СОВРЕМЕННЫЕ СТАНДАРТЫ
В УГОЛОВНОМ ПРАВЕ И УГОЛОВНОМ ПРОЦЕССЕ

Е. И. ПАНФИЛОВА,
А. Н. ПОПОВ

КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ

Санкт-Петербург
1998

САНКТ-ПЕТЕРБУРГСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ
ГЕНЕРАЛЬНОЙ ПРОКУРАТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Е. И. ПАНФИЛОВА,
А. Н. ПОПОВ

КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ

Санкт-Петербург
1998

ББК 67.99(2)8

Панфилова Е. И., Попов А. Н. Компьютерные преступления: Серия “Современные стандарты в уголовном праве и уголовном процессе” / Науч. редактор проф. Б. В. Волженкин. СПб., 1998. 48 с.

Научный редактор
доктор юридич. наук, профессор,
заслуженный деятель науки
Российской Федерации
ВОЛЖЕНКИН Борис Владимирович

Издается по российско-нидерландскому проекту
“Современные стандарты в уголовном праве
и уголовном процессе”

В работе рассматриваются некоторые вопросы правовой регламентации ответственности за преступления в сфере информационных технологий в уголовных законодательствах ряда зарубежных государств. Дан анализ составов “компьютерных” преступлений, предусмотренных уголовным законодательством России. Приведены извлечения из уголовных кодексов Германии, Франции, Испании и Модельного уголовного кодекса для государств — участников СНГ.

ISBN 5–89094–061–9

1. ИНФОРМАЦИОННОЕ ОБЩЕСТВО И НОВЫЕ ОБЩЕСТВЕННО ОПАСНЫЕ ДЕЯНИЯ

Общество становится все более информационно насыщенным. Появилось даже определение — информационное общество. Это понятие возникло под влиянием успехов кибернетики и информатики, где информация — не просто сообщение или знание о чем-либо, а количественно выражаемая мера управляемости той или иной системой.

Отличительной особенностью современного общества является то, что в нем информация, знания, информационные услуги и все отрасли, связанные с их производством, развиваются убыстряющимися темпами. Развитые страны рассматривают возможности информационных технологий как ключ к созданию высокоиндустриального общества в XXI *в.* Правительства многих стран мира приступили к реализации национальных программ развития информационного общества, успешно координируя действия государства, частного сектора и общественных учреждений.

Особое место в информационном обществе принадлежит компьютерным системам, так как они способны интегрировать и обрабатывать информацию из различных источников. Созданы и успешно действуют всемирные глобальные компьютерные сети, связывающие мир в одно целое, такие как Internet.

Широкое распространение компьютеры получили сравнительно недавно, приблизительно с середины 70-х годов. Именно к этому времени относится появление персональных компьютеров, рассчитанных на одного пользователя. Их количество во всем мире стремительно растет. Так, по данным печати, только в России ежегодно продается более миллиона компьютеров.

Компьютер (или ЭВМ — электронно-вычислительная машина) первоначально задумывался как устройство для различных математических вычислений. Постепенно он превратился в универсальное средство обработки любой информации, используемой человеком. С помощью компьютеров управляют страной, банком, предприятием, обороной, космическим кораблем, создают музыку, книги, фильмы, производят сложнейшие расчеты, играют в шахматы, диагностируют и лечат людей и т. д. Практически нет ни одной сферы человеческой деятельности, в которой бы не использовались компьютеры, позволяющие создавать, накапливать, хранить, обрабатывать и передавать огромные объемы информации.

Однако, как известно, научно-технический прогресс имеет и “обратную сторону медали”. Наличие глобальных компьютерных сетей и недостаточная их защищенность от сбоев техники, вызванных самыми различными причинами (в том числе невозможностью создания абсолютно надежных компьютерных

программ, выходом из строя оборудования), от ненадлежащих действий людей, совершенных умышленно или по неосторожности, может породить самые непредсказуемые и страшные последствия.

Так, компьютеры осуществляют управление работой ядерных реакторов, химических заводов, стратегическими ядерными вооруженными силами. Невозможно представить, что произойдет в результате ошибки оператора или компьютерной программы.

Новые технологии порождают и новые преступления. С появлением компьютеров широкое распространение получили компьютерные хищения. Данные зарубежной правоохранительной практики свидетельствуют о том, что, например, в Германии с использованием компьютеров похищается до 4 *млрд* марок ежегодно, во Франции — до 1 *млрд* франков, в США — до нескольких миллиардов долларов[1].

В России компьютерные хищения также имеют место. Например, в одном из филиалов Инкомбанка (Москва) ведущий бухгалтер С., используя свой рабочий компьютер и зная пароль, вошла в директорию "ввод платежей" компьютера и сделала три перевода крупных сумм в иностранной валюте (73 485, 9 300 и 4 2585 долларов) на другой счет, с которого в последующем через посредника их сняла[2].

Компьютерные хищения не знают государственных границ. Они могут быть совершены в любое время из любой точки земли из банка любой страны. В этом смысле характерно дело Левина, похитившего из американского банка в Нью-Йорке денежные средства в размере свыше 10 *млн* долларов, находясь в Санкт-Петербурге. В силу большого общественного резонанса представляется важным остановиться на этом хищении более подробно. В печати делается упор на то, что это преступление было совершено чуть ли не в одиночку талантливым хакером (компьютерным взломщиком). Однако в действительности все было несколько иначе.

Вторжение в систему управления денежными операциями Ситибанка было впервые замечено в июне 1994 г. В суд документы были представлены 18 августа 1995 г., и с этого момента дело получило широкую публичную огласку. Тогда же прокуратура США выдвинула обвинения против гражданина России Владимира Левина, арестованного в Лондоне.

Хакер подделывал пароли клиентов банка с целью выдать себя за владельца того или иного счета. При этом использовались счета клиентов со всего света.

---

[1] См.: Селиванов Н. Проблемы борьбы с компьютерной преступностью // Законность. 1993. № 8.

[2] См.: Чечко Л. "Компьютерные" хищения // Российская юстиция. 1996. № 5.

Российские службы безопасности подключились к делу в 1995 г. До этого времени расследование вели специальные службы США. Была выявлена целая преступная группировка, занимавшаяся входом в компьютерную систему банка, переводом денег со счетов клиентов и получением переведенных сумм в филиалах банка по всему миру.

Счета пострадавших находились в 10-ти странах: США, Канаде, Мексике, Аргентине, Новой Зеландии, Арубе, Колумбии, Гонконге, Индонезии, Уругвае. Переводы приходили в 7 стран: США, Россию, Финляндию, Германию, Нидерланды, Швейцарию и Израиль. В это дело было вовлечено в итоге 14 стран.

Организация использовала услуги хакера для взлома, проникновения в систему и перевода денежных средств со счетов клиентов в другие банки, а также "мулов" — людей, которые непосредственно получали наличную валюту из филиалов Ситибанка или других банков после поступления в них переводов. За весь период своей деятельности (с июня по октябрь 1994 г.) хакер сделал 40 попыток переводов на общую сумму более 10 *млн* долларов США. Однако реальный ущерб удалось свести к 400 тыс. долларов, которые были выплачены из страховых фондов Ситибанка.

Дело было хорошо спланировано и организовано. Сначала переводы делались небольшими суммами с целью проверки качества своей работы, а затем суммы каждого перевода увеличились до одного миллиона. При снятии крупной суммы денег наличными в банке Финляндии, согласно правилам банков, "мул" вынужден был оставить свои координаты. В качестве места своего проживания он указал Санкт-Петербург, а в графе "телефон" — тот же номер, что был засечен при фильтрации запросов и соответствовал номеру в офисе, откуда производилось проникновение. Это дало возможность связать запрос в банк с получателем как одним лицом, хотя хакер и "мул" были разными людьми.

Следует отметить четкое сотрудничество между банками и реагирование полиции на все обращения представителей банковских структур. Были также усилены меры безопасности и защиты информации.

В результате проведенных совместных действий были арестованы: в Сан-Франциско (США) — два человека: муж и жена (русские); в Израиле — один человек (русский), выдан затем властям США; в Нидерландах — два человека: русский выдан затем властям США, другой — гражданин Нидерландов; мозг этой операции — Владимир Левин (русский, житель Санкт-Петербурга, работник "Сатурна", чьи запросы в систему были зафиксированы), арестован в Лондонском аэропорту по пути на компьютерную ярмарку в Амстердаме, затем выдан властям США; другие участники компьютерного мошенничества на территории России.

Задержание преступников стало возможным благодаря тому, что сотрудники и руководство Ситибанка своевременно уведомляли обо всем происходящем в банке правоохранительные органы и банки-получатели переводов. Большую помощь оказали телефонные компании для определения местонахождения хакера, а также система круглосуточного мониторинга за входами в систему "Спринт". Важное значение в расследовании этого транснационального преступления имело взаимодействие правоохранительных органов разных стран, разработка согласившихся на сотрудничество свидетелей, анализ документов со счетов получателей и телеграфных переводов.

Американская сторона была готова предъявить обвинения 13-ти участникам преступной группировки, большинство из которых — русские с иностранным подданством. Многие из арестованных или выданных властям США заключили сделку о признании и были осуждены по законодательству этой страны. Им вменялись в вину: банковское мошенничество (ст. 1344 титула 18 Свода законов США); мошенничество с использованием телеграфа (ст. 1343 титула 18 Свода законов США); мошенничество с использованием компьютера (ст. 1030 титула 18 Свода законов США); преступный сговор (ст. 371 титула 18 Свода законов США).

Наибольшее распространение компьютерные преступления получили в банковской и финансовой сферах, так как именно здесь можно с небольшими затратами значительно обогатиться за чужой счет. Так, если ограбление банка в среднем приносит доход около 15 тыс. долларов, то использование для хищения компьютера — 400 тыс. долларов, при практически ничтожном риске разоблачения[3]. Банкиры и финансисты, как правило, не желают придавать огласке факт хищения, чтобы избежать нежелательных последствий в виде снижения доходов в случае уменьшения числа вкладчиков.

Нередки случаи компьютерного саботажа. В свое время на Волжском автомобильном заводе был изобличен программист, который из мести умышленно внес изменения в программу ЭВМ, в результате чего произошел сбой конвейера и заводу был причинен существенный материальный ущерб.

В США ФБР раскрыло группу хакеров из Милуоки, которые обеспечили себе несанкционированный доступ более чем к 50-ти автоматизированным банкам данных, включая Лос-Аламосскую ядерную лабораторию, крупный раковый центр и другие жизненно важные объекты США.

По сообщениям западной печати, весьма распространенным и прибыльным является компьютерный промышленный шпионаж, осуществляемый в наиболее наукоемких и дорогостоящих сферах

---

[3] См.: Никифоров Б. С., Решетников Ф. М. Современное американское уголовное право. М., 1990. С. 184.

деятельности: научные исследования, финансовые операции, сложные технологические процессы и т. д.

Массовое распространение во всем мире получило компьютерное пиратство. По данным Ассоциации производителей компьютерного обеспечения, уровень компьютерного пиратства в России составляет 94 %, для сравнения, в Германии — 50 %, в США — 35 %. Правда, надо признать, что в Китае уровень компьютерного пиратства еще выше, чем в России, он составляет 98 %.

Разнообразие компьютерных преступлений настолько велико, что на сегодняшний день в уголовном праве пока не выработано единого понятия компьютерного преступления, не разработана система, которая бы исчерпывающим образом описывала и отображала все многообразие действий и последствий, возникающих в результате неправомерного использования ЭВМ.

В свое время Ю. М. Батурин и А. М. Жодзинский называли следующие основные виды преступлений, связанных с вмешательством в работу компьютеров:

несанкционированный доступ к информации, хранящейся в компьютере;

ввод в программное обеспечение “логических бомб”, которые срабатывают при определенных условиях и частично или полностью выводят из строя компьютерную систему;

разработка и распространение компьютерных вирусов;

преступная небрежность в разработке, изготовлении и эксплуатации программно-вычислительных комплексов;

подделка компьютерной информации;

хищение компьютерной информации[4].

Анализ литературы, посвященной ответственности за компьютерные преступления по законодательству зарубежных стран, поможет составить о них более полное представление.

2. ОТВЕТСТВЕННОСТЬ ЗА КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ ПО ЗАКОНОДАТЕЛЬСТВУ НЕКОТОРЫХ ЗАРУБЕЖНЫХ СТРАН

Проблема борьбы с компьютерными (информационными) преступлениями в настоящее время стоит перед многими государствами. Причем настолько остро, что, например, Совет Европы принял несколько рекомендаций, направленных на борьбу с ними[5]. Цель рекомендаций — выработать согласованный подход государств при внесении изменений в уголовно-правовое и уголовно-процессуальное законодательство.

В рекомендациях принято понятие “преступление с использованием компьютера”. Было признано, что дать

---

[4] См.: Батурин Ю. М., Жодзинский А. М. Компьютерная преступность и компьютерная безопасность. М., 1991. С. 11—19.

[5] Например, Recommendation № R (89) 9; Council of Europe (eds) Computer-Related Crime, Strasbourg 1990 и др.

определение компьютерного преступления чрезвычайно сложно. Не всякое использование компьютерной системы образует состав компьютерного преступления. Поэтому в Рекомендации № R (89) 9 понятие преступления с использованием компьютера определяется через примерный перечень конкретных действий, которые в совокупности дают представление о компьютерном преступлении.

Позднее, в Рекомендации № R (95) 13 Совет Европы заменил термин “преступление с использованием компьютера” другим — “преступление, связанное с использованием информационных технологий”. В рекомендациях подчеркивается, что преступления, связанные с информационными технологиями, могут совершаться с помощью компьютерной системы. Система может быть или объектом, или средой преступления.

Многие европейские государства повели решительную борьбу с компьютерными преступлениями с момента их появления в жизни общества. В Нидерландах был создан Консультативный комитет по компьютерным преступлениям, который предложил конкретные рекомендации по внесению изменений в УК и УПК Нидерландов. Консультативный комитет не дал определения компьютерных преступлений, но он разработал их классификацию.

В то же время Полицейское разведывательное управление (ПРУ), занимающееся регистрацией всех случаев компьютерных преступлений, использует следующее определение компьютерного преступления: это поведение, которое (потенциально) вредно и имеет отношение к устройствам, связанным с компьютерами с точки зрения хранения, передачи и обработки данных. ПРУ делает различие между компьютерными преступлениями, в которых компьютер является объектом преступления, и теми, в которых он — орудие преступления.

Начиная с 1987 г. ПРУ использует для анализа пять видов компьютерных преступлений:

совершаемые обычным способом, но с использованием технической поддержки в компьютерной среде;

компьютерное мошенничество;

компьютерный террор (совершение преступлений с целью повреждения компьютерных систем):

а) использование несанкционированного доступа;

б) вредоносных программ, типа компьютерных вирусов;

в) совершение других действий, включая физическое повреждение компьютера;

кража компьютерного обеспечения (пиратство);

остаточная категория, включающая все другие типы преступлений, которые не подпадают под вышеперечисленные категории[6].

Данный перечень видов преступлений в целом соответствует Рекомендации № R (89) 9 Совета Европы, хотя и отличается более простым их описанием.

Причина отсутствия общепризнанного определения компьютерного преступления заключается в том, что, по мнению нидерландских ученых, существует множество трудностей при формулировании определения, которое, с одной стороны, было бы достаточно емким, а с другой — достаточно специальным. 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, в широком — использование компьютера или автоматического устройства как объекта или инструмента преступления.

Нидерландская статистика обнаруживает тенденцию к росту числа компьютерных преступлений. Исследования показывают, что 58 % используемого в Нидерландах компьютерного обеспечения является “пиратским”. Увеличивается количество компьютерных мошенничеств, случаев незаконного доступа, распространения компьютерных вирусов, компьютерного террора и шпионажа.

Наиболее типичные примеры компьютерных преступлений, совершаемых в Нидерландах.

В 1986 г. несколько преступников договорилось с системными операторами, обеспечивающими работу компьютеров на конных бегах. Билеты со ставками записывались в компьютерную систему. Когда победитель представлял часть билета, его сравнивали с электронной копией в компьютере и результатами забега. Преступники подделывали свою копию под комбинацию победителя, и оператор изменял электронную копию средствами оболочки NORTON. Виновные понесли наказание за подлог и кражу путем обмана в марте 1992 г.

В 1989 г. лицо, принимавшее участие в медицинской конференции по СПИДу, распространило среди ее участников дискету с информацией о СПИДе. Использование дискеты было свободным, но очень мелким шрифтом на обратной стороне инструкции было указано, что попытка повторного использования дискеты может причинить вред компьютерной системе. И действительно, после нескольких запусков компьютерная система останавливалась, а пользователю предлагалось перевести некоторое количество денег на счет иностранного банка. Виновный понес

---

[6] Здесь и далее используются материалы, представленные нидерландской стороной для обеспечения совместного проекта, в частности, Национальный отчет о компьютерных преступлениях, сделанный проф. Х. В. К. Касперсеном.

наказание за пределами Нидерландов, так как скрылся с ее территории.

В 1988 г. оператор компьютера отказался от работы, поссорившись с нанимателем. После его ухода компьютерная система перестала работать, так как он изменил пароль и установил код, исключающий реагирование компьютера на обычные команды. Коллеги ушедшего оператора запаниковали и в попытке заставить компьютерную систему работать причинили огромный ущерб. Оператор был осужден за выведение из строя компьютерной системы.

В 1991 г. были обнаружены и осуждены два хакера. Они проникли в компьютерную сеть одного из университетов и вели постоянное наблюдение за программами в сети и прослушивали телефонные линии связи.

В мае 1992 г. служащий авиакомпании совершил незаконный вход в сеть аэропорта и распространил оскорбительный текст, отбивающий у туристов охоту к посещению данной страны. С помощью системных операторов полиция выследила терминал и время, когда послание было запущено в систему, и ей удалось найти преступника.

Несколько клиентов заявили об исчезновении некоторых сумм с их банковских счетов, хотя они указанные суммы не снимали ни через банкомат, ни каким другим способом. Полиция выяснила, что изъятие было сделано через банкоматы с помощью фальшивых банковских карт. Все хищения совершил служащий автозаправочной станции, который копировал банковские карты клиентов, передававшиеся ему для оплаты услуг на автозаправочной станции, с помощью специального устройства.

В 1993 г. в Нидерландах был принят Закон о компьютерных преступлениях, дополняющий Уголовный кодекс новыми составами: несанкционированный доступ в компьютерные сети (ст. 138a (1)); несанкционированное копирование данных (ст. 138 (2)); компьютерный саботаж (ст. 350a (1), 350b (1)); распространение вирусов (ст. 350a (3), 350b); компьютерный шпионаж (ст. 273 (2)). В ряд статей, предусматривающих ответственность за совершение традиционных преступлений (вымогатель-ство (ст.ст. 317, 318); запись (прослушивание, копирование) информационных коммуникаций; кража путем обмана служб (ст. 362c)), были внесены дополнения, в редакции других (саботаж (ст.ст. 161, 351); подлог банковских карточек (ст. 232)) даны специальные разъяснения. Были значительно изменены такие составы, как шпионаж (ст.ст. 98, 98a); вмешательство в коммуникации (ст. 139a, 139b); порнография (ст. 240b).

Таким образом, уголовное законодательство Нидерландов предоставляет широкие возможности для борьбы с различными видами компьютерных преступлений.

В ФРГ с 1 января 1975 г. действует новая редакция Уголовного кодекса 1871 г. С этого же времени началась дискуссия о целесообразности разработки уголовного законодательства, предусматривающего ответственность за действия, связанные с компьютерами. В 1986 г. в Уголовный кодекс было введено несколько новых поправок, содержащих описание компьютерных преступлений. В настоящее время УК ФРГ, по нашим подсчетам, имеет 7 составов компьютерных преступлений.

Предусмотрена уголовная ответственность для лиц, неправомочно приобретающих для себя или иного лица непосредственно не воспринимаемые сведения, которые могут быть воспроизведены или переданы электронным, магнитным или иным способом (ст. 202a). Ответственности за компьютерное мошенничество (ст. 263a) подлежит лицо, оказавшее влияние на результаты процесса обработки информации путем неправильного оформления программ (манипуляцией с программным обеспечением), использования неправильных или неполных данных, а также посредством незаконного использования данных или воздействия на процесс обработки информации. Уголовно наказуемо изменение данных, имеющих доказательственное значение (ст. 269), а также фальсифицированное использование результатов переработки данных в правоприменительной деятельности (ст. 270). УК ФРГ предусматривает наказание за уничтожение, повреждение технических записей, не принадлежащих виновному вообще или исключительно (ст. 274). Подлежит ответственности тот, кто неправомерно аннулирует, уничтожает, делает непригодными или изменяет данные (ст. 303a). Установлена уголовная ответственность за компьютерный саботаж (ст. 303b)[7].

Была вынуждена отреагировать на компьютерные преступления и Великобритания, известная консерватизмом правовой системы. Длительное время она пыталась справляться с этим явлением, используя свой многовековый опыт судопроизводства, но под “напором” компьютерной преступности “сдалась”. С августа 1990 г. вступил в силу Закон о злоупотреблениях компьютерами. Особенностью данного закона является то, что если какое-либо звено компьютерного преступления окажется на территории Великобритании (деяние или последствия), то преступление признается совершенным на ее территории.

Среди уголовных кодексов европейских зарубежных государств особое внимание привлекают кодексы Испании и Франции, недавно вступившие в силу. Кодекс Франции вступил в действие с весны 1994 г., а Испании в 1996 г.

---

[7] См.: Уголовный кодекс ФРГ / Науч. ред. Н. Ф. Кузнецова, Ф. И. Решет-ников. М., 1996.

Кодекс Франции включает составы большого числа компьютерных преступлений. Среди них посягательства на деятельность ЭВМ. Так, в главе 3 устанавливается ответственность за преступления, посягающие на системы автоматизированной обработки данных, такие как незаконный доступ к автоматизированной системе обработки данных или незаконное пребывание в ней (ст. 323-1); воспрепятствование работе или нарушение работы системы (ст. 323-2); ввод обманным путем в систему информации, а также изменение или уничтожение содержащихся в автоматизированной системе данных (ст. 323-3).

В УК Франции предусмотрена ответственность за посягательства, связанные с использованием картотек и обработкой данных на ЭВМ: осуществление или отдача указания об осуществлении автоматизированной обработки поименных данных без осуществления предусмотренных в законе формальностей (ст. 226-16); осуществление или отдача указания об осуществлении обработки этих данных без принятия всех мер предосторожностей, необходимых для того, чтобы обеспечить безопасность данных (ст. 226-17); сбор и обработка данных незаконным способом (ст. 226-18); ввод или хранение в памяти ЭВМ запрещенных законом данных (ст. 226-19); хранение определенных данных сверх установленного законом срока (ст. 226-20); использование данных с иной целью, чем это было предусмотрено (ст. 226-21); разглашение данных, могущее привести к указанным в законе последствиям (ст. 226-22).

Кроме того, Кодекс Франции предусматривает ответственность за действия, совершаемые с компьютерной информацией в ущерб интересам государства. Перечень данных составов преступлений также достаточно велик: 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 (ст.ст. 411-7, 411-8, 413-9, 413-10, 413-11).

В УК Испании, в отличие от УК Франции, нет специальных норм, предусматривающих ответственность за посягательство на компьютерную информацию, но она установлена за преступления, совершаемые с использованием информационных технологий: раскрытие и распространение тайных сведений (ст. 197); посягательство на интеллектуальную собственность (ст. 270) и коммерческую тайну (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 и выдача тайны и информации, связанных с национальной обороной (ст.ст. 598, 599).

В Соединенных Штатах Америки компьютерная преступность появилась на рубеже 70-х годов. Именно с этого времени возник вопрос о том, в какой мере действующее уголовное законодательство обеспечивает потребности борьбы с компьютерными преступлениями. Американские исследователи пришли к выводу, что законодательство нуждается в новых законах, ориентированных на противодействие не известным ранее явлениям. В частности, в США возникла проблема уголовно-правовой оценки действий человека, который делает копию записи информации, а затем продает ее заинтересованным лицам. За что привлекать к ответственности в данном случае? Ведь кражи имущества в традиционном значении этого слова не происходило. Можно ли компьютерную программу считать "имуществом"? Как оценивать действия человека, который продает машинное время, стоимость которого представляется достаточно высокой?

Поэтому не случайно в 1977 г. в США появился законопроект о защите федеральных компьютерных систем. Он предусматривал уголовную ответственность за следующие категории компьютерных преступлений: введение ложных данных в компьютерную систему; незаконное использование компьютерных устройств; внесение изменений в процессы обработки информации или нарушение этих процессов; кража денег, ценных бумаг, имущества, услуг, ценной информации, совершенная электронными или иными средствами.

На основе данного законопроекта в 1984 г. был принят соответствующий федеральный закон, который затем был дополнен в 1986 г.

В настоящее время в Соединенных Штатах преступления с использованием компьютера становятся все более обычным явлением вследствие всеобщей компьютеризации страны, хотя никто в точности не знает, сколько их совершается в действительности. По приблизительным оценкам американских исследователей, ущерб от такого рода преступлений составляет миллиарды долларов ежегодно[8].

Общепринятого определения того, что надо понимать под компьютерным преступлением, в США нет. Каждый штат имеет свой закон, специально рассматривающий преступления, связанные с использованием компьютера. Причем некоторые штаты ограничиваются модификацией традиционных законов, например, предусматривая ответственность за хищения компьютерного времени или данных.

Американские исследователи, основываясь на анализе действующего законодательства, выделяют пять основных форм неправомерного поведения, связанного с использованием

[8] Доклад проф. Эдварда М. Вайза.

компьютеров, которые в той или иной формулировке представлены в законах штатов: неразрешенный доступ; неразрешенное использование; нечестная манипуляция или изменение данных; компьютерный саботаж; хищение информации[9].

Данная классификация не лишена недостатков, которые отмечают и сами американские ученые. В частности, она не включает хищение элементов компьютерного оборудования, не предусматривает ситуации, когда компьютеры используются при совершении других преступлений и т. д.

В связи с необходимостью законодательного реагирования на компьютерную преступность в США отмечались три большие волны, направленные на изменение и дополнение законодательства.

Во-первых,— принятие нескольких федеральных законов, обеспечивающих защиту неприкосновенности частной жизни.

Во-вторых,— появление уголовных законов, предусматривающих ответственность за противоправное использование компьютеров. Первыми штатами, в которых были приняты подобные законы, стали Флорида и Аризона в 1978 г.

Наибольшее применение в США компьютеры получили при совершении хищений. Поэтому помимо традиционных составов, предусматривающих ответственность за преступления против собственности, была предусмотрена ответственность за компьютерное мошенничество.

Весьма широкое распространение получили случаи неразрешенного доступа, а затем последующего изменения или уничтожения данных. Закон установил ответственность за сам факт неразрешенного доступа к компьютерной информации.

В-третьих,— законодательное урегулирование проблем защиты компьютерных программ как формы интеллектуальной собственности. В 1980 г. были внесены соответствующие изменения в Закон об авторском праве.

В настоящее время страна переживает новую, четвертую волну, связанную с разработкой законов, регулирующих информационные процессы.

В частности, в юридической литературе активно дебатируются проблемы, связанные с конфиденциальной информацией. Как отмечают американские ученые, противоречивость законодательства не позволяет в полной мере обеспечить принцип неприкосновенности частной жизни. Поэтому возлагаются большие надежды на законы о преступлениях, связанных с использованием компьютеров. Данные законы устанавливают санкции против неразрешенного вторжения в информационные системы, тем самым они одновременно служат для защиты права неприкосновенности частной жизни.

---

[9] Там же.

Закон о мошенничестве с использованием компьютера и о злоупотреблении компьютерами (ст. 1030 титула 18 Свода законов США) — это основной закон США, касающийся компьютерных преступлений. Он наказывает за несанкционированный доступ или за превышение санкционированного доступа к "защищенным компьютерам".

Защищенный компьютер — компьютер, используемый финансовым учреждением или для такового или же Правительством Соединенных Штатов Америки или для оного.

Несанкционированный доступ — посторонний человек по отношению к системе вторгается в компьютер извне и пользуется им.

Превышение санкционированного доступа — санкционированный пользователь системы, который осуществляет доступ к информации или ее видоизменяет, тогда как ему не позволяется ни осуществлять к ней доступ ни ее видоизменять.

Ст. 1030(a)(1) предусматривает ответственность за компьютерный шпионаж, состоящий в несанкционированном доступе или превышении санкционированного доступа к информации, а также получение информации, имеющей отношение к государственной безопасности, международным отношениям и атомной энергии.

Наказуем по американскому законодательству несанкционированный доступ или превышение санкционированного доступа к информации, а также получение информации из финансового учреждения, из правительственного ведомства США, из какого бы то ни было защищенного компьютера, имеющего отношение к межштатной или международной торговле — статья 1030(a)(2).

Специально устанавливается ответственность за доступ к компьютеру, который полностью или частично используется Правительством США — ст. 1030(a)(3).

В соответствии со ст. 1030(a)(4) "Мошенничество с использованием компьютера" наказуем доступ, осуществляемый с мошенническими намерениями, и использование компьютера с целью получения чего бы то ни было ценного посредством мошенничества, включая "кражу" компьютерного времени стоимостью более 5 тыс. долларов в течение года, т. е. без оплаты использования компьютерных сетей и серверов.

Ст. 1030(a)(5) предусматривает ответственность за умышленное или неосторожное повреждение защищенных компьютеров.

Наказуема по законодательству США торговля компьютерными паролями — ст. 1030(a)(6).

В соответствии с рассматриваемым Законом установлена уголовная ответственность за угрозы, совершаемые с помощью

компьютера — ст. 1030(а)(7), и другие преступления, связанные с компьютерами.

Американское законодательство на федеральном уровне не ограничивается вышеназванным законом. Имеется и ряд других законов США, так или иначе связанных с ответственностью за компьютерные преступления.

Например, в ст. 1029 титула 18 Свода законов США предусматривается ответственность за торговлю краденными или поддельными устройствами доступа, которые могут быть использованы для получения денег, товаров или услуг.

Ст. 1343 титула 18 Свода законов США предусматривает возможность привлечения к уголовной ответственности за какое бы то ни было сообщение, переданное полностью или частично по телеграфу, которое используется для совершения последующего мошенничества.

В соответствии же со ст. 1361-2 титула 18 Свода законов наказуемо злонамеренное повреждение имущества, контрактов, линий или систем связи.

Большое значение американское законодательство уделяет неприкосновенности личной жизни граждан.

В соответствии со ст. 2511 титула 18 наказывается перехват и разглашение сообщений, передаваемых по телеграфу, устно или электронным способом.

Специально охраняется законом конфиденциальность электронной почты и речевой корреспонденции на сервере. В ст. 2701 “Незаконный доступ к хранимым сообщениям” титула 18 Свода законов США определено, что наказуемо умышленное получение или видоизменение сообщений, хранящихся в электронной памяти, а также создание препятствий для санкционированного доступа к таким сообщениям[10].

Определенный законодательный опыт борьбы с компьютерными преступлениями имеют и бывшие республики СССР, так называемые страны “ближнего зарубежья”. Вступили в силу новые уголовные кодексы в республиках Узбекистан, Кыргызстан, Казахстан. Особенностью данных кодексов является то, что в них есть специальные статьи, предусматривающие ответственность за компьютерные преступления. Причем ее законодательное регламентирование отличается от российского.

Кодекс Республики Узбекистан предусматривает такие составы компьютерных преступлений, как хищение путем присвоения и растраты с использованием средств компьютерной техники (п. “г” ч. 3 ст. 167); мошенничество и использованием средств компьютерной техники (п. “в” ч. 3 ст. 168); кража, совершенная с

[10] Материалы российско-американского семинара, посвященного борьбе с компьютерными преступлениями. Санкт-Петербург, июнь 1998 г.

несанкционированным проникновением в компьютерную систему (п. “в” ч. 3 ст. 169); нарушение правил информатизации (ст. 174); незаконное собирание, разглашение или использование информации (ст. 191); дискредитация конкурента (ст. 192).

Несколько иначе подходит к борьбе с компьютерными преступлениями УК Республики Кыргызстан. В нем практически дословно воспроизведены составы компьютерных преступлений, предусмотренных в УК РФ: неправомерный доступ к компьютерной информации (ст. 289); создание, использование и распространение вредоносных программ для ЭВМ (ст. 290); нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 291).

Кроме того, в трех составах законодатель отразил особенности компьютерных преступлений, предусмотрев ответственность за: нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан (ч. 1 ст. 136); совершенное с использованием специальных технических средств, предназначенных для негласного получения информации (ч. 2 ст. 136); незаконное производство, сбыт или приобретение в целях сбыта специальных технических средств, предназначенных для негласного получения информации (ч. 3 ст. 136); нарушение авторских, смежных прав и прав патентообладателей путем выпуска под своим именем чужой программы для ЭВМ либо базы данных, либо иное присвоение авторства на такое произведение, а равно принуждение к соавторству (ч. 1 ст. 150); незаконное использование программы для ЭВМ или базы данных (ч. 2 ст. 150); незаконное получение сведений, составляющих коммерческую или банковскую тайну, путем перехвата информации в средствах связи, незаконного проникновения в компьютерную систему или сеть (ст. 193).

В УК Республики Казахстан 1998 г. предусмотрена уголовная ответственность за неправомерный доступ к компьютерной информации, создание, использование и распространение вредоносных программ для ЭВМ (ст. 227).

Весьма тщательно регламентируется ответственность за компьютерные преступления в Модельном уголовном кодексе для стран — участников СНГ, принятом на седьмом пленарном заседании Межпарламентской Ассамблеи государств — участников Содружества Независимых Государств 17 февраля 1996 г. В соответствии с нормами раздела 12 “Преступления против информационной безопасности” наказуемы: несанкционированный доступ к компьютерной информации (ст. 286); модификация компьютерной информации (ст. 287); компьютерный саботаж (ст. 288); неправомерное завладение компьютерной информацией (ст. 289); изготовление и сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети (ст.

290); разработка, использование и распространение вредоносных программ (ст. 291); нарушение правил эксплуатации компьютерной системы или сети (ст. 292).

Кроме того, в Модельном кодексе предусматривается ответственность за совершение преступлений, связанных с использованием компьютера или посягающих на компьютерную информацию. Например, хищение, совершенное путем использования компьютерной техники (ст. 243); причинение имущественного ущерба путем обмана, злоупотребления доверием или модификации компьютерной информации (ст. 250); незаконное получение информации, составляющей коммерческую или банковскую тайну путем перехвата в средствах связи, незаконного проникновения в компьютерную систему или сеть, использования специальных технических средств (ст. 269); нарушение правил обращения с содержащими государственную тайну документами или компьютерной информацией (ст. 300).

Несомненно, что творческое использование данного акта, а также законодательного опыта зарубежных стран, пошло бы на пользу российскому законодательству. Ибо очевидно, что нормы действующего уголовного кодекса России не охватывают всего круга противоправных деяний, совершаемых в сфере информационных технологий.

3. ОСНОВНЫЕ ЗАКОНЫ И ПОНЯТИЯ ИНФОРМАЦИОННОГО ЗАКОНОДАТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ

Развитие новых информационных технологий, появление компьютерных преступлений заставляют обратить на информационную безопасность самое пристальное внимание.

Безопасность в соответствии с Законом РФ “О безопасности” — это состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.

Информационная безопасность согласно Федеральному закону “Об участии в международном информационном обме-не” — это состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства. Под информационной средой закон понимает сферу деятельности субъектов, связанную с созданием, преобразованием и потреблением информации.

В свою очередь, информация — это сведения о фактах, событиях, явлениях и процессах независимо от формы их представления.

Законодательство, посвященное регулированию общественных отношений в информационной сфере, в настоящее время принято

называть информационным. Оно состоит из всей совокупности нормативных актов, действующих в информационной сфере. Иногда его называют “компьютерным законодательством” по той простой причине, что основным средством развития и использования новых информационных технологий является компьютер. На наш взгляд, более правильно все же определять данный раздел законодательства не компьютерным, а информационным, исходя из предмета правового регулирования.

Международно-правовой основой регулирования информационных процессов является Европейская конвенция о защите прав человека и основных свобод. В ст. 10 данной Конвенции провозглашаются две важнейшие взаимосвязанные свободы — свобода выражения своего мнения и свобода информации. Содержание свободы выражения мнения включает свободу придерживаться своего мнения, получать и распространять информацию и идеи (ч. 1 ст. 10).

Государство не может вмешиваться в этот процесс. За ним закрепляется лишь право вводить лицензирование деятельности радиовещательных, телевизионных или кинематографических предприятий.

Вместе с тем необходимо иметь ввиду, что свобода выражения мнения и свобода информации в обществе не могут быть абсолютными и связаны с определенными обязанностями и ответственностью.

В ч. 2 ст. 10 Конвенции предусмотрена возможность ограничения указанных свобод. Речь фактически идет о различных видах контроля со стороны государства в данной области.

Осуществление информационных свобод сопряжено с формальностями, условиями, ограничениями или штрафными санкциями, установленными государством, необходимыми в демократическом обществе в интересах национальной безопасности, территориальной целостности или общественного спокойствия в целях предотвращения беспорядков и преступлений, защиты здоровья и нравственности, защиты репутации или прав других лиц, предотвращения разглашения информации, полученной конфиденциально, или обеспечения авторитета и беспристрастности правосудия.

Любые ограничения по использованию информационных свобод определяются только законом.

Законодательному регулированию информационных свобод (свободы выражения своего мнения и свободы информации) посвящена ст. 29 Конституции России.

Сравнение ст. 10 Конвенции и ст. 29 Конституции России позволяет сделать вывод о том, что Конституция более широко трактует свободу выражения своего мнения и свободу информации.

Конституция определяет правовые пределы информационных свобод. Не допускается пропаганда или агитация, возбуждающая социальную, расовую, национальную или религиозную ненависть и вражду. Запрещена пропаганда социального, расового, национального, религиозного, языкового превосходства.

Конституцией гарантируется беспрепятственное выражение мнения и убеждения по самым различным вопросам общественной жизни путем устного или письменного слова самыми различными средствами.

Ч. 4 ст. 29 Конституции РФ закрепляет свободу информации. Это означает право каждого на свободу поиска, получения, передачи, производства, распространения информации любыми законными способами. Право на свободу информации требует соблюдения определенных ограничений, связанных с государственной тайной. Перечень сведений, составляющих государственную тайну, определяется федеральным законом.

Конституцией гарантируется свобода массовой информации и установлен запрет цензуры.

Положения ст. 29 Конституции РФ нашли свое дальнейшее развитие в иных нормативных актах информационного законодательства. Среди них особо следует выделить Закон “О средствах массовой информации” 1991 г., Патентный закон РФ 1992 г., Закон “О правовой охране программ для электронных вычислительных машин и баз данных” 1992 г., Закон “О правовой охране топологий интегральных микросхем” 1992 г., Закон “Об авторском праве и смежных правах” 1993 г., Закон “О государственной тайне” 1993 г., Закон “О связи” 1995 г., Федеральный закон “Об участии в международном информационном обмене” 1996 г., Федеральный закон “Об информации, информатизации и защите информации” 1995 г.

Информационное законодательство определяет основные права и обязанности участников, а также субъектов информационной среды, при посредстве которых реализуется свобода придерживаться своего мнения и свобода информации:

собственников-владельцев средств массовой информации: периодических печатных изданий, радио-, теле-, видеопрог-рамм, кинохроникальных программ, иных форм периодического распространения массовой информации;

собственника-владельца информационных ресурсов, информационных систем, технологий и средств их обеспечения, каковым является субъект, осуществляющий владение и пользование указанными объектами и реализующий полномочия распоряжения в пределах, установленных законом;

субъектов средств международного информационного обмена.

Информационная свобода выражается, прежде всего, в праве каждого искать и получать информацию.

В информационном законодательстве урегулированы вопросы, связанные с поиском и получением информации от собственников-владельцев информационных ресурсов. Они в основном раскрыты в ст.ст. 12—15 Федерального закона “Об информации, информатизации и защите информации”. В ст. 12 названного закона регламентируется реализация права на доступ к информации из информационных ресурсов. Пользователи не обязаны обосновывать перед владельцем этих ресурсов необходимость получения запрашиваемой ими информации. Исключение составляет информация с ограниченным доступом. В ст. 13 сформулированы гарантии предоставления информации от органов государственной власти и местного самоуправления.

Право доступа граждан, организаций к информации о них самих закреплено в ст. 14: гражданам и организациям гарантируется доступ к документированной информации о них. Они имеют право знать, кто и в каких целях использует или использовал эту информацию. Ограничение доступа граждан и организаций к информации о них допускается лишь на основаниях, предусмотренных федеральным законом. На владельцев документированной информации о гражданах возлагается обязанность предоставлять информацию бесплатно по требованию тех лиц, которых она касается.

Владелец информационных ресурсов несет юридическую ответственность за нарушение правил работы с информацией в порядке, предусмотренном законодательством РФ.

Доступ к средствам международного информационного обмена и иностранным информационным продуктам определен главным образом в Федеральном законе “Об участии в международном информационном обмене”.

Закон “О средствах массовой информации” устанавливает ряд правовых барьеров, не допуская использование средств массовой информации в целях совершения уголовно наказуемых деяний, для разглашения сведений, составляющих государственную или иную специально охраняемую законом тайну, для призыва к захвату власти, насильственному изменению конституционного строя и целостности государства, разжигания национальной, классовой, социальной, религиозной нетерпимости или розни, для пропаганды войны, а также для пропаганды порнографии, культа насилия и жестокости.

Запрещено использование в теле-, видео-, кинопрограммах, документальных и художественных фильмах, в информационных компьютерных файлах и программах обработки информационных текстов, относящихся к специальным средствам массовой информации, скрытых вставок, воздействующих на подсознание людей или оказывающих вредное влияние на их здоровье.

Российское информационное законодательство достаточно подробно регулирует и отдельные виды ограничений, направленных против злоупотребления свободой мнения, свободой информации. Это касается, прежде всего, охраны государственной тайны и конфиденциальной информации.

Информация подлежит правовой защите и от преступных посягательств.

Какая информация охраняется уголовным законом? Ответ на этот вопрос дает ст. 21 Федерального закона "Об информации, информатизации и защите информации" от 20 февраля 1995 г., в которой предусмотрено, что защите подлежит любая документированная информация, неправомерное обращение к которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу. Под документированной информацией (документом) понимается зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать (ст. 2 Закона).

Понятие "документированная информация" складывается из двух составляющих: информации (сведений) и материального носителя, на котором она отображена каким-либо определенным способом.

Документирование информации является обязательным условием включения информации в информационные ресурсы, а следовательно, выступает и необходимым условием ее правовой защиты. Порядок документирования информации определяется органами государственной власти, ответственными за организацию производства, стандартизацию документов и их массивов, безопасность Российской Федерации (ст. 5 Закона).

Особенностью машиночитаемой информации является то, что она подвержена легкому несанкционированному доступу, копированию и изменению без санкции владельца информации, что предполагает наличие мер, направленных на ее защиту.

В соответствии со ст. 21 Федерального закона "Об информации, информатизации и защите информации" режим защиты информации устанавливается:

в отношении сведений, отнесенных к государственной тайне,— уполномоченными органами на основании Закона Российской Федерации "О государственной тайне";

в отношении конфиденциальной документированной информации — собственником информационных ресурсов или уполномоченным лицом на основании настоящего Федерального закона;

в отношении персональных данных — федеральным законом.

Таким образом, закон определяет круг защищаемой законом информации. Данная информация должна иметь строго определенные атрибуты. Иначе говоря, чтобы информация

получила правовую защиту, она должна обладать указанными в законе свойствами в их совокупности.

С принятием нового УК появилась уголовная ответственность за так называемые компьютерные преступления. Глава 28 УК РФ называется “Преступления в сфере компьютерной информации”. Представляется, что объектом компьютерных преступлений, если придерживаться традиционной трактовки объекта преступления, выступает информационная безопасность — т. е. общественные отношения, образующиеся в сфере функционирования информационной среды и обеспечивающие состояние ее защищенности. Предметом — информационная среда, то есть деятельность субъектов, связанная с созданием, преобразованием и потреблением информации.

Основным законом, регулирующим информационные отношения, является Федеральный закон “Об информации, информатизации и защите информации”. Следовательно, положения названного закона в полной мере относятся и к понятиям, данным в составах компьютерных преступлений. Прежде всего это касается понятия информации, подлежащей уголовно-правовой защите.

Уголовный кодекс предусматривает ответственность за неправомерные действия с охраняемой законом компьютерной информацией. Понятие информации, подлежащей правовой защите, нами было рассмотрено выше. Здесь хотелось бы обратить внимание на специфические особенности компьютерной информации, то есть информации на машинном носителе, в ЭВМ, системе ЭВМ или их сети. В соответствии со ст. 21 вышеназванного Федерального закона, защите подлежит любая *документированная информация*, неправомерное обращение к которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу. Следовательно, компьютерная информация также должна быть документированной, то есть быть зафиксированной на материальном носителе с реквизитами, позволяющими ее идентифицировать. Иначе говоря, под компьютерной информацией понимается электронный документ со всеми полагающимися документу атрибутами, содержащий сведения, доступ к которым законом ограничен.

А как обеспечить идентификацию электронного документа, представленного в цифровой форме? Это ведь не бумага, на которую можно поставить печать, подпись должностного лица, а также иные реквизиты, подтверждающие ее подлинность. Отсюда и возникло понятие “электронная цифровая подпись”, которая посредством специальной программы обеспечивает идентификацию компьютерной информации, то есть подтверждает оригинальность содержащихся в ней сведений, реквизитов документа, факта его “подписания” конкретным лицом.

В ч. 3 ст. 5 Федерального закона “Об информации, информатизации и защите информации” определяется, что юридическая сила документа, хранимого, обрабатываемого и передаваемого с помощью автоматизированных информационных и телекоммуникационных систем, может подтверждаться электронной цифровой подписью при наличии в автоматизированной информационной системе программно-технических средств, обеспечивающих идентификацию подписи и при соблюдении установленного режима их использования. Следовательно, при отсутствии электронной подписи (или иных сведений, реквизитов документа) данная информация не может подлежать уголовно-правовой защите в соответствии с действующим законодательством, так как она является в таком случае не документированной.

4. АНАЛИЗ СОСТАВОВ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ, ПРЕДУСМОТРЕННЫХ УГОЛОВНЫМ ЗАКОНОДАТЕЛЬСТВОМ РОССИИ

УК России предусматривает ответственность за три вида компьютерных преступлений:

неправомерный доступ к компьютерной информации (ст. 272 УК РФ);

создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК РФ);

нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК РФ).

Статья 272 УК РФ устанавливает ответственность за ***неправомерный доступ к охраняемой законом компьютерной информации***, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети.

Под информацией понимаются сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления. Информация должна быть документированной, т. е. зафиксированной на материальном носителе с реквизитами, позволяющими ее идентифицировать. Следовательно, компьютерная информация — это информация, находящаяся в информационной (компьютерной) среде и имеющая идентификационные атрибуты.

Под охраняемой законом информацией понимается документированная информация, для которой установлен специальный режим правовой защиты, например, государственная, служебная, коммерческая тайна, персональные данные.

Ответственность наступает, прежде всего, при неправомерном доступе.

Неправомерный доступ — это незаконное получение возможности манипулирования с информацией, то есть восприятия ее, сбора, обработки, накопления, анализа, хранения, поиска, распространения и совершения с ней иных действий при отсутствии на это у виновного действительного или предполагаемого права. Достигается путем проникновения в компьютерную систему при помощи специальных технических или программных средств, позволяющих преодолеть установленные системы защиты, незаконного использования паролей и иных данных, идентифицирующих законного пользователя.

Объективная сторона преступления, предусмотренного ст. 272 УК РФ, выражается в двух действиях: *неправомерный доступ* к компьютерной информации, находящейся в ЭВМ, системе ЭВМ, сети ЭВМ или на машинном носителе; второе действие закон называет альтернативно — или уничтожение, или блокирование, или модификация либо копирование информации.

Следовательно, если был неправомерный доступ, не повлекший совершение последующих действий, названных в законе, то ответственность не наступает.

Уничтожение информации означает приведение ее в такое состояние, когда она не может быть восстановлена и использована по назначению.

Блокирование — это совершение действий, результатом которых является невозможность получения или использования информации по назначению при ее сохранности.

Модификация — это любые изменения информации, не являющиеся адаптацией, т. е. изменением, осуществляемым исключительно в целях обеспечения нормального функционирования информации.

Копирование — это воспроизведение информации в любой материальной форме.

Нарушить работу ЭВМ, системы ЭВМ или их сети — это значит помешать нормальному функционированию ЭВМ, системы ЭВМ, сети ЭВМ, прервать их работу или прекратить совсем.

С субъективной стороны преступление может быть соверше-но как умышленно, так и по неосторожности. Данный вывод вытекает из смысла ч. 2 ст. 24 УК РФ, поскольку в ст. 272 УК РФ специально не оговорено, что данное преступление может быть совершено только по неосторожности.

При этом, конечно же, надо иметь в виду, что, например, копирование информации может быть совершено только с прямым умыслом, ибо предполагает целенаправленные действия, направленные на достижение определенного результата. А уничтожение информации, ее модификация (изменение),

блокирование и нарушение работы компьютерной системы могут быть совершены как умышленно, так и по неосторожности.

Мотивы преступления значения для квалификации не имеют.

Субъектом преступления может быть любое вменяемое физическое лицо, достигшее 16-летнего возраста, которое совершило неправомерный доступ к охраняемой законом компьютерной информации, вызвавший указанные в законе последствия.

В ч. 2 ст. 272 УК РФ предусмотрена ответственность за то же деяние, но совершенное группой лиц по предварительному сговору, организованной группой, лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети.

Понятие группы лиц по предварительному сговору и организованной группы дается в ст. 35 УК РФ.

Субъекты группового преступления должны выполнять полностью или частично действия, предусмотренные в диспозиции закона, т. е. обеспечивать неправомерный доступ к информации или модифицировать, уничтожать, блокировать, копировать ее.

Для вменения квалифицирующего признака “совершение преступления организованной группой” необходимо установить наличие главаря (организатора, руководителя), согласованное распределение ролей при совершении преступления, внутригрупповую дисциплину, предварительное планирование преступлений (как правило), ярко выраженную направленность на занятие преступной деятельностью, устойчивость группы, связанную с длительностью ее существования, прочность связей между ее членами, наличие постоянных членов (костяка группы), совершение преступлений одним составом или с незначительными изменениями в нем.

Использование служебного положения означает, что лицо получает доступ к компьютерной информации незаконно, используя права, предоставленные ему исключительно в силу выполняемой им служебной деятельности. Повышенную уголовную ответственность за неправомерный доступ к компьютерной информации несет также лицо, имеющее доступ к ЭВМ, системе ЭВМ или их сети.

Необходимо различать лицо, имеющее доступ к ЭВМ (системе, сети ЭВМ), и лицо, имеющее право доступа к компьютерной информации. Необязательно лицо, имеющее доступ к ЭВМ, имеет право на доступ к компьютерной информации, находящейся в ЭВМ. Доступ к ЭВМ, системе ЭВМ или их сети, как правило, имеет лицо в силу выполняемой им работы, связанной с эксплуатацией или обслуживанием ЭВМ, системы ЭВМ или сети ЭВМ.

Статья 273 УК РФ устанавливает ответственность за ***создание, использование и распространение вредоносных программ для ЭВМ.***

Под программой для ЭВМ понимается объективная форма представления совокупности данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств с целью получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ и порождаемые ею аудиовизуальные отображения (ст. 1 Закона "Об авторском праве и смежных правах").

Объективная сторона преступления выражается альтернативно в следующих действиях: создание программ, внесение изменений в существующие программы, использование либо распространение программ, приводящие к несанкционированным действиям — уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или сети ЭВМ.

Состав преступления сконструирован как формальный. Ответственность предусмотрена за сам факт создания, внесения изменений, использования, распространения программ, которые могут вызвать последствия, предусмотренные в диспозиции статьи. Наступления данных последствий для признания деяния оконченным не требуется.

Создание программы — это результат деятельности, выразившийся в представлении в объективной форме совокупности данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств, с целью уничтожения, блокирования, модификации, копирования информации, а также с целью нарушения работы ЭВМ, системы ЭВМ, сети ЭВМ.

Внесение изменений в существующие программы — это модификация (переработка) программы для ЭВМ или других компьютерных устройств, предназначенная для достижения тех же последствий.

Использование программы — это выпуск в свет, воспроизведение, распространение и иные действия по ее введению в хозяйственный оборот (в том числе в модифицированной форме). Например, использование может осуществляться путем записи программы в память ЭВМ.

Распространение программы — это предоставление доступа к воспроизведенной в любой материальной форме программе для ЭВМ, в том числе сетевым и иными способами, а также путем

продажи, проката, сдачи в наем, предоставления взаймы, включая импорт, для любой из этих целей[11].

Несанкционированные действия в компьютерной системе опасны своими последствиями. Например, это может быть полное форматирование жесткого диска (иначе говоря, уничтожение всей информации, которая была на диске), отказ программы от работы, уничтожение файлов определенного содержания и т. д. В настоящее время в мире насчитывается свыше 12 тыс. вредоносных программ. В течение месяца появляется несколько десятков новых видов программ — вирусов, вызывающих "заболевание" компьютерной системы.

Создание, использование и распространение вредоносных программ для ЭВМ — это преступление, совершаемое только с прямым умыслом, так как в диспозиции закона определено, что создание вредоносных программ, внесение изменений в существующие программы, использование и распространение программ заведомо должно привести к несанкционированному уничтожению, блокированию, модификации, копированию информации либо нарушению работы ЭВМ.

"Заведомость" означает достоверное знание. Виновный осознает, что он создает, использует и распространяет вредоносную для ЭВМ программу и желает этого.

Ответственность наступает за любое действие, предусмотренное диспозицией альтернативно. Например, кто-то может нести ответственность за создание вредоносной программы, другой — за ее использование, третий — за распространение вредоносных программ.

Цели и мотивы преступления для квалификации значения не имеют. Они могут учитываться при назначении наказания.

Субъект — лицо, достигшее 16-летнего возраста, которое создало либо использовало, либо распространяло вредоносную программу или машинный носитель с такими программами.

В ч. 2 ст. 273 предусмотрена повышенная ответственность за те же деяния, повлекшие по неосторожности тяжкие последствия. Тяжесть последствий устанавливается применительно к конкретной ситуации. Последствия могут выражаться в различных формах: вынужденном прекращении деятельности юридического или физического лица, потере важной информации и т. д. То есть тяжкими признаются любые последствия, которые суд с учетом конкретных обстоятельств дела может признать таковыми. Речь в данном случае идет о том, что в результате создания, внесения изменений в существующие программы, использования или

[11] См.: ст. 1 Закона "О правовой охране программ для электронных вычислительных машин и баз данных".

распространения вредоносных программ наступили последствия, которые являются результатом действия вредоносной программы.

В соответствии со ст. 274 УК РФ ответственность наступает за ***нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети***.

Данная норма является бланкетной и отсылает к конкретным инструкциям и правилам, регламентирующим работу с ЭВМ на предприятии, учреждении, организации. Эти правила должны устанавливаться уполномоченным лицом в надлежащем порядке.

Объективная сторона состава преступления, предусмотренного ст. 274, выражается в нарушении правил эксплуатации ЭВМ, системы ЭВМ, сети ЭВМ, повлекшем уничтожение, блокирование или модификацию охраняемой законом информации, при условии, что это деяние причинило существенный вред. Между нарушением правил эксплуатации и наступившими последствиями должна быть установлена причинная связь. Степень вреда определяется в каждом конкретном случае, исходя из обстоятельств дела.

Нарушение правил эксплуатации может выражаться в двух формах: в нарушении правил эксплуатации аппаратного обеспечения ЭВМ, системы ЭВМ или сети ЭВМ; в нарушении правил эксплуатации программного обеспечения, предназначенного для функционирования ЭВМ, системы ЭВМ, сети ЭВМ.

Нарушение правил эксплуатации, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации, причинившее существенный вред, может быть совершено как умышлено, так и по неосторожности.

Субъект преступления — специальный. Это лицо, имеющее доступ к ЭВМ, системе ЭВМ или сети ЭВМ по работе, связанной с эксплуатацией или обслуживанием ЭВМ, системы ЭВМ, сети ЭВМ.

Ч. 2 ст. 274 предусматривает ответственность за то же деяние, повлекшее по неосторожности тяжкие последствия. Отношение к последствиям в законе определено в виде неосторожности, что предполагает возможность двойной вины: альтернативно — умысел или неосторожность к нарушению правил эксплуатации и всегда неосторожность — к наступившим последствиям. В случае умысла к тяжким последствиям ответственность должна наступать за то преступление, которое выполнил виновный. Например, умышленное уничтожение или повреждение чужого имущества, если речь идет о компьютерном устройстве.

П Р И Л О Ж Е Н И Я

П р и л о ж е н и е 1

УГОЛОВНЫЙ ЗАКОН ГЕРМАНИИ[12]
(извлечения)

Р а з д е л 15
НАРУШЕНИЕ НЕПРИКОСНОВЕННОСТИ И ТАЙНЫ ЧАСТНОЙ ЖИЗНИ

§ 202а. Действия, направленные на получение сведений

(1) Кто незаконно получает сведения, которые ему не предназ-начаются и особо охраняются от незаконного к ним доступа, или передает их другому лицу, наказывается лишением свободы на срок до трех лет или денежным штрафом.

(2) Сведениями по смыслу абзаца 1 являются только такие, которые могут быть воспроизведены или переданы электронным, магнитным или иным способом и не являются непосредственно воспринимаемыми.

Р а з д е л 22
МОШЕННИЧЕСТВО И ПРЕСТУПНОЕ ЗЛОУПОТРЕБЛЕНИЕ ДОВЕРИЕМ

§ 263а. Компьютерное мошенничество

(1) Кто, действуя с намерением получить для себя или третьего лица имущественную выгоду, причиняет вред имуществу другого лица, воздействуя на результат обработки данных путем неправильного создания программ, использования неправильных или неполных данных, путем неправомочного использования данных или иного неправомочного воздействия на процесс обработки данных, наказывается лишением свободы на срок до пяти лет или денежным штрафом.

(2) § 263, абз. 2—5 действуют соответственно.

§ 269. Подделка данных, имеющих доказательственное значение

(1) Кто в целях совершения обмана в правоприменительной деятельности собирает или изменяет данные, имеющие доказательственное значение, таким образом, что при их восприятии представляются поддельные или фальсифицированные документы или подобным образом применяет собранные или измененные данные, наказывается лишением свободы на срок до пяти лет или денежным штрафом.

(2) Покушение наказуемо.

(3) § 267, абз. 3 применяется.

§ 270. Обман в правоприменительной деятельности путем использования результатов переработки данных

К обману в правоприменительной деятельности приравнивается фальсифицированное использование результатов переработки данных в правоприменительной деятельности.

Р а з д е л 23
ПОДДЕЛКА ДОКУМЕНТОВ

[12] Приводится по: Уголовный кодекс ФРГ / Пер. с нем. А. В. Серебренникова. М., 1996.

§ 274. Утаивание документов, изменение знаков, обозначающих границу

(1) Лишением свободы на срок до пяти лет или денежным штрафом наказывается тот, кто:

1) с намерением причинить другому лицу ущерб уничтожает, повреждает или утаивает документ или техническую запись, которые ему вообще или исключительно не принадлежат;

2) аннулирует, уничтожает, делает непригодными для применения или уничтожает с намерением причинить ущерб другому лицу данные, имеющие доказательственное значение (§ 202a, абз. 2), которыми он не может распоряжаться вообще или исключительно;

3) изымает, уничтожает, делает неузнаваемыми, передвигает или фальсифицирует с намерением причинить ущерб другому лицу пограничные камни или другой предмет, предназначенный для обозначения границы или уровня воды.

(2) Покушение наказуемо.

Р а з д е л 26
ПОВРЕЖДЕНИЕ ИМУЩЕСТВА

§ 303a. Изменение данных

Кто противоправно аннулирует, уничтожает, делает непригодными или изменяет данные, наказывается лишением свободы на срок до двух лет или денежным штрафом.

(2) Покушение наказуемо.

§ 303b. Компьютерный саботаж

(1) Кто нарушает обработку данных, имеющих существенное значение для чужого предприятия, организации или органа таким образом, что он:

1) совершает деяние, предусмотренное § 303a, абз. 1, или

2) разрушает, повреждает, делает непригодной, устраняет или изменяет установку для обработки данных или носителя информации

наказывается лишением свободы на срок до пяти лет или денежным штрафом.

(2) Покушение наказуемо.

П р и л о ж е н и е 2

УГОЛОВНЫЙ ЗАКОН ФРАНЦИИ[13]

(извлечения)

Книга 2. О преступлениях и проступках против человека
Раздел 2. О посягательствах на человеческую личность
Глава 6. О посягательствах на личность
Отдел 4. О посягательстве на тайну
Параграф 2. О посягательстве на тайну корреспонденции

Ст. 226-15. Совершаемые по недобросовестности вскрытие, уничтожение, задержка или хищение корреспонденции, прибывшей или не прибывшей по назначению и адресованной третьим лицам, или

[13] Приводится по: Новый уголовный кодекс Франции / Науч. ред. Н. Ф. Кузнецова, Э. Ф. Побегайло. М., 1994.

мошенническое ознакомление с ней наказываются тюремным заключением на срок один год и штрафом в 300 000 франков.

Караются такими же наказаниями совершаемые по недобросовестности действия по перехватыванию, хищению, использованию или преданию огласке корреспонденции, отправленной, переданной или полученной через средства дальней связи, или по установке аппаратуры, созданной для осуществления таких перехватываний.

Отдел 5. О посягательствах на права человека, связанных с использованием картотек и обработкой данных на ЭВМ

Ст. 266-16. Осуществление или отдача указания об осуществлении автоматизированной обработки поименных данных без выполнения предусмотренных законом формальностей, которые должны этому предшествовать, наказывается тремя годами тюремного заключения и штрафом в 300 000 франков.

Ст. 226-17. Осуществление или отдача указания об осуществлении автоматизированной обработки поименных данных без принятия всех предосторожностей, необходимых для того, чтобы обеспечить безопасность этих данных и, в частности, воспрепятствовать их искажению, причинению им вреда или их передаче третьим лицам, не имеющим на это права, наказывается пятью годами тюремного заключения и штрафом в 2 000 000 франков.

Ст. 226-18. Сбор данных обманным, непорядочным или незаконным способом или обработка поименных данных, касающихся какого-либо лица, несмотря на возражение этого лица, в том случае, если это возражение имеет законные основания, наказывается пятью годами тюремного заключения и штрафом в 2 000 000 франков.

Ст. 226-19. Ввод или хранение в памяти ЭВМ, в не предусмотренных законом случаях и без специального согласия заинтересованного лица, поименных данных, которые, прямо или косвенно, позволяют выявить расовое происхождение, политические, философские или религиозные взгляды, профсоюзную принадлежность или нравы и обычаи людей, наказывается пятью годами лишения свободы и штрафом в 2 000 000 франков.

Карается такими же наказаниями ввод или хранение в памяти ЭВМ в не предусмотренных законом случаях поименных данных, относящихся к преступным деяниям, обвинительным приговорам или мерам безопасности.

Ст. 226-20. Хранение, без согласия Национальной комиссии по информатике и свободам, данных в поименной форме сверх срока, предусмотренного при подаче заявки или декларации, предшествующей введению обработки информации на ЭВМ, наказывается тремя годами тюремного заключения и штрафом в 300 000 франков.

Ст. 226-21. Использование любым лицом, у которого оказались поименные данные в связи с их регистрацией, классификацией, передачей или любой другой формой обработки, этих данных для другой цели, чем та, которая определена законодательным постановлением или подзаконным актом, разрешающим автоматизированную обработку, или декларациями, предшествующими введению этой обработки, наказывается пятью годами тюремного заключения и штрафом в 2 000 000 франков.

Ст. 226-22. Ознакомление любым лицом, которое собрало, в связи с их регистрацией, классификацией, передачей или другой формой обработки, поименные данные, разглашение которых могло бы привести к посягательству на достоинство личности заинтересованного лица или на интимность его личной жизни, без разрешения этого лица, с этими

сведениями третьего лица, которому занимаемое им положение не дает на это право, наказывается тюремным заключением на срок один год и штрафом в 100 000 франков.

Разглашение, предусмотренное в предыдущем абзаце, наказывается штрафом в 50 000 франков, если оно было совершено по неосторожности или по небрежности.

В случаях, предусмотренных в двух предыдущих абзацах, судебное преследование может быть начато лишь на основании жалобы, поданной пострадавшим, его официальным представителем или управомоченными им лицами.

Ст. 226-23. Положения статей с 226-17 по 226-19 применимы к неавтоматизированным или механографическим картотекам, использование которых не подчиняется исключительно осуществлению права на частную жизнь.

Ст. 226-24. Юридические лица могут быть объявлены подлежащими уголовной ответственности в условиях, предусмотренных статьей 121-2, за деяния, определенные в статьях с 226-16 по 226-21 и 226-23, а также в первом абзаце статьи 226-22. Наказания, назначаемые юридическим лицам, следующие:

п. 1. Штраф в соответствии с положениями статьи 131-38;

п. 2. Наказания, упомянутые в пунктах 2, 3, 4, 5, 6, 7, 8 и 9 статьи 131-39.

Запрещение, упомянутое в пункте 2 статьи 131-39, относится к деятельности, при осуществлении которой или в связи с осуществлением которой было совершено деяние.

Книга 3. О преступлениях и проступках против собственности

Раздел 2. О других посягательствах на собственность

Глава 3. О посягательствах на системы автоматизированной обработки данных

Ст. 323-1. Незаконный доступ ко всей или к части системы автоматизированной обработки данных или незаконное пребывание в ней наказывается тюремным заключением сроком на один год и штрафом в 100 000 франков.

Если результатом этого является либо уничтожение или изменение данных, содержащихся в системе, либо ухудшение работы этой системы, наказание составляет два года тюремного заключения и штраф в 200 000 франков.

Ст. 323-2. Действия, направленные на воспрепятствование работе или на нарушение правильности работы системы автоматизированной обработки данных, наказываются тремя годами тюремного заключения и штрафом в 300 000 франков.

Ст. 323-3. Ввод обманным способом информации в систему автоматизированной обработки данных или уничтожение или изменение обманным способом содержащихся в ней данных наказываются тремя годами тюремного заключения и штрафом в 300 000 франков.

Ст. 323-4. Участие в группе, созданной или в сговоре, устроенном, с целью подготовки, характеризующейся одним или несколькими конкретными действиями, одного или нескольких деяний, предусмотренных статьями с 323-1 по 323-3, карается наказаниями, предусмотренными за это деяние или за деяние, караемое наиболее строго.

Ст. 323-5. Физические лица, виновные в одном из деяний, предусмотренных в настоящей главе, подвергаются также следующим дополнительным наказаниям:

п. 1. Временное лишение политических, гражданских и семейных прав, в соответствии с условиями, предусмотренными статьей 131-26;

п. 2. Запрещение, в соответствии с условиями, предусмотренными статьей 131-27, состоять на государственной службе или осуществлять профессиональную или общественную деятельность, при осуществлении которой или в связи с осуществлением которой было совершено деяние;

п. 3. Конфискация предмета, который использовался или предназначался для совершения деяния, или предмета, являющеюся его результатом, за исключением предметов, которые могут быть возвращены;

п. 4. Закрытие, на срок не более пяти лет, всех заведений или одного или нескольких заведений предприятия, использованных для совершения данных преступных деяний;

п. 5. Запрещение заключать сделки с государственными организациями;

п. 6. Запрещение, на срок не более пяти лет, выдавать чеки, кроме тех, которые позволяют получать наличные деньги из вклада чекодержателем в присутствии плательщика по чеку или управомоченных им лиц;

п. 7. Афиширование или распространение сведений о судебном постановлении, объявленном в условиях, предусмотренных статьей 131-35.

Ст. 323-6. Юридические лица могут быть объявлены подлежащими уголовной ответственности в условиях, предусмотренных статьей 121-2, за деяния, предусмотренные в настоящей главе. Наказания, назначаемые юридическим лицам, следующие:

п. 1. Штраф в соответствии с положениями статьи 131-38;

п. 2. Наказания, упомянутые в статье 131-39. Запрещение, упомянутое в пункте 2 статьи 131-39, относится к деятельности, при осуществлении которой или в связи с осуществлением которой было совершено деяние.

Ст. 323-7. Покушение на проступки, предусмотренные статьями с 323-1 по 323-3, карается теми же наказаниями.

Книга 4. О преступлениях и проступках против нации, государства и общественного порядка

Раздел 1. О посягательствах на основополагающие интересы нации

Глава 1. Об измене и шпионаже

Отдел 3. О передаче информации иностранному государству

Ст. 411-6. Передача или обеспечение доступности для иностранного государства, иностранного предприятия или организации или предприятия или организации, находящихся под иностранным контролем, или их представителей сведений, методов, предметов, документов, данных, содержащихся в памяти ЭВМ или в картотеках, использование, разглашение или сбор которых может привести к посягательству на основополагающие интересы нации, карается пятнадцатью годами заключения и штрафом в 1 500 000 франков.

Ст. 411-7. Сбор или сосредоточение с целью передачи иностранному государству, иностранному предприятию или организации, находящимся под иностранным контролем, или их представителям сведений, методов, предметов, документов, данных, содержащихся в памяти ЭВМ или в картотеках, использование, разглашение или сбор которых могут привести к посягательству на основополагающие интересы нации, карается десятью годами тюремного заключения и штрафом в 1 000 000 франков.

Ст. 411-8. Осуществление, за счет иностранного государства, иностранного предприятия или организации или предприятия или

организации, находящихся под иностранным контролем, или их представителей, деятельности, имеющей целью получение или передачу устройств, сведений, методов, предметов, документов, данных, содержащихся в памяти ЭВМ или в картотеках, использование, разглашение или сбор которых может привести к посягательству на основополагающие интересы нации, карается десятью годами тюремного заключения и штрафом в 1 000 000 франков.

Отдел 4. О саботаже

Ст. 411-9. Уничтожение, порча или хищение любого документа, техники, сооружения, оборудования, установки, аппарата, технического устройства или системы автоматизированной обработки информации или внесение в них изъянов, в тех случаях, когда это может привести к посягательству на основополагающие интересы нации, карается пятнадцатью годами заключения и штрафом в 1500 000 франков.

Если это совершено с целью служить интересам иностранного государства, иностранного предприятия или организации или предприятия или организации, находящихся под иностранным контролем, то же деяние карается двадцатью годами заключения и шрафом в 2 000 000 франков.

Глава 3. О других посягательствах на национальную оборону
Отдел 2. О посягательствах на секреты национальной обороны

Ст. 413-9. Носят характер секретов национальной обороны, в смысле настоящего отдела, важные для национальной обороны сведения, методы, предметы, документы, данные, содержащиеся в памяти ЭВМ или в картотеках, которые явились объектом защитных мер с целью ограничить их распространение.

Могут быть объектом таких мер сведения, методы, предметы, документы, данные, содержащиеся в памяти ЭВМ или в картотеках, разглашение которых способно нанести ущерб национальной обороне или могло бы привести к раскрытию секретов национальной обороны.

Уровни классификации сведений, методов, предметов, документов, данных, содержащихся в памяти ЭВМ или в картотеках, носящих характер секретов национальной обороны, и условия, в соответствии с которыми организована их охрана, определены декретом Государственного совета.

Ст. 413-10. Уничтожение, хищение, изъятие или копирование сведений, методов, предметов, документов, данных, содержащихся в памяти ЭВМ или в картотеках, носящих характер секретов национальной обороны, либо ознакомление с ними публики или лица, не имеющего на это права, любым лицом, являющимся их хранителем либо в силу его положения или профессии, либо в связи с выполнением им, временно или постоянно, определенных обязанностей или какого-либо задания, наказывается семью годами тюремного заключения и штрафом в 700 000 франков.

Карается такими же наказаниями лицо, являющееся хранителем сведений, методов, предметов, документов, данных, содержащихся в памяти ЭВМ или в картотеках, о которых идет речь в предыдущем абзаце, допустившее их уничтожение, хищение, изъятие, копирование или разглашение.

Если лицо, являющееся хранителем, действовало по неосторожности или по небрежности, данное деяние карается тремя годами тюремного заключения и штрафом в 300 000 франков.

Ст. 413-11. Наказывается пятью годами тюремного заключения и штрафом в 500 000 франков любое лицо, не упомянутое в статье 413-10, если оно:

п. 1. Завладело сведениями, методами, предметами, документами, данными, содержащимися в памяти ЭВМ или в картотеках, носящими характер секретов национальной обороны;

п. 2. Уничтожило, изъяло или скопировало, каким бы то ни было образом, такие сведения, методы, предметы, документы, данные, содержащиеся в памяти ЭВМ или в картотеках;

п. 3. Ознакомило публику или лицо, на имеющее на это права, с такими сведениями, методами, предметами, документами, данными, содержащимися в памяти ЭВМ или в картотеках.

Ст. 413-12. Покушение на проступки, предусмотренные в первом абзаце статьи 413-10 и в статье 413-11, карается такими же наказаниями.

Раздел 2. О терроризме
Глава 1. О террористических актах

Ст. 421-1. Образуют террористические акты, в тех случаях, когда они связаны с индивидуальным или коллективным предприятием, имеющим целью серьезно нарушить общественный порядок путем запугивания или террора, следующие деяния:

п. 2. Хищения, вымогательства, уничтожение, повреждение или порча, а также деяния в области информатики, предусмотренные книгой 3 настоящего кодекса.

П р и л о ж е н и е 3

УГОЛОВНЫЙ ЗАКОН ИСПАНИИ[14]

(извлечения)

Раздел 10. Преступления против неприкосновенности частной жизни, права на собственное изображение и неприкосновенности жилища
Глава 10. Раскрытие и распространение тайных сведений

Статья 197

1. Тот, кто в целях раскрытия тайных сведений или нарушения неприкосновенности частной жизни другого лица без его ведома завладевает его бумагами, письмами, сообщениями по электронной почте или другими документами либо перехватывает его телефонные разговоры, либо использует различные технические средства для прослушивания передачи, записи или воспроизведения звука или изображения либо другие средства связи, наказывается лишением свободы на срок от года до четырех лет и штрафом в размере от двенадцати до двадцати четырех месячных заработных плат.

[14] Приводится по: Уголовный кодекс Испании / Под ред. Н. Ф. Кузнецовой, Ф. М. Решетникова. М., 1998.

2. Также наказывается тот, кто, не имея на то полномочий, завладевает, использует или преобразовывает во вред другому лицу тайные сведения личного или семейного характера, которые находились в информационных, электронных или телевизионных картотеках либо в других видах частных и общественных архивов или реестров. Подобное наказание назначается тому, кто, не имея на то полномочий, согласился на совершение таких действий, и кто исказил или использовал их во вред.

3. Лишением свободы на срок от двух до пяти лет наказывается тот, кто распространил или выдал третьему лицу полученные сведения, о которых говорится в предыдущих частях.

Лишением свободы на срок от года до трех лет и штрафом в размере от двенадцати до двадцати четырех месячных заработных плат наказывается тот, кто, зная о незаконности получения тайных сведений, совершил действия, указанные в предыдущем абзаце.

4. Если деяния, предусмотренные частями 1 и 2 этой статьи, были совершены лицами, управляющими или ответственными за информационные, электронные или телевизионные картотеки, архивы или регистры, то им назначается наказания в виде лишения свободы на срок от трех до пяти лет, а если содержащиеся в них сведения были распространены или выданы третьим лицам, то на срок от четырех до шести лет.

5. Если вследствие деяний, предусмотренных предыдущими частями, были раскрыты сведения личного характера, обнаруживающие идеологию, религию, верования, состояние здоровья, происхождение или сексуальную жизнь лица, назначаются предусмотренные наказания в их верхнем пределе.

6. Если эти деяния были совершены с целью получения выгоды, то соответственно назначаются наказания, предусмотренные частями 1—4 этой статьи, в их верхнем пределе. Если, кроме того, были раскрыты сведения, указанные в части 5, то назначается соответствующее наказание выше по степени.

Глава 11. О преступлениях, связанных с интеллектуальной и промышленной собственностью, с рынком и потребителями

Отдел 1. О преступлениях, связанных с интеллектуальной собственностью

Статья 270

Наказывается тюремным заключением на срок от шести месяцев до двух лет или штрафом на сумму от шести до двадцати четырех месячных заработных плат тот, кто с целью наживы и во вред третьим лицам воспроизведет, совершит плагиат, распространит или открыто сообщит полностью или частично литературное, художественное или научное произведение, а также его переработку, интерпретацию или художественное исполнение, закрепленное на любом носителе или сообщенное каким либо способом, без разрешения владельцев соответствующих прав интеллектуальной собственности или цессионариев. То же наказание назначается тому, кто умышленно ввезет, вывезет или сохранит экземпляры указанных произведений или исполнений без соответствующего разрешения. То же наказание назначается за серийное производство или владение специфическим способом, облегчающим пропуск запрета или нейтрализацию технических средств, предназначенных для защиты программ ЭВМ.

Отдел 3. О преступлениях, связанных с рынком и потребителями

Статья 278

1. Тот, кто с целью раскрыть коммерческую тайну завладеет каким либо способом сведениями, письменными или электронными документами, информационными устройствами или другими объектами, которые относятся к коммерческой тайне, либо использует какое-либо средство или орудие, указанное в пункте 1 статьи 197, наказывается тюремным заключением на срок от двух до четырех лет и штрафом на сумму от двенадцати до двадцати четырех месячных заработных плат.

2. Назначается тюремное заключение на срок от трех до пяти лет и штраф на сумму от двенадцати до двадцати четырех месячных заработных плат, если раскрытая тайна будет распространяться, выдана или передана третьим лицам.

3. Эти наказания назначаются независимо от тех мер наказания, которые могут быть назначены за завладение или разрушение информационных устройств.

Раздел 18. О фальсификациях

Глава 2. О подделке документов

Отдел 1. О подделке общественных, официальных и коммерческих документов и сообщений, передаваемых по телекоммуникациям

Статья 394

1. Должностное лицо или государственный служащий, ответствен-ный по службе за телекоммуникации, который передаст ложное или сфальсифицирует телеграфное сообщение или любое другое, наказывается тюремным заключением на срок от шести месяцев до трех лет и лишением права занимать определенные должности на срок от двух до шести лет.

2. Тому, кто использует заведомо ложное сообщение с целью навредить третьему лицу, наказание назначается на одну ступень ниже, чем для фальсификатора.

Глава 3. Общие положения

Статья 400

Изготовление или владение инструментами, материалами, орудиями, веществами, машинами, компьютерными программами или аппаратами, специально предназначенными для совершения преступлений, предусмотренных в предыдущих статьях, наказывается соответственно как исполнение этих преступлений.

Глава 3. Преступления против национальной обороны

Отдел 1. О раскрытии и выдаче тайны и информации, связанных с национальной обороной

Статья 598

Тот, кто без цели способствования иностранному государству достанет, выдаст, исказит или уничтожит информацию, определенную Законом как закрытая или секретная, 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.

Статья 599

Наказание, установленное в предыдущей статье, устанавливается ближе к верхнему пределу санкции, если имеется одно из следующих условий:

1) субъект являлся хранителем или владельцем информации в силу занимаемого поста либо должности;

2) выдача состояла в публикации секрета или информации в средствах массовой информации или другим способом, предполагавшим их распространение.

Приложение 4

МОДЕЛЬНЫЙ УГОЛОВНЫЙ КОДЕКС ДЛЯ ГОСУДАРСТВ — УЧАСТНИКОВ СОДРУЖЕСТВА НЕЗАВИСИМЫХ ГОСУДАРСТВ

(принят на седьмом пленарном заседании Межпарламентской Ассамблеи государств — участников Содружества Независимых Государств 17 февраля 1996 года)

(извлечения)

Раздел XII. Преступления против информационной безопасности
Глава 30. Преступления против информационной безопасности

Статья 286. **Несанкционированный доступ к компьютерной информации**

(1) Несанкционированный доступ к информации, хранящейся в компьютерной системе, сети или на машинных носителях, сопровождающийся нарушением системы защиты и повлекший по неосторожности изменение, уничтожение либо блокирование информации, а равно вывод из строя компьютерного оборудования либо иной значительный ущерб,— преступление средней тяжести.

(2) Действия, предусмотренные частью первой настоящей статьи, повлекшие по неосторожности тяжкие последствия,— преступление средней тяжести.

Статья 287. **Модификация компьютерной информации**

(1) Изменение информации, хранящейся в компьютерной системе, сети или на машинных носителях, а равно внесение в них заведомо ложной информации при отсутствии признаков хищения чужого имущества или причинения имущественного ущерба путем обмана или злоупотребления доверием, причинившее значительный ущерб или создавшее угрозу его причинения,— преступление небольшой тяжести.

(2) То же действие:

а) сопряженное с несанкционированным доступом к компьютерной системе или сети;

б) повлекшее по неосторожности тяжкие последствия — преступление средней тяжести.

Статья 288. **Компьютерный саботаж**

(1) Уничтожение, блокирование либо приведение в непригодное состояние компьютерной информации или программы, вывод из строя компьютерного оборудования, а равно разрушение компьютерной системы, сети или машинного носителя — преступление средней тяжести.

То же действие:

а) сопряженное с несанкционированным доступом к компьютерной системе или сети;

б) повлекшее умышленно или по неосторожности тяжкие последствия,— тяжкое преступление.

Статья 289. **Неправомерное завладение компьютерной информацией**

(1) Несанкционированное копирование или иное неправомерное завладение информацией, хранящейся в компьютерной системе, сети или на машинных носителях, а равно перехват информации, передаваемой с использованием средств компьютерной связи,— преступление небольшой тяжести.

(2) Принуждение к передаче информации, хранящейся в компьютерной системе, сети или на машинных носителях, под угрозой оглашения позорящих сведений о лице или его близких, предания гласности сведений о таких обстоятельствах, которые потерпевший желает сохранить в тайне, а равно под угрозой применения насилия над лицом или его близкими либо под угрозой уничтожения либо повреждения имущества лица, его близких и других лиц, в ведении или под охраной которых находится эта информация,— преступление средней тяжести.

(3) Действия, предусмотренные частями первой или второй настоящей статьи:

а) сопряженные с применением насилия над лицом или его близкими;

б) совершенные по предварительному сговору группой лиц;

в) причинившие значительный ущерб потерпевшему;

г) совершенные с целью получения особо ценной информации,— тяжкое преступление.

(4) Действия, предусмотренные частями первой, второй или третьей настоящей статьи:

а) совершенные организованной группой;

б) сопряженные с причинением тяжкого вреда здоровью или по неосторожности смерти либо иных тяжких последствий,— особо тяжкое преступление.

Статья 290. **Изготовление и сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети**

Изготовление с целью сбыта, а равно сбыт специальных программных или аппаратных средств для получения неправомерного доступа к защищенной компьютерной системе или сети,— преступление небольшой тяжести.

Статья 291. **Разработка, использование и распространение вредоносных программ**

(1) Разработка компьютерных программ или внесение изменений в существующие программы с целью несанкционированного уничтожения, блокирования, модификации или копирования информации, хранящейся в компьютерной системе, сети или на машинных носителях, а также разработка специальных вирусных программ, заведомое их использование или распространение носителей с такими программами,— преступление небольшой тяжести.

(2) То же деяние, повлекшее по неосторожности тяжкие последствия,— преступление средней тяжести.

Статья 292. **Нарушение правил эксплуатации компьютерной системы или сети**

(1) Нарушение правил эксплуатации компьютерной системы или сети лицом, имеющим доступ к этой системе или сети, если это повлекло по неосторожности уничтожение, блокирование, модификацию компьютерной информации, нарушение работы компьютерного оборудования или причинение иного значительного ущерба,— преступление небольшой тяжести.

(2) То же деяние, совершенное при эксплуатации компьютерной системы или сети, содержащей информацию особой ценности,— преступление средней тяжести.

(3) Деяния, предусмотренные частями первой или второй настоящей статьи, повлекшие по неосторожности тяжкие последствия, — преступление средней тяжести.

Глава 28. Преступления против собственности

Статья 243. **Хищение, совершенное путем использования компьютерной техники**

(1) Хищение чужого имущества, совершенное путем использования компьютерной техники,— преступление средней тяжести.

(2) То же действие:

а) совершенное группой лиц по предварительному сговору;

б) причинившее значительный ущерб потерпевшему,— преступление средней тяжести.

(3) Действия, предусмотренные частями первой или второй настоящей статьи, совершенные:

а) в крупном размере;

б) организованной группой,— тяжкое преступление.

Статья 250. **Причинение имущественного ущерба путем обмана, злоупотребления доверием или модификации компьютерной информации**

(1) Причинение значительного имущественного ущерба собственнику или иному владельцу имущества путем обмана или злоупотребления доверием либо путем модификации информации, хранящейся в компьютерной системе, сети или на машинных носителях, при отсутствии признаков хищения или иного завладения чужим имуществом — преступление небольшой тяжести.

(2) То же действие, совершенное:

а) группой лиц по предварительному сговору;

б) с использованием служебного положения,— преступление средней тяжести.

(3) Действия, предусмотренные частями первой или второй настоящей статьи, причинившие ущерб в крупном размере,— преступление средней тяжести.

Глава 29. Преступления против порядка осуществления предпринимательской и иной экономической деятельности

Статья 269. **Незаконное получение информации, составляющей коммерческую или банковскую тайну**

Собирание сведений, составляющих коммерческую или банковскую тайну, путем похищения документов, подкупа и угроз в отношении лиц, владеющих коммерческой или банковской тайной, или их близких, перехвата в средствах связи, незаконного проникновения в компьютерную систему или сеть, использования специальных технических средств, а равно иным незаконным способом с целью разглашения либо использования этих сведений — преступление средней тяжести.

Глава 31. Преступления против основ конституционного строя и безопасности государства

Статья 300. Нарушение правил обращения с содержащими государственную тайну документами или компьютерной информацией

Нарушение лицом, имеющим допуск к государственной тайне, установленных правил обращения с содержащими государственную тайну документами или компьютерной информацией, а равно иными предметами, сведения о которых составляют государственную тайну, если это повлекло по неосторожности наступление тяжких последствий,— преступление средней тяжести.

СОДЕРЖАНИЕ

Екатерина Ивановна ПАНФИЛОВА,
кандидат экономич. наук, доцент, младший советник юстиции

Александр Николаевич ПОПОВ,
кандидат юридич. наук, доцент, юрист 1 класса

КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ

ЛР № 020979 от 17 апреля 1995 г.

Редактор Н. Я. Ёлкина
Компьютерная правка
и верстка Н. В. Валерьянова
Корректор Ю. А. Веселова

Подписано к печати 27.07.98 г. Печ. л. 3,0. Уч.-изд. л. 3,25.
Тираж 1000 экз. Заказ 1313.
Редакционно-издательский отдел
Санкт-Петербургского юридического института
Генеральной прокуратуры РФ
191104, Санкт-Петербург, Литейный пр., 44
Отпечатано с оригинал-макета в печатно-множительной лаборатории
Санкт-Петербургского юридического института
Генеральной прокуратуры РФ