2.10. ОТВЕТСТВЕННОСТЬ ЗА КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ В РОМАНО-ГЕРМАНСКОЙ ПРАВОВОЙ СИСТЕМЕ

Пелевина Алла Валерьевна, аспирант. Место учебы: Чебоксарский кооперативный институт. Филиал: Чебоксарский филиал Российского университета кооперации. Подразделение: кафедра уголовного права и судопроизводства. E-mail: allochka_90@bk.ru

Аннотация: В представленной статье исследуются вопросы уголовной ответственности за компьютерные преступления в странах романо-германской правовой системы, дается их общая характеристика, раскрываются характерные особенности и отличительные черты. Рассматривается уголовная ответственность за преступления в сфере компьютерной информации.

Ключевые слова: романо-германская система, компьютерные преступления, уголовная ответственность, информационные технологии, физические и юридические лица.

RESPONSIBILITY FOR COMPUTER CRIMES IN THE ROMAN-GERMANIC LEGAL SYSTEM

Pelevina Alla Valeryevna, postgraduate student. Place of study: Cheboksary cooperation institute. Branch: Cheboksary branch of Russian University of Cooperation. Department: criminal law and legal proceedings chair. E-mail: allochka_90@bk.ru

Annotation: In the presented article the questions of criminal responsibility are investigated for computer crimes in the countries of the roman-germanic legal system, their general description is given, characteristic features and distinguishing features open up. Criminal responsibility is examined for crimes in the field of computer information.

Keywords: the roman-germanic system, computer crimes, criminal responsibility, information technologies, physical and legal persons.

Обзор проблемы. В настоящее время противодействие компьютерным преступлениям осознается мировым сообществом и превратилось в сверх актуальную проблему. Законодатели всех стран включили нормы об ответственности за компьютерные преступления в свои уголовные кодексы. В этой связи развитие и дальнейшее совершенствование российского уголовного законодательства об ответственности за преступления в сфере компьютерной информации невозможно без использования опыта применения уголовного законодательства зарубежных государств. Сравнительное правоведение позволяет исследовать различные уголовно-правовые институты путем их сопоставления с целью выявления передовых юридико-технических решений, раскрыть специфику юридических категорий и таким образом получить научный продукт, материализуемый в дальнейшем в правотворческой и практической деятельности [1,С. 358-389].

В этой связи представляется оправданным рассмотрение некоторых аспектов уголовно-правовой регламентации ответственности за преступления в сфере компьютерной информации в странах романо-германской правовой системы.

Характеристика уголовного законодательства в странах романо-германской правовой системы.

Германия. В Уголовном кодексе Германии [2] компьютерные преступления (преступления в сфере компьютерной информации) структурно размещаются в разных разделах, а именно: предусмотрена в §202a (шпионаж данных), §263a (компьютерное мошенничество), §269 (фальсификация данных, имеющих доказательственное значение), §270 (обман при помощи ЭВМ при обработке данных), §303a (изменение данных), §303b (компьютерный саботаж).

Так, «шпионаж данных» (§202a), включен в раздел15 «Нарушение неприкосновенности и тайны частной жизни», и предусматривает ответственность лица, за незаконное получение данных, которые ему не предназначаются и особо охраняются от незаконного к ним доступа, или кто передает их другому лицу. Данное преступление наказывается на срок до трех лет или денежным штрафом.

«Мошенничество и преступное злоупотребление доверием» (§263a «компьютерное мошенничество»[3]) раздел 22 признается тогда «кто, действуя с намерением получить для себя или третьего лица имущественную выгоду, причиняет вред имуществу другого лица, воздействует на результат обработки данных путем неправильного создания программ, использования неправильных или неполных данных или иного неправомочного воздействия на результат обработки данных». За его совершение, предусмотрена уголовная ответственность до пяти лет лишения свободы или денежный штраф (то есть как за неквалифицированный вид мошенничества).

В разделе 23 «Фальсификация документов» (§269 «фальсификация данных, имеющих доказательственное значение»[4]) устанавливается ответственность за различные способы фальсификации документов. В частности, ответственность наступает за сохранение или изменение при помощи ЭВМ, путем обмана данных, имеющих доказательственное значение, приводящее к восприятию документов как сфальсифицированных или поддельных, либо использование такого рода сохраненных или измененных данных.

В данный раздел включен и §270 «обман при помощи ЭВМ при переработке данных»[4].Под переработкой понимается получение из введенных данных посредством компьютерных программ новых данных. Кроме указанных выше уголовно-правовых запретов имеются и другие запреты. Так, в раздел 27 «Повреждение имущества» включены: §303a[3]«изменение данных» и §303b[4] «компьютерный саботаж».

За совершение деяния, предусмотренного в §303a ответственность наступает в виде лишения свободы до двух лет или денежного штрафа, если лицо «противоправно стирает, делает непригодным для использования или изменяет данные». За деяние, указанное в §303b выразившееся в нарушении обработки данных, имеющих существенное значение для чужого предприятия, организации или органа, если лицо совершило преступление, предусмотренное §303a или испортило, повредило, сделало непригодным для дальнейшего использования по назначению или изменило устройство для переработки данных или носитель информации лицо наказывается лишением свободы на срок до пяти лет или денежным штрафом.

Таким образом, составы компьютерных преступлений сконструированы как квалифицирующие виды простых составов преступлений, имеющих различные объекты посягательств [5]. Необходимо отметить, что в немецком уголовном законе используется специальный термин – Daten – это данные, которые сохранены

или передаются электронным, магнитным или иным, непосредственно визуально не воспринимаемым способом [4].

Нидерланды. Ведущее место среди европейских государств активно противодействующих компьютерным преступлениям с момента их появления в жизни общества является Нидерланды (Голландия). Законодатель Нидерландов в этих целях создал Консультативный комитет по компьютерным преступлениям, который выработал конкретные рекомендации по внесению изменений в Уголовный кодекс и Уголовно-процессуальный кодекс Нидерландов [6].

Проведенное исследование показало, что Консультативный комитет разработал классификацию компьютерных преступлений, но не дефинировал понятие.

Нидерландские ученые считаю, что существует множество трудностей при его формулировании. С одной стороны, оно должно быть достаточно емким, а с другой – достаточно специальным. В настоящее время применяется два понятия компьютерного преступления – в узком и широком смысле. В узком смысле – это совершение преступления, которое невозможно выполнить без использования компьютера или другого автоматического устройства как объекта или инструмента преступления. А в широком смысле – это поведение, которое (потенциально) вредно и имеет отношение к устройствам, связанным с компьютерами с точки зрения хранения, передачи и обработки данных. Последнее определение компьютерного преступления использует полицейское разведывательное управление, занимающееся регистрацией компьютерных преступлений. Управление делает различие между компьютерными преступлениями, в которых компьютер является объектом преступления, и теми, в которых он – орудие преступления.

Полицейское разведывательное управление с 1987 г. использует для изучения пять видов компьютерных преступлений: 1) совершаемые обычным способом, но с использованием технической поддержки в компьютерной среде; 2) компьютерное мошенничество; 3) компьютерный террор (совершение преступлений с целью повреждения компьютерных систем): а) использование несанкционированного доступа; б) использование вредоносных программ, типа компьютерных вирусов; в) совершение других действий, включая физическое повреждение компьютера; 4) кража компьютерного обеспечения (пиратство); 5) остаточная категория, включающая все другие типы преступлений, которые не подпадают под вышеперечисленные категории.

В 1993 г. в Нидерландах был принят Закон о компьютерных преступлениях, дополняющий Уголовный кодекс новыми составами: ст. 138а (1) «несанкционированный доступ в компьютерные сети»; ст. 138а (2) «несанкционированное копирование данных»; ст. 350а (1), 350b (1) «компьютерный саботаж»; ст. 350а (3), 350b (2) «распространение вирусов»; ст. 273 (2) «компьютерный шпионаж» [5].

Так ст. 138а (1) «несанкционированный доступ в компьютерные сети» (раздел V «Преступления против общественного порядка») предусматривает ответственность «лица, которое умышленно незаконно проникает в компьютерное устройство или систему для хранения и обработки данных или в часть такого устройства или системы, виновно в неправомерном вторжении в компьютер». И оно наказывается тюремным заключением не более шести месяцев или штрафом третьей категории.

В ст. 138а (2) «несанкционированное копирование данных» (раздел V «Преступления против общественного порядка»)регламентируется ответственность за «неправомерное проникновение в компьютер». Данный вид деяния наказывается тюремным заключением на срок не более четырех лет или штрафом четвертой категории, если виновный путем копирования данных, хранящихся в компьютерном устройстве или системе, либо он незаконно проник, и записывает такие данные для личного использования или использования другим лицом.

Ст. 350а (1), 350b (1) «компьютерный саботаж» входят в раздел XX VII «Уничтожение или причинение ущерба». В первом случае предусмотрена ответственность «лица, которое умышленно и незаконно изменяет, стирает, делает непригодной или недоступной информацию, хранящуюся, обрабатываемую или передаваемую с помощью компьютерного устройства или системы, или вносит туда дополнительные данные». За совершение указанного преступления предусмотрен срок тюремного заключения не более двух лет или штраф четвертой категории.

Во втором случае предусмотрена ответственность «лица, которое по небрежности или неосторожности незаконно изменяет, стирает, приводит в непригодное состояние или делает недоступными данные, хранящиеся, обрабатываемые или передаваемые с помощью компьютерного устройства или системы, или вносит туда другие данные». За совершение этого деяния к лицу применяется тюремное заключение или заключение на срок не более одного месяца или штрафом второй категории, если таким образом причинен серьезный ущерб этим данным.

В указанный раздел входят еще две ст.ст. 350а (3), 350b (2) «распространение вирусов», относящиеся к компьютерным преступлениям. В ст. 350а (3) регламентируется ответственность «лица, которое умышленно и незаконно делает доступными или распространяет данные, которые направлены на то, чтобы причинить ущерб путем копирования в компьютерном устройстве или системе». Лицо наказывается в виде тюремного заключения не более четырех лет или штрафом пятой категории. Ст. 350b (2) регламентирует ответственность «лица, которое по небрежности или неосторожности незаконно делает доступными или распространяет данные, предназначенные для причинения ущерба путем копирования в компьютерном устройстве или системе» в виде тюремного заключения или заключения не более одного месяца или штрафу второй категории.

Ст. 273 (2) «компьютерный шпионаж» входит в раздел XVII «Разглашение тайны», а именно за «преступление, совершаемое против определенного лица» и оно будет подвергнуто уголовному преследованию только после жалобы этого лица.

Таким образом, уголовное законодательство Нидерландов предоставляет достаточно широкие возможности для противодействия различным видам компьютерных преступлений, устанавливая помимо специальных норм дополнительные квалифицирующие обстоятельства в уже существующие уголовно-правовые нормы.

Испания. В Уголовном кодексе Испании [7], вступившем в действие в 1996 году отсутствуют специальные нормы об ответственности за преступления в сфере компьютерной информации. Уголовная ответственность предусматривается лишь за преступления, совершаемые с использованием информационных тех-

нологий, в частности за: «Раскрытие и распространение тайных сведений» (ст. 197); «Посягательство на интеллектуальную собственность» (ст. 270); «Раскрытие и распространение коммерческой тайны» (ст. 278); «Подделка документов» (ст. 394); «Изготовление и владение средствами (инструмент, материал, орудие, вещество, машина, компьютерная программа, аппарат), специально предназначенными для совершения преступлений, предусмотренных в предыдущих статьях» (ст.400); «Раскрытие тайны и информации, связанной с национальной обороной» (ст. 598); «Выдача тайны и информации, связанной с национальной обороной» (ст. 599).Так в ст. 598 указывается, что тот, кто без цели способствования иностранному государству, достанет, выдаст, исказит или уничтожит информацию, связанную с национальной безопасностью либо национальной обороной, либо связанную с техническими приемами или системами, применяемыми в Вооруженных Силах или в военной промышленности, наказывается тюремным заключением на срок от одного года до четырех лет.

В качестве квалифицирующих признаков указанных составов преступлений, совершаемых с использованием информационных технологий, законодатель признает совершение деяний лицами, управляющими или ответственными за системы, являющимися хранителями или владельцами информации. Кроме этого, законодатель охраняет объекты авторского права [8].

Франция. Уголовный кодекс Франции [9] включает в себя большое число компьютерных преступлений.

В Уголовном кодексе в Книге второй «О преступлениях и проступках против личности» в разделеII «О посягательствах на человеческую личность» в отделе V «О посягательствах на права лица, возникающие в связи с ведением картотек и обработкой информации» предусмотрена ответственность за посягательства, связанные с использованием картотек и обработкой данных на ЭВМ: ст. 226-16 «Осуществление или отдача указания об осуществлении автоматизированной обработки поименных данных без осуществления предусмотренных в законе формальностей»; ст. 226-17 «Осуществление или отдача указания об осуществлении обработки этих данных без принятия всех мер предосторожностей, необходимых для того, чтобы обеспечить безопасность данных»; ст. 226-18 «Сбор и обработка данных незаконным способом»; ст. 226-19 «Ввод или хранение в памяти ЭВМ запрещенных законом данных»; ст. 226-20 «Хранение определенных данных сверх установленного законом срока»; ст. 226-21 «Использование данных с иной целью, чем это было предусмотрено»; ст. 226-22 «Разглашение данных, могущее привести к указанным в законе последствиям». За указанные деяния законодатель предусматривает ответственность в виде лишения свободы на срок пять лет и штрафом в размере 300 000 евро (ст.ст. 226-16, 226-17, 226-18, 226-19, 226-21) либо лишением свободы на срок три года и штрафом в размере 100 000 евро (ст. 226-22).

В Книге третей «Об имущественных преступлениях и проступках» в разделе II «О прочих имущественных посягательствах» в главе III «О посягательствах на системы автоматизированной обработки данных» предусмотрена ответственность за преступления, посягающие на системы автоматизированной обработки данных: ст. 323-1 «Незаконный доступ к автоматизированной системе обработки данных или незаконное пребывание в ней»; ст. 323-2 «Воспрепятствование работе или нарушение работы системы»; ст. 323-3 «Ввод обманным путем в систему информации, а также изменение или уничтожение содержащихся в автоматизированной системе данных». Законодатель за указанные деяния предусматривает ответственность в виде денежных штрафов в размере 150 000 евро и пяти лет лишения свободы (ст. 323-1) либо штрафом 300 000 евро и лишением свободы на срок семь лет (ст.ст. 323-2, 323-3).

В Книге четвертой «О преступлениях и проступках против нации, государства и общественного спокойствия» в разделе I «О посягательствах на основополагающие интересы нации» в главе I «Об измене и шпионаже» в отделе III «О передаче информации иностранному государству» предусмотрена ответственность за действия, совершаемые с компьютерной информацией в ущерб интересам государства ст.ст. 411-7, 411-8 «Сбор или передача содержащейся в памяти ЭВМ или картотеки информации иностранному государству». В отделе IV «О саботаже» и отделе V «О предоставлении ложных сведений» ст.ст. 413-9, 413-10, 413-11 «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». За преступления предусмотренные отделом III «О передаче информации иностранному государству» законодатель установил наказание в виде десяти лет лишения свободы и штрафа в размере 150 000 евро. А за преступления, посягающие на тайну национальной обороны определил наказание в виде трех лет лишения свободы и штрафа в размере 45 000 евро или пяти лет лишения свободы и штрафа в размере 75 000 евро.

Посягательства на информационные системы отнесены законодателем к проступкам. Уголовная ответственность устанавливается в виде лишения свободы от трех до десяти лет и штрафа в размере от сорока пяти тысяч до трехсот тысяч евро.

Вывод. Проведенное исследование регламентации ответственности за компьютерные преступления в странах романо-германской правовой системы показало, что законодатель указанных стран уделяет особое внимание противодействию указанным противоправным деяниям. Характерной особенностью является установление ответственности в виде штрафа или лишения свободы. К числу особенностей французского законодательства следует отнести использование абсолютно определенных санкций.

Список литературы:

1. Кузнецов А.П. Раздел II Принципы уголовного права: сравнительно-правовой анализ // Уголовное право. Общая часть. Академический курс. В 10 т. Т. II. Система, источники и структура уголовного права. Принципы уголовного права / под ред. док. юрид. наук., проф. Н.А. Лопашенко. – М.: Юрлитинформ, 2016. 712 с. (стр.358-389).

2. Strafgesetzbuch mit Einführungsgesetz, Völkerstrafgesetzbuch, Wehrstrafgesetz, Wirtschaftsstrafgesetz, Betäubungsmittelgesetz, Versammlungsgesetz, Auszügen aus dem Jugendgerichtsgesetz und dem Ordnungs widrichkeitengesetz sowie anderen Vorschriften des Nebenstrafrechts. München, 2002.

3. Schönke/Schröder. Strafgesetzbuch. Kommentar. München, 2001. , c. 2105–2115.

4. Joeks Wolfgang. Strafgesetzbuch. Studien kommentar. München, 2003.С. 662–665.

5. Громов Е.В. Развитие уголовного законодательства о преступлениях в сфере компьютерной информации в зарубежных странах (США, Великобритания, ФРГ, Нидерландах. Польше). Вестник ТГПУ. 2006. Выпуск 11 (62). С. 30-35.

6. Уголовный кодекс Голландии / Науч. ред. д.ю.н., проф. Б.В. Волженкин, пер. с англ. И.В. Мироновой. СПб, 2000.

7. Уголовный кодекс Испании // под ред. Кузнецовой Н.Ф. М.: Издательство «Зерцало». 1998. 218с.

8. Кузнецов А.П. Ответственность за преступления в сфере компьютерной информации по зарубежному законодательству/ "Международное публичное и частное право", 2007, № 3.

9. https://www.legifrance.gouv.fr/initRechCodeArticle.do.

Рецензия

на статью аспиранта кафедры уголовного права и судопроизводства Университета потребительской кооперации (Чебоксарский филиал) Пелевиной Аллы Валерьевны на тему: «Ответственность за компьютерные преступления в романо-германской правовой системе»

Компьютерные преступления многоаспектны и потому могут относиться к самым различным видам преступных посягательств и отличаться не только по объекту посягательства, но и по способам, мотивам и другим признакам. Единственным основанием отнесения преступления к данной категории является наличие средства вычислительной техники как носителя охраняемой законом компьютерной информации, выступающего в качестве объекта или орудия совершения преступления.

Последствия совершения компьютерных преступлений могут быть самыми различными, например: нарушение неприкосновенности интеллектуальной собственности, разглашение сведений о частной жизни граждан, имущественный ущерб в виде прямых убытков и неполученных доходов, потеря репутации, различные виды нарушений нормальной деятельности предприятий, учреждений, организаций и целых отраслей и т.д. Все это наглядно демонстрирует высокую общественную опасность рассматриваемых деяний и актуальность настоящей публикации.

Интерес к проведению анализа зарубежного и отечественного уголовного законодательства об ответственности за компьютерные преступления вызван не только стремлением сравнить состояние российского и зарубежного права, но обусловлен также и целесообразностью заимствования положительного опыта. Кроме того, изучение зарубежного законодательства помогает глубже проанализировать отечественное, выдвинуть предложения по его совершенствованию. Как правильно отмечал французский юрист Марк Ансель, «…изучение зарубежного права открывает перед юристом новые горизонты, позволяет ему лучше узнать право своей страны, ибо специфические черты этого права особенно отчетливо выявляются в сравнении с другими системами. Сравнение способно вооружить юриста идеями и аргументами, которые нельзя получить даже при очень хорошем знании только собственного права».

В статье автор подвергает исследованию вопросы, связанные с регламентацией ответственности за компьютерные преступления в странах романо-германской правовой семьи. В частности проанализированы положения уголовных кодексов Германии, Нидерландов, Испании и Франции. Об актуальности публикации свидетельствует и тот факт, что уголовное законодательство России также относится к указанной системе права.

Следует отметить, что отдельные положения, закрепленные в зарубежных нормативных актах, могут представлять практический интерес для дальнейшего совершенствования отечественного уголовного законодательства.

В целом статья Пелевиной Аллы Валерьевны соответствует предъявляемым требованиям и может быть рекомендована к публикации, в т.ч. в издании, включенном в Перечень российских рецензируемых научных журналов, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученых степеней доктора и кандидата наук, рекомендованных ВАК.

Профессор кафедры уголовного права и судопроизводства Университета потребительской кооперации (Чебоксарский филиал), Заслуженный деятель науки РФ, Заслуженный юрист РФ, д.ю.н., профессор А.П. Кузнецов