УДК 343.3/7
DOI https://doi.org/10.17308/vsu.proc.law.2021.1/3295

ЛОГИКО-ЯЗЫКОВЫЕ ФЕНОМЕНЫ, АККУМУЛИРУЮЩИЕ В СВОИХ ЗНАЧЕНИЯХ ПРЕДМЕТ СОСТАВА НЕПРАВОМЕРНОГО ВОЗДЕЙСТВИЯ НА КРИТИЧЕСКУЮ ИНФОРМАЦИОННУЮ ИНФРАСТРУКТУРУ РОССИИ (СТ. 274.1 УК РФ)

И. Г. Пыхтин

Юго-Западный государственный университет (г. Курск)

Поступила в редакцию 26 октября 2020 г.

Аннотация: *обращается внимание на сложность юридико-технической конструкции уголовно-правовой нормы, предусматривающей ответственность и наказание за неправомерное посягательство на важнейшие объекты информационной инфраструктуры страны, а также на проблему правопонимания некоторых логико-языковых феноменов, относящихся к архитектуре состава ст. 274.1 УК РФ. В частности, отмечается, что «компьютерная информация» как предмет преступления, предусмотренный ст. 274.1 УК РФ, нуждается в теоретическом обосновании своей материальной природы как вещи, материальной субстанции, которая является признаком предмета любого общественно опасного деяния.*
Ключевые слова: *компьютерная информация, критическая информационная инфраструктура, неправомерное воздействие, защита информации, состав преступления, предмет преступления.*

Abstract: *the author draws attention to the complexity of the legal and technical construction of the criminal law norm providing for liability and punishment for unlawful encroachment on the most important objects of the country's information infrastructure, as well as the problem of legal understanding of some logical and linguistic phenomena related to the architecture of Art. 274[1] Criminal code of the Russian Federation. In particular, it is noted that "computer information" as the subject of a crime under Art. 274[1] of the Criminal Code of the Russian Federation needs a theoretical substantiation of its material nature as a thing, a material substance, which is a sign of the subject of any socially dangerous act.*
Key words: *computer information, critical information infrastructure, illegal influence, information protection, corpus delicti, subject of crime.*

Проблемы, связанные с посягательством на критическую информационную инфраструктуру, в отечественном праве стали исследоваться недавно. Это связано, в первую очередь, с реализацией основных направлений и стратегий государственной политики России в области экономического и социально-политического развития Российской Федерации, а также разработкой и защитой современных цифровых и информационных технологий, используемых в критической информационной инфраструктуре.

Уголовно-правовая защита наиболее значимых объектов информационной инфраструктуры России от общественно опасных посягательств осуществляется с помощью ст. 274.1 УК РФ, предусматривающей ответ-

ственность и наказание за неправомерное воздействие на критическую информационную инфраструктуру страны[1]. Данная норма состоит из пяти частей. Анализ диспозиций первой, второй и третей части показывает, что они представлены различными, не похожими друг на друга, составами преступлений бланкетного характера, предусматривающими уголовную репрессию за создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации (ч. 1 ст. 274.1 УК РФ); неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре России (ч. 2 ст. 274.1 УК РФ); нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации (ч. 3 ст. 274.1 УК РФ). Иными словами, мы встречаем норму с триединым составом преступления (или с тремя формами одного и того же вида неправомерного воздействия на значимые объекты информационной инфраструктуры), каждый из которых может выступать и квалифицироваться отдельно друг от друга либо выступать совокупно. В целом же ст. 274.1 УК РФ определяется уголовно-правовая охрана критической информационной инфраструктуры в широком смысле, которая выражается в привлечении виновных лиц к уголовной ответственности и назначении им наказания за неправомерное воздействие на охраняемую компьютерную информацию, объекты информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления субъектов критической информационной инфраструктуры, а также сетей электросвязи, используемых для организации взаимодействия особо значимых объектов информационной инфраструктуры страны.

Установлено, что состав неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ) по своим признакам соответствует тем доминантам, которые мы обнаруживаем в преступлениях, предполагающих уголовную ответственность за преступления в сфере компьютерной информации (глава 28 УК РФ, ст. 272–274). Отличительной особенностью ст. 274.1 УК РФ от вышеуказанных норм уголовного закона является существенное различие в предмете преступления. В первом случае (ст. 274.1) предметом преступления выступает компьютерная информация, содержащаяся в критической информационной инфраструктуре России, а во втором случае (ст. 272–274) предметом преступления является компьютерная информация безотносительно субъекта владения и места ее расположения).

[1] О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» : федер. закон от 26 июля 2017 г. № 194-ФЗ // Собр. законодательства Рос. Федерации. 2017. № 31 (ч. 1). Ст. 4743.

Отличают анализируемую уголовно-правовую норму от всех других норм уголовного закона о преступлениях в сфере компьютерной информации и санкции, предусматривающие наказание и по своей строгости превышающие в два-три раза те, которые предусмотрены за «аналогичные» деяния, но не связанные с неправомерным воздействием на критическую часть информационной инфраструктуры России. Например, если за неправомерный доступ к компьютерной информации (ч. 1 ст. 272) любого объекта жизнеобеспечения в стране предусмотрено максимальное наказание в виде двух лет лишения свободы, то за аналогичное преступление, посягающее на критическую сферу жизнедеятельности страны (ч. 2 ст. 274.1), наказание может быть назначено до шести лет лишения свободы.

Согласно правилам квалификации преступлений можно заключить, что ст. 274.1 по отношению к ст. 272–274 УК РФ, имеющим общий характер, выступает в качестве специальной нормы. Следовательно, если преступные деяния, предусмотренные в ст. 272–274, будут аналогичны тем, которые указаны в ч. 1–3 ст. 274.1, но предметом преступления будет являться компьютерная информация, размещенная в критической информационной инфраструктуре России, квалифицировать такое общественно опасное деяние необходимо по соответствующей части ст. 274.1 УК РФ.

Диспозиция анализируемой уголовно-правовой нормы носит бланкетный характер, который присущ всем трем формам неправомерного воздействия на критически важные объекты информационной инфраструктуры (ч. 1–3 ст. 274.1), на что указывают такие логико-языковые образования, как: «компьютерная информация», «компьютерные программы», «информационно-телекоммуникационные сети», «сети электросвязи», «критическая информационная инфраструктура» и другие понятия, большинству из которых уголовный закон определений не дает. Перечисленные выше логико-языковые феномены типичны для научно-технической, цифровой и информационной сферы, поэтому их дефиниции содержатся в нормативно-правовых актах, непосредственно регулирующих отношения в области защиты информации, информационных технологий, обеспечения безопасности критической информационной инфраструктуры и иных общностей правового регулирования[2]. Ученые подчеркивают, что подобная конструкция диспозиции ст. 274.1 УК РФ затрудняет единообразное понимание определения связи предмета неправомерного воздействия именно на критическую информационную

[2] Об информации, информационных технологиях и о защите информации : федер. закон от 27 июля 2006 г. № 149-ФЗ (в ред. от 03.04.2020) // Собр. законодательства Рос. Федерации. 2006. № 31 (ч. 1). Ст. 3448 ; О Стратегии развития информационного общества в Российской Федерации на 2017–2030 гг. : указ Президента РФ от 9 мая 2017 г. № 203 // Там же. 2017. № 20. Ст. 2901 ; О безопасности критической информационной инфраструктуры Российской Федерации : федер. закон от 26 июля 2017 г. № 187-ФЗ // Там же. № 31 (ч. 1). Ст. 4736.

инфраструктуру, а не на иной спектр информационных отношений[3]. Добавим также, что большинство языковых объектов, содержащихся в описании той или иной формы неправомерного воздействия на критическую информационную инфраструктуру, являются оценочными, достаточно сложными для понимания и не отражают завершенности в определении всех признаков преступного деяния. Технические и информационные определения, которые оптимальны и понятны для специалистов соответствующих отраслей научно-прикладного знания, в анализируемом контексте слабо приспособлены для технико-юридических конструкций в уголовном законе и усложняют процесс квалификации преступлений[4]. Поэтому подобные определения, которые отсылают правоприменителя к нормам иных отраслей права, нуждаются в единообразном понимании и толковании. Более того, отдельные из приведенных выше терминов в различных правовых документах закреплены не единожды и при этом отличаются друг от друга. Например, в Доктрине информационной безопасности Российской Федерации 2016 г. под определение критической информационной инфраструктуры подпадает вся совокупность объектов информатизации, информационных систем, сайтов в сети «Интернет» и сетей связи. Однако не все вышеназванные объекты и системы можно считать критическими, а только те, которые расположены на территории нашей страны, на территориях, находящихся под юрисдикцией России или используемых на основании международных договоров Российской Федерации[5]. В принятой «Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» критическая информационная инфраструктура уже представлена как совокупность объектов критической информационной инфраструктуры, а в Федеральном законе 2017 г. «О безопасности критической информационной инфраструкту-

[3] См.: *Дремлюга Р. И., Зотов С. С., Павлинская В. Ю.* Критическая информационная инфраструктура как предмет преступного посягательства // Азиатско-Тихоокеанский регион : экономика, политика, право. Владивосток, 2019. Т. 2. С. 135 ; *Кругликов Л. Л., Соловьев О. Г., Бражник С. Д.* Ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ) в системе экономической и информационной безопасности государства // Вестник ЯрГУ. Серия: Гуманитарные науки. 2019. № 4 (50). С. 52 ; *Шульга А., Галиакбаров Р.* Уголовная ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ) // Гуманитарные, социально-экономические и общественные науки. 2018. № 5. С. 240.

[4] См.: *Бегишев И. Р., Бикеев И. И.* Преступления в сфере обращения цифровой информации. Казань, 2020. С. 40 ; *Русскевич Е. А.* Об уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК России) // Законы России : опыт, анализ, практика. 2018. № 2. С. 52.

[5] Об утверждении Доктрины информационной безопасности Российской Федерации : указ Президента РФ от 5 декабря 2016 г. № 646 // Собр. законодательства Рос. Федерации. 2016. № 50. Ст. 7074.

ры Российской Федерации» это же понятие ограничено только объектами критической информационной инфраструктуры[6].

Кроме того, «Стратегия развития информационного общества…» перечисляет объекты и субъектов критической информационной инфраструктуры России, отнеся к первым: информационные системы и информационно-телекоммуникационные сети, а также информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления технологическими процессами, а ко вторым причислены: государственные органы и учреждения, а также объекты оборонной промышленности, сферы здравоохранения, транспорта, связи, кредитно-финансовой сферы; энергетика; топливная, атомная, ракетно-космическая, горнодобывающая, металлургическая и химическая промышленность[7]. Принятый в этом же году нормативно-правовой акт, регулирующий безопасность критической информационной инфраструктуры Российской Федерации[8], добавляет к списку субъектов еще и отечественных юридических лиц и индивидуальных предпринимателей, которым на законном основании принадлежат перечисленные в «Стратегии…» объекты критической информационной инфраструктуры, а также объекты науки, банковская сфера и сфера финансового рынка. Документом «О безопасности критической информационной инфраструктуры Российской Федерации» устанавливается соответствие указанных выше объектов критической информационной инфраструктуры критериям значимости с присвоением одной из трех категорий.

Очевидно, что лишь одно перечисление в нормативно-правовых документах объектов и субъектов критической информационной инфраструктуры указывает на такое их многообразие, которое, по существу, охватывает все государственные и частные управленческие, а также иные структуры и сферы жизнедеятельности общества и государства. К примеру, федеральным законом определено, что к сетям электросвязи, используемым для организации взаимодействия таких объектов, относятся: а) средства связи, т. е. технические и программные средства, используемые для формирования, приема, обработки, хранения, передачи, доставки сообщений электросвязи или почтовых отправлений, а также иные технические и программные средства, используемые при оказании услуг связи или обеспечении функционирования сетей связи, включая технические системы и устройства с измерительными функциями; б) линии

[6] О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы : указ Президента РФ от 9 мая 2017 г. № 203 // Собр. законодательства Рос. Федерации. 2017. № 20. Ст. 2901 ; О безопасности критической информационной инфраструктуры Российской Федерации : федер. закон от 26 июля 2017 г. № 187-ФЗ // Там же. № 31 (ч. 1). Ст. 4736.

[7] Пункт «м» ст. 4 Указа Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы».

[8] Пункт 7–8 ст. 2 и ч. 1 ст. 7 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

связи, к которым относятся линии передачи, физические цепи и линейно-кабельные сооружения связи, предназначенные для электросвязи или почтовой связи[9].

Анализируя официальные определения рассматриваемых нами феноменов, ученые полагают, что все объекты, отрасли, сферы деятельности управления и обеспечения хозяйством страны могут быть отнесены к объектам критической информационной инфраструктуры («круг субъектов КИИ даже представить сложно»)[10]. Так, на 6 августа 2020 г. из более чем 30 тыс. значимых объектов критической информационной инфраструктуры России в Федеральной службе по техническому и экспортному контролю прошли лицензирование и включены в соответствующий реестр категорий 3794 объекта, обеспечивающих техническую защиту информации, и 1959 объектов по разработке и производству средств защиты конфиденциальной информации критической информационной инфраструктуры[11].

«Компьютерная информация» как предмет преступления не совпадает с классическим понятием «предмета преступления» как материальной субстанции внешнего мира. Никакая иная его причастность и принадлежность в теории уголовного права не рассматривалась до тех пор, пока «информация» и ее виды не стали объектами общественных отношений и «предметом» преступных посягательств.

Между тем в современном мире компьютерная информация, разноаспектная по своей сути, в известной мере, является составной частью общества, государства и различных субъектов управления информационной инфраструктурой.

В дискуссиях по вопросам содержания и овеществления компьютерной информации (как предмета преступления) ученые принципиально соглашаются с тем, что у различных видов информации наличествует существенная мимикрия, например между лексическими символами, фиксируемыми в текстах, и комбинациями двоичных цифр (0 и 1) в программах для ЭВМ, а также между последовательной работой над лексемами формального языка, с его формальной грамматикой и разработкой компьютерных программ, основанных на комбинациях двоичных цифр (0 и 1), впоследствии выступающих в качестве «компьютерного языка»[12]. В том и другом случае в итоге возникают структуры данных или сведе-

[9] О связи : федер. закон от 7 июля 2003 г. № 126-ФЗ (в ред. от 07.04.2020) // Собр. законодательства Рос. Федерации. 2003. № 28. Ст. 2895.

[10] См.: *Кругликов Л. Л., Соловьев О. Г., Бражник С. Д.* Указ. соч. С. 51.

[11] Федеральная служба по техническому и экспортному контролю. Документы по лицензионной деятельности ФСТЭК России. URL: https://fstec.ru/normotvorcheskaya/litsenzirovanie/72-reestry

[12] См.: *Кагиров И. А., Леонтьева А. Б.* Автоматический синтаксический анализ русских текстов на основе грамматики составляющих // Известия высших учебных заведений. Приборостроение. 2008. Т. 51, № 11. С. 48 ; *Ромашов Р. А., Панченко В. Ю.* О соотношении материального и виртуального в современной правовой реальности // Юридическая наука. 2017. № 1. С. 30.

ний, удобных для последующей обработки (например, в виде синтаксического дерева или компьютерной информации).

Уголовно-правовое содержание компьютерной информации раскрывается в первом примечании к ст. 272 УК РФ и касается всех норм главы о преступлениях в сфере компьютерной информации. В примечании определено, что указанный вид информации есть сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Такое определение согласовывается с общим легальным понятием «информация», не противоречит ему, одновременно уточняет формы ее представления, однако не перечисляет средства их хранения, обработки и передачи, по сути, оставляя перечень таких средств открытым. Последнее, на наш взгляд, связано с тем, что средства хранения, обработки и передачи компьютерной информации формируются, совершенствуются и постоянно развиваются. Например, такому прогрессу могут быть подвержены средства блокирования, переформатирования, поиска или извлечения информации, а кроме того, их эволюция не исключает поступательные движения по отдельным векторным процессам и направлениям научно-прикладного знания и унифицированного совершенствования.

Развернувшаяся в науке уголовного права дискуссия о «материальности-нематериальности» компьютерной информации, а также возможности либо невозможности считать ее в качестве предмета в составах преступлений в сфере компьютерной информации сводится к двум аспектам и, соответственно, к двум основным позициям специалистов. Первая позиция отражает мнение тех ученых, которые приводят свои аргументы в пользу того, что компьютерная информация, имея нематериальный характер, тем не менее может считаться предметом всех тех преступлений, которые закреплены в главе 28 УК РФ (ст. 272–274.1)[13]. Другой точки зрения придерживаются те ученые, которые полагают, что компьютерная информация и информация в любом ее проявлении не может быть предметом преступления в силу того, что она не материализована в качестве вещи.

Анализ уголовного закона показывает, что виртуальный характер той или иной информации давно наличествует в нормах российского уголовного закона. В ряде составов преступления для квалификации имеет значение именно информация, содержание которой определяется какими-либо сведениями, определяющими конкретный состав преступления (например, клевета, нарушение неприкосновенности частной жизни, незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну). Однако при том и другом подходе ученые столкнулись с проблемой признаков, которые в полной мере отражали бы определение (понятие) предмета преступления в сфе-

[13] См.: *Ястребов Д. А.* Международно-правовое сотрудничество государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации // Юридический мир. 2008. № 12. С. 75.

ре компьютерной информации. Исследователи, усматривающие материальную природу в предмете преступления в сфере компьютерной информации, исходят из того, что материальность компьютерной информации выражена в вариативной «двоичной цифре», в связи с чем, во-первых, правильнее было бы именовать предмет рассматриваемого преступления как «цифровая информация»; во-вторых, поскольку вариативный двоичный код компьютерной программы (0 и 1) в совокупности является не чем иным, как сосредоточением лексических данных, то материальный носитель программного обеспечения ЭВМ (на котором фиксируются информационные данные) будет считаться вещественной оболочкой информации, формой компьютерной информации. Таким образом, последняя приобретает материальное, вещественное выражение[14].

Соглашаясь в целом с материальной сущностью «компьютерной информации» хотелось бы уточнить и обосновать некоторые аспекты указанных «свойств» компьютерной информации.

Первое. Мы исходим из того, что конструирование того или иного научного понятия должно основываться на определенной философской концепции (материалистическая, идеалистическая или их дуалистическая онтология либо иные нетрадиционные, но научно обоснованные взгляды). При рассмотрении сущности компьютерной информации полагаем, что речь идет о «виртуализированых сведениях», понимание которых одновременно «наполнено объективным и субъективным содержанием, зависящим от современных и последующих временных философских подходов, а также научно-технических преобразований»[15].

Из сказанного следует, что определение «компьютерная информация» должно наполняться не только «материальным» содержанием, но и идеальным (не в понимании «должного», а в субъективным смысле) – подобным архитектуре понятия «состава преступления», совокупности объективных и субъективных признаков.

Второе. В теории термодинамики утверждается, что информация формально образуется движением атомно-молекулярных, химико-физических и иных процессов, происходящих в головном мозге человека (энтропия). Для того чтобы привести оба понятия к одной форме, информацию измеряют так же, как и энтропию, но только со знаком «минус» (в термодинамике речь идет о материальной частице – «психоне»)[16]. Следовательно, формально мы можем отождествить информацию как специфическую физическую, материализованную субстанцию, которая применительно к нашим рассуждениям может считаться предметом преступления.

Третье. При анализе понятия «компьютерная информация» обнаруживается наличие тех признаков, которые относятся к основным призна-

[14] См.: *Бегишев И. Р., Бикеев И. И.* Преступления в сфере обращения цифровой информации. Казань, 2020. С. 40.

[15] *Новичков В. Е.* Прогнозирование социально-правовых аспектов борьбы с преступностью (проблемы теории и практики). Курск, 2004. С. 46.

[16] См.: *Кобозев Н. И.* Исследования в области термодинамики процессов информации и мышления. М., 1971. С. 146.

кам «вещи» (предмета), например: а) внешнее выражение компьютерной информации определяется ее полезностью (априори или по умолчанию); б) принадлежностью компьютерной информации конкретному физическому либо юридическому лицу (субъекту); в) компьютерная информация обладает правом востребования, требования и оборотоспособности; г) понятие «компьютерная информация» наделено признаками визуального восприятия, осязаемостью, динамикой; д) материальностью, т. е. компьютерная информация, как любая вещь, имеет финансовую и материальную ценность. Иными словами, компьютерную информацию можно продать, купить, обменять, использовать для изменения материальных свойств того или иного предмета материального мира, извлекать ценностные свойства из любой вещи и т. п.

Отличительной особенностью предмета состава преступления, предусмотренного ст. 274.1 УК РФ, от иных составов преступлений, закрепленных в главе 28 уголовного закона, является то, что предметом преступления считается не компьютерная информация как таковая, на которую посягает виновное лицо, а только та компьютерная информация, которая содержится в критической информационной инфраструктуре Российской Федерации. Законодатель, указывая таким образом на отличие предмета неправомерного посягательства на критическую информационную инфраструктуру страны, вполне логично отграничил состав ст. 274.1 УК РФ от иных составов преступлений в сфере компьютерной информации. В связи с этим становится понятной и логика технико-юридической конструкции рассматриваемой уголовно-правовой нормы (ст. 274.1 УК РФ), архитектура которой состоит из трех форм, закрепленных в ч. 1–3 ст. 274.1 УК РФ. Поэтому, на наш взгляд, ст. 274.1 УК РФ вполне обоснованно представлена тремя самостоятельными составами преступлений (формами), предусматривающими в целом уголовную ответственность за неправомерное воздействие на критическую информационную инфраструктуру России.

Юго-Западный государственный университет (г. Курск)

Пыхтин И. Г., аспирант кафедры уголовного права

E-mail: abcqip@gmail.com

Southwest State University (Kursk)

Pykhtin I. G., Post-graduate Student of the Criminal Law Department

E-mail: abcqip@gmail.com