Уголовная ответственность за неправомерное получение услуг цифрового телевещания («кард-шаринг»)

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

М. А. Махмудов, *следователь следственного отдела при Советском РОВД г. Махачкалы*

В последнее время Президентом Российской Федерации Д. А. Медведевым и правительством Российской Федерации предпринимаются активные усилия, направленные на скорейшую замену устаревших аналоговых систем трансляции телевизионных программ для населения системами цифрового телевизионного вещания в стандарте DVB. Рынок предоставления таких услуг электросвязи постоянно расширяется, в том числе и по причине хорошо известных огромных преимуществ цифрового телевидения перед аналоговым. Однако этот процесс несет в себе и негативные последствия. Анализ современной следственной и судебной практики свидетельствует об увеличении числа преступлений, связанных с несанкционированным доступам к программам, транслируемым с применением названных компьютерных систем при их передаче по каналам связи, образованным спутниковыми линиями передачи сети связи общего пользования.

Широко известно, что для получения законного доступа к услугам спутникового цифрового телевидения физическое или юридическое лицо должно приобрести у оператора связи абонентский комплект, состоящий из:

- бланка абонентского договора;
- микропроцессорной карты санкционированного доступа (карты абонента);
- руководства пользователя;
- оборудования для приема сигнала со спутника Eutelsat W4 36,0 E (спутниковой антенны, конвертора, цифрового спутникового терминала – приемника со встроенным модулем санкционирования доступа типа Viaccess).

Для первичной активации карты абонента ему необходимо произвести предварительную оплату услуг – минимальный авансовый платеж оператору. В дальнейшем, по мере получения услуг спутникового телевидения, абонент ежемесячно оплачивает их путем внесения абонентской платы, размер которой зависит от выбранного пакета – «тарифного плана».

Правомерное подключение к услугам спутникового телевидения предполагает обязательное наличие у абонента соответствующей идентификационной карты, вставленной в приемник, который через конвертор подключен к спутниковой антенне, направленной на спутник. На спутнике оператор арендует транспондеры, представляющие собой передатчики спутникового сигнала с несущей частотой, на которой передается цифровой сигнал телевизионных каналов. Каждый транспондер позволяет осуществлять вещание определенного количества телевизионных каналов. Сигнал, передаваемый по каждому транспондеру, называется транспортным потоком.

Транспортный поток для каждого телевизионного канала оператора связи содержит в себе скремблированный[1] видеопоток, скремблированный аудиопоток и поток так называемых «ECM-сообщений»[2]. Кроме того, транспортный поток содер-

[1] *Под скремблированием в данном случае понимается процесс шифрования передаваемой информации методом перемещения видео- (аудио-) фрагментов друг относительно друга по определенному закону. При этом видео- и аудиофрагменты одного канала скремблируются по одному закону.*

[2] *EMM-сообщение содержит следующие данные: какой пакет телевизионных программ может просматривать абонент с использованием конкретной «смарт-карты», период ока-зания услуг абоненту (оплаченный период просмотра телепрограмм) и др.*

жит в себе множество других служебных потоков, основным из которых является поток EMM-сообщений. Закон скремблирования меняется каждые 10 секунд. Соответственно, аналогичный закон действует в отношении дескремблирования[3]. В системе защиты информации от несанкционированного доступа Viaccess, лицензионная версия программного обеспечения которой используется оператором для скремблирования транспортного потока, закон дескремблирования описывается контрольным словом, составляющим несколько байт и называемым Descrambling Word (сокр. – DW). Оно меняется каждые десять секунд. Для каждого канала передачи телевизионного сигнала используется отдельное DW.

При выборе абонентом телевизионного канала, приемник определяет, на каком транспондере осуществляется вещание выбранного телевизионного канала. Далее происходит настройка на прием несущей частоты выбранного транспондера. Транспортный поток транспондера поступает в приемник через спутниковую антенну. Приемник проверяет, содержит ли транспортный поток EMM-сообщение для конкретной карты абонента. В случае если транспортный поток содержит EMM-сообщение с указанной информацией, то соответствующая информация записывается в эту карту. Если у абонента есть право просмотра выбранного им телевизионного канала, необходимо получить исходные видео- и аудиосигналы, для чего используется текущее DW. Для получения текущего DW используется ECM-сообщение. Приемник выбирает из транспортного потока ECM-сообщение для текущего телевизионного канала и нужной версии карты абонента по так называемому IDENT-коду и передает его в карту. На основе ECM-сообщения по криптоалгоритму, который содержится в карте, происходит вычисление DW для выбранного канала. Определенное таким образом контрольное слово передается микропроцессорным устройством карты в открытом виде обратно в приемник для дескремблирования транспортного потока выбранного канала. Эта процедура повторяется каждые десять секунд.

Вышеуказанные действия выполняются оператором связи в целях реализации положений, указанных в ч. 2 ст. 12 Федерального закона «О связи» (от 07.07.2003 № 126-ФЗ), а также Требований к защите от несанкционированного доступа к программам, транслируемым с применением системы цифрового телевизионного вещания DVB, при их передаче по каналам связи, образованным спутниковыми линиями передачи сети связи общего пользования, утвержденных приказом Министерства информационных технологий и связи Российской Федерации от 11.01.2006 № 3. Этими правовыми документами устанавливаются следующие ***требования к операторам по защите сетей связи от несанкционированного доступа к ним и передаваемой посредством их информации***.

1. Для защиты от несанкционированного доступа к программам, транслируемым с применением системы цифрового телевизионного вещания стандарта DVB, при их передаче по каналам связи, образованным спутниковыми линиями передачи, между средствами связи передающей земной станции спутниковой связи и средствами связи приемной земной станции спутниковой связи применяются технические и программные средства защиты (далее – средства защиты).

2. Средства защиты выполняют преобразование (кодирование, декодирование) сигналов программ телевизионного вещания независимо от количества таких программ, объединенных в цифровой канал.

3. Средства защиты, применяющие алгоритмы криптографического преобразования, используют алгоритмы, разработанные в соответствии с российскими стандартами.

4. Управление средствами защиты программ телевизионного вещания осуществляется с помощью сигналов, передаваемых за счет избыточности цифрового сигнала стандарта DVB.

5. Смена кодовых комбинаций (ключей), необходимых для выполнения криптографического преобразования, производится одновременно во всех средствах защиты одного типа, применяемых оператором связи.

Функционирование достаточно часто используемой операторами связи системы защиты информации от несанкционированного доступа Viaccess основано на использовании международного стандарта ISO IEC 13818-1 «Information technology – Generic coding of moving pictures and associated audio information: Systems». Однако, как показывает анализ современной следственной и судебной практики, она не в полной мере гарантирует требуемый уровень безопасности информации от ее неправомерного использования.

В последнее время в отечественной криминальной практике все большее распространение получает такой способ совершения преступлений, как неправомерное подключение к услугам спутникового телевидения по технологии «кард-шаринг». Его суть состоит в следующем.

Преступники, организующие «кард-шаринг», различными путями добывают абонентскую карту и специальный приемник конкретного оператора, предоставляющего услуги доступа к программам, транслируемым с применением системы цифрового телевизионного вещания стандарта DVB. При этом приемник представляет собой специализированную ЭВМ, предназначенную для приема, обработки и ретрансляции сигналов спутникового телевещания. Чаще всего ими являются приемники зарубежного производства фирм Dreambox, Seazam и Openbox. Такой приемник в технологии «кард-шаринг» используется преступниками в качестве сервера. Кроме этих радиоэлектронных устройств, роль сервера может также играть обычный персональный компьютер с DVB-картой и картоприемником. В этом случае в картоприемник персональ-

[3] *Дескремблированием называется процесс получения исходного видео- (аудио-) сигнала.*

ного компьютера вставляется абонентская карта конкретного потерпевшего – оператора связи (физического или юридического лица). Сам сервер стандартным способом подключается к глобальной компьютерной сети Интернет. На сервере устанавливается специализированное программное обеспечение, позволяющее копировать контрольное слово (DW) в момент его передачи от абонентской карты в приемник и отсылать его неограниченному кругу нелегальных абонентов – пользователей сети Интернет, реквизиты которых (имя пользователя, пароль) есть в пользовательской базе данных, создаваемой преступниками. Как правило, таким программным обеспечением являются плагины и эмуляторы с конфигурационными файлами, предполагающими подключения к системе «кард-шаринга» нелегальных абонентов. ***С уголовно-правовой точки зрения данные действия квалифицируются как преступления, а именно:***

- неправомерный доступ к охраняемой законом компьютерной информации, ответственность за совершение которого предусмотрена ст. 272 Уголовного кодекса Российской Федерации;
- использование вредоносных программ для ЭВМ, то есть программ для ЭВМ, приводящих к несанкционированному оператором связи копированию информации, ответственность за совершение которого предусмотрена ст. 273 Уголовного кодекса Российской Федерации.

Проиллюстрируем изложенное на примере из судебной практики.

В марте 2007 года трое жителей города Курска – К., П. и Г. – по предварительному сговору объединились в преступную группу для совершения неправомерных доступов к компьютерной информации ОАО «НТВ-ПЛЮС». При этом ими использовались вредоносные программы для ЭВМ.

Как было установлено и доказано в ходе предварительного следствия, компьютерная информация, находящаяся в системе ЭВМ спутникового телевидения ОАО «НТВ-ПЛЮС», в соответствии с Федеральным законом «О коммерческой тайне» (от 29.07.2004 № 98-ФЗ), обладает всеми признаками коммерческой тайны и является охраняемой законом.

Согласно п. 1 ст. 2 Федерального закона «Об информации, информационных технологиях и о защите информации» (от 27.07.2006 № 149-ФЗ) под информацией понимаются «сведения (сообщения, данные) независимо от формы их представления». Таким образом, потоки служебной информации, необходимые для просмотра закрытых каналов спутникового телевидения (ECM-сообщения), а также кодовые слова (DW), которые содержатся в системе ЭВМ спутникового телевидения ОАО «НТВ-ПЛЮС», являются определенной разновидностью информации. Учитывая, что ECM-сообщения и DW-коды генерируются (создаются) в системе ЭВМ спутникового телевидения ОАО «НТВ-ПЛЮС» с использованием специального оборудования, принадлежащего ОАО «НТВ-ПЛЮС», обладателем этой информации в соответствии с п. 5 ст. 2 указанного Федерального закона, является ОАО «НТВ-ПЛЮС». Обладатель данной информации вправе разрешать или ограничивать доступ к ней других лиц (физических и юридических), использовать ее по своему усмотрению, а также защищать установленными законами способами свои права в случае ее незаконного получения или использования иными лицами без его согласия.

К. и П., руководствуясь корыстным мотивом, преследуя цель личного обогащения, действуя умышленно и осознавая, что без использования абонентской карты и заключения абонентского договора, они не обладают правом доступа к компьютерной информации ОАО «НТВ-ПЛЮС», имея специальные знания и опыт работы с компьютерной техникой, решили совершить неправомерный доступ к ней с последующим ее копированием.

27 марта 2007 года в дневное время К. в ходе телефонного разговора с незнакомым ему ранее Б. договорился об установке ему по месту проживания системы спутникового телевидения ОАО «НТВ-ПЛЮС» без использования абонентской карты и заключения абонентского договора. При этом Б. не был осведомлен о том, что в дальнейшем им будет осуществляться несанкционированный просмотр закрытых каналов спутникового телевидения ОАО «НТВ-ПЛЮС».

29 марта в 18 часов К. и П. прибыли на квартиру Б. При себе они имели набор необходимых инструментов и спутниковое оборудование. Там они произвели монтаж спутниковой антенны, которую установили на балконе, и протянули коаксиальный кабель от спутниковой антенны до находящегося в квартире Б. системного блока компьютера. После этого К. и П. осуществили ориентирование спутниковой антенны в направлении спутника Eutelsat W4 ОАО «НТВ-ПЛЮС» и провели настройку антенны на прием сигнала с него, используя принесенный с собой ресивер, при этом подключив его к находящемуся в вышеуказанной квартире компьютеру через ТВ-тюнер. Затем К. получил от Б. денежные средства в сумме 2500 руб. за выполненную работу, и договорился с последним о том, что его компьютер будет настроен для просмотра закрытых каналов спутникового телевидения ОАО «НТВ-ПЛЮС» на следующий день. После этого К. и П., забрав принесенные с собой инструменты и ресивер, ушли из квартиры Б.

30 марта 2007 года примерно в 14 часов П. на принадлежащем ему автомобиле ВАЗ 21093 приехал на квартиру Б. Там он, реализуя их совместный с К. умысел на неправомерный доступ к охраняемой законом компьютерной информации ОАО «НТВ-ПЛЮС», поместил в разъем системного блока персонального компьютера карту для приема сигналов цифрового телевидения (DVB-карту) и присоединил к ней коаксиальный кабель, ведущий к спутниковой антенне, ранее установленной К. на балконе Б. После этого П. посредством мобильного телефона подключился к сети Интернет, скопировал на жесткий диск системного блока компьютера Б. программу для просмотра каналов телевидения и программу-плагин.

Согласно заключению судебной компьютерной экспертизы № 1, программа-плагин является программой для ЭВМ, которая предназначена для имитации работы модуля системы защиты информации от несанкционированного доступа Viaccess, используемой в рамках действующего российского законодательства ОАО «НТВ-ПЛЮС». Программа-плагин позволяет копировать компьютерную информацию, содержащуюся в системах спутникового телевидения, в частности, в системе спутникового телевидения ОАО «НТВ-ПЛЮС». Такой компьютерной информацией являются потоки служебной информации, необходимые для просмотра закрытых телевизионных каналов (ECM-сообщения). Результатом работы данной программы-плагина может быть, в том числе, возможность просмотра закрытых спутниковых телевизионных каналов без абонентской карты, включая возможность просмотра каналов, вещаемых ОАО «НТВ-ПЛЮС».

Из заключения судебной компьютерной экспертизы № 2 следует, что система спутникового телевидения ОАО «НТВ-ПЛЮС» является системой ЭВМ с радиоканалом передачи данных. Кроме того, в системе ЭВМ ОАО «НТВ-ПЛЮС» содержится следующая компьютерная информация:

- скремблированные аудио- и видеопотоки для каждого спутникового телевизионного канала ОАО «НТВ-ПЛЮС»;
- поток ECM-сообщений для каждого спутникового телевизионного канала ОАО «НТВ-ПЛЮС»;
- поток EMM-сообщений для каждого абонента ОАО «НТВ-ПЛЮС»;
- поток DW для каждого спутникового телевизионного канала ОАО «НТВ-ПЛЮС»;
- иные служебные потоки данных.

П., реализуя их совместный с К. умысел на неправомерный доступ к охраняемой законом компьютерной информации ОАО «НТВ-ПЛЮС», копирование информации в системе ЭВМ, настроил программу-плагин для просмотра закрытых спутниковых каналов ОАО «НТВ-ПЛЮС». Для этого П. в конфигурационный файл плагина указал IP-адрес сервера «кард-шаринга» и порт подключения к нему, протокол взаимодействия между клиентом и сервером, имя пользователя и пароль, а также ключ шифрования.

Затем П. запустил установленную им ранее программу для просмотра каналов телевидения со встроенной в нее программой-плагином, после чего начался процесс копирования компьютерной информации ОАО «НТВ-ПЛЮС».

В результате преступных действий К. и П. стал возможным несанкционированный, без абонентской карты и абонентского договора ОАО «НТВ-ПЛЮС», просмотр закрытых телевизионных спутниковых каналов, посредством копирования компьютерной информации ОАО «НТВ-ПЛЮС», а именно потоков служебной информации, необходимых для просмотра закрытых телевизионных каналов (ECM-сообщений). Данная информация относится к конфиденциальной и охраняется законом, так как в соответствии со ст. 16 Федерального закона «Об информации, информационных технологиях и о защите информации» (от 27.07.2006 № 149-ФЗ) *«защита информации представляет собой принятие правовых, организационных и технических мер, направленных на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации; соблюдение конфиденциальности информации ограниченного доступа; реализацию права на доступ к информации».*

За свою работу П. получил от Б. денежные средства в сумме 3000 руб. Затем он пояснил, что за просмотр платных каналов спутникового телевидения ОАО «НТВ-ПЛЮС» Б. необходимо будет платить 250 руб. в месяц. Деньги следует передавать лично Г. («курьеру фирмы»), который будет по предварительному телефонному звонку приезжать к Б.

По описанной схеме К., П. и Г. в течение 2007 года был совершен ряд аналогичных преступлений.

В ходе судебного заседания подсудимые К., П. и Г. в инкриминируемых им деяниях виновными себя признали полностью, согласились с предъявленным им обвинением, указав, что обстоятельства совершения ими неправомерных доступов к компьютерной информации изложены в обвинительном заключении верно, и поддержали свое ходатайство о постановлении приговора без проведения судебного разбирательства (рассмотрение уголовного дела в особом порядке).

30 июля 2008 года К., П. и Г. были признаны виновными в совершении преступлений, предусмотренных ч. 2 ст. 272 и ч. 1 ст. 273 Уголовного кодекса Российской Федерации.

По совокупности совершенных преступных деяний, а также, учитывая роль каждого участника преступной группы, суд определил им следующие виды наказаний:

К., как организатор, был приговорен к трем годам лишения свободы условно с испытательным сроком два года и штрафом в размере 7000 руб.;

П. и Г. было назначено наказание в виде двух лет и шести месяцев лишения свободы условно с испытательным сроком один год и шесть месяцев, а также штрафом в размере 5000 руб. каждому.

Осужденных суд также обязал в течение всего срока отбытия наказания не менять своего место жительства без уведомления специализированного органа, осуществляющего их исправление, и два раза в месяц являться на регистрацию в уголовно-исполнительную инспекцию.

Следует обратить внимание на то, что специализированными подразделениями по борьбе с преступлениями в сфере компьютерной информации и высоких технологий – подразделениями «К» МВД России – в 2007–2008 годах была пресечена деятельность преступных групп, которые совершали преступления аналогичными способами в других регионах Российской Федерации. Практически по всем эпизодам преступной деятельности их вина была полностью доказана, что позволило обоснованно привлечь их к уголовной ответственности и справедливо осудить за совершенные преступные деяния. ■