УДК [343.98:343.53]:656.254.1

СРЕТЕНЦЕВ Н.И.,
СРЕТЕНЦЕВ Д.Н.

Особенности криминалистической характеристики преступлений в сфере спутникового (цифрового) телевидения и расследования данной категории преступлений

Рассматриваются особенности криминалистической характеристики преступлений, связанных с неправомерным использованием услуг в сфере спутникового телевидения. Обращается внимание на высокую латентность преступлений данного вида. Приводятся примеры раскрытия и расследования преступлений данной категории. Выделяется специфика криминалистической характеристики преступлений в сфере спутникового телевидения, которая включает в себя сведения: о личности правонарушителя; о целях и мотивах противоправных действий; о программно-аппаратных средствах и методах совершения преступления; о видах информации и местах противоправных действий в отношении объектов посягательства; о потерпевшей стороне. Рассматриваются особенности получения доказательственной информации при проведении следственных осмотров, обысков, судебных экспертиз в процессе расследования преступлений данной категории.

Ключевые слова: преступления в сфере спутникового (цифрового) телевидения, криминалистическая характеристика преступлений, отдел «К», следственные действия, следственный осмотр, обыск, судебная экспертиза.

Практика последних лет свидетельствует о глобальном внедрении цифровых технологий во все сферы общественных отношений. Существует ряд способов, позволяющих приносить незаконную выгоду путем совершения преступлений, связанных с использованием высоких (информационных) технологий. Один из них – совершение преступлений, совершаемых в сфере спутникового (цифрового) телевидения.

С увеличением количества абонентов спутникового телевидения увеличивается и процент преступлений, связанных с неправомерным использованием данных услуг. При этом истинные сведения о преступной активности в сфере спутникового (цифрового) телевидения до сих пор остаются скрытыми, латентность преступности в рассматриваемой сфере весьма высока.

Анализ следственной практики расследования преступлений в сфере спутникового (цифрового) телевидения свидетельствует о том, что, хотя деятельность правоохранительных органов в этом направлении в последние годы активизировалась, можно привести лишь единичные примеры раскрытия преступлений данной категории.

Так, сотрудниками отдела «К» УВД по Курской области совместно с представителями ОАО «НТВ-ПЛЮС» были выявлены, а затем задержаны участники преступной группы, которые посредством использования специальных программ для ЭВМ осуществляли неправомерный доступ к охраняемой законом компьютерной информации компании «НТВ-ПЛЮС». Это первый в России задокументированный случай хищения «ключей» для просмотра закрытых спутниковых телеканалов.

СУ при УВД по Курской области было возбуждено уголовное дело по признакам состава преступления, предусматривающего

ответственность по ч. 2 ст. 272 УК РФ (неправомерный доступ к компьютерной информации) и ч. 1 ст. 273 УК РФ (создание, использование и распространение вредоносных программ)[1].

Еще один пример. Житель г. Калининграда предлагал услугу по подключению к закрытым спутниковым каналам без заключения договора с соответствующими организациями и уплаты абонентской платы, стоимость нелегального подключения составляла 11 400 рублей.

Проверяя данную информацию, сотрудники отдела «К» УВД по Калининградской области организовали «контрольную закупку» и взяли «умельца» с поличным.

Следствием было установлено, что подключение производилось с использованием компьютерных программ, созданных данным гражданином для копирования конфиденциальной информации. С их помощью могли быть получены коды доступа, после чего подключение особого труда не составляло.

Суд Центрального района признал данного гражданина виновным в совершении преступлений, предусмотренных ч. 1 ст. 272 (неправомерный доступ к компьютерной информации), ч. 1 ст. 273 УК РФ (создание, использование и распространение вредоносных компьютерных программ)[2].

Из приведенных выше примеров видно, что преступления в сфере спутникового (цифрового) телевидения квалифицируются по статьям 272, 273 Уголовного кодекса РФ. Однако на практике встречаются подобные преступления, совершенные иным способом: « … в помещении бара г. Омска гражданин, действуя с корыстной целью, путем обмана, осознавая, что причиняет имущественный ущерб собственнику, то есть ОАО «НТВ ПЛЮС», без цели хищения, установил контрафактную смарт-карту «MYN MM COLDCARD», предназначенную для приема каналов спутникового телевидения, в терминал для приема таких каналов, находящийся в помещении указанного бара…». Данное преступление в ходе его расследования было квалифицировано по ч. 1 ст. 165 УК РФ (причинение имущественного ущерба путем обмана или злоупотребления доверием)[3].

Основой методики расследования любого вида преступления, в том числе преступлений в сфере спутникового телевидения, является криминалистическая характеристика данного вида преступления. С содержательной точки зрения криминалистическая характеристика преступлений трактуется как «система сведений о типичных криминалистически значимых признаках (чертах, особенностях) преступлений определенного вида или категории, анализ которых позволяет делать выводы об оптимальных путях их раскрытия и расследования»[4]. Иными словами, это информационная модель, содержащая комплекс выявленных и взаимосвязанных криминалистически значимых особенностей (признаков), характеризующих отдельные виды и группы преступлений.

Криминалистической характеристике преступлений в сфере спутникового телевидения присуща определенная специфика. Она включает в себя сведения о личности правонарушителя; о целях и мотивах противоправных действий; о способе совершения преступления; о программно-аппаратных средствах и методах совершения преступления; о видах информации и местах противоправных действий в отношении объектов посягательства; о потерпевшей стороне.

Правонарушителями в сфере спутникового телевидения, как правило, являются лица, преследующие корыстные цели. Это профессионалы, представляющие угрозу личности, обществу, государству. В большинстве случаев они входят в криминальные группы.

К мотивам совершения подобных преступлений можно отнести корысть, исследовательский интерес.

Основной целью совершения преступлений в сфере спутникового телевидения, как правило, является получение незаконной прибыли путем хищения электронных данных, составляющих коммерческую тайну, и использования контрафактного оборудования и вредоносного программного обеспечения.

В подобных преступлениях потерпевшей стороной выступают юридические лица (учреждения, организации и предприятия всех форм собственности) и граждане.

Способ совершения подобных преступлений слагается из комплекса специфических действий правонарушителя по подготовке, совершению и маскировке преступления. Обычно преступники, совершая эти действия, оставляют определенные следы, которые впоследствии позволяют восстановить

картину происшедшего, получить представление о своеобразии преступного поведения правонарушителя, о его личностных данных[5].

Типичными орудиями подготовки, совершения и сокрытия преступлений в сфере компьютерной информации (и в частности в сфере спутникового телевидения) являются:

– средства электронно-вычислительной техники (СВТ);

– специальные технические средства (СТС), предназначенные (разработанные, приспособленные, запрограммированные) для негласного получения (изменения, уничтожения, блокирования) информации, нарушения работы ЭВМ, системы ЭВМ или их сети;

– разнообразные магнитные материалы и технические устройства, генерирующие направленное электромагнитное излучение;

– электромонтажный инструмент и материалы;

– контрольно-измерительные приборы и устройства;

– средства систем электросвязи и их компоненты.

Наиболее широко применяемым универсальным орудием совершения преступления в сфере компьютерной информации является ПЭВМ или ПК – персональный компьютер с соответствующим программным обеспечением и периферийным оборудованием[6].

Практика показывает, что преступления в сфере спутникового телевидения совершаются обычно группой из двух и более человек, хотя не исключена возможность работы преступника-одиночки, который умеет работать с компьютерной техникой, хорошо представляет, как функционирует система спутникового телевидения. Интерес обычно представляет информация, содержащая коммерческую тайну (алгоритмы шифрования спутникового сигнала и т.д.).

Как это уже было отмечено выше, криминалистическая характеристика – это информационная модель, содержащая комплекс выявленных и взаимосвязанных криминалистически значимых особенностей (признаков), характеризующих в нашем случае преступления в сфере спутникового телевидения, анализ которых (особенностей, признаков) позволяет делать выводы об оптимальных путях раскрытия и расследования преступлений данного вида. Доказательства совершенного преступления могут быть получены в процессе осуществления следственных действий как на первоначальном, так и на последующих этапах расследования. В настоящей статье авторы рассматривают особенности проведения трех видов следственных действий: следственного осмотра; обыска; судебных экспертиз.

При расследовании преступлений в сфере спутникового (цифрового) телевидения наибольшее количество доказательств может быть получено в ходе следственного осмотра. Следственный осмотр представляет собой непосредственное обнаружение и исследование объектов, их признаков, свойств, состояния, имеющих значение для расследуемого уголовного дела.

Объекты, подлежащие осмотру по данной категории дел, можно условно разделить на четыре основные группы: 1) помещения; 2) средства вычислительной техники и специальное оборудование для приема сигнала цифрового телевидения; 3) носители информации; 4) документы.

Для участия в следственном осмотре обязательно привлечение как специалистов экспертно-криминалистических подразделений, специализирующихся на исследованиях в сфере высоких технологий, так и специалистов в области настройки систем спутникового (цифрового) телевидения. Кроме того, может потребоваться помощь специалиста в области программирования.

Значительную часть доказательств по делам данной категории можно получить в ходе проведения обыска – принудительного процессуального действия, содержанием которого является обследование объектов в целях отыскания и изъятия скрываемых доказательств совершенного преступления.

Цели обыска при расследовании преступлений в сфере спутникового (цифрового) телевидения заключаются в обнаружении, фиксации и изъятии объектов, используемых для несанкционированного приема сигналов спутникового «цифрового» телевидения, а также выявлении и задержании разыскиваемых и подозреваемых лиц.

Результативность обыска напрямую зависит от взаимодействия следователя со специализированным органом дознания –

отделом «К» при Управлении специальных технических мероприятий республики, края (области). С его помощью обеспечивается должная оперативная осведомленность следователя об обстоятельствах, связанных с проведением обыска, которая помогает избежать ряда тактических ошибок, а также грамотно решить вопрос о привлечении к его проведению высококвалифицированных специалистов в области компьютерной техники и понятых, имеющих определенные знания в этой сфере[7].

На заключительном этапе обыска при расследовании преступлений в сфере спутникового (цифрового) телевидения помимо составления протокола обыска и описи к нему целесообразно изготовить схему подключения элементов системы спутникового (цифрового) телевидения.

Механизм следообразования при совершении преступлений, сопряженных с использованием компьютерных средств и технологий, достаточно сложен. Для того чтобы извлечь необходимую криминалистически значимую информацию на этапах предварительного и экспертного исследования различных следов, в процессе расследования преступлений данной категории, необходимо широкое использование специальных знаний. Специальные знания могут применяться как в процессуальной, так и в не процессуальной формах. Об одной из процессуальных форм использования специальных знаний – привлечения специалистов для участия в следственных осмотрах – авторами говорилось выше. Второй процессуальной формой использования специальных знаний является судебная экспертиза.

В настоящее время в следственной практике возникают сложности относительно определения вида экспертных исследований, назначаемых в целях исследования следов «взлома» систем спутникового телевидения. Представляется, что с учетом стоящих перед следствием задач и специфики объектов исследования способ несанкционированного доступа к системам спутникового (цифрового) телевидения может быть установлен исследованием компьютерной информации путем производства компьютерной судебной экспертизы.

Целесообразно представить эксперту всю проектную документацию на исследуемую систему (если таковая имеется), а также имеющиеся данные о ее сертификации.

Объектами компьютерной экспертизы по данным делам могут стать карты для приема сигналов спутникового (цифрового) телевидения и программное обеспечение, предназначенное для имитации санкционированного доступа к системам спутникового (цифрового) телевещания.

В заключение отметим, что методика расследования преступлений в сфере спутникового (цифрового) телевидения как одного из новых видов преступлений требует дальнейшей, более детальной научной разработки. На наш взгляд, это является конкретной задачей как одного из разделов науки криминалистики (криминалистической методики), так и криминалистической науки в целом.

---

[1] Материалы сайта: www.ntvplus.ru [Электронный ресурс].

[2] Материалы сайта: http://mirant.kiev.ua/news/2010-06-01-2500 [Электронный ресурс].

[3] См.: Архив Следственного управления при УВД-2 Центрального АО г. Омска за 2002 г. Уголовное дело № 329462 // Привлечение в качестве обвиняемого: учебно-практическое пособие / Н.П. Ефремова, В.В. Кальницкий. Омск: Омская академия МВД России, 2007. С. 43.

[4] См., например: Криминалистика: Учебник для студентов вузов / Под ред. А.Ф. Волынского, В.П. Лаврова. 2-е изд., перераб. и доп. М.: ЮНИТИ-ДАНА: Закон и право, 2009. С. 29.

[5] См. подр.: Дуленко В.А. Преступления в сфере высоких технологий: учебное пособие / В.А. Дуленко, Р.Р. Мамлеев, В.А. Пестриков. М.: ЦОКР МВД России, 2010. С.135–137.

[6] См. подр.: Вехов В.Б., Рогозин В.Ю. Методика расследования преступлений в сфере компьютерной информации. 2002. [Электронный ресурс]. Режим доступа: http://www. crime.vl.ru/books

[7] Дуленко В.А. Преступления в сфере высоких технологий: Учебное пособие / В.А. Дуленко, Р.Р. Мамлеев, В.А. Пестриков. М.: ЦОКР МВД России, 2010. С. 150.