Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ): некоторые проблемы определения признаков состава преступления

Undue influence on the critical information infrastructure of the Russian Federation (article (Article 274.1 of the Criminal Code of the Russian Federation): some problems of definition of signs of a crime

Кругликов Л.Л.
Д-р юрид. наук, профессор кафедры уголовного права и криминологии юридического факультета Ярославского государственного университета им. П.Г. Демидова, заслуженный деятель науки Российской Федерации, кавалер медали ордена «За заслуги перед отечеством» II степени и знака отличия «За заслуги перед городом Ярославлем».
e-mail: krugliko@uniyar.ac.ru

Kruglikov L.L.
Doctor of Law, Professor of The Criminal Law and Criminology department, Honored Scientist of the Russian Federation, Holder of the Order of Merit for the Fatherland, II degree and the distinction of Merit for the City of Yaroslavl, Demidov Yaroslavl State University
e-mail: krugliko@uniyar.ac.ru

Бражник С.Д.
Канд. юрид. наук, доцент кафедры уголовного права и криминологии юридического факультета Ярославского государственного университета им. П.Г. Демидова
e-mail: bsd2009@mail.ru

Brazhnik S.D.
Candidate of Law, Associate Professor of the Criminal Law and Criminology Department, Demidov Yaroslavl State University
e-mail: bsd2009@mail.ru

Пилясов И.А.
Консультант Ярославского Центра экономического и налогового просвещения Ярославского государственного университета им. П.Г. Демидова
e-mail: pilyasov1999@yandex.ru

Pilyasov I.A.
Consultant of the Yaroslavl Center for Economic and Tax Education, Demidov Yaroslavl State University
e-mail: pilyasov1999@yandex.ru

Аннотация
Статья посвящена анализу новеллы отечественного уголовного законодательства об ответственности за неправомерное воздействие на объекты критической информационной инфраструктуры Российской Федерации, принятой Федеральным законом от 26 июля 2017 г. N 194-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» и

ст. 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации».
Итогом проведенного анализа является вывод об имеющихся недостатках, возникших при реформировании уголовного законодательства, и предложения по их устранению.
Ключевые слова: информационная безопасность, критическая информационная инфраструктура Российской Федерации, киберпреступность, инфраструктура, компьютерные технологии.

Abstract
The article is devoted to the analysis of the novel of the domestic criminal legislation on liability for unlawful impact on the objects of the critical information infrastructure of the Russian Federation, adopted by Federal Law No. 194-ФЗ dated July 26, 2017 «On Amendments to the Criminal Code of the Russian Federation and article 151 of the Criminal Procedure Code of the Russian Federation in connection with the adoption of the Federal Law «On the Security of the Critical Information Infrastructure of the Russian Federation».
The result of the analysis is the conclusion of the existing shortcomings which have arisen in the reform of criminal legislation, and proposals to eliminate them.
Keywords: information security, risk, cybercrime, infrastructure, computer technology.

Состояние информационной безопасности является одной из составляющих национальной безопасности и характеризуется постоянным повышением сложности, увеличением масштабов и ростом скоординированности компьютерных атак, в том числе и на объекты критической информационной инфраструктуры (КИИ)[1]. По мнению специалистов в области кибербезопасности, количество кибератак на объекты КИИ увеличивается с каждым годом [1].

По информации заместителя директора Национального координационного центра по компьютерным инцидентам Н. Мурашова только в 2018 г. на Россию было совершено более 4,3 млрд кибератак (*p.s.: не описка*) на КИИ. Семнадцать тысяч из них – были признаны наиболее опасными. В 2017 г. их число было почти в два раза меньше (2,4 млрд случаев кибератак, 12 тыс. из них – признаны наиболее опасными) [2]. По данным, озвученным секретарем Совета Безопасности РФ Н. Патрушевым, в 2016 г. было зафиксировано около 52,5 млн кибератак на сайты госорганов (в 2015 г. – 14,4 млн). Он отметил, что «защищенность информационных систем от компьютерных атак и средств компьютерной разведки остается недостаточной и в большинстве случаев не отвечает существующим угрозам» [3].

В связи с нарастанием угроз применения информационных технологий и в целях безопасности функционирования информационных и телекоммуникационных систем критически важных объектов инфраструктуры законодатель в 2017 г. криминализировал неправомерное воздействие на КИИ РФ (ст. 274.1 УК).

Не сомневаясь в целесообразности усиления охраны наиболее важных объектов, так называемых критически важных объектов (военные объекты, предприятия, обеспечивающие жизнеобеспечение целых территорий, объекты энергетики (в первую очередь, атомной), транспорт, в первую очередь, воздушный и т.д.)), в том числе и объектов КИИ РФ, анализ нормы дает основание утверждать, что законодатель сделал это, скажем мягко, не совсем хорошо. Норму, с полным основанием, можно отнести в категорию так называемых «мертворожденных», «которые изначально в момент своего создания и закрепления в законе не могли претендовать на широкое применение; качество и культура технического оформления нормы, при котором, возможно, объективно необходимый запрет конструируется таким образом, что лишает правоприменителя возможности не только применять,

[1]Здесь и далее под КИИ понимается критическая информационная инфраструктура.

но и адекватно понимать содержание нормы» [4, с. 8]. Некоторые из критических замечаний уже были высказаны специалистами [5], мы продолжим анализ.

Совершенно не случайно поэтому, как нам представляется, несмотря на динамичный рост числа киберпреступлений в мире и неимоверное количество компьютерных атак на отечественные объекты, количество лиц, ежегодно привлекаемых к уголовной ответственности в России за совершение в сфере компьютерной информации, остается незначительным. Количество же осужденных по ст. 274.1 УК, по данным Судебного департамента при Верховном Суде РФ, за 2018 г. равняется 0 [6].

Первое, что «бросается в глаза» – это чрезмерно широкое, на наш взгляд, законодательное формулирование объектов КИИ, где указывается, что, кроме, собственно, КИИ объекта, сюда входят сети электросвязи, например, и другие информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры [7]. Если следовать логике законодателя, то под объектами КИИ следует понимать некий технологический комплекс, включающий, в том числе и строения – хранилища информации, сети электрические, сети электросвязи, используемые для организации взаимодействия таких объектов.

В качестве примера подобного чрезмерно широкого формулирования определений можно привести ФЗ «О транспортной безопасности», который под объектами транспортной инфраструктуры понимает не только сами по себе транспортные средства (воздушные и морские суда, суда, используемые на внутренних водных путях, железнодорожный подвижной состав, автомобильный транспорт), но и включает сюда технологический комплекс железнодорожных вокзалов, автовокзалов и автостанций, тоннели, эстакады и мосты, морские терминалы, порты (расположенные как во внутренних морских водах, так и в исключительной экономической зоне и на континентальном шельфе РФ), аэродромы и аэропорты, объекты систем связи, навигации и управления движением транспортных средств, участки автомобильных дорог, железнодорожных и внутренних водных путей, вертодромы, посадочные площадки, а также иные обеспечивающие функционирование транспортного комплекса здания, сооружения, устройства и оборудование, определяемые Правительством РФ [8].

Это дает основание считать объектами КИИ все, что их «окружает» (электрические сети, сети электросвязи; автоматизированные системы управления субъектов критической информационной инфраструктуры). В итоге мы «выйдем» на то, что у нас почти все отрасли, без исключения и даже предприятия, их обеспечивающие (например, электроэнергией, связью) будут влиять на национальную безопасность, обороноспособность и выживаемость страны.

Во-вторых, настораживает законодательное формулирование субъектов КИИ [7], из которого следует, что субъектами КИИ могут быть не только органы государственной власти, организации и учреждения государственной власти и субъектов Российской Федерации (*курсив наш: в том числе: МО РФ, МИД РФ, все правоохранительные органы, банковская система и т.д.*), но и иные **юридические лица**, в том числе и **индивидуальные предприниматели**, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности или которые обеспечивают взаимодействие указанных систем или сетей.

Такой круг субъектов КИИ даже представить сложно, не то чтобы организовать какое-либо эффективное управление или взаимодействие. При этом, уполномоченным в области обеспечения безопасности КИИ определена Федеральная служба по техническому и экспортному контролю, со штатной численностью чуть больше 1.000 чел.!

В-третьих, следует заметить, что ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» предусматривает категорирование всех объектов в зависимости от социальной, политической, экономической значимости, а также значимости объекта КИИ для обеспечения обороны страны, безопасности государства и правопорядка. Во исполнение этого положения принят ряд нормативных актов. Это дает основание утверждать, что некоторые из объектов КИИ более важные, другие – менее важные. Из контекста обозначенных документов следует, что КИИ по категории значимости может быть не только первой, второй и третьей, но и без таковой, т.е. при «отсутствии необходимости присвоения ему одной из таких категорий» [9]. Меж тем, исходя из буквального толкования уголовного закона, все объекты КИИ, без исключения, нуждаются в уголовно-правовой защите. Действующая редакция ст. 274.1 УК не учитывает данное деление, что представляется существенным упущением с точки зрения дифференциации уголовной ответственности.

Вполне очевидным, на наш взгляд, является нарушение и межотраслевой дифференциации ответственности в случае неправомерного оборота КИИ без соответствующей категории. В настоящее время на Федеральном портале проектов нормативных правовых актов 26 марта 2019 г. размещено уведомление о начале разработки проекта федерального закона о внесении изменений в КоАП РФ в части установления ответственности за нарушение требований по обеспечению безопасности объектов КИИ в случае, когда имело место несоблюдение указанных требований, но оно не повлекло неправомерного воздействия на КИИ. Следует напомнить, что ч. 1 ст. 274.1 УК сформулирована законодателем по типу формальных составов и, поэтому, не предполагает наступление каких-либо последствий.

В-четвертых, возникает закономерный вопрос: когда «заработает» повышенная защита КИИ, соответственно вновь созданная норма УК? Ответ, на наш взгляд, остается открытым. Известно только то, что согласно информации заместителя начальника Управления ФСТЭК России Е.Б. Торбенко за период действия 187-ФЗ было подано всего 2 000 форм уведомлений о результатах категорирования объектов КИИ (из более 29 000 объектов, подлежащих категорированию), из которых 630 возвращены субъектам КИИ с замечаниями [10]. В 2019 г. процесс категорирования планируют завершить и перейти к следующему этапу – построению системы безопасности [11]. То есть получается, что круг субъектов КИИ до сих пор не определен! Хотя норма уголовного закона вступила в силу с 1 января 2018 г.

Настораживает еще и то, что в соответствие с законодательством и нормативными актами, регулирующими оборот КИИ, следует то, что субъекты КИИ на основе установленных показателей критериев значимости и их значений **самостоятельно** определяют категорию принадлежащих им объектов КИИ. Учитывая столь неопределенный круг субъектов и то, что это связано с дополнительными существенными расходами, процесс категорирования КИИ и внесения в соответствующий Реестр может затянуться. Думается, что круг субъектов КИИ должен быть существенно ограничен.

После всего сказанного возникает достаточно много вопросов, первыми из которых являются следующие: А сколько это все будет стоить? Кто за это все будет платить? А насколько эффективно работает законодательство о КИИ? Не следует забывать, что возможности уголовного воздействия определяются не только количеством и качеством статей в Уголовном кодексе, но и количеством, а главное, качеством имеющегося ресурсного обеспечения. При совершенствовании уголовного законодательства можно «замахиваться» только на те задачи, до реализации которых мы «доросли» в финансово-экономическом, организационном, аналитическом, научно-методическом, кадровом, нормативном и пропагандистском обеспечении. «По одежке протягивай ножки», «выше головы не прыгнешь», «дурная голова ногам покоя не дает» – правила, «отлитые» народом в пословицы, чрезвычайно актуальны и для современного этапа развития уголовного права.

Как бы это не звучало парадоксально, но на данный момент сложилась правовая ситуация, в которой виновное лицо подлежит уголовной ответственности за совершение деяния, не имеющего четких границ и критериев его установления. В исследуемом информационном законодательстве и нормативной базе, принятой на его основании, что ни слово, то бесконечные вопросы. Определения, которые допустимы / приемлемы в информационном законодательстве и в общем не вызывают особых разночтений у специалистов в области информационных технологий, как правило, не пригодны в уголовном законе, обреченном на применение.

Как следует из Доктрины информационной безопасности, утвержденной Президентом РФ, состояние информационной безопасности является одной из составляющих национальной безопасности. К сожалению, это лишь теоретическая посылка, законодательно не подкрепленная. В ст. 2 УК, как известно, перечислены объекты уголовно-правовой охраны. Компьютерной информации там нет. Таким образом, ни информационная, ни компьютерная безопасность не названа в числе объектов уголовно-правовой охраны. Можно, конечно, сказать, что информационная безопасность опосредованно включена в объект общественная безопасность и общественный порядок. Это так. Однако, думается, что ст. 2 УК следует дополнить новым самостоятельным объектом уголовно-правовой охраны – информационной безопасностью.

По вполне понятным причинам настоящая публикация не может претендовать на всестороннее и полное освещение проблемы правотворческих ошибок, допущенных законодателем, доскональный юридический анализ. Мы обращаем внимание лишь на некоторые из проблем.

Первый и основной недостаток исследуемой нормы «вытекает» из «ущербной» уголовной политики, которая чаще всего сводится к попыткам совершенствовать уголовный закон преимущественно за счет неоправданной криминализации все новых и новых форм общественно опасного поведения путем выделения специальных норм. Такие предложения подкупают простотой решения вопроса и, на первый взгляд, привлекают внешне надежными способами усиления охраны соответствующего объекта (в данном случае КИИ). Вместе с тем должно быть, очевидно, что практическая реализация подобных идей способна объективно снизить безопасность охраняемого объекта, породить серьезные проблемы, например, с квалификацией преступлений. Об одном из печальных опытов выделения специальных видов мошенничества было написано достаточно. Однако законодатель, с завидной настойчивостью, продолжает эту серию экспериментов. Думается, что конструирование специальных норм имеет смысл тогда, когда вновь создаваемые составы существенно отличаются (в том числе по степени общественной опасности) от «основного» состава, в связи с чем необходима дифференциация ответственности. В данном конкретном случае мы такого не наблюдаем. Законодатель мог бы избежать множества проблем, пойди он по пути углубления дифференциации уголовной ответственности за преступления в сфере компьютерной информации, наполнив соответствующие составы особо квалифицирующими признаками «в отношении объектов критической информационной инфраструктуры».

Законодателем в ст. 274.1 УК РФ не исполняется одно из основных правил законодательной техники, согласно которому в каждой статье Уголовного кодекса должна быть изложена самостоятельная норма, чтобы различные по своему содержанию нормы, несмотря на их органическую связь, на взаимообусловленность и дополняемость, формулировались в различных статьях закона.

Пожалуй, следующим из существенных недостатков ст. 274.1 УК является то, что характеристика наиболее важного признака – объективной стороны состава преступления перегружена узкоспециальными техническими терминами и оценочными категориями [12]. Введение законодателем специальных составов, которые фактически представляют собой объединение трех традиционных для отечественного законодательства форм преступного посягательства в сфере компьютерной информации (неправомерный доступ; оборот вредо-

носных компьютерных программ; нарушение правил эксплуатации) законодатель создает конкуренцию уголовно-правовых норм и проблемы для правоприменителя (при квалификации преступлений). Учитывая специфику объектов посягательства, следует отметить, что совершение компьютерных атак на КИИ транспорта, с очевидностью содержат признаки преступлений, предусмотренных ст. 167, 267 и 205 УК, тогда как взрыв объектов КИИ (здание, в котором осуществляется оборот соответствующей информации, электрических сетей, сетей электросвязи) – как 274.1 УК; неправомерное воздействие на коммуникации КИИ в целях подрыва экономической безопасности – ст. 281 УК; передача иностранному государству информации, отнесенной к КИИ – ст. 275 и 276 УК; разглашение сведений, содержащих государственную тайну – ст. 283, 283.1 УК, воздействие на соответствующую информацию на объектах атомной энергетики – ст. 215 УК. Так фантазировать можно долго. Приняв подобную норму, законодатель просто открывает «ящик Пандоры», который закрыть будет непросто.

Говоря о предмете данного преступления в сфере компьютерной информации, большинство исследователей, пишущих на эту тему, немало не задумываясь, указывают, что предметом преступлений в сфере компьютерной информации является компьютерная информация, средства хранения, обработки или передачи охраняемой компьютерной информации, информационно-телекоммуникационные сети, оконечное оборудование, а также КИИ РФ. И это правильно. Но, что же такое КИИ РФ? Исходя из буквального толкования уголовного закона – это, прежде всего, компьютерная информация и компьютерные программы, представляющие особую важность, ограниченные в обороте, находящиеся в обороте субъектов, определенных законом и другими нормативными актами. Именно на основании этих отличительных признаков законодатель и выделяет ст. 274.1 УК. Имея в виду то, что каждый предмет преступления должен характеризоваться определенными качественными и количественными признаками, зададимся вопросом: Чем же предмет ст. 274.1 УК принципиально отличается от предмета ст.ст. 272-274 УК? Похоже ничем, за исключением сферы оборота данной информации!

В ситуации когда объекты и субъекты КИИ РФ надлежащим образом не определены; соответствующего Реестра информации и программ, представляющих особую важность, нет; режим оборота подобной информации не организован[2]; пределы наказуемости составов (ст.ст. 272-274УК и ст. 274.1 УК) – существенно не отличаются и, соответственно, не свидетельствуют об особой важности предмета, предусмотренного ст. 274.1 УК, несложно спрогнозировать проблемы квалификации исследуемых составов.

Не понятно, чем руководствовался законодатель, формулируя принципиально разные подходы в избрании конструкции основных составов ст. 274.1 УК. Например, ч. 1 по конструкции состава является формальным (вред не конкретизирован), тогда как в ч. 2 и 3 – материальным (необходимо наступление причинение вреда КИИ РФ). Говорить о повышенной / пониженной опасности указанных составов – не приходится. Пределы наказуемости, также – вполне сопоставимы. Принципиальным отличием от санкций, предусмотренных в ст. 272-274 УК? Так и здесь нет принципиальных различий.

Существенным, на наш взгляд, признаком исследуемого состава преступления, является признак «заведомости». Законодатель более 130 раз использует термин «заведомость» в качестве криминообразующего и квалифицирующего признака в УК РФ. Не лишним было бы напомнить, что в большинство словарей русского языка (в том числе,

[2]Под режимом оборота понимается необходимость принятия целого комплекса мероприятий (правовых, организационных и технических), принимаемые обладателем соответствующей информации. Это, прежде всего: определение перечня соответствующей информации; выделение ее из обычного информационного оборота (на отдельные носители / компьютеры?), установление порядка обращения с этой информацией (место, время, круг лиц, допущенных к данной информации), установление мер по ее охране и защите конфиденциальности; установление контроля за ее соблюдением; урегулирование трудовых отношений с работниками, допущенными к соответствующей информации и т.д.

С.И. Ожегова и Н.Ю. Шведова) слово «заведомый» определяется как «хорошо известный», «несомненный».

Относительно признака «заведомости», в преступлениях против личности, собственности правоприменительная и судебная практика устоялась и не представляет особых проблем, чего нельзя сказать о преступлениях в сфере компьютерной информации. Следует заметить, что ранее уже было высказано сомнение в целесообразности использования признака «заведомости» в преступлениях в сфере компьютерной информации. Например, нами еще в 2002 г. обращалось внимание на это обстоятельство [12, С. 95, 105-106] и предлагалось признак «заведомости» исключить из диспозиции ст. 273 УК. Не изменилась эта позиция сейчас, применительно к ст. 274.1 УК.

Конструкция объективной стороны исследуемого преступления такова, что предполагает «хорошо известное» / «несомненное» знание виновным вредоносных качеств компьютерной программы или компьютерной информации, предназначенных для неправомерного воздействия именно на КИИ РФ, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или для нейтрализации средств защиты указанной информации. В настоящее время, когда уровень развития компьютерной техники столь высок, а программы достигли чрезвычайной сложности, одни и те же действия часто приводят к разным последствиям (в зависимости от состояния ЭВМ, степени её надежности и защищенности) – воздействие на КИИ, а равно ее уничтожение, блокирование, модификация или копирование может произойти по самой непредсказуемой причине. В подобной ситуации, как нам представляется, презумпция знания закона («хорошо известное» / «несомненное» знание виновным вредоносных качеств компьютерной программы или компьютерной информации) оказывается вполне опровержимой.

Исходя из изложенного, представляется целесообразным исключить из диспозиций ст. 273 и ч. 1, 2 ст. 274.1 УК указание на «заведомость», чтобы избежать проблем при квалификации указанных деяний, которые с неизбежностью будут возникать у правоприменителя.

Аксиомой в уголовном праве является положение о том, что те или иные признаки состава преступления и в том числе квалифицирующие признаки состава должны и могут осознаваться виновным. В нашем случае – все с большой натяжкой. Например, исходя из положений ФЗ «О КИИ», под последним понимается объект, нарушение функционирования которого приводит к потере управления, разрушению инфраструктуры, необратимому негативному изменению экономики страны, субъекта РФ либо административно-территориальной единицы или существенному ухудшению безопасности жизнедеятельности населения, проживающего на этих территориях, на длительный срок. Может ли виновный, осуществляя свои неправомерные действия, осознавать важность этого объекта, предвидеть столь серьезные последствия? Сомнительно.

Квалифицирующие составы и квалифицирующие признаки, как известно, являются одним из наиболее распространенных средств дифференциации уголовной ответственности в статьях Особенной части уголовного закона. Профессор Л.Л. Кругликов, выясняя содержательную сторону «тяжких последствий», установил, что: а) частота использования квалифицирующего признака «тяжкие последствия» в уголовном законе устойчиво занимает второе место после группового характера преступления; б) содержание этого признака во всех главах существенно разнится! Из этих посылок он делает вывод, с которым невозможно не согласиться, что толкование «тяжких последствий» целесообразно осуществлять применительно к отдельным главам Особенной части УК [13, С. 38].

Во всех без исключения составах преступлений в сфере компьютерной информации предусмотрен квалифицирующий признак совершения деяния, «повлекшего тяжкие последствия». Определения указанной дефиниции не содержится ни в Уголовном кодексе, ни в информационном законодательстве, ни в разъяснениях Верховного Суда РФ, что не лучшим образом сказывается на правоприменении.

До сих пор уголовно-правовой наукой не сформирована единая позиция по отно-

шению к «тяжкому вреду» в информационных преступлениях. Остаются без ответов вопросы: чему или кому должен быть причинен вред? В чем должен состоять вред: жизни, здоровью или информации (в данном случае, содержащейся в КИИ), бизнесу, репутации? А, может быть, сведен к определенному ущербу?

Изучение юридической литературы показало, что в оценке «тяжких последствий» применительно к исследуемым составам сложились несколько подходов. Первый из них понимает «гибель людей, причинение вреда здоровью, дезорганизация производства на предприятии или в отрасли промышленности и т.д.». Второй из них подразумевает потерю «исключительно важной информации», «незаменимой информации», необходимую для функционирования физического или юридического лица; информацию, которая может быть заменена, но это связано с большими затратами и трудностями». Третий подход, сформировавшийся с принятием исследуемой нормы (ст. 274.1 УК), под которой понимают неправомерное воздействие на информационные ресурсы стратегического значения, связанные с обеспечением общественной и государственной безопасности.

В юридической литературе не раз отмечалась законодательная линия на уточнение содержания так называемых оценочных признаков состава преступления. Представляется, что именно законодатель обязан устранять пробелы законодательства (в соответствии с принципом законности). Однако этот идеал далеко не всегда реализуем. Один из способов решения указанной проблемы, хотя и не самый удачный, видится в раскрытии содержания указанных оценочных понятий путем формулирования примерного перечня в самом законе, который поможет правоприменителю правильно понять смысл того или иного правового установления. Например, «повлекшее по неосторожности причинение тяжкого вреда здоровью потерпевшей, заражение ее ВИЧ-инфекцией или иные тяжкие последствия» (ч. 3 ст. 131 УК); «повлекли по неосторожности смерть человека или иные тяжкие последствия» (ч. 3 ст. 211 УК); «деяние, повлекшее по неосторожности смерть человека, радиоактивное заражение окружающей среды или иные тяжкие последствия» (ч. 2 ст. 215 УК). Приведение законодателем в качестве ориентира отдельных видов тяжких последствий, конечно же, полезно для практики, однако оно не заменяет соответствующей дефиниции и как итог, не снимает сложностей в правоприменительной практике [13, с. 38]. Думается, что подобная законодательная конструкция могла бы послужить промежуточным этапом к последующей полной конкретизации исследуемого квалифицирующего признака. При этом приходится признать, что недостатком указанного способа является определенное увеличение объема законодательного материала в норме.

Другим из способов решения проблемы оценочных категорий является их судебное толкование, даваемое в постановлениях Пленума Верховного Суда РФ. Конечно, разъяснения Пленумов Верховного Суда не могут заменить закона, однако оперативно и квалифицированно разъясняя те или иные положения, обязательные для правоприменителя, несомненно, они могли бы облегчить правоприменительный процесс, а, следовательно, способствовали бы более эффективной борьбе с преступлениями исследуемой категории. Не лучший, на наш взгляд, способ избежать указанных издержек, однако это лучше, чем ничего.

Результаты проведенных опросов практических работников показали, что подавляющее большинство из них (94%) испытывает необходимость в издании специального акта высшего судебного органа, посвященного преступлениям в сфере компьютерной информации, об этом же не один год говорят и ученые.

По степени реализации общественно опасные последствия, как известно, подразделяются на реальный ущерб (вред) и угрозу или опасность их причинения. В трех из четырех случаях главы 28 УК, законодатель предусмотрел в качестве особо отягчающего обстоятельства наступление «тяжких последствий или создание угрозы их наступления» (ст. 272–274 УК). В этих случаях достаточно угрозы наступления тяжких последствий. Составы угрозы причинения вреда конструируются законодателем обычно в случаях посягательств на особо ценные объекты (ст. 205. Террористический акт; ч.2 ст. 225. Ненад-

лежащее исполнение обязанностей по охране ядерного, химического или других видов оружия массового поражения; ст. 247. Нарушение правил обращения экологически опасных веществ и отходов и др.).

Анализ исследуемого состава дает основание утверждать, что законодатель крайне небрежно подошел к формулированию особо квалифицированных признаков ч. 5 ст. 274.1 УК, не использовав устоявшуюся в законодательной практике формулу «если оно (т.е. деяние) повлекло тяжкие последствия или **создало угрозу их наступления**». Вполне обосновано, на наш взгляд, законодатель использует данную конструкцию «создающих опасность» в составах ст. 272-274 УК, тогда как при охране более значимого объекта (ст. 274.1 УК) законодатель попросту ее игнорирует. Представляется, что в процессе развития уголовного законодательства эта ошибка должна быть исправлена.

В заключение остается напомнить старую истину о том, что ошибки, допущенные в процессе правотворчества, приводят к снижению качества действующего уголовного законодательства, дефектам правового регулирования, что, в свою очередь, может породить ошибки в правоприменительной деятельности, а это прямой путь к нарушениям прав и законных интересов субъектов правоотношений. Выявленные недостатки законодательной техники при построении уголовно-правовой нормы, закрепленной ст. 274.1 УК РФ, должны быть устранены.

Литература

1. Критическая инфраструктура России[Электронный ресурс].URL: http://dialog-e.ru/market-news/626/ (дата обращения: 25.06.2019).
2. *Захарова Л.* За год на Россию было совершено более четырех миллиардов кибератак[Электронный ресурс]. URL: https://rg.ru/2018/12/12/za-god-na-rossiiu-bylo-sovershenobolee-chetyreh-milliardov-kiberatak.html (дата обращения: 25.06.2019).
3. Более 52 млн атак на сайты госорганов РФ совершено в 2016 году [Электронный ресурс].URL: https://www.interfax.ru/russia/552174 (дата обращения: 25.06.2019).
4. *Бабаев М., Пудовочкин Ю.* «Мертвые» нормы в уголовном кодексе: проблемы и решения [Текст] / М. Бабаев, Ю. Пудовочкин // Уголовное право. – 2010. – № 6. – С. 4–10.
5. Например: *Лапунин М.М.* Обеспечение безопасности критической информационной инфраструктуры и новелла уголовного закона [Текст] / М.М. Лапунин // Уголовное право: стратегия развития в XXI веке. - М.: Проспект, 2018. - С. 633 - 636; *Решетников А.Ю., Русскевич Е.А.* Об уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК России) [Текст] / А.Ю. Решетников, Е.А. Русскевич // Законы России: опыт, анализ, практика. - 2018. - № 2. - С. 51-55; *Ларина Л.Ю.* Уголовная ответственность за неправомерное воздействие на критическую информационную инфраструктуру России [Текст] /Л.Ю.Ларина // Актуальные вопросы борьбы с преступлениями. – 2017. – № 3. – С. 22-25.
6. «Отчет о видах наказания по наиболее тяжкому преступлению (без учета сложения) за 2018 год» [Электронный ресурс].URL: http://www.cdep.ru/index.php?id=79&item=4759 // (дата обращения: 25.06.2019). (Официальный сайт Судебного департамента при Верховном Суде Российской Федерации).
7. О безопасности критической информационной инфраструктуры Российской Федерации: федер.закон Рос. Федерации от 26 июля 2017 г. № 187-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации от 12 июля 2017 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 19 июля 2017 г.// Рос.газ.- 2017. - 31 июля.
8. О транспортной безопасности: федер. закон Рос. Федерации от 09 февр. 2007 г. № 16-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации от 19 января 2007 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 02 февр. 2007 г. // Рос. газ. - 2007. - 14 февр.
9. Информационное письмо от 24 августа 2018 г. № 240/25/3752 «По вопросам представления перечней объектов критической информационной инфраструктуры, подлежащих

категорированию, и направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий» [Электронный ресурс].URL: https://fstec.ru/component/attachments/download/2006 (дата обращения: 25.06.2019).
10. ИБКВО 2019. Е. Торбенко. ФСТЭК: О категорировании объектов [Электронный ресурс]. URL: http://json.tv/ict_video_watch/ibkvo-2019-elena-torbenko-fstek-bolee-29-tysyach-obektov-kategorirovaniya-napravleny-nam-20190319030955 (дата обращения: 25.06.2019).
11. По оценке заместителя директора ФСТЭК В. Лютикова в 2019 г. процесс категорирования планируется завершить и перейти к следующему этапу - построению системы безопасности. *Шпун Я.* Информационную безопасность рассмотрели в практической плоскости [Электронный ресурс].URL: https://www.comnews.ru/content/116102/2018-11-29/ib-rassmotreli-v-prakticheskoy-ploskosti (дата обращения: 25.06.2019).
12. *Бражник С.Д.* Преступления в сфере компьютерной информации: проблемы законодательной техники [Текст]: дис. …канд. юрид. наук: 12.00.08 / - Ижевск, 2002. – 189 с.
13. *Кругликов Л.Л.* Тяжкие последствия в уголовном праве: объективные и субъективные признаки [Текст] /Л.Л. Кругликов // Уголовное право. – 2010. – № 5. – С. 38–46.