На правах рукописи

Суслопаров Алексей Валерьевич

ИНФОРМАЦИОННЫЕ ПРЕСТУПЛЕНИЯ

Специальность 12.00.08 - уголовное право и криминология;
уголовно-исполнительное право

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата юридических наук

Красноярск 2008

Диссертация выполнена на кафедре уголовного права
Юридического института Сибирского федерального университета

Научный руководитель: кандидат юридических наук, доцент
Мицкевич Александр Федорович

Официальные оппоненты: доктор юридических наук, профессор
Щедрин Николай Васильевич

кандидат юридических наук, доцент
Бунева Ирина Юрьевна

Ведущая организация: Кемеровский государственный университет

Защита состоится 20 января 2009 г. в 15.00 часов на заседании диссертационного совета ДМ 212.099.14 по защите диссертаций на соискание ученой степени доктора юридических наук при Сибирском федеральном университете по адресу: 660075, г.Красноярск, ул. Маерчака, 6, зал заседаний совета.

С диссертацией можно ознакомиться в библиотеке Юридического института Сибирского федерального университета.

Автореферат разослан "11" декабря 2008 г.

Ученый секретарь
диссертационного совета
кандидат юридических наук, доцент В.В. Питецкий

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы диссертационного исследования. Стремительный рост информационных технологий закономерно обусловливает интерес исследователей к ним из разных областей науки. Право, в том числе уголовное, не является исключением. Имеются многочисленные работы учёных, посвящённые исследованию компьютерных преступлений, киберпреступлений, информации, информационной безопасности и прочих явлений, связанных с информацией. Формируется отдельная отрасль права – информационное право. Несмотря на это, до сих пор в науке не выработаны единые подходы к анализу информационно-правовых явлений. В частности, отсутствует понятие информации, которое удовлетворяло бы большинство исследователей и которое можно было бы применять в уголовно-правовой сфере. Такое положение дел нельзя признать удовлетворительным.

В 1998 г. была разработана и одобрена Концепция государственной информационной политики РФ, одним из назначений которой является обращение внимания органов государственной власти, средств массовой информации, всех заинтересованных лиц на проблемы подготовки государства, общества, личности к условиям жизни в информационном обществе[1]. В соответствии с данной Концепцией одной из основных задач государственной информационной политики является обеспечение информационной безопасности. В числе основных положений правового обеспечения государственной информационной политики находится защита законными средствами личности, общества, государства от ложной, искажённой и недостоверной информации[2]. В развитие положений Концепции в 2000 году была утверждена Доктрина информационной безопасности Российской Федерации. В июле 2000 г. в Окинаве «восьмёрка» приняла Хартию Глобального информационного общества, в которой устанавливаются основные принципы вхождения государств в такое общество. 27 июля 2006 года принят закон Российской Федерации «Об информации, информационных технологиях и о защите информации».

Сказанное свидетельствует об осознании государством и всем мировым сообществом важности информационных процессов, происходящих в современном мире. Указанные выше документы носят программный характер и задают цели, достижение которых является приоритетной задачей современных правопорядков. Выработка адекватных мер борьбы с компьютерными преступлениями находится в их числе. И хотя до сих пор многие явления в сфере компьютерных преступлений остаются неизученными, у большинства исследователей

[1] См.: Финько О.А. Правовое обеспечение Государственной информационной политики // Сб. НТИ. Сер. 1. 1999. № 8.
[2] Цит. по: Копылов В.А. Информационное право. М., 2003. С. 36.

имеется общий взгляд на способы борьбы с ними. В частности, подвергаются детальному анализу понятия компьютерной информации и отдельные виды компьютерных преступлений. Таким образом, в уголовном праве понятие информации изучается, прежде всего, в связи с компьютерными преступлениями и для определения мер борьбы с ними.

Вместе с тем, изучение компьютерных преступлений и компьютерной информации позволит решить проблему уголовно-правового регулирования информационных отношений лишь частично. Связано это с тем, что информационная безопасность, а также защита от ложной, искажённой и недостоверной информации обеспечиваются не только мерами борьбы с компьютерными преступлениями. Для реализации положений Концепции государственной информационной политики необходим комплексный взгляд на информационные явления, которые подлежат защите уголовно-правовыми средствами. В этой связи приобретают особую значимость исследования, посвящённые изучению понятия социальной информации в уголовном праве, в частности, определению информации как предмета преступления. Совсем недавно также стали подвергаться изучению понятия информационной безопасности, а также специфические виды информационного воздействия, предусмотренные УК РФ[3]. Связано это с тем, что в современном мире информационные процессы занимают ведущее место наряду с другими процессами: физическими, химическими, энергетическими, а информационный способ совершения преступления по своей общественной опасности сравнялся с традиционными способами. Также как и общественно опасные посягательства против информационных объектов являются равными посягательствам на иные объекты.

Сказанное свидетельствует об осознании учёными и практиками важности анализа всего спектра информационных явлений в уголовно-правовой области. Вместе с тем, к настоящему времени отсутствуют комплексные уголовно-правовые исследования, объединяющие работы учёных по изучению отдельных аспектов информационно-правовых явлений.

Практическая ценность работ, посвящённых изучению информационных явлений в уголовно-правовой сфере, заключается в

---

[3] См., напр.: Гертель Е.В. Уголовная ответственность за угрозу. Автореф. дис… канд. юрид. наук: 12.00.08 / Е.В. Гертель. – Омск, 2006 [Электронный ресурс]. – Доступно из URL: http://sartraccc.sgap.ru [Дата обращения: 07.09.2006]; Жданухин Д.Ю. Уголовно-правовая характеристика шантажа. Автореф. дис… канд. юрид. наук: 12.00.08 / Д.Ю. Жданухин – Екатеринбург, 2005 [Электронный ресурс]. – Доступно из URL: http://sartraccc.sgap.ru/Disser/gdanuhin.htm [Дата обращения: 07.09.2006]; Калмыков Д.А. Информационная безопасность: понятие, место в системе уголовного законодательства РФ, проблемы правовой охраны. Автореф. дис… канд. юрид. наук: 12.00.08 / Д.А. Калмыков – Казань, 2005 [Электронный ресурс]. – Доступно из URL: http://sartraccc.sgap.ru/Disser/kalmykov.htm [Дата обращения: 07.09.2006]; Коростылёв О.И. Уголовно-правовая характеристика угрозы. Автореф. дис… канд. юрид. наук: 12.00.08 / ОИ. Коростылёв. – Ставрополь, 2004. – 26 с.; Красненкова Е.В. Обеспечение информационной безопасности в Российской Федерации уголовно-правовыми средствами: дис. … канд. юрид. наук: 12.00.08 / Е.В. Красненкова. – М., 2006. – 188 с.

выработке общих подходов к криминализации и декриминализации информационных преступлений. На необходимость постоянной предварительной криминологической оценки обоснованности тех или иных проектируемых законодательных новаций указывают, в частности, В.Н. Кудрявцев и В.Е. Эминов[4].

С учётом изложенного, тема настоящего исследования, сформулированная как «Информационные преступления», представляется достаточно актуальной, а исследование, проведенное в рамках данной темы, позволяет сформировать новый взгляд на многие традиционные уголовно-правовые явления, более точно сформулировать признаки некоторых составов преступлений и, в конечном счете, способствовать повышению эффективности борьбы с общественно-опасными деяниями в информационной, в том числе компьютерной, области.

Цели и задачи диссертационного исследования. Целью данного исследования является изучение специфического вида преступлений – информационных преступлений – путём выделения их признаков, составных элементов, а также анализ мер уголовно-правовой борьбы с ними и разработка предложений, направленных на повышение эффективности уголовно-правового регулирования борьбы с информационными преступлениями.

Основные задачи исследования заключаются в следующем.

1. Формулирование понятия информационных преступлений, выделение их видов.
2. Характеристика видов информационных преступлений, классификация информационных преступлений внутри этих видов.
3. Выявление конкретных составов информационных преступлений, содержащихся в УК РФ.
4. Сравнительный уголовно-правовой анализ компьютерных преступлений как одного из основных видов информационных преступлений.
5. Формулирование предложений по совершенствованию уголовного законодательства в области регулирования информационных, включая компьютерные, преступлений.

Объект исследования. Объектом настоящего диссертационного исследования являются информационные преступления.

Предметом исследования выступают признаки и виды информационных, включая компьютерные, преступлений, а также национальные и международные уголовно-правовые нормы, предусматривающие ответственность за информационные преступления.

Методологическая основа исследования. При написании работы были использованы положения диалектического метода познания социальных явлений, а также приёмы формальной логики и такие

[4] Кудрявцев В.Н., Эминов В.Е. Криминология и проблемы криминализации // Журнал российского права. 2004. № 12. С. 46 – 50.

общенаучные методы, как анализ, синтез, аналогия, сравнение, индукция, дедукция, системный анализ. Кроме этого, были использованы частно-научные методы: метод системного, сравнительного анализа и иные методы. Системный метод позволил выявить в информационных общественных отношениях определённые закономерности их функционирования в уголовно-правовой сфере. Сравнительно-правовой метод основан на обращении к теоретическому и законодательному опыту зарубежных стран, на сопоставлении российских и зарубежных правовых институтов и, как следствие, более глубоком уяснении сущности изучаемых явлений, выявлении недочётов в законодательстве отдельных стран. Правовой анализ построен на оценке формулировок действующего законодательства с позиций их эффективности в борьбе с отдельными группами преступлений.

Теоретической базой исследования выступила общетеоретическая литература по теории информации, общей теории права, уголовному праву, криминологии, а также публикации в Интернете и зарубежные источники.

Нормативная основа диссертации представлена Конституцией РФ, нормативно-правовыми актами Российской Федерации, включающими в себя как уголовное, так и информационное законодательство, а также правовыми актами зарубежных стран, посвящёнными компьютерным преступлениям.

Перевод зарубежной литературы и национального законодательства стран мира с иностранных языков осуществлён автором самостоятельно.

Эмпирическую основу исследования составляют статистические данные об информационных, в том числе компьютерных, преступлениях. Изучена статистика зарегистрированных компьютерных преступлений по Российской Федерации и по Сибирскому федеральному округу за 2002 - 2006 годы на основе статистических сборников Главного информационного центра МВД России, статистическая отчетность о деятельности подразделений К У(О)СТМ МВД, ГУВД, УВД субъектов РФ, а также статистика, предоставленная Управлением Судебного департамента в Красноярском крае, о количестве осуждённых районными (городскими) судами Красноярского края по статьям 138, 179, 183, 207, 237, 242, 242.1, 272, 273, 274, 280, 283, 284, 287, 296, 297, 298, 302, 303, 305, 306, 307, 308, 309, 310, 311, 319, 320, 324, 325, 326, 327, 327.1 УК РФ с 2000 по 1 полугодие 2007 года. Проведено собственное исследование в виде интервьюирования сотрудников отдела «К» при ГУВД Красноярского края, анкетирования пользователей персональных компьютеров из числа студентов 4-5 курса Юридического института СФУ. В диссертации использована опубликованная судебная практика Верховного суда РФ, сведения об уголовных делах из научной литературы. В ходе проведённого исследования изучено 16 уголовных дел о преступлениях в сфере компьютерной информации, рассмотренных Красноярским краевым судом, Центральным, Ленинским, Октябрьским, Советским, Кировским и

Свердловским районными судами г. Красноярска, Сосновоборским городским судом Красноярского края, Железногорским городским судом Красноярского края за период с 1999 по 1 полугодие 2007 года.

Теоретической основой диссертационного исследования являются работы отечественных и зарубежных учёных по понятию информации. Сущность информации, её природа и роль в жизни общества были освещены в исследованиях Н.М. Амосова, А.А. Вишневского, Д.И.Дубровского, В.Г. Афанасьева, Г.Б. Жданова, А.Н. Колмогорова, Н.А.Кузнецова, К.Е. Морозова, А.Д. Урсула, К.Э. Шеннона, Ю.А.Шрейдера, У.Р. Эшби.

Вместе с тем, несмотря на многочисленные работы по понятию информации, ощущается нехватка исследований, посвящённых изучению информационных преступлений, среди авторов, занимавшихся данной проблематикой, можно отметить В.В. Крылова, Л.А. Букалерову, исследовавшую в диссертации информационные преступления в сфере государственного и муниципального управления, и А.А. Турышева, посвятившего свою работу изучению информационных преступлений в сфере экономической деятельности.

В то же время, отдельные аспекты информационных преступлений изучены учёными достаточно подробно. В начале 21 века, когда бурное развитие информационных технологий поставило вопрос о совершенствовании уголовно-правовых мер борьбы с компьютерными преступлениями, были защищены диссертации, посвящённые анализу компьютерной преступности, в том числе с использованием зарубежного опыта. К числу авторов таких работ относятся С.Д. Бражник, С.Ю. Бытко, В.В. Воробьёв, М.С. Гаджиев, Д.В. Добровольский, А.М. Доронин, А.А.Жмыхов, М.М. Менжега, В.Г. Степанов-Егиянц, Т.Л. Тропина, А.Е.Шарков, С.А. Яшков. В это же время повышается интерес исследователей к сопутствующим уголовно-правовым явлениям, таким как информационная безопасность, угроза, тайна, шантаж и др. Свой вклад в их изучение внесли Е.В. Гертель, Д.Ю. Жданухин, Д.А. Калмыков, Л.Р.Клебанов, О.И. Коростылёв, Е.В. Красненкова, С.М. Паршин, А.Е.Ратникова.

Из более ранних работ, посвящённых изучению компьютерных преступлений, следует отметить написанные в 90-х годах прошлого века работы Ю.М. Батурина, В.Б. Вехова, А.Г. Волеводза, Б.Д. Завидова, В.В.Крылова, В.Д. Курушина, В.А. Мазурова, В.А. Минаева, В.А.Номоконова, Д.Б. Фролова, А.В. Черных.

За рубежом изучение проблем компьютерной преступности началось гораздо раньше, чем в России. Данной проблематике посвящены работы таких зарубежных учёных, как Д.Айков, С. Бреннер, У. Зибер, М. Роджерс, Р. Холлинджер, Д. Шиндер и др.

Научная новизна исследования заключается в том, что впервые на уровне самостоятельного исследования был выделен отдельный вид преступлений – информационных преступлений. Предпосылками для

этого послужили программные документы, принятые как на международном, так и на национальном уровне, которые посвящены формированию информационного общества. Кроме этого, анализ современных работ в области уголовного права выявил необходимость комплексной оценки ряда указанных в них информационных явлений. В диссертации предпринята попытка систематизации таких явлений, выделены их сущностные признаки, а также проведена классификация. Компьютерные преступления, уже неоднократно рассматривавшиеся в исследованиях других авторов, были проанализированы сквозь призму информационных преступлений, в том числе с учётом международного опыта в их регулировании.

Основные положения, выносимые на защиту.

1. Необходимость выделения информационных преступлений продиктована возросшим значением информации и информационных процессов в современном обществе, переживающем переход к стадии информационного общества. Особое значение, в связи с этим, обретает точная формулировка понятия информации, а также адекватное уяснение сущности информационных процессов в уголовно-правовой сфере. Под информацией предлагается понимать сведения, передающиеся между субъектами посредством сигналов в форме определённого кода и представляющие собой целенаправленное управленческое воздействие.

2. Информационными преступлениями являются общественно опасные противоправные деяния, причиняющие вред общественным отношениям по обеспечению информационной безопасности, способом совершения которых является информационное воздействие или (и) предметом которых является информация как особый нематериальный объект. Соответственно, выделяются два вида информационных преступлений: преступления, предметом которых является информация, и преступления, способом совершения которых является информационное воздействие.

3. Дополнительным родовым объектом, общим для всех видов информационных преступлений, являются общественные отношения по поводу обеспечения информационной безопасности личности, общества и государства. Выделение данного объекта обусловлено логикой построения уголовного закона, в котором разделы посвящены охране общественных отношений применительно к отдельной личности (раздел 7), к обществу (разделы 8-9) и государству (разделы 10-11). Применительно к предлагаемому в работе подходу это означает охрану информационной безопасности личности, общества и государства составами информационных преступлений, расположенных в соответствующих разделах.

4. Информация как предмет информационных преступлений имеет нематериальную форму, хранится на каком-либо материальном носителе, но не имеет какой-либо жёстко детерминированной связи с этим носителем. В уголовном законе такой предмет преступления выражается

путём непосредственного указания на информацию, путём указания на материальный носитель информации, а также путём упоминания документов как информации, закреплённой на особом материальном носителе.

5. Информационное воздействие как способ совершения информационных преступлений может быть направлено на конкретного человека и на неопределённый круг лиц.

6. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации» запрещает распространение отдельных видов информации в отношении неопределённого круга лиц. Вместе с тем, аналогичное правило в отношении конкретных получателей информации отсутствует. Кроме этого, в указанном законе отсутствует определение одного из базовых понятий информационной сферы – понятие информационной безопасности.

С учётом сказанного, в работе предлагается внести соответствующие дополнения в Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации».

7. По результатам рассмотрения ст.ст. 179 и 183 УК РФ на предмет соответствия их формулировок принципам криминализации – беспробельности закона и неизбыточности запрета, а также принципу определённости и единства терминологии в информационной сфере – предлагаются следующие редакции диспозиций этих статей УК РФ:

«Статья 179. Принуждение к совершению сделки или к отказу от её совершения

1. Требование совершения сделки или отказа от ее совершения под угрозой применения насилия, уничтожения или повреждения чужого имущества, а равно распространения сведений, которые могут причинить существенный вред правам и законным интересам потерпевшего или его близких, при отсутствии признаков вымогательства – …

Статья 183. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну

1. Собирание сведений, составляющих коммерческую, налоговую или банковскую тайну, путём похищения носителей информации, копирования информации, подкупа или угроз, а равно иным незаконным способом – …».

8. Под компьютерными преступлениями предлагается понимать общественно опасные противоправные деяния, которые имеют своим дополнительным родовым объектом общественные отношения по обеспечению информационной безопасности общества, посягающие на нормальный режим хранения, обработки и передачи данных в компьютерах (компьютерных системах).

Любое компьютерное преступление должно в обязательном порядке обладать признаками информационного преступления, поскольку понятие

информационного преступления целиком охватывает понятие компьютерного преступления, хотя и не ограничивается им.

9. Для успешной борьбы с компьютерными преступлениями необходима координация деятельности разных государств и унификация их законодательства, в том числе со стороны России. Европейская практика идёт по пути приведения национального законодательства в соответствие с Конвенцией Совета Европы о киберпреступности от 23.11.2001. В связи этим, и учитывая также иные принципы криминализации, предлагается изменить название главы 28 УК РФ и включить в нее составы преступлений по статьям 272-274 в новых редакциях, а также новую статью 274.1:

«Глава 28. Преступления, посягающие на нормальный режим хранения, обработки и передачи данных в компьютерных системах

Статья 272. Незаконный доступ к компьютеру

Статья 273. Незаконное использование компьютерных программ

Статья 274. Логический (компьютерный) саботаж

Статья 274.1. Незаконный перехват данных».

В работе предложены также новые редакции составов ст.ст. 272-274.1 УК РФ.

Теоретическая и практическая значимость результатов исследования заключается в том, что оно, в числе прочих исследований, может служить базой для дальнейшего изучения информационных преступлений. Кроме этого, выводы диссертации по отдельным вопросам, вынесенным на обсуждение, могут способствовать совершенствованию законодательства и правоприменительной практики в сфере компьютерных преступлений, а также иных информационных преступлений. Положения исследования могут быть использованы при преподавании курса Особенной части уголовного права и специального курса.

Апробация результатов исследования. Основные положения диссертации были опубликованы в виде двух статей в периодических изданиях, а также обсуждались на двух международных и одной межвузовской конференциях.

Выводы, изложенные в работе, были использованы при подготовке и проведении семинаров по спецкурсу «Компьютерные преступления» в Юридическом институте Сибирского федерального университета.

Объем и структура диссертации. Работа выполнена в соответствии с требованиями ВАК Российской Федерации. Структура и объем диссертации определяется целью и задачами исследования. Диссертация состоит из введения, трёх глав, заключения, приложений и списка литературы, использованной при написании работы.

СОДЕРЖАНИЕ РАБОТЫ

Во введении автором обосновывается актуальность темы, определяется объект и предмет исследования, обозначаются цели и задачи, методологическая основа исследования, раскрываются научная новизна теоретическая и практическая значимость работы, формулируются основные положения, выносимые на защиту, а также приводятся сведения об апробации результатов исследования.

Первая глава «Понятие и признаки информационных преступлений, общая характеристика составов информационных преступлений, содержащихся в УК РФ» состоит из трёх параграфов.

В первом параграфе «Понятие информации, компьютерной информации в уголовном праве» отмечается повышенный интерес со стороны учёных к информационным отношениям в связи со становлением информационного общества. Как следствие, повышается роль и значение информации в праве.

Цель данного параграфа – рассмотреть различные понятия информации, предлагаемые в науке, в первую очередь, в философии, и сформулировать своё понятие информации, применимое для оценки уголовно-правовых явлений. В различных философских концепциях существуют относительно самостоятельные определения информации. Вместе с тем, их главным недостатком является то, что они не могут быть непосредственно применены к правовой действительности в силу их всеобщности и иной научной направленности. Поэтому существует необходимость в формулировании понятия информации, которое может быть применено в уголовно-правовых исследованиях в качестве средства, позволяющего проанализировать составы преступлений в УК РФ с позиции наиболее важных положений теории информации. С этой целью были выделены признаки информации, предлагаемые в философии, затем из них были отобраны наиболее существенные признаки, которые в дальнейшем использовались для выделения составов преступлений, связанных с использованием информации и проведения анализа содержания этих составов.

Самыми важными из выделенных признаков, на наш взгляд, являются следующие:

1. Информация содержится и передаётся при помощи материального динамического или статического объекта – сигнала.

2. Информация является сведениями и сама по себе не имеет каких-либо физических характеристик.

3. Информация существует лишь в форме определённого кода и может быть закодирована неограниченным числом способов (принцип инвариантности).

4. Информация способна порождать новую информацию у принимающего субъекта на основе имеющегося у него запаса знаний (тезауруса, информации).

5. Информация является атрибутом управления.

6. Информация в полной мере проявляет свои признаки лишь в информационном взаимодействии (совокупности объекта, субъекта, канала, передатчика, приёмника, источника помех).

На основе выделенных признаков автор рассмотрел существующие в праве определения информации и выявил их достоинства и недостатки, после чего было предложено следующее определение информации. Под информацией понимаются сведения, передающиеся между субъектами посредством сигналов в форме определённого кода и представляющие собой целенаправленное управленческое воздействие. Эти сведения не имеют физических характеристик, не могут быть поняты вне информационного взаимодействия и способны порождать новую информацию у принимающего субъекта.

Одним из наиболее востребованных в настоящее время видов информации является компьютерная информация. Её существование во многом определяет специфику общественных отношений в информационном обществе. В отечественном уголовном праве под компьютерной информацией понимается любая информация, которая содержится на электронном материальном носителе. За рубежом вместо термина «компьютерная информация» используется термин «данные» как набор символов, интерпретация которых позволяет получить информацию.

Европейские законодатели при определении компьютерных данных акцентируют внимание не на месте их нахождения, не на их материальном носителе, а считают принципиальным указание на форму их представления. На основе сравнительно-правового анализа, а также с учетом сформулированного общего определения информации был сделан вывод о том, что понимание данных в зарубежном законодательстве является более глубоким и акцентирующим внимание на их сущностных характеристиках, чем понимание компьютерной информации в российском уголовном законе. Соответственно, было предложено следующее определение данных (компьютерной информации): данными (компьютерной информацией) являются сведения, передающиеся между субъектами посредством сигналов в форме электронного кода, пригодного для обработки их компьютерными средствами, и представляющие собой целенаправленное управленческое воздействие.

Во втором параграфе «Понятие и признаки информационных преступлений» был проведён анализ того, как признак информации закреплён в элементах состава преступления.

Объект преступления может быть представлен информационными общественными отношениями, которые выражаются в наличии у субъектов этих отношений взаимных прав и обязанностей в информационной сфере. Следовательно, можно утверждать, что информационные преступления являются разновидностью преступлений, закреплённых в различных главах УК, и имеют своим объектом информационные общественные отношения. Поскольку информационные

общественные отношения достаточно разнообразны, автор на основе рассмотрения их различных видов сделал вывод о том, что объектом информационных преступлений являются не все информационные отношения, а только те, которые обеспечивают информационную безопасность личности, общества и государства. Как представляется, наиболее удачное определение информационной безопасности содержится в работе В.А.Мазурова: он рассматривает информационную безопасность как состояние защищённости жизненно важных интересов личности, общества, государства в информационной среде (сфере) от внешних и внутренних угроз, обеспечивающее её формирование, использование и развитие в интересах граждан, общества, государства[5]. Традиционно родовой объект преступлений определяется путём обращения к названиям разделов УК РФ. Информационная безопасность как особый родовой объект информационных преступлений в этом смысле не является исключением. В зависимости от характера охраняемых общественных отношений можно выделять следующие общественные отношения по обеспечению информационной безопасности: общественные отношения по обеспечению информационной безопасности личности (для информационных преступлений, расположенных в разделе 7 УК РФ «Преступления против личности»), общества (для информационных преступлений, расположенных в разделе 8 «Преступления в сфере экономики» и 9 «Преступления против общественной безопасности и общественного порядка»), и государства (для информационных преступлений, расположенных в разделах 10 «Преступления против государственной власти» и 11 «Преступления против военной службы»). Таким образом, первым признаком информационных преступлений является наличие дополнительного родового объекта в виде общественных отношений по поводу обеспечения информационной безопасности личности, общества и государства.

Информационный компонент часто представлен также в предмете преступления. Автором на основе изучения работ учёных, посвящённых предмету преступления, была поддержана точка зрения о нематериальной природе предмета преступления и выведен второй признак информационных преступлений: их предметом может являться информация, которая не имеет материальной формы и не зависит от своего материального носителя. В каждом конкретном случае преступного посягательства информация хранится на таком носителе, однако не имеет жёстко детерминированной связи с ним.

Наряду с предметом преступления наиболее ярко информационную безопасность характеризует такой элемент состава преступления, как деяние. Многие статьи УК предусматривают в качестве деяния различные виды информационного воздействия: ст.ст. 119, 129, 137, 155, 197 УК РФ и

[5] Мазуров В.А. Компьютерные преступления: классификация и способы противодействия. М., 2002. С.21.

др. Кроме этого, значительный объём статей в УК РФ предусматривает наказание за деяния, имеющие информационное воздействие в качестве способа совершения преступления, под которым понимаются те приёмы и методы, которые использовал преступник для совершения преступления. Таким образом, третьим признаком информационных преступлений является то, что их объективная сторона в части деяния и способа совершения преступления может быть представлена различными видами информационного воздействия.

Следовательно, имеется две разновидности информационных преступлений, имеющих своим дополнительным родовым объектом общественные отношения по обеспечению информационной безопасности личности, общества и государства, но отличающиеся друг от друга элементами состава преступления, содержащими информацию:

1. Информационные преступления, предметом которых является информация.

2. Информационные преступления, способом совершения которых является информационное воздействие.

Признак информации не содержится в описании субъекта преступления в статьях особенной части УК РФ. Субъективная сторона преступления не представляет интереса для анализа в рамках настоящей работы, поскольку все психические процессы, которые являются одновременно и процессами информационными, необходимо присутствуют в составе любого преступления, предусмотренного уголовным законом.

На основе выделенных признаков информационных преступлений были проанализированы иные определения информационных преступлений, предлагаемые в доктрине, а также сформулировано собственное определение. Информационными преступлениями являются общественно опасные противоправные деяния, причиняющие вред общественным отношениям по обеспечению информационной безопасности личности, общества и государства, способом совершения которых является информационное воздействие или (и) предметом которых является информация как особый нематериальный объект.

В третьем параграфе «Общая характеристика составов информационных преступлений, содержащихся в УК РФ» была проведена работа по выявлению конкретных составов информационных преступлений и их групп, предлагаемых другими учёными, и сделан вывод о неудовлетворительном состоянии исследований в этой области. Автором были проверены все составы преступлений в УК РФ на предмет наличия в их предмете или объективной стороне выделенных признаков информации, результаты такого исследования были обобщены в таблицах. Данные таблиц позволяют сделать следующие выводы:

- доля составов информационных преступлений в УК РФ составляет 37,3 %;

- разделы 7 «Преступления против личности», 8 «Преступления в сфере экономики» и 10 «Преступления против государственной власти» УК РФ содержат наибольшее количество составов информационных преступлений: 39,3; 47,5 и 50,4 % от общего числа составов преступлений соответственно;

- в разделе 10 количество информационных преступлений превосходит количество иных составов преступлений. Сказанное объясняется тем, что в этом разделе главы 31 УК РФ «Преступления против правосудия» и 32 «Преступления против порядка управления» имеют дело, в основном, с противоправными деяниями в сфере управления, которая является информационной по определению. На основе анализа статистических данных Управления Судебного департамента в Красноярском крае отмечено, что наиболее часто судами за совершение информационных преступлений главы 31 УК РФ применяются ст.ст. 306 «Заведомо ложный донос» и 307 «Заведомо ложные показания…» УК РФ. Начиная с 2002 года наблюдается устойчивая положительная динамика числа осуждённых по статьям 306 и 307 УК РФ. Сказанное подтверждает возрастающее значение информационных отношений в современном обществе и свидетельствует о повышенном внимании со стороны правоохранительных органов к общественно опасным деяниям в информационной сфере, закреплённым, в частности, в ст.ст. 306 и 307 УК РФ;

- все составы главы 28 УК РФ «Преступления в сфере компьютерной информации» являются составами информационных преступлений;

- большинство информационных преступлений в УК РФ составляют преступления, способом совершения которых является информационное воздействие (53,8 % от числа всех информационных преступлений). На втором месте идут информационные преступления, предметом которых является информация (31,6 %). Наконец, относительно небольшую часть информационных преступлений составляют информационные преступления, в которых сочетаются признаки обоих названных видов информационных преступлений (14,7 %);

Кроме этого, в параграфе были выделены две группы информационных преступлений. К первой группе относятся информационные преступления, где деяние как элемент объективной стороны носит информационный характер. Ко второй группе информационных преступлений относятся преступления, в которых деяние не носит информационного характера. Все преступления первой группы также были обобщены в таблице, данные которой позволили сделать следующие выводы:

- доля составов информационных преступлений первой группы в УК РФ равняется 32 %;

- число составов информационных преступлений в УК РФ выросло примерно в 1,5 раза по сравнению с УК РСФСР 1960 года (с 20 % до 32 % от общего числа составов). Сказанное наглядно иллюстрирует возросшую

роль информационных процессов в жизни современного общества и, в частности, в отношениях, регулируемых уголовным правом;

Вторая глава «Виды информационных преступлений» включает в себя два параграфа.

В первом параграфе «Информационные преступления, предметом которых является информация» автором даётся определение указанным преступлениям. Под ними понимаются общественно опасные противоправные деяния, причиняющие вред общественным отношениям по обеспечению информационной безопасности личности, общества и государства, имеющие своим предметом информацию как особый нематериальный объект.

По рассматриваемым преступлениям также были составлены аналитические таблицы. Их сопоставление подтверждает общую тенденцию, выявленную в главе 1, о постепенном росте числа информационных преступлений в УК РФ по сравнению с УК РСФСР 1960 года. Кроме этого, были сделаны следующие выводы:

- информационные преступления, предметом которых является информация, содержатся не во всех главах уголовного кодекса РФ. Указанные информационные преступления представлены примерно в половине глав уголовного закона;

- наибольшее число информационных преступлений, предметом которых является информация, в относительном выражении содержится в главе 28 УК «Преступления в сфере компьютерной информации» (100 %), а также в главе 19 УК «Преступления против конституционных прав и свобод…» (47 %);

- информационные преступления, предметом которых является информация, в одинаковой мере защищают как информационную безопасность государства, так и общества.

При рассмотрении информационных преступлений, в которых предметом преступления является информация, большое значение приобретает вопрос о том, какими вербальными (языковыми) средствами выражается признак «информация» как предмет преступления. Законодатель при обозначении информационного предмета преступлений использует достаточно много терминов. Все они были разбиты на две группы. Первая группа терминов представлена различными видами информации как особого нематериального объекта. Вторая группа – терминами, в которых содержится указание на материальный носитель информации. Количество составов преступлений, содержащих термины второй группы больше составов, содержащих термины первой группы, примерно в 1,5 раза. Все термины, представляющие информационный предмет, были проанализированы с применением информационного подхода, обосновывающего отнесение их к той или иной группе.

Информационные преступления, предметом которых является информация, классифицируются по различным основаниям. 1. В зависимости от способа кодирования информации они подразделяются на:

а) информационные преступления, имеющие своим предметом компьютерные данные; б) информационные преступления, имеющие своим предметом иные виды информации. 2. В зависимости от терминологического закрепления информации как предмета преступления они подразделяются на: а) информационные преступления, предмет которых выражен путём указания на саму информацию как на нематериальный объект; б) информационные преступления, предмет которых выражен опосредованно путём указания на материальный носитель информации. 3. В зависимости от характера информации они подразделяются на: а) информационные преступления, имеющие своим предметом официальную информацию; б) информационные преступления, имеющие в качестве предмета неофициальную информацию.

Составы преступлений, предметом которых является информация, могут быть проанализированы с учётом требований соблюдения при криминализации деяний таких принципов, как определённость и единство и терминологии в информационной сфере, а также беспробельность закона и неизбыточность запрета, что позволит выявить различные неточности и противоречия в содержании статей уголовного закона, как это и было продемонстрировано на примере анализа ст. 183 УК РФ.

Во втором параграфе «Информационные преступления, способом совершения которых является информационное воздействие» автором даётся определение указанным преступлениям. Под ними понимаются общественно опасные противоправные деяния, причиняющие вред общественным отношениям по обеспечению информационной безопасности личности, общества и государства, имеющие в качестве способа совершения информационное воздействие.

По рассматриваемым преступлениям составлены аналитические таблицы, результаты анализа которых позволили прийти к следующим выводам:

- информационные преступления, способом совершения которых является информационное воздействие, представлены в большинстве глав уголовного закона. Следовательно, в отличие от информационного предмета преступлений способ совершения преступления в виде какого-либо информационного воздействия широко распространён в разных главах уголовного закона;

- наибольшее число статей уголовного закона, содержащих информационные преступления, способом совершения которых является информационное воздействие, защищают посредством закрепления данных преступлений информационную безопасность общества и государства;

- значительная часть информационных преступлений, способом совершения которых является информационное воздействие, составляют преступления, в которых информационный способ вынесен в качестве квалифицирующего признака, в то время как основное деяние в рамках

объективной стороны, закреплённое в ч. 1 соответствующей статьи, не носит информационного характера.

При рассмотрении информационных преступлений, способом совершения которых является информационное воздействие, большое значение приобретает вопрос о том, какими вербальными (языковыми) средствами выражается признак «информация» как способ совершения преступления. Законодатель при обозначении такого способа использует достаточно много терминов. Большинство способов информационного воздействия в УК РФ относится к различным видам психического насилия. В целом, существует 6 наиболее распространённых терминов, закрепляющих способы информационного воздействия, используемые при совершении информационных преступлений: угроза, принуждение, обман, вовлечение, разглашение и вымогательство. Автором было отмечено нарушение принципа определённости и единства терминологии при криминализации деяний, которые описываются терминами, характеризующими различные способы информационного воздействия, в частности, термином «принуждение».

Все информационные преступления, способом совершения которых является информационное воздействие, можно разделить в зависимости от получателя сведений на: а) информационные преступления, в которых получателем сведений является конкретное лицо, на которого оказывается информационное (управленческое) воздействие; б) информационные преступления, в которых получателем сведений является неопределённый круг лиц. На основе рассмотрения данной классификации автором сделаны предложения по включению в ст. 2 Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и защите информации» пунктов 13 и 14, содержащих следующие термины:

«13) информационное воздействие – действия, направленные на передачу информации от одного человека (группы лиц) к другому с целью побуждения его к определённому поведению;

14) информационная безопасность – состояние защищённости жизненно важных интересов личности, общества, государства в информационной среде (сфере) от внешних и внутренних угроз, обеспечивающее её формирование, использование и развитие в интересах граждан, общества, государства».

В статью 3 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации» предлагается включить пункт 9, изложив её в следующей редакции:

«Статья 3. Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации

Правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах:

…

9) обеспечение информационной безопасности личности, общества и государства».

В указанный закон предлагается ввести ст. 10.1 «Информационное воздействие» следующего содержания:

«1. Запрещается общественно опасное информационное воздействие на сознание человека.

2. Любой человек имеет право на защиту от общественно опасного информационного воздействия».

Все составы информационных преступлений, способом совершения которых является информационное воздействие, могут быть проанализированы с применением информационного подхода, который позволяет проверить, насколько законодатель учитывал принципы криминализации при конструировании составов информационных преступлений, что и было продемонстрировано на примере анализа ст. 179 УК РФ.

Третья глава «Правовое регулирование компьютерных преступлений в России и за рубежом» включает в себя два параграфа.

В первом параграфе «Понятие компьютерных преступлений, их место среди информационных преступлений» проводится сравнительно-правовой анализ определений компьютерных преступлений, имеющихся в зарубежном уголовном праве и отечественной доктрине, а также понятия компьютера (ЭВМ), приводятся результаты интервьюирования сотрудников отдела «К» ГУВД Красноярского края и анкетирования пользователей компьютеров из числа студентов старших курсов юридического факультета СФУ по данному вопросу. При определении компьютера представляется необходимым использовать терминологию Конвенции о киберпреступности 2001 года и употреблять вместо термина «ЭВМ и система ЭВМ» термины «компьютер (компьютерное устройство), компьютерная система», понимая под ними любое устройство или группу соединённых или взаимосвязанных устройств, одно или несколько из которых, выполняя программу, осуществляют автоматическую обработку данных.

Во всех проанализированных автором признаках компьютерных преступлений речь идёт об автоматической обработке данных с использованием компьютеров; о видовом объекте компьютерных преступлений в виде общественных отношений, обеспечивающих нормальный режим хранения, обработки и передачи данных в компьютерах (компьютерных системах); об обеспечении конфиденциальности, целостности и доступности данных и компьютерных систем; об информационной безопасности и безопасности данных (компьютерных систем). На основе изложенного для целей исследования выделяется следующий перечень признаков компьютерных преступлений:

1. Дополнительным родовым объектом компьютерных преступлений являются общественные отношения по обеспечению информационной безопасности общества;

2. Видовым объектом компьютерных преступлений являются общественные отношения, обеспечивающие нормальный режим хранения, обработки и передачи данных в компьютерах (компьютерных системах);

3. Предметом компьютерных преступлений выступают данные.

Выделенные признаки компьютерных преступлений позволяют соотнести их с информационными преступлениями. Компьютерные преступления являются видом информационных преступлений, предметом которых является информация. Любое компьютерное преступление должно обладать признаками информационного преступления, поскольку понятие информационного преступления целиком охватывает понятие компьютерного преступления, хотя и не ограничивается им.

Второй параграф «Виды компьютерных преступлений» посвящён анализу видов компьютерных преступлений по зарубежному и российскому законодательству. Отдельно рассматриваются компьютерные преступления в широком смысле и компьютерные преступления в узком смысле. На основе сравнения видов компьютерных преступлений в широком смысле по законодательству разных стран, результатов анкетирования пользователей компьютеров автор делает вывод об отставании УК РФ от ведущих зарубежных стран в деле борьбы с компьютерными преступлениями в широком смысле, поскольку ни одно такое компьютерное преступление не нашло своего отражения в тексте уголовного закона.

Компьютерные преступления в узком смысле представлены в УК РФ в главе 28 «Преступления в сфере компьютерной информации». Родовым объектом рассматриваемых преступлений являются общественные отношения по обеспечению общественной безопасности и общественного порядка; дополнительным родовым объектом – общественные отношения по обеспечению информационной безопасности общества; видовым объектом – общественные отношения, обеспечивающие нормальный режим хранения, обработки и передачи данных в компьютерах (компьютерных системах). Предметом рассматриваемых составов выступают компьютерные данные.

Существует заметное расхождение в содержании статей о компьютерных преступлениях в УК РФ и в Конвенции о киберпреступности 2001 года. В одной и той же статье УК РФ закреплены, как правило, элементы нескольких самостоятельных преступлений, предусмотренных Конвенцией. Таким образом, состояние действующего уголовного закона не может быть признано удовлетворительным, поскольку несоответствие УК РФ нормам европейского права, во-первых, игнорирует весь богатый опыт борьбы с компьютерными преступлениями, который имеется у европейских стран, а, во-вторых, не позволяет должным образом сотрудничать с европейскими коллегами в деле расследования компьютерных преступлений, которые часто носят транснациональный характер. Отсутствие адекватного законодательного регулирования компьютерных преступлений в УК РФ подтверждается также результатами

анализа уголовных дел о компьютерных преступлениях, рассмотренных судами Красноярского края, статистическими данными, в том числе, данными статистической отчетности о деятельности подразделений К У(О)СТМ МВД, ГУВД, УВД субъектов РФ, статистическими данными Управления Судебного департамента в Красноярском крае о количестве осуждённых, а также результатами анкетирования пользователей компьютеров.

Действующая редакция статьи 272 УК РФ помимо неправомерного доступа к компьютерной информации устанавливает ответственность также за логический (компьютерный) саботаж. Кроме этого, статья 272 содержит устаревшие формулировки, в частности, термин «ЭВМ». В связи с этим предлагается изменить статью 272 УК РФ следующим образом:

«Статья 272. Незаконный доступ к компьютеру

1. Умышленный незаконный доступ к компьютеру (компьютерной системе) в обход средств защиты, установленных законным пользователем компьютера (компьютерной системы), если это деяние повлекло незаконное копирование данных или совершение другого преступления, –

наказывается …

2. То же деяние, совершённое группой лиц по предварительному сговору или организованной группой, –

наказывается …».

Анализ отечественных нормативных и доктринальных источников показывает, что определение вредоносной программы, указанное в статье 273 УК РФ, не отражает сущности таких программ, с чем согласны правоприменители из числа сотрудников отдела «К» ГУВД Красноярского края. Кроме этого, состав статьи 273 пересекается с составами иных видов компьютерных преступлений, в частности, незаконного доступа и логического саботажа. Зарубежный опыт борьбы с вредоносными программами также свидетельствует о несовершенстве статьи 273 УК РФ, в связи с чем предлагается следующая её редакция:

«Статья 273. Незаконное использование компьютерных программ

1. Создание компьютерной программы, переработка существующей программы, а также распространение таких программ с целью совершения какого-либо из преступлений, предусмотренных настоящей главой,–

наказываются …

2. Те же деяния, совершённые группой лиц по предварительному сговору или организованной группой, –

наказываются …».

Статистика применения правоохранительными органами статьи 274 УК РФ «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети», а также публикации отечественных учёных и свидетельствуют о необходимости декриминализации статьи 274 УК РФ в её нынешнем виде. Правоприменители из числа сотрудников отдела «К» ГУВД Красноярского края также отмечают, как таковые правила эксплуатации ЭВМ на практике не составляются, поэтому ст. 274 не работает. Вместо нарушения

указанных правил в статье 274 предлагается криминализовать логический (компьютерный) саботаж – преступление, имеющееся в большинстве уголовных законов зарубежных стран. В связи с этим предлагается новая редакция статьи 274 УК РФ:

«Статья 274. Логический (компьютерный) саботаж

1. Умышленное незаконное повреждение, удаление или изменение данных, причинившее существенный вред или повлекшее создание препятствий работе компьютерной системы, –

наказывается …

2. Умышленное уничтожение или повреждение компьютеров или компьютерных систем, причинившее существенный вред, –

наказываются …

3. Деяния, предусмотренные частями первой или второй настоящей статьи, повлекшие по неосторожности тяжкие последствия, –

наказываются …».

Современное состояние сферы высоких технологий и связанной с ней сферы телекоммуникаций позволяет утверждать, что статья 138 УК РФ не отвечает требованиям времени о борьбе с нарушением тайны сообщений. Для успешной защиты сообщений, передающихся электронно-цифровым способом, необходимо выделение самостоятельного состава компьютерных преступлений. Такой состав содержится в Конвенции о киберпреступности 2001 года и закреплён в большинстве уголовных законов зарубежных стран. Включение статьи за незаконный перехват текст УК РФ и отнесение её в главу 28 кодекса соответствовало бы логике построения уголовного закона и принципу беспробельности закона и неизбыточности запрета. С этой целью предлагается дополнить главу 28 УК РФ статьёй 274.1 следующего содержания:

«Статья 274.1. Незаконный перехват данных

Умышленный незаконный перехват данных, передающихся внутри компьютерной системы или между такими системами различными способами, в том числе путём электромагнитных излучений, совершённый с использованием компьютерных устройств, кроме технических устройств, указанных в частях 2 и 3 статьи 138 настоящего Кодекса, с преодолением средств защиты, установленных законным владельцем данных, если такой перехват причинил существенный вред, –

наказывается …».

В заключении работы излагаются выводы и обозначаются пути дальнейшего совершенствования уголовного законодательства и практики его применения. Основным итогом диссертационного исследования являются предложения по совершенствованию норм УК РФ и Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации».

СПИСОК НАУЧНЫХ ПУБЛИКАЦИЙ ПО ТЕМЕ ДИССЕРТАЦИИ

1. Суслопаров А.В. Понятие информации как базового элемента информационных преступлений / А.В. Суслопаров // Вестник Красноярского государственного университета, 2006. № 6. С. 325 – 331.

2. Суслопаров А.В. Статья 183 УК РФ с позиции общей теории информации / А.В. Суслопаров // Аспирант и соискатель. 2006. № 3. С. 66 – 71.

3. Суслопаров А.В. Объективные признаки принуждения к совершению сделки или к отказу от её совершения с позиции общей теории информации / А.В. Суслопаров // Актуальные проблемы борьбы с преступностью в Сибирском регионе: сб. материалов междунар. науч. конф. (15-16 февраля 2007 г.): в 2 ч. Ч. 1. / отв. ред. С.Д. Назаров. – Красноярск: Сибирский юридический институт МВД России, 2007. С. 175 – 178.

4. Суслопаров А.В. Виды компьютерных преступлений по зарубежному и российскому законодательству / А.В. Суслопаров // Сравнительное правоведение: наука, методология, учебная дисциплина: материалы междунар. научн.-практ. конф.: в 2 ч. Ч. 2. / отв. ред. В.В. Терешкова. – Красноярск: ИПК СФУ, 2008. С. 116 – 122.

Суслопаров Алексей Валерьевич

ИНФОРМАЦИОННЫЕ ПРЕСТУПЛЕНИЯ

Автореферат
диссертации на соискание ученой степени
кандидата юридических наук