Преступления, связанные с неправомерным использованием баз данных и содержащейся в них компьютерной информации

В. Б. Вехов, к. ю. н., доцент
Волгоградская академия МВД России

Начало XXI века характеризуется бурным процессом глобализации и переходом от индустриального общества к обществу информационному. Под воздействием научно-технического прогресса повсеместно внедряются новые информационные технологии, которые создают уникальные возможности для быстрого и эффективного развития как государства в целом, так и отдельно взятой личности. Это привело к тому, что информация превратилась в основной товар, обладающий значительной ценностью, в своеобразный стратегический ресурс. Многие субъекты общественных отношений уже не могут существовать и нормально функционировать без взаимного информационного обмена и использования в своих технологических процессах различных информационных систем.

В соответствии с п. 3 ст. 2 Федерального закона от 27.07.06 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» информационная система – это совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств. При этом информация представляет собой сведения (сообщения, данные) независимо от формы их представления (п. 1 ст. 2 указанного ФЗ), а база данных есть объективная форма представления и организации совокупности данных (например, статей, расчетов), систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью ЭВМ (ст. 1 Закона РФ от 23.09.92 № 3523-I).

Обработанная таким образом информация объективно переходит в категорию *компьютерной информации.*

Практика показывает: с каждым днем возрастает число учреждений, предприятий и организаций, применяющих разнообразные информационные системы управления, обработки и электронной передачи различных данных, от сохранности которых зависит нормальная жизнедеятельность и безопасность как отдельно взятого юридического лица, так и российского государства в целом. Данные системы стали неотъемлемой частью высокодоходных технологий, используемых в стратегических сферах хозяйства страны. Причем циркулирующая в них компьютерная информация, как правило, относится к категории охраняемой законом информации, то есть конфиденциальной. Все это в совокупности с широкими возможностями и доступностью средств электронно-вычислительной техники и цифровой электросвязи, особенностями технологий дистанционной

обработки компьютерной информации, не скованных рамками административных и государственных границ, отсутствием должного контроля за соблюдением имеющихся специальных требований и рекомендаций по защите такой информации привлекает внимание криминальных структур и отдельных преступных элементов.

В последнее время количество преступлений, связанных с неправомерным использованием баз данных и содержащейся в них охраняемой законом компьютерной информации, неуклонно увеличивается. Они наносят существенный материальный и моральный вред как *операторам информационных систем* – гражданам или юридическим лицам, осуществляющим деятельность по эксплуатации информационных систем, в том числе по обработке информации, содержащейся в их базах данных (п. 12 ст. 2 Федерального закона от 27.07.06 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»), так и их клиентам – физическим и юридическим лицам, конфиденциальные сведения о которых находятся в этих базах данных.

Анализ состояния дел в различных областях экономики страны свидетельствует о том, что из всех известных видов угроз безопасности информации, обрабатываемой с помощью существующих информационных систем, самой распространенной, чрезвычайно опасной и трудноустранимой является человеческий фактор. При этом опасность в равной мере исходит как от внутренних источников угроз – персонала оператора информационной системы, так и внешних – пользователей конкретной информационной системы и иных лиц. В подтверждение сказанному приведем следующие примеры.

Как следует из обвинительного заключения по уголовному делу, студент 5 курса одного из вузов Санкт-Петербурга Б., 1984 года рождения, работал продавцом-консультантом торговой точки ООО «В-Телеком». В силу занимаемой должности он имел доступ к служебному компьютеру этой торговой точки. В его функциональные обязанности входил прием платежей от абонентов операторов сотовой связи и осуществление платежных операций во внешней расчетно-платежной системе «Киберплат». В течение нескольких месяцев 2006 года он умышленно, из корыстных побуждений, используя свое служебное положение, совершил серию неправомерных доступов к охраняемой п. 2 ст. 1 Федерального закона от 29.07.2004 № 98-ФЗ «О коммерческой тайне» компьютерной информации, являющейся коммерческой тайной ООО «В-Телеком», то есть конфиденциальной информацией, позволяющей ее обладателю при существующих обстоятельствах увеличить доходы или получить иную коммерческую выгоду. Эта информация была объективно представлена в виде файлов – идентификаторов указанной торговой точки ООО «В-Телеком», использующихся для ее авторизации и идентификации во внешней расчетно-платежной системе «Киберплат». Файлы находились на жестком магнитном диске системного блока служебного компьютера данной торговой точки. В отношении этих файлов их законным обладателем – ООО «В-Телеком» – был установлен режим коммерческой тайны, то есть приняты правовые, организационные и технические меры по охране их конфиденциальности. Однако Б. в нарушение установленных ООО «В-Телеком» порядка и правил неправомерно скопировал файлы-идентификаторы на свой машинный носитель информации, то есть совершил следующие преступления:

- *неправомерный доступ к охраняемой законом компьютерной информации, то есть информации в ЭВМ и системе ЭВМ, лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, и это деяние повлекло копирование информации (**ч. 2 ст. 272 УК РФ**);*
- *собирание сведений незаконным способом, что повлекло незаконное получение сведений, составляющих коммерческую тайну (**ч. 3 ст. 183 УК РФ**).*

В последующем, Б., находясь у себя дома, с помощью принадлежащих ему компьютера, модема и соответствующего программного обеспечения неоднократно выходил в сеть Интернет на сервер ОАО «Киберплат.ком». Не являясь законным пользователем системы «КиберПлат» и используя при проведении процедур авторизации и идентификации уникальные идентификационные данные – кодовую фразу и ранее незаконно скопированные файлы-идентификаторы торговой точки ООО «В-Телеком», он неправомерно совершил 12 платежно-расчетных операций по зачислению денежных средств на лицевые счета абонентов сотовой связи различных операторов – свой, жены, подруги жены и своего близкого друга. Иными словами, Б. осуществил 12 неправомерных доступов к охраняемой п. 4 ст. 3 Федерального закона от 23.09.92 № 3523-I «О правовой охране программ для электронных вычислительных машин и баз данных» информации – базе данных. При этом он незаконно получал полный объем прав законного пользователя – торговой точки ООО «В-Телеком», включая право модификации базы данных учета платежных операций системы «КиберПлат». Затем он неправомерно вносил в указанную базу данных заведомо ложную информацию – записи о поступлении платежей на лицевые счета указанных абонентов операторов сотовой связи. То есть путем внесения дополнительной информации осуществлял изменение целостности базы данных учета платежных операций системы «КиберПлат», не связанные с ее адаптацией, что повлекло незаконную модификацию охраняемой законом компьютерной информации и причинение имущественного ущерба ООО «В-Телеком» на несколько тысяч рублей.

Таким образом, в дополнение к вышеуказанным преступным деяниям, гражданином Б. также были совершены следующие двенадцать преступлений:

- *неправомерный доступ к охраняемой законом компьютерной информации, то есть информации в ЭВМ и системе ЭВМ, повлекший моди-*

*фикацию информации (**ч. 1 ст. 272 УК РФ**);*

- *причинение имущественного ущерба собственнику – ООО «В-Телеком» путем обмана при отсутствии признаков хищения (**ч. 1 ст. 165 УК РФ**).*

Похожим способом в 2007 году действовал неоднократно судимый за хищения петербуржец Ч., 1975 года рождения. Как было установлено следствием, он, являясь стажером установщика терминалов по приему платежей ООО «Де-та», в силу занимаемой должности узнал уникальные идентификаторы (логин и пароль) учетной записи, использующейся ООО «Де-та» для доступа терминалов по приему платежей к серверу компании «Объединенная система моментальных платежей» (ОСМП), а также неправомерно скопировал на принадлежащий ему домашний компьютер служебную программу «Диллер» версии 3.32 по организации проведения платежей в системе ОСМП.

Находясь по месту своего жительства, выходя в сеть Интернет и не являясь законным пользователем платежной системы компании ОСМП, Ч. умышленно, с целью причинения имущественного ущерба ООО «Де-та», путем обмана, используя при проведении процедур авторизации и идентификации пользователя платежной системы компании ОСМП логин и пароль ООО «Де-та», с помощью программы «Диллер» создавал виртуальный платежный терминал. После чего он осуществлял неправомерные доступы к охраняемой п. 4 ст. 3 Федерального закона от 23.09.92 № 3523-I информации – базе данных учета платежных операций внешней расчетно-платежной системы ОСМП, находящейся на сервере этой компании. При этом Ч. незаконно получал полный объем прав законного пользователя – ООО «Де-та» и модифицировал указанную базу данных, внося в нее заведомо ложную информацию – записи о поступлении платежей и зачисления денежных средств на электронные счета, открытые им в системах MoneyMail, WebMoney, «Яндекс.Деньги» для аккумулирования похищаемых денежных средств. Таким способом в базу данных им было внесено 86 записей, чем ООО «Де-та» был причинен материальный ущерб в размере 511 тыс. руб.

К., 1978 года рождения, работая исполнительным директором ООО «Э-сервис» и используя паспорт своего отца, заключил с Орловским филиалом ОАО «ЦентрТелеком» договор о предоставлении доступа в Интернет с телефона, установленного по его месту жительства.

Обладая достаточными знаниями в области пользования компьютерной техникой и опытом работы в Интернете, К. с помощью специализированной программы X.Scanner сканировал заданные диапазоны IP-адресов компьютеров пользователей в ходе сеанса их работы в сети Интернет и обнаруживал информационные ресурсы, содержащие базы данных с конфиденциальной компьютерной информацией. Затем он подбирал к ним пароли и подключал их в качестве сетевых дисков своего домашнего компьютера.

К. удалось получить неправомерный доступ к сетевым ресурсам ЗАО «Компания «АП» и скопировать на свой домашний компьютер базу данных абонентов сотовой телефонной сети «БиЛайн», включающую в себя их фамилии, имена, отчества, номера телефонов, а также данные о вносимых платежах. В соответствии со ст. 53 Федерального закона от 07.07.03 № 126-ФЗ «О связи», п. 4 ст. 3 Федерального закона от 23.09.92 № 3523-I «О правовой охране программ для электронных вычислительных машин и баз данных» данная компьютерная информация является конфиденциальной и охраняется указанными законами.

В дальнейшем К. получил неправомерный доступ к базе данных, принадлежащей индивидуальному предпринимателю Ч., в результате чего скопировал на жесткий магнитный диск своего компьютера файлы «апрель.xls» и «книга учета март 04 (1).111.x1s», содержащие информацию, которая относится к финансово-экономической деятельности индивидуального предпринимателя Ч. Как было установлено следствием, эта компьютерная информация имеет потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа и ее обладатель принимает меры к охране ее конфиденциальности. Согласно ст. 139 ГК РФ, данная компьютерная информация является коммерческой тайной Ч., относится к охраняемой законом информации и подлежит защите.

В Ростове-на-Дону, безработный Ч. А., 1982 года рождения, описанным выше способом неправомерно получил из сети Интернет и скопировал на жесткий магнитный диск своего домашнего компьютера базу данных ЗАО «Инвестиционная компания Ф.», содержащую сведения, составляющие в соответствии с Федеральным законом от 29.07.04 № 98 «О коммерческой тайне» коммерческую тайну ЗАО «Инвестиционная компания Ф.»: списки клиентов, их местоположение (юридические и фактические адреса), идентификационный номер клиентов, условия договоров с клиентами.

Реализуя свой преступный умысел, из корыстной заинтересованности Ч. А., используя принадлежащий ему домашний компьютер, модем, а также телефон, подключился к сети Интернет. Там, действуя анонимно и скрыв свои сетевые реквизиты путем обращения на web-сайт «anonymouse.org», используя адрес электронной почты «webwo@list.ru», предложил ЗАО «А. ИНВЕСТ», являющемуся прямым конкурентом ЗАО «Инвестиционная компания Ф.» приобрести вышеуказанные сведения, составляющие коммерческую тайну ЗАО «Инвестиционная компания Ф.». При этом в электронном почтовом отправлении Ч. А. указал реквизиты микропроцессорной карты «Сберкарт» и привязанного к ней Специального карточного счета, открытого в Юго-Западном банке СБ РФ на имя Д. – друга Ч. А., на который следовало перечислить денежные средства в сумме 43 тыс. руб.

Требуемая сумма была перечислена на указанный счет. По карте, выданной на имя Д., Ч. А. получил деньги с помощью банкомата и,

используя анонимный адрес электронной почты, отправил на электронный адрес представителей ЗАО «А. ИНВЕСТ» неправомерно полученные сведения, составляющие коммерческую тайну ЗАО «Инвестиционная компания Ф.».

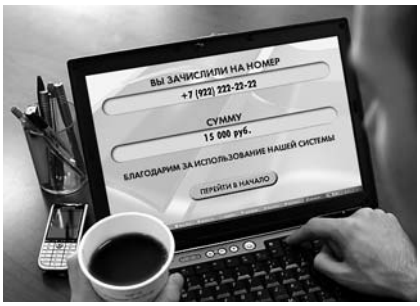
Своими действиями Ч. А. совершил преступление, *предусмотренное* ***ч. 1 ст. 272 УК РФ****, квалифицируемое как неправомерный доступ к охраняемой законом компьютерной информации, находящейся в системе и сети ЭВМ, повлекший ее копирование, а также преступление, предусмотренное* ***ч. 3 ст. 183 УК РФ****, квалифицируемое как собирание сведений, составляющих коммерческую тайну, незаконным способом, незаконное разглашение сведений составляющих коммерческую тайну, без согласия их владельца, совершенное из корыстной заинтересованности.*

Следует обратить внимание на то обстоятельство, что преступления, связанные с неправомерным использованием баз данных и содержащейся в них охраняемой законом компьютерной информации, совершаются не только из корыстной заинтересованности, но и из хулиганских побуждений.

Так, 19-летний студент челябинского юридического вуза А. был осужден Тракторозаводским районным судом Челябинска к одному году лишения свободы условно со штрафом 3000 рублей в доход государства за совершение следующих деяний.

Обладая достаточными знаниями в области информационных технологий, навыками обработки информации и пользования компьютерной техникой, опытом работы в сети Интернет, владея языком программирования Perl, он создал вредоносную программу для ЭВМ sendsms.pl. Эта программа предназначалась для массовой рассылки коротких текстовых сообщений (SMS-сообщений) путем их копирования с сервера оператора сотовой радиотелефонной связи ЗАО «У. GSM», сайт которого находился в сети Интернет, в память сотовых радиотелефонов его абонентов. Данную программу А. использовал при следующих обстоятельствах.

На своем персональном компьютере, установленном у него дома, желая убедиться в работоспособности созданной им программы sendsms.pl, в строке задания параметров, необходимых программе для рассылки SMS-сообщений, ввел данные, позволяющие произвести рассылку 10 нецензурных текстовых сообщений одинакового содержания абоненту сети радиотелефонной связи «Мегафон» с номером телефона +79222222222, принадлежащему М., после чего привел программу в действие. В результате этого данный абонент получил 10 SMS-сообщений нецензурного содержания, то есть произошло копирование компьютерной информации с сервера ЗАО «У. GSM» в память телефонного аппарата сотовой радиосвязи, являющегося персональной ЭВМ. Убедившись в работоспособности компьютерной программы sendsms.pl, А. замыслил осуществление массовой рассылки SMS-сообщений нецензурного содержания всем абонентам Челябинского фрагмента сети радиотелефонной связи «Мегафон», обслуживаемого ЗАО «У. GSM».



Исполняя задуманное и достоверно зная, что использование данной вредоносной программы повлечет за собой несанкционированные блокирование и копирование информации, а также нарушение работы указанной сети ЭВМ, А., пытаясь скрыть следы своей преступной деятельности, воспользовался известными ему от знакомого по переписке в сети Интернет П. логином и соответствующим ему паролем, которые П. использовал для выхода на свой сайт, размещенный на сервере провайдера ООО «Нокс», Санкт-Петербург, и с помощью своего персонального компьютера и модема зашел на указанный сайт.

Там А. разместил программу sendsms.pl, в которую заложил текст SMS-сообщения нецензурного содержания. После этого он, не уведомляя ЗАО «У. GSM» – обладателя компьютерной информации – клиентской базы данных о характере выполняемых программой sendsms.pl функций и не получив от него согласия на реализацию программой своего назначения, привел ее в действие. В программу была заложена функция автоматической рассылки SMS-сообщений с использованием соответствующей услуги по их отправке, реализованной на сайте компании «У. GSM». При этом программа произвольно выбирала из клиентской базы данных телефонные номера абонентов Челябинского фрагмента сети радиотелефонной связи «Мегафон», обслуживаемого ЗАО «У. GSM».

В результате незаконных действий А. и достаточно продолжительного времени работы вредоносной программы 15 тыс. 148 человек получили SMS-сообщения нецензурного содержания, что привело к нарушению заданного технологического режима работы компьютерной сети ЗАО «У. GSM», то есть возникновению ситуации, классифицируемой в соответствии с Инструкцией о порядке действий инженера группы оперативно-технического управления в аварийных ситуациях как событие первой категории «авария». С технической точки зрения авария произошла в результате перегрузки коммутационного оборудования, вызванного пересылкой слишком большого объема компьютерной информации за установленную единицу времени, и временного создания помех в его работе в соответствии с заданным функциональным назначением.

Помимо указанного, действия А. привели к блокированию компьютерной информации, так как абоненты Челябинского фрагмента сети радиотелефонной связи «Мегафон», который обслуживается ЗАО «У. GSM» во время работы вредоносной программы для ЭВМ были лишены физической возможности принимать и отправлять иные SMS-сообщения. ■