DOI: 10.25586/RNU.V9276.18.06.P.27 УДК 349

А.А. Тыртышный, И.С. Рекунков, И.А. Атрехалина

ИСТОРИЯ И ЗАРУБЕЖНЫЙ ОПЫТ ПРАВОВОЙ РЕГЛАМЕНТАЦИИ КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ

Компьютерная преступность представляет собой очень серьезную угрозу как для отдельных государств, так и для всего мирового сообщества, в связи с чем необходимо разработать и реализовать на практике действенные механизмы противодействия подобным явлениям.

В статье проведен анализ зарубежного опыта правовой регламентации компьютерной преступности.

***Ключевые слова*:** *компьютерная преступность, информационное пространство.*

A.A. Tyrtyshniy, I.S. Rekunkov, I.A. Atrehalina

HISTORY AND FOREIGN EXPERIENCE IN LEGAL REGULATION OF COMPUTER CRIME

Computer crime poses a very serious threat, both for separate States and for the international community, in connection with which it is necessary to develop and implement effective mechanisms of counteraction to such phenomena.

The article analyzes the foreign experience in legal regulation of computer crime.

***Keywords*:** *computer crime, information space.*

Современный этап в истории Российского государства отличается появлением новых видов преступлений и качественным изменением уже известных ранее.

В последние десятилетия отмечается бурное развитие компьютерных технологий и их активное внедрение во все без исключения сферы жизни общества. Огромные массивы различных сведений представлены в виде компьютерной информации, что существенно облегчает работу с ними. Информационные сети локального характера, а также Интернет позволяют обмениваться информацией за секунды, координировать действия различных служб, органов, подразделений и организаций, создавать единое информационное пространство. Кроме того, внедрение компьютерных технологий в значительной степени позволило автоматизировать различные производственные и управленческие процессы, что способствовало увеличению производительности труда. Это далеко не все плюсы массовой компьютеризации, которая имеет место во всех развитых странах.

Вместе с тем, появление ЭВМ и дальнейшее развитие компьютерных технологий привело к возникновению совершенно нового вида преступности – компьютерной.

Родиной термина «компьютерная преступность» считается США, где в 1960-х годах подобное словосочетание впервые появилось в СМИ в связи с выявлением первых преступлений, совершённых с использованием ЭВМ [3]. Так, в 1969 г. Альфонсе Конфессоре, получив незаконно доступ к информации в электронно-вычислительной сети, совершил налоговое преступление, ущерб от которого составил $620 000, а в 1970 году, также путем незаконного доступа к информации «Секьюрити пэсификбэнк», с одного из счетов банка было незаконно списано $10,2 миллиона.

Первое преступление, совершенное с использованием ЭВМ в бывшем СССР, было зарегистрировано в 1979 году в Вильнюсе – это было хищение, ущерб от которого составил 78 584 руб. [4].

В 1983 году в Париже группой экспертов Организации экономического сотрудничества и развития (ОЭСР) было дано криминологическое определение компьютерного преступления, под которым понималось любое незаконное, неэтичное или неразрешенное поведение, затрагивающее автоматизированную обработку и (или) передачу данных [3].

Подобные преступления стали совершаться всё чаще, а их сложность и причиняемый ими ущерб только возрастали.

Всплеск компьютерной преступности вызвало появление сети Интернет.

Так, в 1988 г. студент Корнельского университета Роберт Моррис создал компьютерную программу, названную позже «червь», предназначенную специально для атаки компьютеров через сеть Internet. В отличие от компьютерных вирусов, которые автоматически присоединяются к той или иной программе, нарушая ее работу, созданная им программа «червь», попав в компьютер-жертву, размножается и проникает во все системы компьютера, вызывая его сбой главным образом за счет «съедания» ресурсов памяти. До того, как данная программа была нейтрализована, она вызвала сбои в работе примерно 6200 компьютеров в США и других странах, повлекла за собой ущерб на сумму более 98 миллионов долларов США [3].

Что же касается России, то первые преступления с использованием компьютерной техники, совершённые на территории РСФСР, были зарегистрированы в 1991 году, когда было похищено 125,5 тыс. долларов США во Внешэкономбанке СССР [6].

С появлением новой угрозы на законодательном уровне стали предприниматься попытки регламентации ответственности за совершение компьютерных преступлений: 6 декабря 1991 года был представлен проект Закона РСФСР «Об ответственности за правонарушения при работе с информацией», который предусматривал введение в действующий УК РСФСР норм, устанавливающих ответственность за совершение компьютерных преступлений [5]; Постановлением Верховного Совета РФ от 23.09.92 № 3524-1 «О порядке введения в действие Закона Российской Федерации “О правовой охране программ для электронных вычислительных машин и баз данных”» предполагалось внесение изменений и дополнений в Гражданский, Уголовный кодексы РСФСР и другие законодательные акты, связанные с вопросами правовой охраны программ для электронных вычислительных машин и баз данных [3]; в 1994 году был разработан проект закона о внесении дополнений в УК РСФСР, которым устанавливалась ответственность за ряд противоправных действий в сфере компьютерной информации [5]; в 1995 году был опубликован проект УК РФ, в котором предусматривалась Глава 29 «Компьютерные преступления», включавшая в себя составы: самовольное проникновение в автоматизированную компьютерную систему (ст. 271); неправомерное завладение программами для ЭВМ, файлами или базами данных (ст. 272); самовольная модификация, повреждение, уничтожение баз данных или программ для ЭВМ (ст. 273); внесение или распространение вирусных программ для ЭВМ (ст. 274); нарушение правил, обеспечивающих безопасность

информационной системы (ст. 275) [2]. 1 января 1997 г. вступил в силу новый Уголовный кодекс Российской Федерации, в котором имеется Глава 28 «Преступления в сфере компьютерной информации», объединяющая ст. 272 «Неправомерный доступ к компьютерной информации», ст. 273 «Создание, использование и распространение вредоносных программ для ЭВМ» и ст. 274 «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети» [1], который с изменениями действует и в настоящее время [9].

Дальнейшее развитие информационных технологий, появление и активное внедрение сети Интернет и массовая компьютеризация привели к бурному развитию компьютерной преступности как на уровне отдельных государств, в том числе России, так и на международном уровне.

С 1997 года по 2005 наметился резкий всплеск компьютерной преступности. Если в 1997 году таких преступлений было зарегистрировано всего 33, то в 2005 году – уже 10 214. Пик роста компьютерной преступности приходится на 2009 год – было зарегистрировано 11 636 преступлений подобного рода [8]. Это связано с тем, что, во-первых, данный вид преступности обладает высокой степенью латентности, и повышение уровня знаний и умений, а также мастерства сотрудников подразделений, занимающихся борьбой с компьютерной преступностью, привело к повышению эффективности их работы и, соответственно, количеству выявленных и раскрытых преступлений такого рода, а во-вторых, таких преступлений стало совершаться гораздо больше.

Далее наметилась тенденция к снижению количества зарегистрированных преступлений подобного рода и, вместе с тем, рост их качественных показателей. Так, если в 2009 году было зарегистрировано 11636 преступлений, то в 2010 году – 7 398, а в 2011 году – всего 2 698 [8]. Причиной тому послужила как активизация работы правоохранительных органов, так и повышение мастерства лиц, их совершающих, что позволяет им оставаться безнаказанными.

По данным, которые предоставил 21.02.2012 года на пресс-конференции в агентстве РИА «Новости» Илья Сачков, генеральный директор компании Group-IB, занимающейся расследованием компьютерных преступлений, ущерб от действий российских киберпреступников составил около $2,3 миллиарда, тогда как в 2010 году ущерб от подобных действий составил $1,3 миллиарда. По данным этой же компании, вырос и мировой рынок киберпреступности – в 2011 году его объем составил 12,5 миллиарда долларов, а в 2010 году он был на уровне $7 миллиардов.

Что же касается дальнейшей динамики развития киберпреступности, то по данным, которые предоставил глава управления «К» МВД Алексей Мошков, большинство преступлений совершается в сфере дистанционного банковского обслуживания. Количество компьютерных преступлений за январь – ноябрь 2017 года составило около 82,4 тыс.

В 2016 году Group-IB оценивала суммарный ущерб экономике России от киберпреступности в 203,3 миллиарда рублей, или 0,25% от ВВП России, что равняется почти половине бюджетных расходов на здравоохранение в 2015 году. В 2017 году, по оценке Сбербанка, ежегодные убытки России от кибератак составляют уже 600–650 млрд рублей, а в мире сумма убытков от кибератак уже приблизилась к $1 трлн.

На основании изложенного можно с уверенностью утверждать, что компьютерная преступность представляет собой очень серьезную угрозу как для отдельных государств, так и для всего мирового сообщества, в связи с чем необходимо разработать и реализовать на практике действенные механизмы противодействия подобным явлениям.

Разработка таких механизмов невозможна без изучения зарубежного опыта борьбы с киберпреступностью, поэтому рассмотрим опыт законодательной ре-

гламентации уголовной ответственности за подобные деяния на примерах США, Германии и Франции.

Как уже отмечалось ранее, первые компьютерные преступления были совершены на территории США, поэтому неудивительно, что именно Америка одной из первых законодательно установила уголовную ответственность за их совершение.

Так, в 1977 г. в США был разработан законопроект о защите федеральных компьютерных систем. Он предусматривал уголовную ответственность за такие деяния, как введение заведомо ложных данных в компьютерную систему; незаконное использование компьютерных устройств; внесение изменений в процессы обработки информации или нарушение этих процессов; хищения денежных средств, ценных бумаг, имущества, услуг, ценной информации, совершённые с использованием возможностей компьютерных технологий или с использованием компьютерной информации. На основе данного законопроекта в октябре 1984 г. был принят Закон о мошенничестве и злоупотреблении с использованием компьютеров – основной нормативно-правовой акт, устанавливающий уголовную ответственность за преступления в сфере компьютерной информации. В последующем он неоднократно (в 1986, 1988, 1989, 1990, 1994 и 1996 гг.) дополнялся, а в настоящее время он включен в виде § 1030 в Титул 18 Свода законов США [3].

В Германии уголовная ответственность за компьютерные преступления была установлена в 1986 году, когда были внесены соответствующие изменения в УК ФРГ.

К преступлениям в сфере компьютерной информации, согласно УК Германии, отнесены: действия лиц, неправомочно приобретающих для себя или иного лица непосредственно не воспринимаемые сведения, которые могут быть воспроизведены или переданы электронным, магнитным или иным способом (§ 202a); умышленные деяния лиц с намерением получить для себя или третьих лиц имущественную выгоду, заключающуюся в причинении вреда чужому имуществу путем воздействия на результат обработки данных путем неправильного создания программ, использования неправильных данных, неправомочного использования данных или иного воздействия на результат обработки данных (§ 263a); учиняющих подделку или использующих поддельные технические записи, под которыми, в числе иного, понимаются данные, полностью или частично регистрируемые автоматическими устройствами (§ 268); аналогичная подделка данных, имеющих доказательственное значение (§ 269); уничтожающих, изменяющих или утаивающих технические записи (§ 274); противоправно аннулирующих, уничтожающих, приводящих в негодность или изменяющих данные (§ 303a); нарушающих обработку данных путем разрушения, повреждения, приведения в негодность либо приведения в негодность установки для обработки данных или носителей информации (§ 303b) [4].

УК Германии также предусматривает уголовную ответственность за преступления, совершаемые в компьютерном пространстве, а именно: нарушение тайны телекоммуникационной связи (§ 206); незаконное вмешательство в деятельность телекоммуникационных установок (§ 317) [4].

Уголовный кодекс Франции, вступивший в силу весной 1994 г., также предусматривает уголовную ответственность за ряд компьютерных преступлений. В сфере компьютерной информации УК Франции устанавливает ответственность за совершение следующих преступлений: перехват, хищение, использование или предание огласке сообщений, передаваемых средствами дальней связи (ст. 226-15); незаконный доступ к автоматизированной системе обработки данных или незаконное пребывание в ней (ст. 323-1); воспрепятствование работе или нарушение работы компьютерной системы (ст. 323-2); ввод обманным путем в систему информации, а также из-

менение или уничтожение содержащихся в автоматизированной системе данных (ст. 323-3); ввод или хранение в памяти ЭВМ запрещенных законом данных (ст. 226-19) [7].

К преступлениям в информационном компьютерном пространстве, в соответствии с УК Франции, могут быть отнесены: осуществление или отдача указания об осуществлении автоматизированной обработки поименных данных без осуществления предусмотренных в законе формальностей (ст. 226-16); осуществление или отдача указания об осуществлении обработки этих данных без принятия всех мер предосторожностей, необходимых для того, чтобы обеспечить безопасность данных (ст. 226-17); сбор и обработка данных незаконным способом (ст. 226-18); хранение определенных данных сверх установленного законом срока (ст. 226-20); использование данных с иной целью, чем это было предусмотрено (ст. 226-21); разглашение данных, могущее привести к указанным в законе последствиям (ст. 226-22); уничтожение, порча или хищение любого документа, техники, сооружения, оборудования, установки, аппарата, технического устройства или системы автоматизированной обработки данных или внесение в них изъянов (ст. 411-9) [7].

К иным преступлениям в рассматриваемой сфере по УК Франции отнесены: деяния, связанные с изготовлением и распространением по телекоммуникационным сетям детской порнографии (ст. 227-23); сбор или передача содержащейся в памяти ЭВМ или картотеке информации иностранному государству, уничтожение, хищение, изъятие или копирование данных, носящих характер секретов национальной обороны, содержащихся в памяти ЭВМ или в картотеках, а также ознакомление с этими данными посторонних лиц (ст. ст. 411-7, 411-8, 4139, 413-10, 413-11); террористические акты, связанные с деяниями в области информатики (ст. 421-1) [7].

Кроме того, следует отметить, что за рассматриваемые деяния УК Франции предусматривает уголовную ответственность не только для физических, но и для юридических лиц [10].

На основании изложенного можно сделать вывод о том, что компьютерная преступность является одной из самых специфических, сложно устроенных и динамично развивающихся видов преступности. Современная киберпреступность является серьезнейшей угрозой как для отдельных государств, так и для всего мирового сообщества. Ущерб от действий киберпреступников огромен и исчисляется миллиардами долларов. Для эффективной борьбы с данным явлением необходимо совершенствование законодательства, регламентирующего уголовную ответственность за совершение компьютерных преступлений. Анализ законодательства ряда государств показывает, что зарубежные нормативные акты более детально определяют круг противоправных деяний в сфере компьютерной информации, что позволяет эффективнее противодействовать данной угрозе. Необходимо, опираясь на положительный опыт ряда зарубежных стран, модернизировать действующее законодательство России в указанной области, в том числе – в УК РФ.

Литература

1. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ.

2. Ведомости Съезда Народных Депутатов Российской Федерации и Верховного Совета Российской Федерации. – 1992. – № 42. – Ст. 2326.

3. *Волеводз А.Г.* Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. – М. : Юрлитинформ, 2001. – 496 с.

4. *Батурин Ю.М.* Проблемы компьютерного права. – М. : Юридическая литература, 1991. – С. 272.

5. *Курушин В.Д., Минаев В.А.* Компьютерные преступления и информационная безопасность. – М. : Новый Юрист, 1998. – С. 257.
6. *Сычев Ю.Н.* Основы информационной безопасности : учебно-практическое пособие. – М. : Изд. центр ЕАОИ, 2007. – 300 с.
7. Новый Уголовный кодекс Франции / научн. ред. Н.Ф. Кузнецова, Э.Ф. Побегайло. – М., 1994. – 265 с.
8. Официальный сайт МВД России. – URL: http://www.mvd.ru
9. *Уткин Н.И., Меньшиков А.В., Муталиева Л.С., Бибарсова Г.Ш., Гареев А.А., Муслов Б.В., Савин И.Г., Тыртышный А.А.* Правоведение : учебник для военных вузов / под ред. О.Ю. Ефремова. – СПб., 2015. – (Сер. Учебник для военных вузов.)
10. *Tyrtyshny, A., Tomas, S.* Interaction of European and Russian legal consciousness // BRICS Law Journal. – 2015. – Т. II. – № 2. – С. 34–49.

Literatura

1. Ugolovnyj kodeks Rossijskoj Federacii ot 13 iyunya 1996 g. № 63-FZ.
2. Vedomosti s'ezda Narodnyh Deputatov Rossijskoj Federacii i Verhovnogo Soveta Rossijskoj Federacii. – 1992. – № 42. – St. 2326.
3. *Volevodz, A.G.* Protivodejstvie komp'yuternym prestupleniyam: pravovye osnovy mezhdunarodnogo sotrudnichestva. – M. : Yurlitinform, 2001. – 496 s.
4. *Baturin, Yu.M.* Problemy komp'yuternogo prava. – M. : Yuridicheskaya literatura, 1991 g. – S. 272.
5. *Kurushin, V.D., Minaev, V.A.* Komp'yuternye prestupleniya i informacionnaya bezopasnost'. – M. : Novyj Yurist, 1998. – S. 257.
6. *Sychev ,Yu.N.* Osnovy informacionnoj bezopasnosti : uchebno-prakticheskoe posobie. – M. : Izd. centr EAOI, 2007. – 300 s.
7. Novyj Ugolovnyj kodeks Francii / nauchn. red. N.F. Kuznecova, Eh.F. Pobegajlo. – M., 1994. – 265 s.
8. Oficial'nyj sajt MVD Rossii. – URL: http://www.mvd.ru
9. *Utkin, N.I., Men'shikov, A.V., Mutalieva, L.S., Bibarsova, G.SH., Gareev, A.A., Muslov, B.V., Savin, I.G., Tyrtyshnyj, A.A.* Pravovedenie : uchebnik dlya voennyh vuzov / pod red. O.Yu. Efremova. – SPb., 2015. – (Ser. Uchebnik dlya voennyh vuzov.)
10. *Tyrtyshny, A., Tomas, S.* Interaction of European and Russian legal consciousness // BRICS Law Journal. – 2015. – T. II. – № 2. – C. 34–49.