УДК/UDC 343

# Специальная превенция преступлений в сфере компьютерной информации: уголовно-правовой аспект

Абашина Людмила Александровна
кандидат юридических наук, доцент, заведующая кафедрой уголовного права
Юридический институт Орловского государственного университета им. И. С. Тургенева
г. Орел, Россия
e-mail: abashinala@yandex.ru
SPIN-код: 9137-1296

Ефремова Ольга Валентиновна
старший преподаватель кафедры теории и истории права и государства
Международный юридический институт
г. Москва, Россия
e-mail: eov2209@mail.ru
SPIN-код: 7572-6350

**Аннотация**

В статье авторы, рассматривая уголовно-правовые меры социальной превенции преступлений в сфере компьютерной информации, пришли к выводу, что необходима дальнейшая корректировка текста уголовного закона Российской Федерации, при проведении которой следует руководствоваться уже сделанными предложениями криминологов, а также соотнесением имеющихся норм с минимальным перечнем деяний в сфере информационных технологий, рекомендованных на европейском уровне для криминализации, опытом государств СНГ. Редакционная правка не предполагает качественных структурных изменений гл. 28 Уголовного кодекса Российской Федерации, однако некоторые предложения могут и должны быть реализованы в рамках редакционной и концептуальной правки. При проведении концептуальной правки следует руководствоваться уже сделанными предложениями криминологов по соотнесению имеющихся норм с минимальным перечнем деяний в сфере информационных технологий. Она потребует не только «разукрупнения» статей и помещения в отдельные нормы обособленных составов (поскольку сейчас некоторые из них объединены в рамках одной статьи), расширения круга криминализированных дея-

ний, изменения наименований статей, но и введения административной преюдиции.

**Ключевые слова:**преступления в сфере компьютерной информации, киберпреступность, компьютерные преступления, преступления в сфере информационных технологий.

# Special prevention of crimes in the field of computer information: criminal-legal aspect

Abashina Lyudmila Aleksandrovna
Candidate of Law, assistant professor, head of a chair of the Department of Criminal Law Law Institute of Orel State University named after I. S. Turgenev
Orel, Russia
e-mail: abashinala@yandex.ru
SPIN Code: 9137-1296

Yefremova Olga Valentinovna
senior lecturer of the Department of Legal Theory and History
International Law Institute
Moscow, Russia
e-mail: eov2209@mail.ru
SPIN Code: 7572-6350

**Abstract**

In the article, the authors, considering the criminal-legal measures of social prevention of crimes in the field of computer information, came to the conclusion that further correction of the text of the criminal law of the Russian Federation is necessary, during which one should be guided by the proposals already made by criminologists, as well as the correlation of existing norms with the minimum list of acts in the field of information technologies, recommended at the European level for criminalization, by the experience of the CIS states. The editorial revision does not imply qualitative structural changes in Ch. 28 of the Criminal Code of the Russian Federation, however, some proposals can and should be implemented within the framework of editorial and conceptual revisions. When carrying out conceptual changes, one should be guided by the proposals already made by criminologists to correlate existing norms with the minimum list of acts in the field of information technology. It will require not only the "unbundling"of articles and the placement of separate compositions into separate norms (since now some of them are

combined under one article), expanding the range of criminalized acts, changing the titles of articles, but also the introduction of administrative prejudice.

**Key words:** crimes in the field of computer information, cybercrime, computer crimes, crimes in the field of information technology.

Представляется, что как мера специального предупреждения корректировка текста уголовного закона необходима, несмотря на то, что правка гл. 28 Уголовного кодекса Российской Федерации (далее по тексту - УК РФ) с момента ее появления уже была проведена шесть раз). Вопрос в том, по какой модели она должна осуществляться.

Анализ показал, что гл. 28 УК РФ имеет структурно-содержательные проблемы, наличие которых пагубно сказывается на правореализационной практике. Преодоление данных недостатков может происходить в процессе редакционной правки или в рамках концептуальных изменений гл. 28 УК РФ.

При проведении редакционной правки, практически не предполагающей изменения структуры данной главы, нужно:

1. Изменить наименование гл. 28 УК РФ с «Преступление в сфере компьютерной информации» на «Преступления в сфере информационных технологий», что будет точнее отражать ее содержательный компонент, отвечать европейской практике и соответствовать тексту межгосударственных соглашений государств СНГ.
2. Закрепить понятийно-терминологический аппарат на уровне легального прояснения («компьютерная программа», «вредоносная программа» и пр.), сделав это либо в тексте УК РФ в примечаниях (вариант: изменив структуру, собрав в одну из начальных статей все термины и определения, применяемые в УК РФ), либо в информационном законодательстве.
3. Ст. 272 УК РФ следует дополнить третьим примечанием, распространив его действие на всю главу, в котором можно преду-

смотреть поощрительные меры в виде освобождения от уголовной ответственности лиц, добровольно отказавшихся от совершения киберпреступлений или деятельно раскаивающихся и компенсировавших нанесенный ущерб.

4. Создать в ст. 273 УК РФ еще один квалифицированный состав, дифференцировав ответственность за «создание» и «распространение и использование» вредоносных программ, что повлечет за собой корректировку нумерации ее частей (ч. 2 и 3 в ее актуальной редакции станут ч. 3 и 4 соответственно после подобной редакционной правки).
5. В ч. 2 ст. 272 УК РФ и ч. 3 (сейчас - ч. 2) ст. 273 УК РФ целесообразно внести два новых квалифицирующих признака: «совершение деяния из хулиганских побуждений» и «совершение деяния лицом, уже ранее осужденным за совершение преступлений в сфере информационных технологий» без корректировки санкций.
6. Из особо квалифицированных составов всех статей гл. 28 УК РФ убрать неопределенно-оценочный критерий «тяжкие последствия» с угрозой их наступления или без таковой, как в ст. 274.1 УК РФ, заменив его стоимостными критериями, как ранее оценочный критерий «существенный вред» был заменен стоимостным критерием «крупный ущерб». Первое примечание в ст. 272 УК РФ можно было бы расширить, установив там не только размер крупного ущерба, но и значительного, и особо крупного.
7. При сохранении в тексте гл. 28 УК РФ оценочного критерия «тяжкие последствия» с угрозой их наступления или без таковой следует принять Постановление Пленума Верховного Суда Российской Федерации, в котором дать пояснение этих понятий, а также обобщить и систематизировать судебную практику по правоприменению норм гл. 28 УК РФ и разъяснить судам проблемные вопросы квалификации этих преступлений.

8. Устранить ст. 274.1 УК РФ, текст которой и содержательно, и структурно представляется крайне неудачным и нарушающим правила законодательной техники, а признак «посягательство на критическую информационную инфраструктуру» сделать не криминообразующим для формирования специальных составов ст. 273, 272 и 274 УК РФ, как это сделано сейчас, а квалифицирующим, поместив его в квалифицированные составы этих статей. А если законодатель сочтет, что совершение деяний, посягающих на критическую информационную инфраструктуру, имеет высокую степень общественной опасности, то поместить в особо квалифицированные составы.

Следует отметить, что некоторые предложения криминологов уже были положительно восприняты законодателем и претворены в жизнь. Так, например, Т. М. Лопатина еще в 2006 г. предлагала криминализировать мошенничество в сфере информационных технологий [1, с. 21], что пятью годами спустя и было проделано законодателем при внесении в УК РФ специальных составов мошенничества (появилась ст. 159.6 УК РФ «Мошенничество в сфере компьютерной информации»). Правда, ее предложение заключалось не только в добавлении этой статьи в содержание российского уголовного закона, но и в помещении ее в структуру гл. 28 УК РФ. Оказалось реализованным, хотя и не в таком виде, как предлагалось ей в исследовании, ее же предложение о криминализации производства детской порнографической продукции с целью распространения: законодатель не только дополнил ч. 2 ст. 242.1 УК РФ «Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних», содержащую квалифицированный состав, квалифицирующим признаком, в котором есть п. «г» - «С использованием средств массовой информации, в т. ч. информационно-телекоммуникационных сетей (включая сеть “Интернет”)», но и ввел новую ст. 2422 УК РФ «Использование несовершеннолетнего в целях изготовления порнографических материалов или предметов» [2], где также в квалифицирующем составе ч. 2 есть пункт «г» - «С использовани-

ем информационно-телекоммуникационных сетей (включая сеть “Интернет”)». В обоих случаях законодатель предусмотрел достаточно суровое наказание: если в первом случае срок лишения свободы составляет от 3 до 10 лет, то во втором - от 8 до 15. Сама Т. М. Лопатина предлагала установить срок от 10 до 12 лет лишения свободы, причем не проводила дифференциации ответственности в отношении изготовителей и приобретателей такой порнопродукции.

Однако другое ее предложение пока осталось невостребованным законодателем: она, помимо криминализации компьютерного мошенничества, еще предлагала криминализировать подлог с использованием компьютерных технологий, чего до сих пор сделано не было. Отдельные ученые предлагают свой перечень расширения составов гл. 28 УК РФ, куда тоже включают такой вид подлога. Например, С. Д. Бражник предлагал следующий перечень составов этой главы: «несанкционированный доступ к компьютерной информации, создавший угрозу национальной безопасности», «умышленное уничтожение или повреждение компьютерной информации», «компьютерное мошенничество», «причинение имущественного ущерба путем изменения компьютерной информации», «компьютерное вымогательство», «компьютерный терроризм», «подлог компьютерной информации», «компьютерный шпионаж», «незаконное производство, использование или сбыт специальных технических средств» [3, с. 155].

В. С. Карпов, также рекомендуя криминализировать компьютерное мошенничество, причем разместив его не в гл. 28 УК РФ, а в качестве специального состава к ст. 159 УК РФ, предлагал некоторые статьи гл. 28 (ст. 272 УК РФ) изложить в новой редакции, установив уголовную ответственность за компьютерный саботаж с легальным прояснением этого понятия в примечании, и дополнив главу несколькими специальными составами и новыми составами: ст. 272.1 УК РФ «Несанкционированный доступ к компьютерной информации», ст. 272.2 УК РФ «Неправомерное завладение компьютерной информацией», ст. 272.3 УК РФ «Модификация компьютерной информации», ст. 272.4 УК РФ «Изготовление и

сбыт специальных средств для получения несанкционированного доступа к компьютерной системе или сети» [4, с. 7].

Вместе с тем в криминологической доктрине есть мнение [5], что подход к коррекции законодательства, продемонстрированный и рекомендованный С. Д. Бражником, предлагавшим в 2002 г. расширять перечень криминализируемых деяний в сфере информационных технологий во многом путем «перевода» уже существующих составов в их «компьютерный» вид, хотя и используется в англо-американской практике, однако страдает ограниченностью и крайне непродуктивен. В. М. Быков и В. Н. Черкасов, будучи противниками этого подхода, полагают, что, пойдя по этому пути, копирующему англосаксонские стандарты, где, например, есть понятие кибертерроризма, законодатель вынужден будет неоправданно «раздувать» содержание российского уголовного закона, добавляя в него до бесконечности все новые и новые составы (кибершпионаж, киберсаботаж, кибермошенничество, киберхалатность и пр.).

В. М. Быков и В. Н. Черкасов считают, что возможны три основные модели коррекции отечественного уголовного закона. В рамках первой модели вообще предлагается отказаться от понятия «компьютерные преступления» и рассматривать электронную информацию, а также интеллектуальные продукты в этой сфере как предметы преступных посягательств и квалифицировать преступные деяния, совершенные с ними, по статьям, которые уже есть в составе УК РФ (например, кража и пр.). Ученые называют это голландской моделью, снимающей сложности и проблемы с квалификацией киберпреступлений, хотя и требующей подготовки специалистов, а также экспертного сопровождения процесса расследования таких преступлений. Однако наше исследование не подтверждает их вывод: в Нидерландах компьютерные преступления вполне наличествуют. К аналогичному заключению ранее пришел и М. М. Малыковцев, указавший, что «ст. 138a, 139b, 139c, 139d, 139e, 161b, 350a, 350b, 351 Уголовного кодекса Нидерландов содержат деликты, отнесенные к компьютерным преступлениям» [6, с. 13].

Второй вариант, о котором говорят В. М. Быков и В. Н. Черкасов, весьма спорен. Они предлагают оставить гл. 28 УК РФ, но переделать ее содержание по модели предыдущей главы российского уголовного закона - гл. 27 УК РФ «Преступления против безопасности движения и эксплуатации транспорта» и считать информационные технологии источником повышенной опасности аналогично тому, как в гл. 27 УК РФ расценивается «транспортное средство». При таком подходе, по их мнению, уйдет множество проблем, связанных с квалификацией, и это поможет охватить максимально широкий круг антиобщественных деяний в указанной сфере.

Третья модель криминализации, которую описывают В. М. Быков и В. Н. Черкасов, представляет собой структурное выделение отдельной главы, посвященной уголовно-правовой ответственности за преступления в сфере компьютерной информации, и добавление квалифицирующих признаков в составы, сосредоточенные в других главах. В. М. Быков и В. Н. Черкасов полагают, что против добавления квалифицирующего признака «с использованием компьютерных/информационных технологий» возражений в научном сообществе не будет. Наш анализ показал, что такая модель уже во многом воспринята действующим российским уголовным законом в его актуальной редакции, однако законодатель, корректируя действующий УК РФ, дополнил эту модель еще и криминообразующими признаками, как, например, в ст. 159.6 УК РФ «Мошенничество в сфере компьютерной информации», однако не перенес ее в состав гл. 28 УК РФ.

Можно предположить, что и далее законодатель сочтет возможным сохранить уже действующую модель, несмотря на существующие в научной доктрине предложения о возможности реализации других концептуальных моделей, поэтому следует исходить из уже сложившейся концепции при решении вопроса о необходимости коррекции ответственности за компьютерные преступления в имеющихся составах и при добавлении новых составов, в которых была бы установлена ответственность за возможное совершение преступлений посредством

использования информационных технологий и/или в информационно-телекоммуникационных сетях, включая сеть «Интернет».

В начале данной статьи нами уже были предложены варианты редакционной правки гл. 28 УК РФ, однако, безусловно, концептуальная корректировка должна быть более масштабной. Обозначим ее возможные направления.

В ст. 272 гл. 28 УК РФ стоит изменить название «Неправомерный доступ к компьютерной информации», признав его не раскрывающим содержание диспозиции самой нормы. Нами вслед за С. Д. Бражником предлагается следующая редакция названия ст. 272 УК РФ «Несанкционированный доступ к защищенной компьютерной информации» и ее диспозиции - «Несанкционированный доступ к защищенной компьютерной информации, сопряженный с умышленным уничтожением или повреждением компьютерной информации, причинившим значительный ущерб, наказывается...». В тех случаях, когда нет тяжких последствий или деяние было совершено неосторожно, рекомендуется использовать административную преюдицию, перенеся в содержание Кодекса Российской Федерации об административных правонарушениях (далее по тексту -КоАП РФ) и сформулировав там как правонарушение с формальным составом [3]. Во втором примечании следует легально определить в стоимостном выражении для целей гл. 28 УК РФ не только размер крупного ущерба, но и особо крупного, и значительного.

Из названия ст. 273 УК РФ следует устранить неоправданную и ошибочную синонимию (приравнивание единственного и множественного числа, т. е. одной и нескольких вредоносных программ друг к другу), что может при буквальном толковании повлечь за собой декриминализацию деяния, совершенного в рамках создания одной вредоносной программы, сформулировав наименование этой статьи в следующей редакции: ст. 273 УК РФ «Создание или использование вредоносной компьютерной программы, причинившее значительный ущерб», исключив крупный ущерб в качестве квалифицирующего признака из квалифицированного состава ч. 2 этой статьи.

Ст. 274 УК РФ следует «разукрупнить», поскольку в ней описательная диспозиция представлена как сложная, содержащая в объективной стороне четыре деяния, а также ликвидировать перегруженность удвоением причинно-следственной связи в ее особо квалифицированном составе.

Ст. 274.1 УК РФ следует устранить из содержания гл. 28 УК РФ и дополнить предыдущие статьи гл. 28 УК РФ содержанием ст. 274.1 в качестве квалифицирующих признаков признак «посягательство на критическую информационную инфраструктуру» в квалифицированные или, если законодатель сочтет большой степень общественной опасности таких деяний, то в особо квалифицированные составы с соответствующей корректировкой санкций.

Решению ряда проблем, возникающих при квалификации в связи с невозможностью точного определения момента окончания преступления из-за структурного несовершенства норм и использования в них отглагольных существительных («уничтожение», «блокирование», «модификация», «копирование», «создание», «распространение», «использование», «нарушение» и др.), может помочь или разъяснение этих понятий на законодательном уровне, или устранение их из текста уголовного закона с добавлением в диспозицию причастия «причинившее», или прояснение их в соответствующем Постановлении Пленума Верховного Суда Российской Федерации (которое, кстати, до сих пор отсутствует, но оно необходимо с целью упорядочения правореализационной практики, придания ей единообразия и прояснения сложных вопросов, возникающих в процессе правоприменения уголовно-правовых норм, регламентирующих компьютерную преступность, о чем неоднократно говорили и писали криминологи).

Итак, с целью осуществления мер специальной превенции преступлений в сфере компьютерной информации назрела необходимость продолжения редакционной и/или концептуальной правки гл. 28 УК РФ, несмотря на уже имеющиеся шесть ее редакций. Редакционная корректировка почти не предполагает коренного изменения структуры гл. 28

УК РФ, в отличие от правки концептуальной, которая по своему характеру более масштабна, однако некоторые предложения могут и должны быть реализованы в рамках как редакционной, так и концептуальной правки (например, устранение ст. 274.1 УК РФ из содержания этой главы).

При проведении концептуальной правки, которая потребует значительной содержательно-структурной перестройки гл. 28 УК РФ, следует руководствоваться уже сделанными предложениями криминологов по соотнесению имеющихся норм с минимальным перечнем деяний в сфере информационных технологий, рекомендованных на европейском уровне для криминализации, опытом государств СНГ. Мы полагаем, что предложения С. Д. Бражника, сформулированные им с учетом требований и правил законодательной техники и отвечающие международному и зарубежному опыту регламентации ответственности за киберпреступления, вполне могут быть рассмотрены и востребованы законодателем. Концептуальная правка потребует не только «разукрупнения» статей и помещения в отдельные нормы обособленных составов (поскольку сейчас некоторые из них объединены в рамках одной статьи), расширения круга криминализированных деяний, изменения наименований статей, но и введения административной преюдиции с возможностью привлекать за антиобщественные деяния в сфере информационных технологий, совершение которых повлекло наступление последствий в виде значительного ущерба и/или иных последствий, к уголовной ответственности, в противном случае - к административной, что потребует разработки новой главы в КоАП РФ.

**Список литературы**

1. Лопатина Т. М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности: автореф. дисс. ...д-ра юрид. наук. М., 2007. 62 с.

2. О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации в целях усиления ответственности за преступления сексуального характера, совершенные в отношении несовершенно-

летних: Федеральный закон от 29.02.2012 № 14-ФЗ // Собрание законодательства РФ. 2012. № 10. Ст. 1162.

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

4. Карпов В. С. Уголовная ответственность за преступления в сфере компьютерной информации: дисс. ...канд. юрид. наук. Красноярск, 2002. 202 с.

5. Быков В. М., Черкасов В. Н. Правовые проблемы борьбы с компьютерными преступлениями // Актуальные проблемы экономики и права. 2008. № 1 (5). С. 103–112.

6. Малыковцев М. М. Уголовная ответственность за создание, использование и распространение вредоносных программ для ЭВМ: автореф. дисс. ...канд. юрид. наук. М., 2007. 24 с.

## References

1. Lopatina T. M. Criminological and criminal-legal foundations of combating computer crime: author. diss. ... Dr. legal sciences. M., 2007. 62 p.

2. On amendments to the Criminal Code of the Russian Federation and certain legislative acts of the Russian Federation in order to increase responsibility for crimes of a sexual nature committed against minors: Federal Law of 29.02.2012 No. 14-FZ // Collected Legislation of the Russian Federation. 2012. No. 10. Art. 1162.

3. Brazhnik S. D. Crimes in the field of computer information: problems of legislative technology: diss. ... Cand. legal sciences. Izhevsk, 2002. 189 p.

4. Karpov V. S. Criminal liability for crimes in the field of computer information: diss. ... Cand. legal sciences. Krasnoyarsk, 2002. 202 p.

5. Bykov V. M., Cherkasov V. N. Legal problems of combating computer crimes // Actual problems of economics and law. 2008. No. 1 (5). Pp. 103–112.

6. Malykovtsev M. M. Criminal liability for the creation, use and distribution of malicious computer programs: author. diss. ... Cand. legal sciences. M., 2007. 24 p.