Evdokimov K.N.

COMPARATIVE LEGAL ANALYSIS OF THE LEGISLATION OF RUSSIA AND FOREIGN COUNTRIES, REGULATING THE CRIMINAL LIABILITY FOR COMMITTING COMPUTER CRIMES

Evdokimov Konstantin Nikolaevich, Associate Professor of the Chair of State and Law Disciplines of the Irkutsk Law Institute Affiliated with the Academy of the General Prosecutor's Office of the Russian Federation, PhD in Law, Associate Professor, Russian Federation, Irkutsk

Abstract

This article examines the criminal legislation of Russia and foreign countries providing for liability for committing computer crimes. Comparative legal analysis of legislation is conducted at the level of national criminal legal systems (Russia, USA, China, France, Germany, CIS countries, etc.), and at the level of legal families: the Anglo-American (UK, USA), Romano Germanic (France, Germany, etc.), the Scandinavian (Sweden, Denmark), socialist (China).

Criteria for comparative legal research were: the source of law stipulating the criminal responsibility for the Commission of computer crimes, as well as objective and subjective signs of a crime.

The author reveals the advantages and disadvantages of the Russian legislation regarding the criminalization of computer crimes. General conclusion of the trend towards "hybridization" of national criminal law systems, which finds its expression in the normative consolidation of separate (special) offences for the Commission of criminal acts in the field of computer information in Russian and foreign legislation.

Put forward proposals on the improvement of criminal law articles 272 – 274 of the criminal code.

Keywords: computer crime; crimes in the sphere of computer information; criminal law; criminal liability; criminal and legal system

В настоящее время, существование компьютерной преступности причиняет огромный ущерб экономике России, а также угрожает информационной безопасности российского государства и общества.

По данным исследования Cost of Cyber Crime Study 2014, проведенного компанией Ponemon Institute при поддержке HP Enterprise Security, среднегодовой ущерб российской организации от киберпреступлений в 2014 году составил 3,3 млн. долларов[2].

В свою очередь, по мнению экспертов «Лаборатории Касперского», в случае успешной атаки киберпреступников крупные компании в России теряют около 20 млн. рублей, а предприятия среднего и малого бизнеса в среднем 780 тыс. рублей – за счет вынужденного простоя, упущенной прибыли и расходов на дополнительные услуги специалистов. На ликвидацию последствий инцидента и профилактику крупные компании дополнительно тратят около 2,1 млн. рублей, а небольшие – около 300 тыс. рублей[3].

В результате совместного исследования Фонда развития интернет-инициатив (ФРИИ) и международных компаний Group-IB, Microsoft было установлено, что ущерб экономике России от киберпреступности в 2015 году превысил 200 миллиардов рублей, что составило 0,25% от ВВП Российской Федерации[4].

Поэтому, безусловно, противодействие компьютерной преступности и совершенствование уголовно-правовых средств борьбы с преступлениями в сфере компьютерной информации, является одной из первоочередных задач российского научного сообщества и правоохранительных органов.

Одним из эффективных способов совершенствования отечественного уголовного права, регламентирующего ответственность за компьютерные преступления, является анализ зарубежного законодательства и использование положительного опыта борьбы с компьютерной преступностью, например, в США или странах Западной

---

[2] Российские компании теряют миллионы в результате кибератак [Электронный ресурс] – URL: https://rg.ru/2014/10/20/ataki-site.html (Дата обращения: 09.11. 2016).

[3] Так ли страшен Интернет. О настоящей опасности киберугроз рассказывает «Газета.Ru» [Электронный ресурс] - URL: http://www.gazeta.ru/tech/2014/11/05_a_6289085.shtml (Дата обращения 29.05.2016).

[4] Ущерб экономике России от киберпреступности превысил 200 млрд рублей [Электронный ресурс] – URL: http://ria.ru/economy/20160413/1409855094.html#ixzz45jCApNtn (Дата обращения: 09.11. 2016).

Европы, где процесс криминализации правонарушений в сфере информационных технологий начался значительно раньше, чем в России.

Проанализируем уголовно-правовые нормы законодательства России, США, Франции, Германии, Швеции и других развитых стран, относящихся к различным правовым семьям, для выявления особенностей регламентации преступлений в сфере компьютерной информации и ответственности за их совершение.

Англо-американская правовая семья. Соединенные Штаты Америки явились одной из первых стран мира, принявших меры по установлению уголовной ответственности за компьютерные преступления, и страной, где компьютерная преступность появилась раньше, чем в других государствах. Отличительной особенностью уголовного законодательства США является его двухуровневая структура: федеральное законодательство и законодательство отдельных штатов.

На федеральном уровне в 1977 г. в США был разработан законопроект о защите федеральных компьютерных систем. Он предусматривал уголовную ответственность за: введение заведомо ложных данных в компьютерную систему; незаконное использование компьютерных устройств; внесение изменений в процессы обработки информации или нарушение этих процессов; хищение денежных средств, ценных бумаг, имущества, услуг, ценной информации, совершенные с использованием возможностей компьютерных технологий или с использованием компьютерной информации. На основе данного законопроекта в октябре 1984 года был принят Закон «О мошенничестве и злоупотреблении с использованием компьютеров» – основной нормативно-правовой акт, устанавливающий уголовную ответственность за неправомерный доступ к компьютерной информации, впоследствии включённый в § 1030 Титула 18 Свода законов США[5].

В связи с тем, что исследование посвящено компьютерным преступлениям, то обратим внимание на §1029 и §1030 Титула 18 Свода законов США.

Так § 1029 Титула 18 Свода законов США устанавливает ответственность за:

- производство, использование и торговлю поддельными средствами доступа;
- использование или получение приборов для несанкционированного доступа с целью получения материальной выгоды в размере более 1000 долларов США;

[5] Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества / А.Г. Волеводз. – М.: ООО Изд-во «Юрлитинформ», 2002. С.88.

• обладание 15 и более поддельными или неразрешенными средствами доступа;

• производство, продажу или владение оборудованием для изготовления поддельных средств доступа;

• совершение сделок с помощью средств доступа, предназначенных для другого лица;

• предложение какому-либо лицу средств доступа или приобретения за плату информации, которая может быть использована для получения средств доступа;

• использование, производство, продажу или владение телекоммуникационным диагностическим оборудованием, модифицированным или приспособленным для несанкционированного получения телекоммуникационных услуг;

• использование, производство, продажу или владение сканирующими приемниками, оборудованием или программным обеспечением для модификации телекоммуникационной аппаратуры с целью несанкционированного использования телекоммуникационных услуг;

• принуждение какого-либо лица представить члену кредитной системы или его агенту для оплаты записи транзакций, сделанных с помощью средств несанкционированного доступа.

В свою очередь, п. «а» § 1030 предусматривает ответственность за семь составов преступлений, которые прямо или косвенно связанны с созданием, использованием и распространением вредоносных компьютерных программ:

1. Компьютерный шпионаж, состоящий в несанкционированном доступе или превышении санкционированного доступа к информации, а также получение информации, имеющей отношение к государственной безопасности, международным отношениям и вопросам атомной энергетики.

2. Несанкционированный доступ или превышение санкционированного доступа к информации из правительственного ведомства США, из какого бы то ни было защищенного компьютера, имеющего отношение к межштатной или международной торговле, а также получение информации из финансовых записей финансового учреждения, эмитента карт или информации о потребителях, содержащейся в файле управления потребителей.

3. Воздействие на компьютер, находящийся в исключительном пользовании правительственного ведомства США, или нарушение функционирования компьютера, используемого полностью или частично Правительством США.

4. Мошенничество с использованием компьютера – доступ, осуществляемый с мошенническими намерениями, и использование

компьютера с целью получения чего бы то ни было ценного посредством мошенничества, включая незаконное использование машинного времени стоимостью более 5 тысяч долларов в течение года, т.е. без оплаты использования компьютерных сетей и серверов.

5. Умышленное или по неосторожности повреждение защищенных компьютеров.

6. Мошенничество путем торговли компьютерными паролями или аналогичной информацией, позволяющей получить несанкционированный доступ, если такая торговля влияет на торговые отношения между штатами и с другими государствами или на компьютер, используемый правительством США.

7. Угрозы, вымогательство, шантаж и другие противоправные деяния, совершаемые с использованием компьютерных технологий.

Санкции за преступные деяния, предусмотренные § 1030(a), являются достаточно жесткими. До 10 лет тюремного заключения практически по всем перечисленным пунктам и до 20 лет тюремного заключения в случае рецидива или получения (сбора) секретной информации. Однако санкции предусматривают и низший предел в виде штрафа или 1 года заключения, в случае совершения преступления впервые и при наличии смягчающих вину обстоятельств[6].

Таким образом, можно сделать вывод, что законодательство США достаточно подробно регулирует ответственность за компьютерные преступления, предусматривая суровые санкции за совершение преступления на всех его стадиях: приготовление, покушение, оконченное преступление.

Кроме того, диспозиции статей уголовного законодательства наряду с непосредственным объектом преступления – компьютерной информацией, содержат в качестве дополнительных объектов наиболее важные сферы деятельности государства и личности: деятельность правительственных и финансовых учреждений, телекоммуникационные сети и услуги, государственная безопасность, государственная тайна, тайна личной жизни, коммерческая тайна и др., что упрощает квалификацию совершенных компьютерных преступлений при решении вопросов о привлечении виновного к ответственности и размере уголовного наказания.

Однако специальной статьи, например, посвященной созданию, использованию и распространению «компьютерных вирусов» или

[6] Свод законодательства США Раздел 18, часть 1, глава 47, §1029, §1030 Computer Fraud and Abuse Act (CFAA) [Электронный ресурс] // URL: http://www.law.cornell.edu/uscode/text/18/1030 (Дата обращения: 20.06.2016).

вредоносных компьютерных программ (как, например, в ст. 273 УК РФ) федеральное уголовное законодательство США не содержит.

Скандинавская правовая семья. Анализ уголовного законодательства зарубежных стран показывает, что первый шаг в направлении защиты компьютерной информации был сделан законодателем не в США, а в Швеции, где 4 апреля 1973 года был принят «Закон о данных», который ввёл новое понятие в традиционное законодательство – «злоупотребление при помощи компьютера»[7].

В настоящее время Уголовный кодекс Королевства Швеции не содержит специальной главы о компьютерных преступлениях. Составы преступлений данного вида и ответственность за их совершение, расположены в различных статьях УК Швеции.

Так, например, ст. 9c гл. 4 УК Швеции предусматривает, что «Лицо, которое в иных случаях, чем указанные в Статьях 8 и 9, незаконно получает доступ к записи в системе автоматической обработки данных или незаконно изменяет, стирает или добавляет такую запись в реестр, должно быть приговорено за нарушение секретности данных к штрафу или к тюремному заключению на срок не более двух лет. Запись в этом контексте включает в себя даже информацию, которая обрабатывается электронным или сходными способами для использования в автоматической обработке данных»[8].

Между тем, ст. 1 гл. 9 УК Швеции закрепляет, что к тюремному заключению на срок не более двух лет должно быть приговорено лицо, которое путем предоставления неправильной или неполной информации, или внесения изменений в программу или отчетность, или какими-либо другими способами незаконно влияет на результат автоматической обработки информации или любой другой сходной автоматической обработки, которая влечет выгоду для лица, совершившего преступление и убытки для любого другого лица[9].

В Уголовном кодексе Дании также нет главы и специальных статей, посвященных ответственности за компьютерные преступления, но виновный в случае их совершения может быть привлечен к уголовной ответственности на общих основаниях. Например, в §193 УК Дании предусматривается, что любое лицо, которое незаконным способом вызывает серьезные сбои в работе публичных средств связи, публичных

---

[7] Законодательные меры по борьбе с компьютерной преступностью // Проблемы преступности в капиталистических странах. – 1988. - № 10. - С.40

[8] Уголовный кодекс Швеции / Научные редакторы проф. Н. Ф. Кузнецова и канд. юрид. наук С. С. Беляев. Перевод на русский язык С. С. Беляева. — СПб.: Издательство «Юридический центр Пресс», 2001.

[9] Там же.

почтовых служб, публично используемых телеграфных или телефонных служб, радио или телевизионных установок, *систем обработки данных* (Выделение – Авт.) или установок публичного водо-, газо-, электро- или теплопровода, подлежит простому заключению под стражу или тюремному заключению на любой срок, не превышающий четырех лет, или при смягчающих обстоятельствах — штрафу.

Если данное деяние было совершено по небрежности, то наказанием должны быть штраф или простое заключение под стражу[10].

Романо-германская правовая семья. На заседании Комитета министров Европейского Совета 13 сентября 1989 г. был определён список компьютерных правонарушений на основании, которого европейскому законодателю было рекомендовано разработать и принять соответствующие уголовно-правовые нормы. В полном объёме он включал в себя так называемый «Минимальный и Необязательный список нарушений».

«Минимальный список нарушений» содержал восемь видов компьютерных преступлений: компьютерное мошенничество; подделка компьютерной информации; повреждение данных ЭВМ и программ ЭВМ; компьютерный саботаж; несанкционированный доступ; несанкционированный перехват данных; несанкционированное использование защищённых компьютерных программ; несанкционированное воспроизведение схем.

«Необязательный список нарушений» включал в себя четыре вида компьютерных преступлений: изменение данных ЭВМ или программ ЭВМ; компьютерный шпионаж; неразрешённое использование ЭВМ; неразрешённое использование защищённой программы ЭВМ[11].

Поэтому до 1995 года в европейских странах, таких как Франция, ФРГ, Австрия, Нидерланды, Португалия были приняты законы, устанавливающие уголовную ответственность за деяния в сфере компьютерной информации.

Так, например, в Федеративной Республике Германия в 1994 году был принят федеральный закон «О защите информации»[12], а в Уголовный кодекс ФРГ были включены составы компьютерных преступлений, предусматривая ответственность для лиц:

---

[10] Уголовный кодекс Дании / Научное редактирование и предисловие С. С. Беляева, канд. юрид. наук (МГУ им. М. В. Ломоносова). Перевод с датского и английского канд. юрид. наук С. С. Беляева, А.Н. Рычевой. — СПб.: Издательство «Юридический центр Пресс», 2001.

[11] Курушин В.Д., Минаев В.А. Компьютерные преступления и информационная безопасность / В.Д. Курушин, В.А. Минаев - М.: Новый Юрист,1998. С.96-97.

[12] Geandert durth Art. 126 vom. 14/9.1994.(BGBIIS 2325).

- неправомочно приобретающих для себя или иного лица непосредственно не воспринимаемые сведения, которые могут быть воспроизведены или переданы электронным, магнитным или иным способом (§ 202a);
- 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 доказательное 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);

Также в числе преступлений, совершающихся в компьютерном пространстве (киберпространстве), в УК ФРГ следует выделить нарушение тайны телекоммуникационной связи (§ 206); незаконное вмешательство в деятельность телекоммуникационных установок (§ 317).

В разделе № 22 УК ФРГ «Мошенничество и преступное злоупотребление доверием» содержится § 263a «Компьютерное мошенничество», под которым понимается умышленное деяние с намерением получить для себя или третьих лиц имущественную выгоду, заключающееся в причинении вреда чужому имуществу путем воздействия на результат обработки данных путем неправильного создания программ, использования неправильных или неполных данных, неправомочного использования данных или иного воздействия на результат обработки данных.

За совершение всех указанных выше преступлений предусмотрены альтернативные санкции, устанавливающие два возможных вида наказаний: лишение свободы на определенный срок (§ 303a – до 2 лет, §§ 202a, 206 – до 3 лет, §§ 263a, 268, 269, 274, 303b, 317 – до 5 лет) или денежный штраф[13].

Стоит отметить такую особенность УК ФРГ, что уголовно-правовые нормы, регулирующие ответственность за компьютерные преступления не объединены в отдельный раздел (главу), а являются

[13] Уголовный кодекс Германии с изменениями от 28 декабря 2003 года. [Электронный ресурс] URL: http://lexetius.com/StGB/263a (Дата обращения: 20.06.2016).

специальными, дополняющими нормами к уже известным («классическим») видам преступлений, и содержатся в одних с ними разделах, отличаясь от них только элементами состава преступлений: предметом преступного посягательства, способом совершения преступного деяния, орудием совершения преступления и т.д. Например: § 202a выступает специальной нормой по отношению к § 202 «Нарушение тайны переписки». Эти статьи находятся в одном (общем) разделе 15 «Нарушение неприкосновенности и тайны частной жизни», имеют общий объект «неприкосновенность частной жизни» и отличаются только предметом преступления: в § 202 – чужие письма и документы, в § 202a – машинные носители информации или информация, находящаяся на них.

Данная конструкция Уголовного кодекса Германии является достаточно прагматичной, что облегчает правоприменителю квалификацию преступных деяний.

Похожий подход к ответственности за компьютерные преступления прослеживается и в уголовном законодательстве Франции.

Так, глава № 6 тома № 2 УК Франции содержит статьи предусматривающие уголовную ответственность за:

- Посягательство на права человека, связанные с использованием компьютерных данных (например, ст. ст. 226-8, 226-9) – 1 год тюремного заключения;
- Сбор данных обманным, самоуправным или запрещенным законом способом, либо обработка именной информации, касающейся физического лица (ст. 226-18) – 5 лет тюремного заключения;
- Ввод или хранение в памяти ЭВМ без согласия заинтересованного лица и помимо случаев, предусмотренных законом, именной информации (ст. 226-19) – 5 лет тюремного заключения;

Помимо перечисленных статей второй том УК Франции содержит уголовные нормы, предусматривающие санкции за посягательство на системы автоматизированной обработки данных (ст. ст. 323-1 – 323-4):

1. Незаконный доступ к автоматизированной системе обработки данных или незаконное пребывание в ней (ст. 323-1);
2. Воспрепятствование работе или нарушение работы компьютерной системы (ст. 323-2);
3. Ввод обманным путем в систему информации, а также изменение или уничтожение содержащихся в автоматизированной системе данных (ст. 323-3);
4. Совершение вышеуказанных деяний группой лиц, группой лиц по предварительному сговору, организованной группой (ст. 323-4). Наказание до 5 лет тюремного заключения.

В разделе 3 четвертого тома УК Франции «Преступления против нации, государства и общественного порядка» также содержится ряд

статей прямо или косвенно, предусматривающий ответственность за компьютерные преступления:

- 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, 413-9, 413-10, 413-11) – до семи лет тюремного заключения;
- Уничтожение, повреждение или похищение любого документа, оборудования, сооружения, снаряжения, установки, аппарата, технического устройства или системы автоматизированной обработки информации либо внесение неполадок в их работу, если эти деяния способны причинить вред основополагающим интересам нации, наказываются пятнадцатью годами уголовного заточения (ст. 411-9);
- Террористические акты в области информатики (ст. 421-1) – до тридцати лет уголовного заключения[14].

К особенностям УК Франции в части уголовно-правовой регламентации компьютерных преступлений, можно отнести то, что к ответственности привлекаются не только физические, но и юридические лица. В частности ст. 131-38 УК Франции предусматривает, что максимальный размер штрафа, применяемого к юридическим лицам, равен пятикратному размеру штрафа, предусмотренного для физических лиц законом, наказывающим преступное деяние. Кроме того, в соответствии со ст. 131-39 УК Франции к юридическим лицам могут быть применены такие наказания как: прекращение деятельности; бессрочное или сроком не более пяти лет запрещение осуществлять прямо или косвенно один или несколько видов профессиональной или общественной деятельности; помещение под судебный надзор сроком не более пяти лет; бессрочное или сроком не более пяти лет закрытие всех заведений либо одного или нескольких из заведений предприятия, служивших совершению вменяемых в вину деяний; конфискация вещи, которая служила или была предназначена для совершения преступного деяния, или вещи, которая получена в результате преступного деяния и др. [15]

Анализируя уголовное законодательство зарубежных стран, следует отдельно остановиться на законодательстве Китайской Народной Республике, которое относится к **социалистической правовой семье** и,

---

[14] Зарубежные уголовные кодексы. Уголовный кодекс Франции [Электронный ресурс] - http://crimpravo.ru/codecs/france/2.doc (Дата обращения 03.11.2016).

[15] Зарубежные уголовные кодексы. УК Франции [Электронный ресурс] - http://crimpravo.ru/codecs/france/2.doc (Дата обращения 03.11.2016).

безусловно, представляет научный интерес в части регламентации компьютерных преступлений и ответственности за их совершение.

Следует отметить, что до недавнего времени, Китай занимал 1-е место в мире по созданию, использованию и распространению вредоносных компьютерных программ. Однако жесткая и грамотная политика правительства КНР в сфере защиты информации и борьбы с компьютерными преступлениями, осуществляемая последние 5 лет, позволила существенно снизить количество преступных деяний. Наряду с предупредительными мерами (запрет пользоваться услугами зарубежных Интернет-провайдеров и социальными сетями, запрет регистрации в сети «Интернет» под вымышленными аккаунтами и др.), немаловажную роль в противодействии компьютерной преступности играет национальное уголовное законодательство Китая, устанавливающее достаточно суровые санкции за совершение преступных деяний данного вида.

Так, в частности УК КНР закрепляет следующие составы преступлений в сфере компьютерной информации и санкции за их совершение:

Статья 285. Незаконное вторжение в компьютерные информационные системы, имеющие отношение к новейшим научно-техническим разработкам, к строительству системы государственной безопасности и государственным делам, — наказывается лишением свободы на срок до 3 лет или арестом.

Статья 286. Незаконное совершение с компьютерными информационными системами таких действий, как сокращение (изъятие) текста, исправление, дополнение, создание помех, приведшее к невозможности нормального функционирования компьютерной информационной системы, если это повлекло серьезные последствия, — наказывается лишением свободы на срок до 5 лет или арестом;

то же деяние при наличии особо серьезных последствий, — наказывается лишением свободы на срок свыше 5 лет.

Незаконное совершение с передаточными, оперативными и хранящимися в базе данными компьютерных информационных систем таких действий, как сокращение, исправление, дополнение, повлекшее серьезные последствия, — наказывается в соответствии с частью первой настоящей статьи.

Умышленное создание и распространение компьютерных вирусов и иных программ деструктивного характера, оказывающих влияние на нормальнее функционирование компьютерных систем, повлекшие серьезные последствия, — наказываются в соответствии с частью первой настоящей статьи.

Статья 287. Использование компьютера для завладения деньгами путем мошенничества или их хищения, дня взяточничества и нецелевого использования общественных средств, для завладения путем хищения

государственной тайной и совершения иных преступлений, — наказывается согласно соответствующим статьям данного Кодекса (от 5 лет до пожизненного лишения свободы – Авт.)[16].

Особенностью уголовного законодательства Китая является возможность применения к компьютерным преступникам в качестве основного (преступления против государственной безопасности) или дополнительного наказания (преступления против общественного порядка) - лишения политических прав (права избирать и быть избранным; права свободы слова, печати, собраний, союзов, уличных шествий и демонстраций; права занимать должности в государственных органах; права занимать руководящие должности в государственных компаниях, на предприятиях, в непроизводственных единицах и народных организациях) сроком от одного до пяти лет, либо пожизненно в случае осуждения к смертной казни или пожизненному лишению свободы (ст. ст. 54 – 57 УК КНР).

Проводя сравнительно-правовой анализ зарубежного законодательства в части уголовной ответственности за компьютерные преступления, следует заметить, что 23.11.2001 года в г. Будапеште была принята Конвенция Совета Европы о преступности в сфере компьютерной информации (далее – Конвенция)[17], содержащая перечень компьютерных правонарушений, подлежащих криминализации в законодательстве стран-участниц Конвенции. На данный момент Конвенцию ратифицировали 47 государств, включая также такие неевропейские страны как США, Канада, Южно-Африканская Республика, Япония.

Россия по ряду политических и юридических причин (например, обязательство о предоставлении свободного доступа к информационным ресурсам России со стороны других иностранных государств-членов Конвенции, в частности США и стран НАТО; применение уголовной ответственности для юридических лиц – Авт.) указанный международно-правовой акт не ратифицировала.

Однако Конвенция, также оказала серьезное влияние на дальнейшее развитие российского уголовного законодательства, предусматривающего ответственность за компьютерные преступления.

Рассматривая законодательство Российской Федерации, предусматривающее наказание за совершение компьютерных преступлений, следует отметить, что переломным моментом в

[16] Уголовный кодекс Китайской Народной Республики [Электронный ресурс]. – URL: http://www.asia-business.ru/law/law1/criminalcode/code/#6 (Дата обращения 20.06.2016).

[17] «Конвенция о преступности в сфере компьютерной информации» (ETS N 185) [рус., англ.] (Заключена в г. Будапеште 23.11.2001) [Электронный ресурс] // СПС КонсультантПлюс (Дата обращения 27.07.2015)

противодействии компьютерной преступности, явилось вступление 1 января 1997 года в силу Уголовного кодекса РФ, криминализировавшего основные общественно-опасные деяния в данной сфере, необходимость борьбы с которыми была к тому времени осознана.

Однако российский законодатель, в отличие от европейского, американского или китайского, ввел в Уголовный кодекс РФ специальную главу №28 «Преступления в сфере компьютерной информации», которая включает 3 законодательные статьи, закрепляющие уголовную ответственность за следующие составы преступлений:

- Ст. 272 УК РФ «Неправомерный доступ к компьютерной информации»
- Ст. 273 УК РФ «Создание, использование и распространение вредоносных программ для ЭВМ»
- Ст. 274 «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети»[18].

Нельзя не отметить, что 17 февраля 1996г. на VII пленарном заседании Межпарламентской ассамблеи государств-участников СНГ был принят «Модельный Уголовный кодекс», включающий раздел XII «Преступления против информационной безопасности», который содержал целый перечень деяний, подлежащих криминализации и закреплению в законодательстве стран СНГ. Такие, например, как: ст. 243 «Хищения путем использования компьютерной техники», ст. 286 «Несанкционированный доступ к компьютерной информации»; ст.287 «Модификация компьютерной информации»; ст.288 «Компьютерный саботаж»; ст.289 «Неправомерное завладение компьютерной информацией»; ст.290 «Изготовление и сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети»[19].

Как видно из приведенного перечня, в данном «Модельном Уголовном кодексе» гораздо полнее представлены варианты и возможности для уголовно-правового противодействия компьютерным преступлениям. Однако, Россия и большинство стран СНГ, так и не воспользовались трудами ученых-юристов, затративших достаточно много сил и времени на создание «универсального уголовного кодекса». Из 12 стран СНГ только республика Беларусь (частично Россия, Азербайджан, Грузия, Казахстан, Украина) взяла положения данного

[18] Уголовный кодекс Российской Федерации: федеральный закон от 13 июня 1996г. № 63 – ФЗ // Собрание законодательства Российской Федерации. - 1996. - № 25. - Ст.2954.

[19] Модельный Уголовный кодекс / Приложение к информационному бюллетеню Межпарламентской ассамблеи СНГ// СПб., 1996. - № 10.

законопроекта за основу своего национального уголовного законодательства.

В ст. ст. 272 – 274 УК РФ законодателем неоднократно вносились изменения и дополнения. Последние изменения были введены федеральным законом от 07.12.2011 № 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации». Вследствие чего, редакции статей 272, 273, 274 УК РФ претерпели существенные изменения. В частности, были ужесточены санкции за совершение преступлений в сфере компьютерной информации (до семи лет лишения свободы), претерпели серьезную трансформацию диспозиции ст. 272 – 274 УК РФ, юридическая терминология, дополнены квалифицирующие и особо квалифицирующие признаки преступлений (например, совершение преступления из корыстной заинтересованности; деяния, повлекшие тяжкие последствия или создавшие угрозу их наступления), а также в примечании к ст. 272 УК было определено понятие «компьютерной информации» и установлен размер крупного ущерба в сумме свыше одного миллиона рублей.

Новеллой в развитии российского уголовного законодательства стало введение Федеральным законом от 29.11.2012 № 207-ФЗ в главу № 21 УК РФ «Преступления против собственности» ряда новых составов преступлений, среди которых можно выделить и несколько составов компьютерных преступлений, таких как: мошенничество с использованием платежных карт (статья 159.3 УК РФ) и мошенничество в сфере компьютерной информации (статья 159.6 УК РФ).

Тем самым у правоохранительных органов Российской Федерации появились дополнительные уголовно-правовые средства борьбы с компьютерным мошенничеством, предполагающим использование для совершения хищений компьютерной информации, а также различных средств создания, хранения, обработки, передачи компьютерной информации, включая платежные карты.

Кроме того, Федеральным законом от 08.06.2015 № 153-ФЗ были внесены изменения в диспозицию ч. 1 ст. 187 УК РФ «Неправомерный оборот средств платежей». Новая редакция, закрепляет ответственность в виде лишения свободы на срок до шести лет - за изготовление, приобретение, хранение, транспортировку в целях использования или сбыта, а равно сбыт поддельных платежных карт, распоряжений о переводе денежных средств, документов или средств оплаты, а также электронных средств, электронных носителей информации, технических устройств, компьютерных программ, предназначенных для неправомерного осуществления приема, выдачи, перевода денежных средств, что позволяет эффективно бороться с таким компьютерным преступлением как «скимминг», предполагающим установку на банкоматах, электронных терминалах и т.п., специального оборудования

для считывания и копирования компьютерной информации с банковских электронных карт.

Проводя сравнительно-правовой анализ зарубежного и российского законодательства, регламентирующего уголовную ответственность за компьютерные преступления, можно сделать несколько существенных выводов.

Во-первых, в уголовно-правовых системах англо-американской, скандинавской, романо-германской и социалистической правовых семей отмечается общая тенденция к закреплению уголовной ответственности за компьютерные преступления в законодательных актах (уголовных кодексах, либо специальных законах) как источниках права.

Во-вторых, несмотря на определенные различия существующих правовых семей, можно отметить общую тенденцию к «гибридизации» национальных уголовно-правовых систем, что находит свое выражение в законодательном закреплении отдельных (специальных) составов преступлений за совершение преступных деяний в сфере компьютерной информации (Россия, США, Китай, страны СНГ).

В-третьих, в отличие от УК РФ, компьютерные преступления в зарубежном уголовном законодательстве могут закрепляться в других составах преступлений в качестве квалифицирующего признака, либо способа совершения другого преступного деяния (Например, ст. 9с гл. 4, ст.1 гл.9 УК Швеции; § 206, § 317, § 263а УК ФРГ; ст. ст. 226-18, 226-19 УК Франции).

В-четвертых, российским законодателем, с позиции правил юридической техники, основные компьютерные преступления объединены в одну главу УК РФ (Глава 28 «Преступления в сфере компьютерной информации»). Между тем, в зарубежном уголовном законодательстве составы компьютерных преступлений расположены в разных разделах, главах, отделах (подотделах) уголовных кодексов или законов (УК Швеции, УК Дании, УК ФРГ, УК Франции, УК КНР, Уголовное законодательство Великобритании: Акт о злоупотреблении компьютерами 1990 г., Акт о персональных данных 1998 г., Акт о терроризме 2000 г.).

В-пятых, в зарубежном уголовном законодательстве основным объектом преступления выступают не только общественные отношения в сфере безопасного функционирования компьютерной информации (УК РФ), но и другие объекты преступного посягательства (Например, права и свободы человека – уголовное законодательство Великобритании, Франции и ФРГ; свобода и общественное спокойствие – УК Швеции; государственная безопасность – уголовное законодательство США, общественный порядок и общественная безопасность – УК КНР).

В-шестых, анализируя объективную сторону компьютерных преступлений, можно сделать заключение о том, что УК РФ закрепляет

формальный состав преступления при создании, использовании и распространении вредоносных компьютерных программ (ч.1 ст. 273 УК РФ), не связывая его с наступлением общественно опасных последствий. В уголовном законодательстве зарубежных стран, где создание, использование и распространение вредоносных компьютерных программ рассматривается как способ совершения других преступлений, состав преступления является материальным (УК Швеции, УК Дании, УК ФРГ, УК Франции).

В-седьмых, в уголовном кодексе России в качестве субъекта компьютерного преступления признается только физическое лицо. В свою очередь в уголовном законодательстве скандинавской и романо-германской правовых семей виновным может выступать и юридическое лицо (УК Швеции, УК Дании, УК Франции и др.).

В-восьмых, субъективная сторона компьютерных преступлений в уголовном законодательстве России в отличие от зарубежного законодательства характеризуется только умышленной формой вины.

В-девятых, в ст. ст. 272, 273 УК РФ в качестве квалифицированного состава закрепляется деяние, совершенное из корыстной заинтересованности, т.е. в качестве обязательного признака субъективной стороны состава преступления выступает мотив преступного деяния. Между тем, законодательство зарубежных стран (Германия, Дания, Китай, Швеция и др.), включая страны СНГ (УК Беларуси, УК Грузии, УК Азербайджана, УК Казахстана и др.), уголовно-правовые нормы которых основываются на «Модельном Уголовном кодексе», не учитывают мотивы и цели преступного деяния при квалификации компьютерного преступления.

В-десятых, к уголовной ответственности в Российской Федерации за совершение компьютерных преступлений привлекаются вменяемые физические лица, достигшие возраста 16 лет. В УК Латвии (ст.11) – возраст привлечения к уголовной ответственности физических лиц наступает с 14 лет, УК Дании (§15) – с 15 лет, УК КНР (ст.17) – с 14 до 16 лет.

В-одиннадцатых, следует отметить большой временной разрыв между возникновением компьютерных преступлений и созданием соответствующих уголовно-правовых механизмов борьбы с ними в Российской Федерации и зарубежных странах. Криминализация компьютерных преступлений в России началась с 1 января 1997 года, в отличие от США, Швеции и других стран, где уголовная ответственность была введена в 1970-х – 1980-х годах.

В-двенадцатых, максимальный размер санкции за совершение компьютерного преступления в России составляет 7 лет лишения свободы (в реальности преступники приговариваются судами к наказаниям в виде штрафа, исправительных работ, условного лишения свободы). Между тем,

в развитых зарубежных странах (США, Китай, Франция и др.) виновному в совершении указанных преступных деяний, повлекших тяжкие последствия, грозит наказание от 10 лет до пожизненного лишения свободы.

С учетом вышесказанного, автор предлагает снизить возраст уголовной ответственности физических лиц за совершение преступления в сфере компьютерной информации, если данное деяние повлекло наступление тяжких последствий (ч. 4 ст. 272, ч. 3 ст. 273, ч. 2 ст. 274 УК РФ) с 16 до 14 лет. При этом, установив наказание за причинение тяжких последствий до 15 лет лишения свободы.

Полагаем целесообразным ужесточить ответственность за компьютерные преступления, с учетом признаков, характеризующих субъективную сторону преступления и включив некоторые цели совершения преступного деяния в диспозиции ч. 3 ст. 272, ч. 2 ст. 273, ч. 1 ст. 274 УК РФ, в частности:

1. «Те же деяния, совершенные с целью скрыть другое преступление или облегчить его совершение»;
2. «Те же деяния, совершенные с целью устрашения населения или воздействия на принятие решения органами государственной власти и (или) местного самоуправления, а также воспрепятствования нормальной деятельности средств массовой информации, органов государственной власти и (или) местного самоуправления, государственных и (или) муниципальных учреждений, предприятий».

Предусмотрев санкцию за указанные деяния до 10 лет лишения свободы.

Данную авторскую позицию, обосновываем тем, что компьютерные преступники своими действиями причиняют огромный экономический ущерб.

Так, например, 21 января 2016 года с корреспондентского счета Русского международного банка в Центральном Банке России хакеры похитили годовую прибыль - более полумиллиарда рублей. В ЦБ подтвердили факт кражи, указав, что потери банков от хакерских атак за 4 квартал 2015 года и 1 квартал 2016 года превысили 2 млрд. рублей. При этом хакеры, в этот же период, покушались на хищение с банковских счетов еще 1,5 млрд. рублей, но эти атаки удалось отразить[20].

Кроме того, с 2012 года хакеры, хактивистские движения, иностранные спецслужбы стали совершать большое количество

[20] С корсчета Центробанка хакеры украли более 500 млн рублей [Электронный ресурс] – URL: http://rg.ru/2016/05/04/s-korscheta-centrobanka-hakery-ukrali-bolee-500-mln-rublej.html (Дата обращения 09.11.2016).

компьютерных преступлений по политическим мотивам (DDoS-атаки на государственные информационные ресурсы; применение вредоносных компьютерных программ для кибершпионажа, киберсаботажа, кибертерроризма и пр.), что является уже угрозой для национальной безопасности России.

Поэтому, по мнению автора, законодатель должен занять более активную позицию по защите законных интересов общества и государства от возникающих киберугроз, в т.ч. путем совершенствования конструкций составов преступлений в сфере компьютерной информации и ужесточения наказания для виновных в совершении данных преступных деяний.

Кроме того, полагаем, что правоохранительным органам следует более активно привлекать институты гражданского общества (средства массовой информации, научные и образовательные организации, общественные движения, общественные советы, политические партии, профсоюзы, религиозные объединения и т.д.) для предупреждения компьютерной преступности.

References:

[1] Volevodz A.G. Protivodejstvie komp'yuternym prestupleniyam: pravovye osnovy mezhdunarodnogo sotrudnichestva. – M.: OOO Izd-vo «Yurlitinform», 2002. – 496 p.

[2] Zakonodatel'nye mery po bor'be s komp'yuternoj prestupnost'yu // Problemy prestupnosti v kapitalisticheskikh stranakh. – 1988. – Vol. 10. - P.40

[3] Kurushin V.D., Minaev V.A. Komp'yuternye prestupleniya i informatsionnaya bezopasnost' / V.D. Kurushin, V.A. Minaev - M.: Novyj Yurist,1998. – 256 p.