация (факты, сведения, программы и понятия), пригодные для работы, обработки в компьютерной системе» (примечание 2 ст. 271.1) [24]. Азербайджанский законодатель не делает акцента на том, какими способами хранится и доставляется информация в компьютерную систему, а подчёркивает *пригодность* (курсив авт. – А. В.) информации для обработки в компьютерных системах. Аналогичное понятие компьютерной информации закреплено в УК Грузии: «Компьютерные данные – информация, изображенная в любой удобной для обработки в компьютерной системе форме…» (примечание 2 ст. 284) [25]. Нормы уголовных кодексов Азербайджанской Республики и Грузии фактически воспроизводят суть дефиниции компьютерной информации из ст. 1 Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации [20].

Приемлемым для целей правоприменения, по нашему мнению, является приём, использованный киргизским законодателем, который отказался от нормативного закрепления понятия компьютерной информации в уголовном законе, использовав при конструировании уголовно-правовых запретов, направленных на обеспечение информационной безопасности, бланкетные диспозиции (ст. 304) [26].

В научной юридической литературе нет единого понимания того, что такое компьютерная информация. Так, В. В. Крылов определяет компьютерную информацию как «сведения, знания или набор команд (программ), предназначенных для использования в ЭВМ или управления ею, находящиеся в ЭВМ или на машинных носителях, – идентифицируемый элемент информационной системы, имеющей собственника, установившего правила ее использования» [1, с. 294–297]. Цитируемое определение содержит указание на такой признак информации, как наличие особого правового режима, и соответствует п. 2.5.2 ГОСТ Р 50922-2006, в котором подчёркивается, что охраняемая информация является

предметом собственности и подлежит защите в соответствии с требованиями, устанавливаемыми собственником информации, или нормативными правовыми актами. Собственником информации могут быть государство, юридическое лицо, группа физических лиц, физическое лицо [16].

Иной взгляд на предмет компьютерных преступлений у А. Н. Попова и Е.И. Панфиловой, считающих, что предметом преступного посягательства является не компьютерная информация, а информационная среда, связанная с созданием, преобразованием и потреблением информации [12]. Информация должна обладать признаками (реквизитами), позволяющими её идентифицировать, и фиксироваться на материальном носителе. С таким подходом сложно не согласиться, поскольку отсутствие индивидуализации информации приводит к трудностям с конкретизацией предмета преступления.

Множественность доктринальных понятий компьютерной информации, дефектность легальной формулировки в совокупности с отмечавшимися нами особенностями толкования уголовного закона (недопустимость расширительного толкования) и информационная революция делают насущной корректировку закона. Как представляется, в силу изложенного выше это должен быть подход, подобный имеющемуся в уголовном законе Кыргызстана, – отказ от легальной конкретизации понятия «компьютерная информация».

Предметом компьютерных преступлений с точки зрения российского законодательства является не просто компьютерная информация, а компьютерная информация, охраняемая законом. В российском уголовном законе не перечисляются виды охраняемой законом информации. Федеральный закон «Об информации…» делит информацию на общедоступную и ограниченного доступа (ч. 2 ст. 5) [20]. В России 80 нормативных правовых актов устанавливают ограниченный доступ к информации [21]. Исходя из того, что уголовный закон оперирует термином «охраняемая законом компьютерная информация», можно предположить, что предметом преступления, предусмотренного ст. 272 УК РФ, является информация ограниченного доступа (термин ФЗ «Об информации»). Этой позиции придерживается Генеральная прокуратура РФ [19]. Судебная практика не столь однозначна. В некоторых случаях суды по собственному усмотрению устанавливают, является или не является компьютерная информация охраняемой законом. В частности, по делу В. В. Широкова апелляционная инстанция, опровергая довод стороны защиты о том, что ни органы предварительного расследования, ни суд первой инстанции не обосновали, к какой именно информации, из перечисленных в ФЗ «Об информации», осуществил неправомерный доступ осуждённый, указала, что факт отмены некоторых ведомственных приказов и изменения федеральных законов (вероятно, изменяющих статус информации, к которой имел доступ осужденный – *разъяснение А.В.*) «не влекут за собой декриминализацию общественно опасного деяния, за которое В. В. Широков осуждён» [39]. Словом, суд самостоятельно отнёс информацию к информации, охраняемой законом. Иногда, напротив, суды требуют от органов предварительного расследования подтверждения со ссылкой на закон, что компьютерная информация охраняется законом [43]. Встречаются решения диаметральные по пре-

ступлениям со схожими обстоятельствами объективной стороны. Гр. О. В. Никитин обвинялся в использовании интернет-ресурсов под логином и паролем бывшей супруги, которая после развода не сменила пароли, не запрещала их использовать и посещать ранее используемые ими совместно сайты. Уголовное преследование в отношении О. В. Никитина суд прекратил в связи с отсутствием в его действиях состава преступления. Суд указал, что не может считаться преступлением действие, хотя и содержащее признаки какого-либо деяния, но в силу малозначительности не представляющее общественной опасности [36]. При подобных обстоятельствах совершён доступ к компьютерной информации А.С. Лизуновым, которого осудили за совершение преступления, предусмотренного ч. 1 ст. 272 УК РФ [40].

В уголовных законах государств СНГ, за исключением Казахстана, наказуемость деяния не обусловлена неправомерным доступом *только к охраняемой законом* компьютерной информации. Несмотря на имеющееся терминологическое разнообразие в формулировках объективной стороны: неправомерный, несанкционированный, незаконный, самовольный доступы (см. ст. 271 УК Азербайджанской Республики, ст. 284 УК Грузии, ст. 251 Республики Армения, ст. 349 УК Республики Беларусь, ст. 205 Республики Казахстан, ст. 304 Республики Кыргызстан, ст. 259 УК Республики Молдова, ст. 298 УК Республики Таджикистан, ст. 278-2 УК Республики Узбекистан, ст. 361 УК Украины) [24; 25; 26; 27; 28; 29; 30; 31; 32; 34], фактически в государствах постсоветского пространства законодатель исходит из априорности защиты любой компьютерной информации (без уточнения, что информация охраняется законом), неправомерный доступ к которой повлёк предусмотренные законом последствия. Есть лишь различия в степени детализации того, что закон понимает под незаконным, несанкционированным, самовольным, неправомерным. На наш взгляд, наиболее интересна молдавская регламентация, в которой несанкционированный доступ – это отсутствие права у лица в силу закона или договора, либо превышение пределов разрешения, либо неполучение разрешения у правомочного лица на осуществление каких-либо операций в информационной системе, которые повлекли предусмотренные законом последствия (ст. 259 УК РМ) [30]. Привлекательность такой формулировки облегчает правоприменение, поскольку определение правомерности или неправомерности доступа не сводится к поиску соответствующей нормы в законе, а может быть установлено исходя из содержания соглашения, наличия или отсутствия дозволения собственника и т.п. Это важно, поскольку идеально прописать все виды охраняемой законом информации невозможно. К тому же означенный молдавский подход будет соответствовать российскому ФЗ «Об информации» (ст. 5) [20] и имеющейся судебной практике, особенно по преступлениям о неправомерном доступе к компьютерной информации, содержащей коммерческую тайну либо принадлежащей частному лицу, когда суды в приговорах подробно излагают характер взаимоотношений между работником и работодателем или частными лицами и пределы возможностей по использованию компьютерной информации [37; 41; 44].

С предметом компьютерных преступлений связана проблема ограничительного содержания понятия «охрана информации», которая сводится к соблюдению режима конфиденциальности, достоверности и своевременности её предоставления и оставляет без внимания доступность и целостность информации, которые также нуждаются в защите [16]. Конфиденциальность означает обязательное исполнение требования о неразглашении лицом, получившим доступ к охраняемым данным; доступность – это право доступа субъекта к компьютерной информации без каких-либо ограничений и изъятий. Целостность – это либо отсутствие изменения информации, либо допустимость её изменения только лицами, имеющими на это право. Даже в сравнении с изложенным стандартом, придерживающимся классической триады «конфиденциальность, целостность и доступность» (сокращенно – КЦД) или «confidentiality, integrity, availability» (сокращенно – CIA), который, по мнению специалистов, уже неактуален, закон минимизировал легальное содержание охраны информации, которое не соответствует уровню развития информационных технологий [10].

Выводы. Цифровая революция презюмирует необходимость совершенствования норм, регулирующих различные общественные отношения, возникающие в сфере компьютерной безопасности. Нормативная регламентация предмета преступления, предусмотренного ст. 272 УК РФ, позволяет констатировать, что, несмотря на корректировку понятия «охраняемая законом компьютерная информация», в законе есть ряд моментов, затрудняющих расследование и рассмотрение уголовных дел.

Желательно в закон внести следующие коррективы:

1. Отказаться в легальном определении компьютерной информации от использования технических терминов, которые затрудняют правоприменение.

2. Заменить имеющуюся формулировку предмета преступления «охраняемая законом компьютерная информация» на «компьютерная информация».

3. Расширить содержание понятия «неправомерный доступ к компьютерной информации», под которым предлагается понимать отсутствие у лица права на доступ к компьютерной информации в силу закона, договора, превышение пределов разрешения или отсутствие разрешения на доступ к компьютерной информации.

Устранение отмеченных недостатков нормативной регламентации предмета преступления (неправомерный доступ к охраняемой законом компьютерной информации), по нашему мнению, будет способствовать оптимизации расследования и разрешения уголовных дел, возбуждаемых по фактам совершения преступлений, предусмотренных ст. 272 УК РФ.

1. Ананиан Л.Л. Реферат к научно-практическому пособию Шурухнова Н.Г. «Расследование неправомерного доступа к компьютерной информации» // Право и информатизация общества: сб. научных трудов / отв. ред. И. Л. Бачило; Центр социальных науч.-инфор. исслед.; Отдел правоведения; РАН ИГП. Центр публичного права. Сектор информационного права. – Москва: Изд-во Института научной информации по общественным наукам РАН, 2002. – С. 294–297.

2. Быков В., Черкасов В. Понятие компьютерной информации как объекта преступлений // Законность. – 2013. – №12 (950). – С. 37–40.
3. Винокуров В. Н. Предмет преступления: отличие от смежных понятий // Журнал российского права. – 2011. – № 12. – С. 56–62.
4. Гавло В. К., Поляков В. В. Следовая картина и ее значение для расследования преступлений, связанных с неправомерным удаленным доступом к компьютерной информации // Российский юридический журнал. – 2007. – № 5 (57). – С. 146–152.
5. Дворецкий М.Ю. Проблемы толкования терминов при квалификации преступлений по ст. 272 Уголовного кодекса РФ // Вестник Тамбовского университета. Серия: Гуманитарные науки. – 2013. – № 12. – С. 527–532.
6. Ефремова М. А. Ответственность за неправомерный доступ к компьютерной информации по действующему уголовному законодательству // Вестник Казанского юридического института МВД России. – 2012. – № 2 (8). – С. 54–56.
7. Епифанов Б. В. Предмет преступления: понятие и проблемы правотворчества // Вестник Санкт-Петербургского университета МВД России. – 2015. – № 2(66). – С. 70–74.
8. Коровин Н. К. Тактические особенности следственного осмотра при расследовании неправомерного доступа к компьютерной информации // Проблемы современной науки и образования. – 2017. – № 7 (89). – С. 92–94.
9. Кузнецова Н. И. Объект преступления: некоторые размышления о понятии, значении, видах и отличии от предмета преступления // Юридическая наука: история и современность. – 2018. – №8. – С. 133–149.
10. Лукацкий А. В. Триада «конфиденциальность, целостность, доступность»: откуда она? – Текст: электронный // Информационный портал по безопасности: [сайт]. – URL: https://www.securitylab.ru/blog/personal/Business_without_danger/24456.php (дата обращения: 08.05.2020).
11. Неймарк М. А. Некоторые способы хищений денежных средств путем неправомерного доступа к компьютерной информации банков // Сборник материалов криминалистических чтений. – Барнаул: Изд-во Барнаульского юридического института МВД РФ. – 2006. – №2. – С. 29–31.
12. Панфилова Е. И., Попов А. Н. Компьютерные преступления. Серия «Современные стандарты в уголовном праве и уголовном процессе» / науч. ред. проф. Б. В. Волженкин. – Санкт-Петербург: Институт Генеральной прокуратуры Российской Федерации, 1998. – 48 с.
13. Таций В. Я. Предмет преступления // Известия высших учебных заведений. Правоведение. – 1984. – №4. – С. 51-57.
14. Шевченко В. Ю. Объект и предмет преступления // Современная наука. – 2013. – № 1. – С. 17–22.
15. Базовые понятия цифровой электроники. – Текст: электронный // Национальный открытый университет ИНТУИТ: [сайт]. – URL: https://www.intuit.ru/studies/courses/104/104/lecture/3029 (дата обращения: 08.05.2020).
16. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – Текст: электронный // Электронный фонд правовой и научно-технической документации: [сайт]. – URL: http://dehack.ru/zak_akt/standart/gost_r_50922-2006/ (дата обращения: 08.05.2020).
17. ГОСТ 16465-70. Межгосударственный стандарт. Сигналы радиотехнические измерительные. Термины и определения. – Текст: электронный // Электронный фонд правовой и научно-технической документации: [сайт]. – URL: http://docs.cntd.ru/document/gost-16465-70 (дата обращения: 08.05.2020).

18. Краткая характеристика состояния преступности за январь – декабрь 2019 года. Состояние преступности (архивные данные). – Текст: электронный // Министерство внутренних дел Российской Федерации: [сайт]. – URL: https://xn--b1aew.xn--p1ai/reports/1/ (дата обращения: 27.04.2020).
19. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации: утв. Генпрокуратурой России. – Текст: электронный // СПС «КонсультантПлюс»: [сайт]. – URL: http://www.consultant.ru/document/cons_doc_LAW_161817/ (дата обращения: 08.05.2020).
20. Об информации, информационных технологиях и о защите информации: федеральный закон от 27.07.2006 № 149-ФЗ (ред. 03.04.2020). – Текст: электронный // СПС «КонсультантПлюс»: [сайт]. – URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 26.04.2020).
21. Перечень нормативных актов, относящих сведения к категории ограниченного доступа. – Текст: электронный // СПС «КонсультантПлюс»: [сайт]. – URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=93980&fld=134&dst=1000000001,0&rnd=0.2132412527499723#04276956757057855 (дата обращения: 01.05.2020).
22. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (Минск, 1 июня 2001 г.). – Текст: электронный // СПС «Гарант»: [сайт]. – URL: http: // base.garant.ru/12123778/ (дата обращения: 05.05.2020).
23. Судебная статистика. – Текст: электронный // Судебный Департамент Верховного Суда Российской Федерации: [сайт]. – URL: http://www.cdep.ru (дата обращения: 26.04.2020).
24. Уголовный кодекс Азербайджанской Республики от 26.015.2000 №886-IQ (с изм. и доп. на 09.07.2019). – Текст: электронный // ИС «Параграф»: [сайт]. – URL: https://online.zakon.kz/Document/?doc_id=30420353 (дата обращения: 27.04.2020).
25. Уголовный кодекс Грузии от 22.07.1999 № 2287-вс. – Текст: электронный // Законодательный вестник Грузии: [сайт]. – URL: http://www.matsne.gov.ge (дата обращения: 27.04.2020).
26. Уголовный кодекс Кыргызской Республики от 24.01.2017 № 10 (с изм. и доп. на 03.04.2020). – Текст: электронный // ИС «Параграф»: [сайт]. – URL: https://online.zakon.kz/document/?doc_id=34350840 (дата обращения: 27.04.2020).
27. Уголовный кодекс Республики Армения от 18.04.2003 (с изм. и доп. на 19.04.2020 №ЗР-207). – Текст: электронный // ИС «Законодательство стран СНГ»: [сайт]. – URL: http://base.spinform.ru/show_doc.fwx?rgn=7472 (дата обращения: 10.05.2020).
28. Уголовный кодекс Республики Беларусь от 09.07.1999 № 275-З (с изм. и доп. по сост. на 11.11.2019). – Текст: электронный // ИС «Параграф»: [сайт]. – URL: https://online.zakon.kz/document/?doc_id=30414984#pos=2958;-45 (дата обращения: 27.04.2020).
29. Уголовный кодекс Республики Казахстан от 03.07.2014 № 226-V ЗРК (с изм. и доп. по сост. на 11.01.2020.). – Текст: электронный // ИС «Параграф»: [сайт]. – URL: https://online.zakon.kz/document/?doc_id=31575252 (дата обращения: 27.04.2020).
30. Уголовный кодекс Республики Молдова от 18.04.2002 № 985-XV (с изм. и доп. по сост. на 12.03.2020.). – Текст: электронный // ИС «Параграф»: [сайт]. – URL: https://online.zakon.kz/document/?doc_id=30394923 (дата обращения: 27.04.2020).

31. Уголовный кодекс Республики Таджикистан от 21.05.1998 № 574 (с изм. и доп. по сост. на 02.01.2020) – Текст: электронный // ИС «Континент»: [сайт]. – URL: http://continent-online.com/Document/?doc_id=30397325 (дата обращения: 27.04.2020).
32. Уголовный кодекс Республики Узбекистан (утв. Законом Республики Узбекистан от 22.09.1994 № 2012-XII) (с изм. и доп. по сост. на 26.03.2020). – Текст: электронный // ИС «Параграф»: [сайт]. – URL: https://online.zakon.kz/document/?doc_id=30421110 (дата обращения: 27.04.2020).

Транслитерация

1. Ananian L.L. Referat k nauchno-prakticheskomu posobiyu SHuruhnova N.G. «Rassledovanie nepravomernogo dostupa k komp'yuternoj informacii» // Pravo i informati-zaciya obshchestva: sb. nauchnyh trudov / otv. red. I. L. Bachilo; Centr social'nyh na-uch.-infor. issled.; Otdel pravovedeniya; RAN IGP. Centr publichnogo prava. Sektor informacionnogo prava. – Moskva: Izd-vo Instituta nauchnoj informacii po ob-shchestvennym naukam RAN, 2002. – S. 294–297.
2. Bykov V., CHerkasov V. Ponyatie komp'yuternoj informacii kak ob"ekta prestuple-nij // Zakonnost'. – 2013. – №12 (950). – S. 37–40.
3. Vinokurov V. N. Predmet prestupleniya: otlichie ot smezhnyh ponyatij // ZHurnal ros-sijskogo prava. – 2011. – № 12. – S. 56–62.
4. Gavlo V. K., Polyakov V. V. Sledovaya kartina i ee znachenie dlya rassledovaniya pre-stuplenij, svyazannyh s nepravomernym udalennym dostupom k komp'yuternoj in-formacii // Rossijskij yuridicheskij zhurnal. – 2007. – № 5 (57). – S. 146–152.
5. Dvoreckij M.YU. Problemy tolkovaniya terminov pri kvalifikacii prestuplenij po st. 272 Ugolovnogo kodeksa RF // Vestnik Tambovskogo universiteta. Seriya: Gu-manitarnye nauki. – 2013. – № 12. – S. 527-532.
6. Efremova M. A. Otvetstvennost' za nepravomernyj dostup k komp'yuternoj infor-macii po dejstvuyushchemu ugolovnomu zakonodatel'stvu // Vestnik Kazanskogo yuri-dicheskogo instituta MVD Rossii. – 2012. – № 2 (8). – S. 54–56.
7. Epifanov B. V. Predmet prestupleniya: ponyatie i problemy pravotvorchestva // Vest-nik Sankt-Peterburgskogo universiteta MVD Rossii. – 2015. – № 2(66). – S. 70–74.
8. Korovin N. K. Takticheskie osobennosti sledstvennogo osmotra pri rassledovanii nepravo-mernogo dostupa k komp'yuternoj informacii // Problemy sovremennoj nauki i obra-zovaniya. – 2017. – № 7 (89). – S. 92–94.
9. Kuznecova N. I. Ob"ekt prestupleniya: nekotorye razmyshleniya o ponyatii, znache-nii, vidah i otlichii ot predmeta prestupleniya // Yuridicheskaya nauka: istoriya i so-vremennost'. – 2018. – № 8. – S. 133–149.
10. Lukackij A. V. Triada «konfidencial'nost', celostnost', dostupnost'»: otkuda ona? – Tekst: elektronnyj // Informacionnyj portal po bezopasnosti: [sajt]. – URL: https://www.securitylab.ru/blog/personal/Business_without_danger/24456.php (data obrashcheniya: 08.05.2020).
11. Nejmark M. A. Nekotorye sposoby hishchenij denezhnyh sredstv putem nepravomer-nogo dostupa k komp'yuternoj informacii bankov // Sbornik materialov krimina-listicheskih chtenij. – Barnaul: Izd-vo Barnaul'skogo yuridicheskogo instituta MVD RF. – 2006. – № 2. – S. 29–31.
12. Panfilova E. I., Popov A. N. Komp'yuternye prestupleniya. Seriya «Sovremennye standarty v ugolovnom prave i ugolovnom processe» / nauch. red. prof. B. V. Volzhenkin. – Sankt-Peterburg: Institut General'noj prokuratury Rossijskoj Federacii, 1998. – 48 s.
13. Tacij V. Ya. Predmet prestupleniya // Izvestiya vysshih uchebnyh zavedenij. Pravove-denie. – 1984. – № 4. – S. 51–57.

14. SHevchenko V. Yu. Ob"ekt i predmet prestupleniya // Sovremennaya nauka. – 2013. – № 1. – S. 17–22.
15. Bazovye ponyatiya cifrovoj elektroniki. – Tekst: elektronnyj // Nacional'nyj ot-krytyj universitet INTUIT: [sajt]. – URL: https://www.intuit.ru/studies/ courses/104/104/lecture/3029 (data obrashcheniya: 08.05.2020).
16. GOST R 50922-2006. Zashchita informacii. Osnovnye terminy i opredeleniya. – Tekst: elektronnyj // Elektronnyj fond pravovoj i nauchno-tekhnicheskoj dokumen-tacii: [sajt]. – URL: http://dehack.ru/zak_akt/standart/gost_r_50922-2006/ (data obra-shcheniya: 08.05.2020).
17. GOST 16465-70. Mezhgosudarstvennyj standart. Signaly radiotekhnicheskie izmeri-tel'nye. Terminy i opredeleniya. – Tekst: elektronnyj // Elektronnyj fond pravo-voj i nauchno-tekhnicheskoj dokumentacii: [sajt]. –URL: http://docs.cntd.ru/document/gost-16465-70 (data obrashcheniya: 08.05.2020).
18. Kratkaya harakteristika sostoyaniya prestupnosti za yanvar' – dekabr' 2019 goda. Sostoyanie prestupnosti (arhivnye dannye). – Tekst: elektronnyj // Ministerstvo vnutrennih del Rossijskoj Federacii: [sajt]. – URL: https://xn--b1aew.xn--p1ai/reports/1/ (data obrashcheniya: 27.04.2020).
19. Metodicheskie rekomendacii po osushchestvleniyu prokurorskogo nadzora za ispolne-niem zakonov pri rassledovanii prestuplenij v sfere komp'yuternoj informacii: utv. Genprokuraturoj Rossii. – Tekst: elektronnyj // SPS «Konsul'tantPlyus»: [sajt]. – URL: http://www.consultant.ru/document/cons_doc_LAW_161817/ (data obra-shcheniya: 08.05.2020).
20. Ob informacii, informacionnyh tekhnologiyah i o zashchite informacii: federal'-nyj zakon ot 27.07.2006 № 149-FZ (red. 03.04.2020). – Tekst: elektronnyj // SPS «Konsul'tantPlyus»: [sajt]. – URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (data obrashcheniya: 26.04.2020).
21. Perechen' normativnyh aktov, otnosyashchih svedeniya k kategorii ogranichennogo dostupa. – Tekst: elektronnyj // SPS «Konsul'tantPlyus»: [sajt]. – URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=93980&fld=134&dst=1000000001,0&rnd=0.2132412527499723#04276956757057855 (data obrashcheniya: 01.05.2020).
22. Soglashenie o sotrudnichestve gosudarstv – uchastnikov Sodruzhestva Nezavisimyh Gosudarstv v bor'be s prestupleniyami v sfere komp'yuternoj informacii (Minsk, 1 iyunya 2001 g.). – Tekst: elektronnyj // SPS «Garant»: [sajt]. – URL: http: // base.garant.ru/12123778/ (data obrashcheniya: 05.05.2020).
23. Sudebnaya statistika. – Tekst: elektronnyj // Sudebnyj Departament Verhovnogo Suda Rossijskoj Federacii: [sajt]. – URL: http://www.cdep.ru (data obrashcheniya: 26.04.2020).
24. Ugolovnyj kodeks Azerbajdzhanskoj Respubliki ot 26.015.2000 №886-IQ (s izm. i dop. na 09.07.2019). – Tekst: elektronnyj // IS «Paragraf»: [sajt]. – URL: https://online.zakon.kz/Document/?doc_id=30420353 (data obrashcheniya: 27.04.2020).
25. Ugolovnyj kodeks Gruzii ot 22.07.1999 № 2287-vs. – Tekst: elektronnyj // Zakonodatel'nyj vestnik Gruzii: [sajt]. – URL: http://www.matsne.gov.ge (data obrashcheniya: 27.04.2020).
26. Ugolovnyj kodeks Kyrgyzskoj Respubliki ot 24.01.2017 № 10 (s izm. i dop. na 03.04.2020). – Tekst: elektronnyj // IS «Paragraf»: [sajt]. – URL: https://online.zakon.kz/document/?doc_id=34350840 (data obrashcheniya: 27.04.2020).
27. Ugolovnyj kodeks Respubliki Armeniya ot 18.04.2003 (s izm. i dop. na 19.04.2020 №ZR-207). – Tekst: elektronnyj // IS «Zakonodatel'stvo stran SNG»: [sajt]. – URL: http://base.spinform.ru/show_doc.fwx?rgn=7472 (data obrashcheniya: 10.05.2020).

28. Ugolovnyj kodeks Respubliki Belarus' ot 09.07.1999 № 275-Z (s izm. i dop. po sost. na 11.11.2019). – Tekst: elektronnyj // IS «Paragraf»: [sajt]. – URL: https://online.zakon.kz/document/?doc_id=30414984#pos=2958;-45 (data obrashcheniya: 27.04.2020).
29. Ugolovnyj kodeks Respubliki Kazahstan ot 03.07.2014 № 226-V ZRK (s izm. i dop. po sost. na 11.01.2020.). – Tekst: elektronnyj // IS «Paragraf»: [sajt]. – URL: https://online.zakon.kz/document/?doc_id=31575252 (data obrashcheniya: 27.04.2020).
30. Ugolovnyj kodeks Respubliki Moldova ot 18.04.2002 № 985-XV (s izm. i dop. po sost. na 12.03.2020.). – Tekst: elektronnyj // IS «Paragraf»: [sajt]. – URL: https://online.zakon.kz/document/?doc_id=30394923 (data obrashcheniya: 27.04.2020).
31. Ugolovnyj kodeks Respubliki Tadzhikistan ot 21.05.1998 № 574 (s izm. i dop. po sost. na 02.01.2020) – Tekst: elektronnyj // IS «Kontinent»: [sajt]. – URL: http://continent-online.com/Document/?doc_id=30397325 (data obrashcheniya: 27.04.2020).
32. Ugolovnyj kodeks Respubliki Uzbekistan (utv. Zakonom Respubliki Uzbekistan ot 22.09.1994 № 2012-XII) (s izm. i dop. po sost. na 26.03.2020). – Tekst: elektronnyj // IS «Paragraf»: [sajt]. – URL: https://online.zakon.kz/document/?doc_id=30421110 (da-ta obrashcheniya: 27.04.2020).

Для цитирования: Верещагина А.В. К вопросу о предмете неправомерного доступа к компьютерной информации // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. – 2020. – Т. 12, № 2. – С. 103–117.

For citation: Vereschagina A.V. On the subject of unauthorized access to computer information, *The Territory of New Opportunities. The Herald of Vladivostok State University of Economics and Service*, 2020, Vol. 12, № 2, pp. 103–117.

DOI dx.doi.org/10.24866/VVSU/2073-3984/2020-2/103-117

Дата поступления: 12.05.2020.