ЗАКОНОДАТЕЛЬНЫЕ ПОДХОДЫ К КРИМИНАЛИЗАЦИИ ДЕЯНИЙ, СВЯЗАННЫХ С НЕПРАВОМЕРНЫМ ДОСТУПОМ К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ В СТРАНАХ СОДРУЖЕСТВА НЕЗАВИСИМЫХ ГОСУДАРСТВ

РУСКЕВИЧ Евгений Александрович, старший преподаватель кафедры уголовного права Московского университета МВД России им. В. Я. Кикотя, кандидат юридических наук
117437, Россия, г. Москва, ул. Академика Волгина, 12
E-mail: russkevich@mail.ru

За последние годы национальные уголовные законодательства стран Содружества Независимых Государств потеряли былое единство в регламентации ответственности за преступления в сфере компьютерной информации. Это обуславливает ряд проблем сугубо практического свойства (на уровне обеспечения эффективного взаимодействия судебно-следственных органов), а также актуализирует потребность в познании законодательского опыта стран Содружества, чтобы обогатить отечественную науку, критически осмыслить национальное законодательство, выявить его слабые и сильные стороны, указать на очевидные проблемы, сформулировать наиболее целесообразные пути их разрешения.

Цель работы состоит в проведении комплексного сравнительного исследования уголовной ответственности за неправомерный доступ к компьютерной информации в странах СНГ, в разработке на этой основе предложений по совершенствованию конструкции ст. 272 УК РФ. Реализация указанной цели достигалась путем оценки состояния уголовных законодательств стран СНГ в части регламентации ответственности за неправомерный доступ к компьютерной информации, выявления их достоинств и недостатков, определения основных направлений модернизации ст. 272 УК РФ.

Исследование главным образом основано на применении сравнительно-правового метода. Также были использованы общенаучные и специальные методы (анализ, синтез, индукция, формально-юридический, абстрактно-логический и др.).

Выводы: 1) действия, предусмотренные ст. 272 УК РФ, в абсолютном большинстве национальных законодательств пространства СНГ рассредоточены сразу по нескольким составам преступлений: а) несанкционированный доступ к информации; б) ее неправомерная модификация; в) умышленное уничтожение, блокирование, приведение в непригодное состояние (компьютерный саботаж); г) несанкционированное копирование либо иное неправомерное завладение; 2) отечественное законодательство об ответственности за неправомерный доступ к компьютерной информации нуждается в коррекции. К числу первоочередных мер следует отнести дифференциацию ответственности за неправомерный доступ в зависимости от формы вины субъекта и характера наступивших последствий.

Ключевые слова: уголовное право, компьютерные преступления, информационно-коммуникационные технологии, неправомерный доступ.

LEGISLATIVE APPROACHES TO THE CRIMINALIZATION OF ACTS RELATED TO ILLEGAL ACCESS TO COMPUTER INFORMATION IN THE COUNTRIES OF THE COMMONWEALTH OF INDEPENDENT STATES

E. A. RUSSKEVICH, senior lecturer at the Department of criminal law of the Kikot Moscow University of the Ministry of Internal Affairs of the Russian Federation
12, Akademik Volgin st., Moscow, Russia, 117437
E-mail: russkevich@mail.ru

In recent years, the national criminal laws of the countries of the Commonwealth of Independent States have lost their former unity in the regulation of liability for crimes in the field of computer information. This causes a few problems of a purely practical nature (at the level of ensuring effective interaction of judicial and investigative bodies), and actualizes the need for knowledge of the legislative experience of the CIS countries in order to enrich Russian science, to critically reflect on national legislation, to identify its weak and strong sides, to point out the obvious problems, formulate the most expedient ways to resolve them.

The purpose of the work is to conduct a comprehensive comparative study of criminal liability for illegal access to computer information in CIS countries, to develop the proposals for improving of the design of Art. 272 of the Criminal Code on this basis. The implementation of these goals were achieved with the help of evaluation of the criminal legislation of the CIS countries, including the regulation of the liability for illegal access to computer information, identification of their merits and shortcomings, identification of the main directions for modernization of Art. 272 of the Criminal Code.

The study is mainly based on the application of a comparative-legal method. At the same time, general scientific and special methods (analysis, synthesis, induction, formal-legal, abstract-logical, etc.) were also used.

Conclusions: 1) the actions regulated by the Art. 272 of the Criminal Code of the Russian Federation, in the most national legislations of the CIS space are dispersed to several elements of crimes at once: a) illegal access to information, b) its illegal modification, c) intentional destruction, blocking, scrapping (computer sabotage), d) unauthorized copying or other illegal taking over; 2) domestic legislation on liability for unauthorized access to computer information needs to be correlated. The differentiation of liability for illegal access, depending on the form of the guilt of the subject and the nature of the consequences, has to be recognized as the priority measure.

Keywords: criminal law, computer crimes, information and communication technologies, illegal access.

DOI: 10.12737/art.2018.1.16

Положение о трансграничности преступлений, совершаемых с использованием современных информационно-коммуникационных технологий, уже является truismом. Действительно, не требует дополнительной аргументации, что инфраструктура и механизм компьютерных преступлений закономерно обуславливают их экстерриториальный характер — киберпреступник и потерпевший зачастую могут находиться на разных концах света, разговаривать на разных языках, принадлежать к разным культурам и т. д.

Следует согласиться с М. А. Простосердовым, что зарубежный опыт противодействия киберпреступности можно охарактеризовать как несогласованный и поэтому малоэффективный. На национальных уровнях сложились свои направления уголовно-правовой политики противодействия киберпреступности и подходы построения уголовно-правовых норм¹. В свою очередь, это помогает совершенно по-другому взглянуть на роль и значение сравнительного правоведения в решении конкретных отраслевых проблем отечественного уголовного права. Познание опыта зарубежных стран в противодействии компьютерным преступлениям позволяет не только обогатить отечественную науку, но и критически осмыслить национальное законодательство, выявить его слабые и сильные стороны, указать на очевидные проблемы, а также предложить наиболее правильные пути их разрешения. Не менее важным является и то, что отчетливое понимание особенностей установления и реализации ответственности за компьютерные преступления — непереносимое условие эффективного взаимодействия с правоохранительными органами и правовыми системами других государств.

Ввиду многих причин политического, экономического, социального и культурного характера при проведении сравнительного исследования наиболее пристальное внимание традиционно уделяется законодательству стран Содружества Независимых Государств². Нельзя не отметить, что в этом есть и сугубо практический смысл — учитывая сложившиеся процессы миграции населения, судебно-следственные органы стран Содружества гораздо чаще вынужде-

ны взаимодействовать друг с другом в рамках правовой помощи по уголовным делам.

Как известно, в рамках СНГ в 2001 г. было принято Соглашение о сотрудничестве государств — участников СНГ в борьбе с преступлениями в сфере компьютерной информации, которое рекомендовало странам-участницам признавать уголовно наказуемыми следующие деяния, если они совершены умышленно: 1) осуществление неправомерного доступа к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети; 2) создание, использование или распространение вредоносных программ; 3) нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред или тяжкие последствия; 4) незаконное использование программ для ЭВМ и баз данных, являющихся объектами авторского права, а равно присвоение авторства, если это деяние причинило существенный ущерб³.

На первоначальном этапе все страны Содружества так или иначе регламентировали ответственность за три традиционных компьютерных преступления: 1) неправомерный доступ к компьютерным данным; 2) незаконное создание и распространение вредоносного программного обеспечения; 3) нарушение правил эксплуатации средств хранения, обработки и передачи компьютерных данных.

Однако за прошедшее время «правовой ландшафт» противодействия компьютерной преступности в рамках СНГ претерпел существенные изменения. Следует констатировать, что в основной массе страны пошли по пути детализации уголовной ответственности за посягательства на отношения информационной безопасности и, как следствие, расширения перечня соответствующих составов. В настоящее время УК Республики Молдова содержит уже 10 составов компьютерных преступлений, УК Республики Казахстан — 9, УК Армении — 7, УК Республики Беларусь — 7, УК Республики Таджикистан — 7, УК Республики Узбекистан — 6, УК Азербайджана — 5.

¹ См.: Простосердов М. А. Экономические преступления, совершаемые в киберпространстве: монография. М., 2017. С. 41.

² Далее — Содружество или СНГ.

³ URL: <http://www.cis.minsk.by/page.php?id=866> (дата обращения: 06.10.2017).

Пожалуй, наименее проработанным в части обеспечения информационной безопасности является УК Кыргызской Республики, который в настоящее время содержит лишь уголовно-правовой запрет на создание, использование и распространение вредоносных программ для ЭВМ (ст. 290). Между тем в проекте нового УК Кыргызстана (вступит в силу с 1 января 2019 г.) регламентированы уже три преступления против информационной безопасности (гл. 42): неправомерный доступ к компьютерной информации (ст. 304), создание вредоносных компьютерных программ (ст. 305) и компьютерный саботаж (ст. 306)⁴.

Принимая во внимание значительное количество нормативного материала и сложность его качественного компаративного анализа в рамках отдельной научной статьи, представляется целесообразным обратиться к более частному вопросу — особенностям законодательного определения в пределах СНГ ответственности за традиционное и весьма распространенное компьютерное преступление — неправомерный доступ к компьютерной информации.

Прежде всего следует отметить, что действия, охватываемые ст. 272 УК РФ, в абсолютном большинстве национальных законодательств пространства СНГ рассредоточены сразу по нескольким составам. Как метко замечает по этому поводу О. И. Семькина, законодательствам стран Содружества характерно так называемое распиливание признаков неправомерного доступа к компьютерной информации на самостоятельные составы преступления путем конкретизации в них общественно опасных последствий⁵. Так, УК Республики Беларусь отдельно устанавливает ответственность за несанкционированный доступ (ст. 349), модификацию компьютерной информации, сопряженную с несанкционированным доступом к компьютерной системе (ч. 2 ст. 350), умышленное уничтожение, блокирование, приведение в непригодное состояние компьютерной информации (компьютерный саботаж), сопряженные с неправомерным доступом к компьютерной системе (ч. 2 ст. 351), несанкционированное копирование либо иное неправомерное завладение информацией (ст. 352). Сопоставление санкций показывает, что по белорусскому законодательству наименее тяжким является неправомерное копирование (завладение) компьютерных данных (наказывается лишением свободы на срок

до двух лет), в то время как наиболее строгое наказание предусмотрено за компьютерный саботаж, сопряженный с неправомерным доступом к компьютерной системе (наказывается лишением свободы на срок от трех до десяти лет)⁶.

Практически таким же образом дифференцирует посягательства на информационные данные законодатель Казахстана, отдельно устанавливая ответственность за неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций (ст. 205), неправомерное уничтожение или модификацию информации (ст. 206), неправомерное завладение информацией (ст. 208), неправомерное изменение идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента (ст. 213)⁷. Похожий подход реализован в уголовных кодексах Азербайджана, Армении, Молдовы, Таджикистана и Узбекистана.

Полагаем, что курс указанных государств на дифференциацию ответственности в зависимости от последствий неправомерного доступа к компьютерным данным следует оценить положительно. Такое решение в большей мере способствует реализации основополагающих принципов уголовного права и прежде всего принципа справедливости. Кроме того, наличие специальных норм об ответственности за уничтожение (блокирование), модификацию и копирование информационных данных, на наш взгляд, обладает значительно большим превентивным зарядом. Как справедливо писал В. Н. Кудрявцев, общая, абстрактная норма значительно удобнее для квалифицированного юриста. Но ведь уголовные законы создаются не только для юристов. Они имеют воспитательное и предупредительное значение. Простой и понятный текст закона, устанавливающего ответственность за конкретные действия, смысл которых ясен любому гражданину, имеет важное профилактическое значение. Поэтому наряду с общими нормами, которые уже имеются в законодательстве, в некоторых случаях оправданно появление новых законов, подчеркивающих общественную опасность тех или иных форм поведения, причиняющих вред обществу⁸.

Сравнительно-правовой анализ показывает, что не все государства Содружества используют такой конструктивный признак диспозиции ст. 272 УК РФ, как *охраняемая законом информация*. Так, диспозиция ст. 278² УК Республики Узбекистан не содержит указания на то, что компьютерная информация, к которой осуществляется неправомерный доступ,

⁴ Сведения приведены на основании обращения к текстам нормативных актов, размещенных в справочных правовых системах или на официальных сайтах правительств соответствующих государств. Исследование проведено исключительно на основе законодательств стран Содружества, подписавших договор: Азербайджана, Армении, Белоруссии, Казахстана, Кыргызстана, Молдовы, Таджикистана, Узбекистана.

⁵ См.: Семькина О. И. Противодействие киберпреступности за рубежом // Журнал зарубежного законодательства и сравнительного правоведения. 2016. № 6. С. 112.

⁶ URL: <http://www.pravo.by/document/?guid=3871&p0=Hk9900275> (дата обращения: 05.09.2017).

⁷ URL: http://online.zakon.kz/m/Document/?doc_id=31575252#sub_id=2050000 (дата обращения: 07.10.2017).

⁸ См.: Кудрявцев В. Н. Общая теория квалификации преступлений. М., 1972. С. 248—249.

должна быть охраняемой законом⁹. В статье 349 УК Республики Беларусь указывается лишь на несанкционированный доступ к «информации, хранящейся в компьютерной системе, сети или на машинных носителях».

Как известно, указание в ст. 272 УК РФ на то, что информация должна быть «охраняемой законом», привело к весьма ограничительному толкованию предмета данного преступления как лишь закрытой информации — государственной, служебной, коммерческой, банковской, врачебной, нотариальной, адвокатской тайны, персональных данных и т. д.¹⁰ В Методических рекомендациях Генеральной прокуратуры РФ по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации также указано, что по смыслу ст. 272 УК РФ охраняемой законом информацией являются лишь сведения, в отношении которых установлен специальный режим правовой защиты (например, государственная, служебная и коммерческая тайна, персональные данные и т. д.). Отсутствие общепринятого толкования «охраняемой законом информации» закономерно обусловило неединообразную практику применения ст. 272 УК РФ. Отдельные суды, придерживаясь рекомендаций Генеральной прокуратуры РФ, указывают, что неправомерные манипуляции с открытой (общедоступной) информацией не подпадают под действие данной статьи¹¹. Другие, наоборот, применяют ст. 272 УК РФ при оценке действий, связанных с неправомерным доступом и к общедоступной информации, хранящейся в сети Интернет, в отношении которой законным владельцем были приняты специальные меры защиты по обеспечению ее доступности и целостности¹². Полагаем, что описание деяния по типу «неправомерный» или «несанкционированный доступ» к компьютерной информации указывает на то, что деяние осуществляется вопреки воле владельца информационного актива, угрожает не только его конфиденциальности, но и целостности или доступности. В связи с этим специальное указание на то, что информация должна быть «охраняемой законом», на наш взгляд, является излишним.

Другим значимым элементом сравнительной характеристики являются особенности регламентации последствий неправомерного доступа к компьютерной информации, с наступлением которых нацио-

нальные законодательства стран связывают момент его окончания. Следует отметить, что за неправомерный доступ к компьютерной информации *per se*, т. е. за так называемое чистое хакерство без последствий для конфиденциальности, доступности и целостности информации, установлена ответственность по УК Азербайджана (ст. 271)¹³ и УК Республики Таджикистан (ст. 298)¹⁴.

По уголовному законодательству Казахстана неправомерный доступ к охраняемой законом компьютерной информации должен быть сопряжен с общественно опасными последствиями в виде «существенного нарушения прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства». Белорусский законодатель в ряду альтернативных последствий несанкционированного доступа называет «существенный вред».

Активное использование таких оценочных признаков вряд ли следует признать обоснованным. Как известно, в теории уголовного права нет общепринятого толкования «существенности» нарушения или вреда, что закономерно порождает неоднозначную правоприменительную практику, когда тождественные по сути деяния получают разную правовую оценку¹⁵.

Еще более неудачную модель регламентации общественно опасных последствий неправомерного доступа к компьютерной информации использует законодатель Республики Молдова. В соответствии со ст. 259 УК Молдовы неправомерный доступ к информационным активам будет окончательным преступлением только при условии наступления двухуровневых последствий: 1) уничтожения, повреждения, модификации, блокирования или копирования информации, нарушения работы компьютеров, информационной системы или сети и 2) причинения ущерба в крупном размере¹⁶. Очевидно, что на практике установление причинно-следственной связи между самим неправомерным доступом и имущественными потерями потерпевшего может вызывать значительные трудности. Причем при подобной конструкции уголовно-правовой нормы нельзя будет квалифицировать как окончательное преступление, когда потерпевший своевременными действиями смог предот-

⁹ URL: http://www.lex.uz/pages/getact.aspx?lact_id=111457 (дата обращения: 17.11.2017).

¹⁰ См.: Гузеева О. С. Квалификация преступлений в сфере компьютерной информации. М., 2016. С. 30.

¹¹ См.: Апелляционный приговор Судебной коллегии по уголовным делам Верховного суда Чувашской Республики от 3 июня 2015 г. по делу № 22-1054/2015.

¹² См.: Приговор Волжского городского суда Волгоградской области от 17 ноября 2016 г. по делу № 1-1105/2016.

¹³ URL: <https://courts.gov.az/ru> (дата обращения: 24.11.2017).

¹⁴ URL: http://base.spinform.ru/show_red.fwx?rid=9895 (дата обращения: 17.11.2017).

¹⁵ Как известно, неопределенность признака существенно нарушения прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства становилась предметом рассмотрения Конституционным Судом РФ (см., например, определение Конституционного Суда РФ от 23 марта 2010 г. № 368-О-О).

¹⁶ URL: <http://lex.justice.md/ru/331268/> (дата обращения: 21.11.2017).

вратить наступление ущерба (например, восстановив утраченные данные).

В определении признаков субъекта неправомерного доступа к компьютерной информации страны Содружества в целом демонстрируют единообразный подход — как правило, им признается физическое вменяемое лицо, достигшее шестнадцатилетнего возраста. Уголовная ответственность юридических лиц предусмотрена по законодательству Молдовы (ст. 259). Возможными наказаниями для организаций выступают штраф и лишение права заниматься определенной деятельностью или ликвидация.

В отечественной доктрине уголовного права вопрос об ответственности организаций является предметом острой дискуссии. Понятно, что в рамках отдельной научной статьи было бы самонадеянным претендовать на решение такой сложной проблемы. Однако представляется, что все же необходимо сформулировать авторскую позицию, выразить отношение к проблеме. Полагаем, что для принятия решения по этому вопросу прежде всего следует руководствоваться сугубо практическими соображениями. Иными словами: имеет ли положительное решение вопроса о введении института уголовной ответственности юридических лиц реальное позитивное содержание; не создаст ли это еще больше проблем для и без того проблемного правоприменения?

Отвечая на первую часть поставленного вопроса, следует, пожалуй, высказаться отрицательно — отечественное законодательство располагает достаточным инструментарием для осуществления эффективного наказательного воздействия на организации от штрафа до принудительной ликвидации. Примеры подобных решений без труда можно найти в современной правоприменительной практике.

В то же время введение ответственности юридических лиц несомненно породит множество дополнительных проблем на уровне правоприменения. Следователям придется разбираться в запутанных вопросах причастности организации к преступной деятельности конкретного работника, в субъектах осуществления актуального контроля юридического лица и т. п. Нельзя не указать и на определенные коррупционные риски.

В связи с этим полагаем, что законодательный опыт отдельных стран СНГ в части введения уголовной ответственности юридических лиц за совершение преступлений, в том числе в сфере компьютерной информации, требует дальнейшего осмысления (научной проработки) и не может быть реализован в национальном законодательстве на современном этапе.

Как известно, диспозиция ст. 272 УК РФ не дает прямых указаний относительно субъективной стороны рассматриваемого преступления. В теории уголовного права высказываются различные сужде-

ния по этому вопросу¹⁷. Некоторые авторы настаивают на том, что неправомерный доступ к компьютерной информации предполагает только умышленную форму вины. В Методических рекомендациях Генеральной прокуратуры РФ выражена следующая позиция: субъективная сторона данного преступления характеризуется виной в форме умысла (прямого или косвенного) или неосторожности¹⁸. В связи с этим следует положительно оценить подход отдельных стран СНГ, дифференцировавших ответственность за неправомерный доступ к компьютерной информации в зависимости от содержания психического отношения субъекта. Так, ст. 349 Республики Беларусь предусматривает ответственность за несанкционированный доступ к компьютерной информации, совершенный умышленно (ч. 2) и по неосторожности (ч. 1).

УК Армении описывает несанкционированный доступ к компьютерной информации в целом как неосторожное преступление: «Несанкционированный доступ (проникновение) к какой-либо части системы информации или ко всей системе информации, хранящейся в компьютере, компьютерной системе, сети или на машинных носителях и охраняемой законом, совершенный с нарушением системы защиты и повлекший *по неосторожности* (курсив мой. — Е. Р.) изменение, копирование, уничтожение или блокирование информации, либо вывод из строя компьютера, компьютерной системы, сети или компьютерного оборудования либо иной значительный ущерб»¹⁹. Вместе с тем умышленные посяательства на конфиденциальность, целостность и доступность компьютерных данных предусмотрены ст. 252 (изменение компьютерной информации), ст. 253 (компьютерный саботаж) и ст. 254 (неправомерное завладение компьютерной информацией).

Отсутствие четкого разделения ответственности за неосторожное и умышленное уничтожение, блокирование, модификацию или копирование информации при неправомерном доступе является серьезным изъяном действующей редакции ст. 272 УК РФ. Как представляется, заимствование приведенного выше

¹⁷ См., например: *Ефремова М. А.* Уголовная ответственность за преступления, совершаемые с использованием информационно-коммуникационных технологий: монография. М., 2015; *Русскиевич Е. А.* Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий: учеб. пособие. М., 2017; *Швед Н. А.* Неправомерный доступ к компьютерной информации: уголовно-правовая защита в РФ и Республике Беларусь // Информационное право. 2016. № 2.

¹⁸ См. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации.

¹⁹ URL: <http://www.parliament.am/legislation.php?ID=1349&sel=show&lang=rus#24> (дата обращения: 21.10.2017).

опыта стран Содружества могло бы способствовать успешному устранению данной проблемы.

Проведенное исследование позволило выявить следующие типичные для пространства СНГ обстоятельства, усиливающие ответственность за неправомерный доступ к компьютерной информации: 1) совершение преступления группой лиц по предварительному сговору или организованной группой (ст. 271.2.2 УК Азербайджана, ч. 2 ст. 252 УК Армении, ч. 2 ст. 349 УК Белоруссии, ч. 2 ст. 206 УК Казахстана, п. «б» ч. 2 ст. 259 УК Молдовы, п. «а» ч. 2 ст. 278² УК Узбекистана); 2) наступление в результате совершения преступления тяжких последствий (ч. 3 ст. 251 УК Армении, ч. 3 ст. 349 УК Белоруссии, ч. 3 ст. 205 УК Казахстана, ч. 3 ст. 298 УК Таджикистана); 3) совершение преступления из корыстных побуждений (ч. 2 ст. 349 УК Белоруссии); 4) совершение преступления лицом с использованием своего служебного положения (ст. 271.2.3 УК Азербайджана, ч. 2 ст. 251 УК Армении, п. «в» ч. 2 ст. 278² УК Узбекистана); 5) совершение преступления повторно (ст. 271.2.1 УК Азербайджана, п. «б» ч. 2 ст. 278² УК Узбекистана).

Отечественное уголовное законодательство в целом отражает главенствующий в пространстве СНГ подход к конструированию квалифицирующих признаков.

По УК Азербайджана отягчающим обстоятельством неправомерного доступа к компьютерной информации является совершение данного деяния в отношении «инфраструктурных объектов общественного значения». В соответствии с примечанием к ст. 271 УК Азербайджана под такими объектами подразумеваются государственные учреждения, предприятия, организации, неправительственные организации (общественные объединения и фонды), кредитные организации, страховые компании, ин-

вестиционные фонды, которые представляют большую значимость для государства и общества. Можно констатировать, что отечественное законодательство в этом аспекте уже было доработано. С 1 января 2018 г. вступил в силу Федеральный закон от 26 июля 2017 г. № 194-ФЗ «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”», согласно которому гл. 28 УК РФ дополнена специальной нормой об ответственности за неправомерное воздействие на объекты критической информационной инфраструктуры Российской Федерации (ст. 274¹).

Следует констатировать, что отечественное законодательство об ответственности за неправомерный доступ к компьютерной информации (ст. 272 УК РФ) нуждается в коррекции. К числу первоочередных мер, на наш взгляд, следует отнести: 1) разделение ответственности за неправомерный доступ к компьютерной информации в зависимости от психического отношения субъекта к наступлению общественно опасных последствий (умысла или неосторожности); 2) дифференциацию ответственности за неправомерный доступ к информации в зависимости от наступивших последствий: а) уничтожение, блокирование, приведение в непригодное состояние компьютерной информации, б) ее модификация (изменение) и в) копирование (завладение); 3) в целях устранения смысловой неопределенности из диспозиции ст. 272 УК РФ необходимо исключить указание на то, что предметом данного преступления является исключительно *охраняемая законом* (т. е. конфиденциальная) информация. Общедоступная информация отнюдь не является информацией, лишенной защиты в части ее доступности и целостности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

- Гузеева О. С. Квалификация преступлений в сфере компьютерной информации. М., 2016.
- Ефремова М. А. Уголовная ответственность за преступления, совершаемые с использованием информационно-коммуникационных технологий: монография. М., 2015.
- Кудрявцев В. Н. Общая теория квалификации преступлений. М., 1972.
- Простосердов М. А. Экономические преступления, совершаемые в киберпространстве: монография. М., 2017.
- Русскевич Е. А. Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий: учеб. пособие. М., 2017.
- Семыкина О. И. Противодействие киберпреступности за рубежом // Журнал зарубежного законодательства и сравнительного правоведения. 2016. № 6.
- Швед Н. А. Неправомерный доступ к компьютерной информации: уголовно-правовая защита в РФ и Республике Беларусь // Информационное право. 2016. № 2.