КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ ПО УК РФ: ОЦЕНКА КРИМИНАЛИЗАЦИИ И РЕЗУЛЬТАТЫ ПРАВОПРИМЕНЕНИЯ

Н.А. Лопашенко

дюн, професор, професор Саратовской государственной юридической академии (СГЮА), г. Саратов, Россия

Высокие технологии, ворвавшись в нашу жизнь, сегодня уже заполнили многие ее стороны и аспекты, и стали совершенно необходимыми. Трудно себе представить, например, как можно обойтись без компьютера и Интернет. Оказывая бесценную помощь человеку в решении многих его проблем, они являются безусловным благом в процессе развития цивилизации. Однако, как однобоко и неправильно усматривать в любом явлении только позитивные моменты, так и высокие технологии должны быть оценены с точки зрения того вреда, который они приносят или могут принести человечеству. Соответственно, с точки зрения специалиста в уголовно-правовой науке, хотела бы подчеркнуть обязательность юридической квалификации этого вреда.

Видимо, есть вред, причиняемый техническим фактором, технической составляющей высоких технологий. Анализировать его, порождающие его причины и пути преодоления, – не моя епархия; это удел специалистов соответствующих отраслей научного знания. Качественно подобный вред, очевидно, может заключаться в причинении вреда жизни и здоровью людей, состоянию окружающей природной среды, собственности, и другим охраняемым уголовным законодательством благам. В случае умышленного или неосторожного отношения к нему лиц, допустивших такой вред, они могут быть, почти без каких-либо проблем, привлечены к уголовной ответственности за умышленные или неосторожные деяния.

Думаю, что использование высоких технологий, особенно, биотехнологий, уже сегодня вызывает массу этических проблем, поскольку ломает традиционные стереотипы восприятия биологической природы человека. Но эти проблемы пока еще проходят только стадию выявления, констатации; зачастую общество не готово даже к их обсуждению, не говоря уж о правовом решении. В действующем уголовном законодательстве России, естественно, нет и намека на возможное регулирование упомянутых проблем, хотя, рано или поздно, вопрос о нем встанет с неизбежностью. Поэтому и указанная группа проблем останется за рамками настоящей статьи.

Рассмотрим только те проблемы, связанные с высокими технологиями, которые уже сейчас восприняты уголовно-правовой и криминологической наукой как свои, – это проблемы самостоятельного существования так называемых компьютерных преступлений[1] и проблемы противодействия преступности, использующей компьютер-

[1] В литературе существуют позиции, согласно которым, термины „компьютерные преступления" и преступления в сфере компьютерной информации" – не совпадают друг с другом по объему (см., напр. Преступления в сфере компьютерной информации: квалификация и доказывание / Под ред. Ю.В. Гаврилина. – М.: ЮИ МВД РФ, 2003. – С. 11 и др.), при этом понятие „компьютерные преступления" – это больше криминалистическое понятие (См.: Там же; *Вехов В.Б., Голубев В.А.* Расследование компьютерных преступлений в странах СНГ. – Волгоград, 2004. – С. 56-57), с чем, однако, другие криминалисты не очень соглашаются (см., напр.: *Крылов В.В.* Информационные компьютерные преступления. – М.: Издательская группа ИНФРА-М-НОРМА, 1997. – С. 10).

ные технологии (если позволительно вообще употребление подобной терминологии). Посмотрим на них с точки зрения уголовно-правовой и криминологической политики.

2. Криминализация (декриминализация)

Криминализация каких-либо деяний оправдана только тогда, когда она осуществляется в соответствии с основанием и принципами криминализации.

Основанием криминализации большинство исследователей признает наличие общественно опасного деяния, требующего самостоятельного уголовно-правового запрета. Лежит ли оно в основе современных компьютерных преступлений, известных России и некоторым другим государствам?

В УК РФ преступления в сфере компьютерной информации сформулированы в гл. 28 УК и включают в себя в настоящее время[2] три состава преступления: неправомерный доступ к компьютерной информации (ст. 272 УК), создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК) и (ст. 274 УК). Рассмотрим их с точки зрения главной составляющей уголовной политики – криминализации, принимая во внимание тот факт, что сама идея криминализации компьютерных преступлений до сегодняшнего дня далеко не принимается всеми в науке безоговорочно.

Неправомерный доступ наказуем, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации. Таким образом, криминообразующими (свидетельствующими о достаточной для уровня преступного степени общественной опасности) признаками этого деяния выступают: 1) неправомерность действий лица, которое осуществляет доступ к чужой информации, на ознакомление с которой оно права не имеет; и 2) состоящие в причинной связи с таким поведением лица, наступившие негативные для владельца информации последствия (хотя бы одно из пяти перечисленных выше). Исходя из того, что при неправомерном доступе серьезно нарушаются права лица на обладание информацией и часто причиняется ущерб и самой этой информации, следует признать, что основание для криминализации отклоняющегося поведения, действительно, имело место. Создание и самостоятельное существование анализируемой нормы было необходимо, поскольку другие существующие уголовно-правовые нормы не в полной мере охватывают неправомерный доступ к компьютерной информации (в частности, в отдельных случаях к виновным возможно применение составов нарушения неприкосновенности частной жизни – ст. 137 УК, нарушения тайны переписки или иных сообщений – ст. 138 УК, незаконного получения и разглашения сведений, составляющих коммерческую, налоговую или банковскую тайну – ст. 183 УК, государственной измены и шпионажа – ст. ст. 275, 276 УК).

В равной степени можно констатировать наличие основания для криминализации таких действий, как создание, использование и распространение вредоносных компьютерных программ[3]. Их общественная опасность очевидна и перерастает ту, которая характерна для административного правонарушения, поскольку лицо не просто предпринимает действия, которые могут причинить вред правоохраня-

[2] Предложений о расширении этого перечня в науке – более, чем достаточно. См., напр.: *Курушин В.Д., Минаев В.А.* Компьютерные преступления и информационная безопасность. – М.: Новый Юрист, 1998. – 127-130 и др.

[3] Разумеется, сказанное не означает декларацию высокого качества законодательной техники, которая была использована при создании анализируемых уголовно-правовых норм. Однако, ее оценка остается за рамками настоящей статьи.

емым интересам других лиц, но делает это целенаправленно, осознавая, что создаваемая или распространяемая программа ведет к несанкционированным и негативным для владельца информации последствиям.

Думаю, что при осуществлении российской криминализации названных двух компьютерных преступлений, в основном, соблюдались и принципы криминализации: принципы достаточной общественной опасности криминализируемых деяний, их относительной распространенности, возможности позитивного воздействия уголовно-правовой нормы на общественно-опасное поведение, преобладания позитивных последствий криминализации, неизбыточности уголовно-правового запрета, своевременности криминализации. Можно, разумеется, рассуждать, что криминализация компьютерных преступлений, все же, несколько запоздала, однако, это будут, скорее, теоретические рассуждения. Массовая компьютеризация пришла в Россию совсем недавно, во второй половине девяностых годов; до этого большинство населения страны едва ли представляло себе, как выглядит персональный компьютер. Наверное, подобное отклоняющееся поведение было и раньше, но оно явно носило единичный характер, и проведение криминализации, положим, в конце восьмидесятых или начале девяностых годов прошлого столетия нарушило бы другой принцип криминализации – принцип относительной распространенности общественно опасных явлений.

Что же касается третьей статьи компьютерных преступлений, то она претерпела очень большие изменения в конце 2011 г., и оценка ее криминализации существенно поменялась. Прежняя редакция статьи предусматривала ответственность за нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети Речь, таким образом, шла об установлении уголовной ответственности для правомерного (допущенного к обладанию информацией) пользователя ЭВМ, системы ЭВМ или их сети (мы, наконец, в 2011 г. отказались от этих понятий), который, нарушая правила пользования, причинял ущерб владельцу информации. Суть отклоняющегося поведения, которое может быть общественно опасно, коль скоро причиняет вред (достаточный ли для преступного – другой вопрос), вроде бы, была ясна, но только на первый взгляд. Возникал немедленно вопрос: что следует понимать под „правилами пользования ЭВМ, системы ЭВМ или их сети", который не знал единственного, и, следовательно, верного, ответа вплоть до изменения редакции ст. 274 УК. Имелись ли в виду технические правила обращения с ЭВМ и т.д. (условно говоря – не бить, не ронять и т.п.), или же речь шла о правилах обращения с информацией, хранящейся в ЭВМ, или той, которую можно получить, используя ЭВМ? А может быть, возможно было понимать под этими правилами все вместе, включая еще и специфические правила, например, правила бухгалтерского учета, или, как предлагалось в литературе, „во-первых, гигиенические требования к видеодисплейным терминалам, персональным электронно-вычислительным машинам и организации работы, во-вторых, техническая документация на приобретаемые компьютеры, в-третьих, конкретные, принимаемые в определенном учреждении или организации, оформленные нормативно и подлежащие доведению до сведения соответствующих работников правила внутреннего распорядка, в-четвертых, требования по сертификации компьютерных сетей и оборудования, в-пятых, должностные инструкции конкретных сотрудников, в-шестых, правила пользования компьютерными сетями"[4]? Ответов на эти вопросы не было. Соответст-

[4] См.: Преступления в сфере компьютерной информации: квалификация и доказывание / Под ред. Ю.В. Гаврилина. – М.: ЮИ МВД РФ, 2003. – С. 47. Здесь же хотелось бы заметить, что такое понимание правил вызывает у меня яростное сопротивление, в связи с тем, что сфера криминализации, если исходить из него, расширяется мультикратно, и напоминает мне известную присказку: „Шаг вправо, шаг влево, – попытка к бегству, расстрел".

венно, сфера преступного деяния оставалась совершенно неопределенной, а границы криминализации – сверх подвижными и наполнялись реальным содержанием правоприменителем, что недопустимо, поскольку противоречит принципу законности уголовного законодательства.

Кроме того, нельзя не сказать еще и том, что в большинстве случаев преследующему, например, корыстные цели правомерному пользователю ЭВМ, для их достижения вовсе не требовалось нарушение правил пользования; он действовал методично в соответствии с ними.

Не меньше проблем было с формой вины. Законодатель прямо в диспозиции статьи ее не указывал (в ч. 2 было упоминание о неосторожном отношении к тяжким последствиям), что рождало, по крайней мере, две возможных версии о ее содержании: преступление может быть совершено с прямым или косвенным умыслом[5], или: возможна как умышленная, так и неосторожная формы вины[6]. Сам же термин «нарушение правил» - более, на мой взгляд, свидетельствовал (и свидетельствует, он остался в новой редакции) о неосторожной форме вины, нежели об умышленной. И разница в позициях здесь – принципиальна, каждая позиция (а на практике они тоже присутствовали) формулировала свой круг преступного и наказуемого и, соответственно, свои пределы криминализации.

Далее. Российский законодатель использовал в анализируемом составе несколько криминообразующих признаков сразу: 1) нарушение правил пользования ЭВМ, системой ЭВМ или их сетью – в этом была суть отклоняющегося поведения, которое, как мы видели выше, было абсолютно лишено точных границ; 2) последовавшие в результате этого уничтожение, блокирование или модификация охраняемой законом информации; и 3) причинение существенного вреда. Таким образом, о наличии состава преступления должны были свидетельствовать сразу два возможных последствия: последствие первого порядка – в отношении информации, и последствие второго порядка – существенный ущерб, принадлежность и содержание которого в законе не были обозначены. В каких отношениях должны были находиться между собой названные последствия? Между чем и чем должна была устанавливаться на практике причинная связь? Сколько ее видов должно было быть констатировано? Очевидно, должна была быть причинная связь между нарушением правил пользования ЭВМ и т.д. и последствиями первого порядка – в отношении информации. Что же дальше? Уничтожение, блокирование или модификация охраняемой законом информации должны стать причиной существенного ущерба, или последний должен был быть причинен в результате того же нарушения правил?

Не следует забывать, однако, что после установления причинной связи мы должны были установить не менее сложную виновную связь, и, следовательно, с известной корректировкой вновь пойти по тем вопросам, которые я выше поставила.

---

[5] См., напр.: Российское уголовное право: Курс лекций. Т. 5. Преступления против общественной безопасности и общественного порядка / Под ред. А.И. Коробеева. – Владивосток, 2001. – С. 587. Автор главы – В.В. Крылов; *Бытко С.Ю.* Преступления в сфере компьютерной информации. – Саратов, 2004. – С. 39.

[6] См., напр.: Практический комментарий к Уголовному кодексу Российской Федерации / Под общей ред. Х.Д. Аликперова и Э.Ф. Побегайло. – М., 2001. – С. 685. Автор главы – С.В. Полубинская; *Панфилова Е.И., Попов А.С.* Компьютерные преступления. – СПб, 1998. – С. 32-33; *Бражник С.Д.* Преступления в сфере компьютерной информации. – Ярославль, 2000. – С. 25; *Вехов В.Б., Голубев В.А.* Расследование компьютерных преступлений в странах СНГ. – Волгоград, 2004. – С. 96.

Но если с доказательством прямого умысла проблем не возникало, то с косвенным, а, тем паче, с неосторожной виной – правоприменители в полной мере хлебнули горя.

Конечно, можно объяснить все мои вопросы и очевидные проблемы в законодательном регулировании недостатками одной только законодательной техники, которая неудачно применялась при формулировании состава нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети. Думаю, однако, дело – в другом: в нарушении принципов криминализации такого отклоняющегося поведения. Использование законодателем двух уровней последствий в качестве обязательных признаков состава подчеркивает то, что опасность самого деяния – не велика, если рассматривать понятие деяния – нарушение правил пользования – самым простым образом. Не достигало степени преступного и деяние, сопровождаемое ближайшими, – не отдаленными (существенный вред) последствиями. Следовательно, вполне возможно было, на мой взгляд, влиять на такое поведение мерами других правовых отраслей, прежде всего, – гражданского и административного. Распространенность подобных деяний также, полагаю, едва ли, свидетельствует о необходимости самостоятельного уголовно-правового запрета (в 1997 г. в целом по России было возбуждено по ст. 274 УК 11, в 1998 г. – 1, в 1999 г. – 0, в 2000 г. – 44, в 2001 г. – 119, в 2002 г. - 8, в 2003 г. - 1, в 2004 г. - 11, в 2005 г. - 2, в 2006 г. - 3, в 2007 г. - 7, в 2008 г. - 17, в 2009 г. - 5, в 2010 г. - 0, в 2011 - 0, в 2012 г. - 1, в 2013 г. - 0, в 2014 г. - 3 уголовных дела; за все годы действия УК привлечено к ответственности 13 человек – по данным МВД РФ). И, наконец, ст. 274 УК давала нам пример избыточной криминализации. Очевидно, что при ее проведении преследовалась цель привлечения к ответственности как раз тех лиц, которые, используя свое служебное положение, совершали хищения, применяя высокие технологии. Хищение – это материальный состав; для его наличия требуется причинение материального вреда. Состав нарушения правил, если можно так выразиться, - дважды материальный, одно из возможных последствий – существенный вред. Однако, если имелся в виду тот же вред, который причиняется хищением, мы нарушали принцип справедливости уголовного законодательства и дважды привлекали к уголовной ответственности за одно и то же.

В прежней редакции, поэтому, на мой взгляд, деяние, предусмотренное ст. 274 УК, должно было быть декриминализировано.

В настоящее время, как отмечалось выше, состав ст. 274 УК в значительной мере изменен. Суть самых важных изменений сводится к следующему (не оговариваю здесь изменение понятийного аппарата – ЭВМ – компьютерная информация, верное и давно ожидаемое):

1) вместо одной формы деяния стало две, и обе связаны с тем же понятием, что и было раньше – нарушение правил, однако, правила разнятся – речь идет в первом деянии о правилах эксплуатации, во втором – о правилах доступа, и соответственно, и деяния разные;

2) не смотря на то, что на первый взгляд мало что изменилось по первой форме – как было нарушение правил эксплуатации, так и осталось, – за счет конкретного законодательного очерчивания предмета этих правил стало совершенно конкретным и само деяние: должны быть нарушены правила эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования;

3) достаточно конкретным является и предмет нарушения других правил – законодатель отмечает, что нарушаются правила доступа к информационно-телекоммуникационным сетям;

4) схема двойных последствий осталась, и последствия первого порядка расширены за счет добавления еще одного, – копирования компьютерной информации, наряду с уничтожением, блокированием, модификацией, что вполне согласуется с тем, как выстроены другие составы компьютерных преступлений;

5) изменилось понятие последствия второго порядка – вместо существенного вреда, о котором речь шла в первой редакции статьи, теперь необходимо причинение крупного ущерба. По логике законодательства он связывается, в отличие от существенного вреда, исключительно с имущественным характером (в примечании 2 к ст. 272 УК этот размер определен, он должен превышать один миллион рублей);

6) ушло из диспозиции статьи упоминание о субъекте преступления – лице, имеющем доступ к ЭВМ, системе ЭВМ или их сети. Это означает, что субъект значительно расширен, теперь в качестве него может выступать и не специальный субъект.

Таким образом, сфера криминализации по этой статье, с одной стороны, значительно сужена (за счет отказа от понятия существенного вреда и уточнения тех правил, которые могут быть нарушены), с другой стороны – в какой-то степени расширена (за счет расширения субъекта), и уточнена до тех пределов, что правоприменение стало возможным.

3. Пенализация (депенализация)

Компьютерные преступления в российском уголовном законодательстве ныне включают в себя преступления трех первых категорий степени тяжести, о чем свидетельствует следующая таблица:

Категория преступлений и максимальный срок лишения свободы в рамках категории / часть статьи	**Небольшая тяжесть**	**Средняя тяжесть**	**Тяжкие**	**Особо тяжкие**
Ч. 1 ст. 272 УК	**Лишение свободы до двух лет**	**-**	**-**	
Ч. 2 ст. 272 УК	**-**	**Лишение свободы до четырех лет**	**-**	
Ч. 3 ст. 272 УК	**-**	**Лишение свободы до пяти лет**	**-**	
Ч. 4 ст. 272 УК	**-**	**-**	**Лишение свободы до семи лет**	
Ч. 1 ст. 273 УК	**-**	**Лишение свободы до четырех лет**	**-**	
Ч. 2 ст. 273 УК	**-**	**Лишение свободы до пяти лет**	**-**	
Ч. 3 ст. 273 УК	**-**	**-**	**Лишение свободы до семи лет**	
Ч. 1 ст. 274 УК	**Лишение свободы до двух лет**	**-**	**-**	
Ч. 2 ст. 274 УК	**-**	**Лишение свободы до пяти лет**	**-**	

Таким образом, компьютерные преступления не представлены только особо тяжкими преступлениями.

Палитра наказаний, которые могут быть назначены за компьютерные преступления в России, – достаточно широка: штраф в качестве основного или дополнительного наказания (ч. 1 – 3 ст. 272 (основное), ч. 1 и ч. 2 ст. 273 УК (дополнительное), ч. 1 ст. 274 УК (основное)), лишение права занимать определенные должности или заниматься определенной деятельностью в качестве дополнительного наказания (ч. 3 ст. 272, ч. 2 ст. 273 УК), исправительные работы (ч. 1 и ч. 2 ст. 272, ч. 1 ст. 274 УК), ограничение свободы (ч.ч. 1-3 ст. 272, ч.ч. 1 и 2 ст. 273, ч. 1 ст. 274 УК), принудительные работы (ч.ч. 1 – 3 ст. 272, ч.ч. 1-2 ст. 273, ст. 274 УК), лишение свободы (по всем простым и квалифицированным составам, исключений, как раньше в отношении прежней редакции ч. 1 ст. 274 УК, нет). Из системы наказаний за компьютерные преступления ушли в 2011 г. обязательные работы (ч. 1 ст. 274 УК в прежней редакции) и арест (ч. 2 ст. 272 УК в прежней редакции), вновь включены принудительные работы. Думаю, сам факт значительного количества возможных к применению уголовных наказаний должен восприниматься, как положительная тенденция, поскольку непосредственно позитивно влияет на дифференциацию и индивидуализацию ответственности. В то же время обращает на себя внимание явная тенденция к ужесточению наказаний за компьютерные преступления.

Использование чужого, зарубежного опыта противодействия компьютерной преступности и международная кооперация ученых и практиков в этом важном деле, вполне реально может привести к положительным сдвигам в пресечении и предупреждении преступлений в сфере высоких технологий, известных мировому сообществу уже сегодня.