АКТУАЛЬНЫЕ ПРОБЛЕМЫ УГОЛОВНОГО ПРАВА В БОРЬБЕ С ПРЕСТУПЛЕНИЯМИ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ПУТИ ИХ РЕШЕНИЯ

© Авторы, 2016
Трофимов Д. В.,
магистрант 1 курса факультета права,
Рузевич О. Р.,
канд. юрид. наук, заведующий кафедрой
административно-правовых дисциплин,
Владимирский филиал РАНХиГС

Аннотация: в данной статье рассмотрены некоторые проблемы определения преступлений в сфере компьютерной информации. Авторы, проанализировав сущность данных преступлений, предлагают новые редакции статей главы 28 Уголовного кодекса Российской Федерации.

Ключевые слова: информационные технологии, сеть «Интернет», компьютерные преступления, киберпреступность.

Abstract: in this article, we consider some problems of definition of crimes in the sphere of computer information. The authors, after analyzing the nature of these crimes, I propose new wording of articles of Chapter 28 of the Criminal code of the Russian Federation.

Keywords: nformation technology, the Internet, computer crime, cybercrime.

Вхождение информационных технологий и сети «Интернет» в повседневную жизнь людей в корне поменяло то, как люди во всем мире осуществляют коммуникации, получают и обрабатывают информацию, осуществляют покупки и проводят время. Без сети «Интернет» и различных вычислительных устройств невозможно представить современное, динамично развивающееся общество. Политика государственного принуждения должна дополняться повышением как правовой, так и общей культуры людей, их правосознания, своевременной деятельностью компетентных органов по предупреждению преступлений. Потребность осуществления вышеуказанных направлений деятельности вызвана постоянно растущей ролью информационных технологий в обществе. В период с 2000 по 2015 год удельный вес пользователей Интернета увеличился почти в семь раз − с 6,5 до 43 процентов мирового населения. Число пользователей Интернета в России составляет 87,5 млн человек[1].

Рост количества пользователей Интернета в России вынуждает государство повышать уровень информационной безопасности и акцентировать внимание на борьбе с компьютерными преступлениями. Улучшая и упрощая жизнь, информационные технологии при этом дают новые возможности для противозаконного поведения. Так число зарегистрированных компьютерных преступлений за 2014 год составило 11000[2].

Развитие Интернета как средства общения и обмена информацией стерло границы для развития многих преступных банд. Используя современные технологии, злоумышленники имеют возможность осуществления неправомерного доступа к информации, хранящейся в памяти различных устройств, находящихся в разных точках мира. С ростом числа пользователей сети «Интернет» многократно увеличилось количество пе-

[1] МСЭ публикует данные по ИКТ за 2015 год [Электронный ресурс]. URL: http://www.itu.int/net/pressoffice/press_releases/2015/pdf/17-ru.pdf.

[2] МВД зарегистрировало около 11 000 киберпреступлений в 2014 г. [Электронный ресурс]. URL: http://www.vedomosti.ru/technology/articles/2015/02/06/kiberprestupniki-v-spiskah-ne-znachatsya.

реданной с помощью компьютеров и их сетей информации (военной, разведывательной, коммерческой и банковской тайны, а также личных сообщений), а компьютерная преступность приобрела транснациональный характер.

Компьютерная преступность чрезвычайно латентна (от 85 до 99 %). Латентность преступлений объясняется сложностью выявления этого вида преступлений, отсутствием уверенности потерпевшей стороны в наказании виновных, возврате потерянных денежных средств, необходимостью сохранения престижа, нежеланием раскрытия конфиденциальной информации. Очевидна повышающаяся опасность компьютерных преступлений, так при хорошо продуманной и организованной атаке на сайт интернет-магазина ущерб может многократно превышать ущерб от «стандартного» ограбления[3].

Компьютерные преступления тем опаснее, что могут причинить ущерб практически любым правоохраняемым интересам, начиная от частных неимущественных интересов отдельных граждан и заканчивая интересами государственной безопасности. На сегодняшний день в Уголовном кодексе Российской Федерации практически все преступления могут быть совершены с использованием электронных средств обработки информации (за исключением некоторых составов преступлений против жизни и здоровья). Важно отметить, что сильно поменялась тенденция совершаемых компьютерных преступлений. Если на раннем этапе развития они зачастую совершались из хулиганских побуждений, то сейчас основной целью является получение прибыли (наживы). В настоящее время киберпреступность приобрела организованный вид, став источником дохода, и относиться к ней нужно соответственно. Многие имущественные и другие преступления совершаются с помощью электронно-вычислительных устройств. Даже если говорить о чисто «компьютерных» составах преступлений, то и они совершаются чаще всего с корыстной целью - продать информацию, получить право на чужое имущество или имущественные права. Кроме того, компьютерная преступность становится все более квалифицированной и должна рассматриваться обществом и государством как серьезная угроза его стабильному существованию. Вышесказанное говорит об острой необходимости обдуманного и очень детального законодательного регулирования ответственности за компьютерные преступления.

Доктрина информационной безопасности Российской Федерации утверждена Президентом РФ 9 сентября 2000 г. № Пр-1895[4]. В Доктрине определены основные направления уголовно-правовой политики по борьбе с компьютерными преступлениями. Важно отметить, что национальная безопасность в большей степени зависит от информационной безопасности, и с развитием технических средств и информационного общества эта зависимость будет расти. Под «информационной безопасностью Российской Федерации» в Доктрине понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства. Уголовно-правовая политика в сфере борьбы с компьютерными преступлениями должна строиться на основе национальных интересов Российской Федерации.

Одним из четырех основных составляющих национальных интересов государства в Доктрине выделяется защита информационных ресурсов и телекоммуникационных систем на территории России. Доктрина информационной безопасности Российской Федерации также отражает различные виды угроз информационной безопасности России,

---

[3] Степанов-Егиянц В. Г. Преступления против компьютерной информации: сравнительный анализ. - М., 2010. С. 7.

[4] Доктрина информационной безопасности РФ [Электронный ресурс]. URL: http://www.scrf.gov.ru/documents/6/5.html.

одной из которых является угроза безопасности информационных и телекоммуникационных средств и систем как уже развернутых, так и создаваемых на территории страны. Именно к данной категории угроз информационной безопасности Российской Федерации и относятся компьютерные преступления.

Наиболее распространенными преступлениями с использованием компьютерной техники являются: неправомерный доступ к компьютерной информации, мошенничество, распространение программ, предназначенных для несанкционированного доступа, незаконное использование объектов авторского права или смежных прав. Основная цель неправомерного доступа - несанкционированное получение доступа к информации, представляющей интерес для злоумышленников. В зависимости от специфики компьютерных преступлений их выделяют в отдельные виды такие, как кардинг (вид мошенничества, при котором производится операция с использованием платежной карты или её реквизитов, не инициированная или не подтвержденная её держателем), фишинг (вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям), фрикинг (вид мошенничества, при котором производится взлом телефонных автоматов, телефонных сетей и сетей мобильной связи, с использованием скрытых от пользователя или недокументированных функций). Генеральным секретариатом Интерпола была разработана специальная классификация компьютерных преступлений, включающая в себя следующие их виды:

QA - несанкционированный доступ и перехват (QAH - компьютерный абордаж; QAI – перехват; QAT - кража времени; QAZ - прочие виды несанкционированного доступа и перехвата);

QD - изменение компьютерных данных (QDL - логическая бомба; QDT - троянский конь; QDV - компьютерный вирус; QDW - компьютерный червь; QDZ - прочие виды изменения данных);

QF - компьютерное мошенничество (QFC - мошенничество с банкоматами; QFF - компьютерная подделка; QFG - мошенничество с игровыми автоматами; QFM - манипуляции с программами ввода-вывода; QFP - мошенничества с платежными средствами; QFT - телефонное мошенничество; QFZ - прочие компьютерные мошенничества);

QR - незаконное копирование (QRG - компьютерные игры; QRS - прочее программное обеспечение; QRT - топография полупроводниковых изделий; QRZ - прочее незаконное копирование);

QS - компьютерный саботаж (QSH - с аппаратным обеспечением; QSS - с программным обеспечением; QSZ - прочие виды саботажа);

QZ - прочие компьютерные преступления (QZB - с использованием компьютерных досок объявлений; QZE - хищение информации, составляющей коммерческую тайну; QZS - передача информации конфиденциального характера; QZZ - прочие компьютерные преступления)[5].

Формулировки статей 28 главы УК РФ[6], существовавшие до вступления в силу Федерального закона № 420-ФЗ от 7 декабря 2011 года, вызывали много критики[7]. Действующая редакция статей главы 28 УК РФ вызывает множество вопросов и проблем как у правоприменителя, так и в теории уголовного права.

Во-первых, вызывает сомнение определение компьютерной информации, данное в примечании 1 к ст. 272 УК РФ, где сказано, что компьютерная информация - это

---

[5] URL: http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime.

[6] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // СПС «Консультант плюс».

[7] Федеральный закон от 07.12.2011 № 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» // СПС «Консультант плюс».

сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Законодатель пошел по пути, избранному Конвенцией о преступности в сфере компьютерной информации (Будапешт, 23 ноября 2001 г.)[8], в которой акцент сделан на форме представления информации. По нормам Конвенции, предмет определяемых ею посягательств образует информация в форме, доступной восприятию ЭВМ или передающаяся по каналам связи. В каком виде ЭВМ и иные технические средства могут воспринимать компьютерную информацию? Представление компьютерной информации осуществляется с помощью языка, содержащего всего два символа алфавита – 0 и 1. Инженеров такой способ представления информации привлек простотой технической реализации проблемы кодирования. Легко различимые состояния – есть электрический сигнал (1) или нет сигнала (0) – позволяют разными способами двоичного кодирования и декодирования, в основе которых лежат логика и математика, распознать и обработать техническими средствами для достижения поставленной задачи любые сведения (сообщения, данные).

Научный и технический поиск новых путей и способов представления компьютерной информации говорит нам о том, что появляются новые формы существования компьютерной информации, отличные от «электрической». Имеются сообщения о все более широком применении микросхем с использованием магниторезистивной памяти с произвольным доступом. Данные в микросхему записываются не с помощью электрических зарядов, а с помощью магнитной поляризации элементов памяти, что обеспечивает важное для этого типа памяти свойство – возможность сохранять записанные в ячейки данные даже в случае отключения питания[9]. Если исходить из формулировки статьи, законодательная дефиниция не соответствует отражаемой ей действительности. Тем самым информация, передаваемая таким способом, окажется вне поля правового регулирования, оказывая негативное влияние на правоприменительную деятельность.

К сожалению, замечания Комитета по информационной политике при Государственной Думе РФ, предложившего альтернативное определение[10], не были учтены, и, если в ближайшее время не выйдет комментирующего главу 28 УК РФ постановления Пленума Верховного Суда Российской Федерации, мы можем ожидать значительных разногласий в процессе правоприменения ст. 272 УК РФ.

Проанализировав существующие в настоящее время определения «компьютерной информации», предлагаем следующее определение.

Компьютерная информация - это сведения (сообщения, данные), манипуляция над которыми осуществляется с использованием электронно-вычислительной техники, независимо от средств их хранения, обработки и передачи.

В связи с быстрым развитием науки указывать конкретный носитель информации не имеет смысла, важнее обозначить факт обязательного присутствия электронных устройств при обработке информации. Этого достаточно для отграничения понятия компьютерной информации от смежных.

Во-вторых, вызывает много вопросов название самой главы 28 УК РФ: «Преступ-

---

[8] Конвенция о преступности в сфере компьютерной информации (ETS N 185) (Будапешт, 23 ноября 2001 года) [Электронный ресурс]. URL: https://rm.coe.int.

[9] URL: http://www/top.rbc.ru/economics/19/08/2014/943629.shtml.

[10] Заключение Комитета по информационной политике, информационным технологиям и связи от 05.07.2011 на проект федерального закона № 559740-5 «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» [Электронный ресурс]. URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=PRJ;n=90718.

ления в сфере компьютерной информации». На сегодняшний день существует множество устройств, которые не являются компьютером, с помощью которых осуществляется сбор, передача и хранение различных данных в электронном виде, а также осуществляется доступ в сеть «Интернет» и к различным ресурсам. И, естественно, указанные электронные устройства можно использовать для осуществления преступлений, закрепленных в главе 28 Уголовного кодекса РФ. Например, можно осуществить неправомерный доступ к информации, хранящейся на электронной почте или сервере, с помощью телефона, имеющего доступ в сеть «Интернет» (и других электронных устройств). Данные устройства не являются компьютерами, соответственно и преступления к компьютерным не относятся, тогда понятие «компьютерная преступность» утрачивает свою специфику.

Следовательно, понятие «компьютерная преступность» в формулировке названия главы 28 УК РФ должно быть заменено на более широкое по значению - «преступность в сфере информационных технологий». Иначе какой смысл называть «компьютерными» преступления, которые с компьютерами никак не связаны? В соответствии с этим название главы 28 УК РФ должно быть изменено и представлено в следующем виде - «Преступления в сфере информационных технологий».

На основании вышеизложенного перенос статьи 138.1 УК РФ «Незаконный оборот специальных технических средств, предназначенных для негласного получения информации» в 28-ю главу УК выглядит уместным.

В-третьих, проблемным вопросом видится формулировка диспозиции ч. 1 ст. 272 УК РФ, подразумевающая наступление уголовной ответственности лишь в случае наступления последствий неправомерного доступа в виде уничтожения, блокирования, модификации либо копирования компьютерной информации. Сам по себе доступ к закрытой компьютерной информации не является преступлением, лицо может нарушить работоспособность системы защиты любого устройства, посмотреть содержащиеся там данные, и наказание за данное действие не последует, что неприемлемо в правовом государстве.

Формулировка состава соответствующей статьи свойственна правовым нормам многих стран, включая большинство стран СНГ. В качестве примера можно привести статью 271 УК Республики Азербайджан[11], практически не отличающуюся по названию и содержанию от ст. 272 УК РФ. В превалирующей части Уголовных кодексов стран СНГ мы встретим схожие формулировки данной статьи. Тем не менее в нормах уголовного права Республики Таджикистан нами был обнаружен наиболее эффективный способ решения данного вопроса. Диспозиция ст. 298 Уголовного кодекса Республики Таджикистан выглядит следующим образом:

«Неправомерный доступ к информации, хранящейся в компьютерной системе, сети или на машинных носителях, сопровождающийся нарушением системы защиты»[12].

Статья ст. 298 Уголовного кодекса Республики Таджикистан имеет формальный состав, но в ней присутствует обязательное условие о сознательном преодолении преступником средств защиты, что исключает саму возможность привлечения к уголовной ответственности лиц, узнавших тайную информацию неумышленно.

Законодатель Республики Беларусь пошел по пути разделения, выделив непра-

---

[11] Утвержден Законом Азербайджанской Республики от 30 декабря 1999 года [Электронный ресурс]. URL: http://law.edu.ru/norm/norm.asp?normID=1242908&subID=10010%204131,100104133,100104143,100104744,100104975#text.

[12] Закон Республики Таджикистан от 21 мая 1998 года № 574 [Электронный ресурс]. URL: http://law.edu.ru/norm/norm.asp?normID=1242456&subID=100100844,100100857,100100935,100101578,100101580.

вомерный доступ, компьютерный саботаж, копирование и модификацию компьютерной информации в отдельные статьи[13]. На наш взгляд, данный подход оправдан, но такое разделение статей необязательно.

На основании вышеизложенного можно сформулировать статью 272 УК РФ в следующем виде:

«1. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние сопровождалось нарушением правил, систем защиты средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, -

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. То же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности и (или) повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, -

наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, -

наказываются штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок.

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, -

наказываются лишением свободы на срок до семи лет».

Таким образом, первая часть предлагаемой формулировки статьи имеет формальный состав, а незаконное копирование, модификация, блокирование или уничтожение информации вынесено в квалифицированный состав.

Несмотря на то, что статья 167 Уголовного кодекса Российской Федерации предусматривает ответственность за умышленные уничтожение или повреждение чужого имущества, разумным выглядит дополнение статьи 274 УК РФ частью 3 о компьютерном саботаже как выводе из строя электронно-вычислительного оборудования либо разрушении компьютерной системы, сети или носителя информации. Учитывая специфику компьютерного саботажа, в частности возможность его совершения посредством удалённого доступа к информации, содержащейся на электронном устройстве, логичным будет дополнить уже существующую статью 274 УК РФ нормой о предусмотренном в ней деянии, совершённом с умышленной формой вины. Наиболее правильной видится формулировка диспозиции данной нормы, отчасти заимствованная в Уголовном кодексе

[13] Уголовный кодекс Республики Беларусь от 9 июля 1999 г. № 275-З [Электронный ресурс]. URL: http://www.newsby.org/documents/kodeks/kod21/page27.htm.

Республики Беларусь: «Умышленные уничтожение, блокирование, приведение в непригодное состояние компьютерной информации или программы, либо вывод из строя электронно-вычислительного оборудования, либо разрушение компьютерной системы, сети или носителя информации».