УДК 343.2/7 DOI 10.51980/2686-939X_2021_3_135

НЕКОТОРЫЕ НОВАЦИИ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ В СФЕРЕ ТЕЛЕКОММУНИКАЦИИ И КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

SOME INNOVATIONS OF CRIMES COMMITTED IN THE FIELD OF TELECOMMUNICATIONS AND COMPUTER INFORMATION

Алескеров Вагиф Исмаилович,
профессор кафедры оперативно-технических мероприятий органов внутренних дел Всероссийского института повышения квалификации сотрудников МВД России (г. Домодедово), кандидат юридических наук, доцент

valeskerov@mvd.ru

Малыгина Ольга Валериевна,
доцент кафедры оперативно-технических мероприятий органов внутренних дел Всероссийского института повышения квалификации сотрудников МВД России (г. Домодедово), кандидат психологических наук

olia.vod@yandex.ru

Ключевые слова:
криминогенная обстановка, телекоммуникации, компьютерная информация, несанкционированное использование информации, субъективная особенность личности преступника.

В статье рассматриваются вопросы криминогенной обстановки, складывающейся в современных реалияха, а также некоторые статистические сведения о совершаемых преступлениях на территории Российской Федерации. Аргументируется потребность в урегулировании некоторых пробелов в действующем уголовном законодательстве и усилении ответственности в отношении вопроса несанкционированного использования информации, хранящейся на различных электронных носителях.

Keywords:
criminal situation, telecommunications, computer information, unauthorized use of information, subjective feature of the criminal's personality.

The article deals with the issues of the criminogenic situation, as well as some statistical information about the crimes committed on the territory of the Russian Federation, which is developing in modern realities. In this connection, there is a need to address some gaps in the current criminal legislation and strengthen responsibility in relation to the issue of unauthorized use of information stored on various electronic media.

В настоящее время анализ складывающейся криминогенной обстановки, а также имеющиеся статистические сведения о совершаемых преступлениях на территории Российской Федерации позволяют сделать вывод о том, что преступления, совершаемые в сфере телекоммуникаций и компьютерной информации, ежегодно имеют тенденцию к значительному росту (рис. 1).

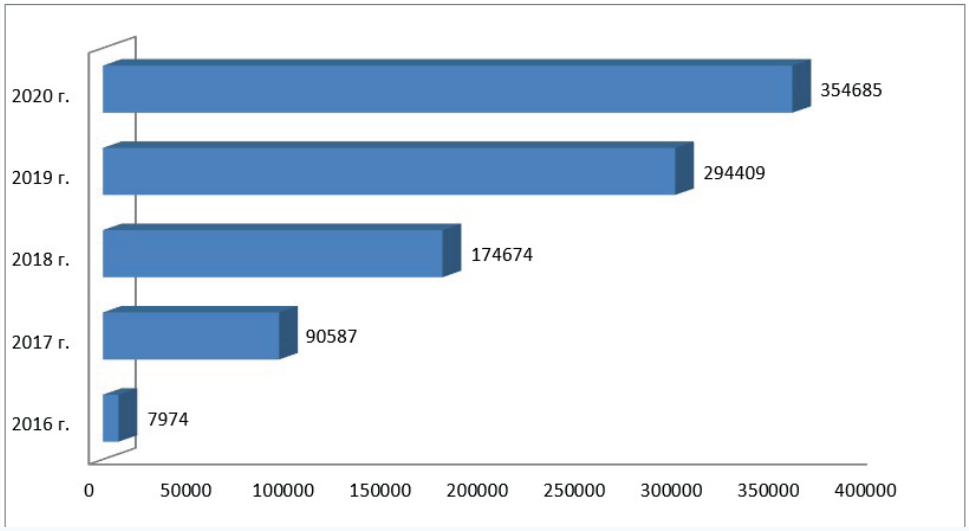

Рис. 1. Сведения о количестве зарегистрированных преступлений в сфере телекоммуникаций и компьютерной информации

Рассматриваемый вид преступлений в отечественном уголовном законодательстве появился сравнительно недавно. Данные преступления в подавляющем большинстве совершаются изощренно, носят многогранный и латентный характер, их совершение причиняет огромный вред современному обществу, в результате которого создаются порой непоправимые проблемы правообладателям информации разного рода во многих сферах деятельности.

На сегодняшний день участились случаи незаконного использования компьютерной информации, в связи с чем возникает потребность в урегулировании некоторых пробелов в действующем уголовном законодательстве и усилении ответственности в отношении лиц, совершающих несанкциониро-

ванное использование информации, хранящейся на различных электронных носителях.

Уголовные дела, возбужденные по преступлениям в сфере телекоммуникаций и компьютерной информации, имеющиеся в производстве и оконченные расследованием, переданные в суд для дальнейшего их рассмотрения и полного разрешения, позволяют сделать вывод, что в сложившейся ситуации во многих организациях, предприятиях, учреждениях и отраслях производства накопленная компьютерная информация остается наиболее уязвимой и создает лицам, склонным к совершению преступлений рассматриваемого вида, благоприятные условия для совершения противоправных деяний.

Оперативные сотрудники, наделенные правами раскрывать преступления в сфере телекоммуникаций и компьютерной информации, ранее не имели практических наработок и теоретических рекомендаций по раскрытию и расследованию преступлений в этой сфере.

Компьютеризация всех слоев населения представляет собой социально значимое явление, ее достижения могут быть использованы не только в хороших, позитивных намерениях (познавательных целях, в целях реализации прав пользователей), но и в целях совершения преступлений компьютерной направленности. Компьютерные преступления носят специфичный характер, в настоящее время они являются новацией в системе уголовного права. Способы их совершения настолько разнообразны и изощренны, что порой сотрудникам управлений «К» при документировании и раскрытии данного вида преступлений приходится сталкиваться с определенными трудностями, в связи с чем разрабатываются и внедряются новые формы и методы оперативно-розыскной деятельности. Необходимо заметить, что одним из важнейших составляющих элементов криминалистической характеристики методики раскрытия преступлений в сфере телекоммуникаций и компьютерной информации (компьютерных преступлений) является субъективная особенность личности преступника, которая на начальном этапе раскрытия преступлений характеризуется лишь скудной информацией, в связи с чем нельзя не согласиться с рядом мнений специалистов, проводивших исследования в данной области, которые предлагают учитывать такие составляющие, как пол, возраст, социальное происхождение, уровень образования, род занятий, наличие специальности, семейное положение, социальный статус, уровень материальной обеспеченности, место жительства, а также места проведения досуга и возможная принадлежность к определенной субкультуре [3, с. 5]. Иными словами, немаловажное значение в раскрытии любого вида компьютерного преступления играет характерологическая особенность психологии личности преступника. Именно детальная информация о личности преступника позволит при глубоком анализе определить и сузить круг подозреваемых лиц, установить мотив

и способ совершения преступления, а также выдвинуть версии, что верно сориентирует и приблизит оперативных сотрудников и следователей к проведению оперативно-розыскных (далее – ОРМ), специальных технических мероприятий (далее – СТМ) и следственных действий, способствующих раскрытию данного вида преступлений.

Понятие «компьютерная информация» является не менее многозначным, чем понятие «информация». Ее место в системе правоотношений, возникающих в информационной сфере, до сих пор является предметом научных дискуссий, которые пока не завершились формированием общепризнанного научного и законодательного определения, поскольку многообразие его толкования отображает весьма сложный характер реального мира.

Проблемы в правоприменительной практике связаны с тем, что, несмотря на важность точного формализованного представления о сущности и свойствах компьютерной информации (как предмета преступления), на законодательном уровне определение «компьютерная информация» появилось относительно недавно. Однако в специальной и учебной литературе предложено множество определений рассматриваемого термина.

Мы попытались дать определения понятиям «компьютерная информация» и «телекоммуникационная сеть» с позиции науки криминалистики. Так, по нашему видению, компьютерная информация как предмет преступления является организационно-упорядоченными сведениями (сообщениями, данными), зафиксированными на машинном носителе или находящимися в оперативной памяти компьютера либо в информационно-телекоммуникационной сети, с реквизитами, позволяющими их идентифицировать, имеющими собственника либо иного законного владельца. Телекоммуникационные сети нами представляются как технические средства (механизмы, оборудование) и устройства информационного обмена, а также программные средства, при помощи которых субъекты информационного права могут обмениваться информацией и обращать информацию в пространстве и времени через технические каналы связи (электросвязи, светоканалы, радиоканалы), представляющие собой технологические системы с различными видами передач (аналоговое и цифровое телевидение, различные виды работы в Интернете, факсимильная, телеграфная, телефонная и др., включая обмен информацией между электронными устройствами и другие виды документальных сообщений) (рис. 2).

Таким образом, уголовно-правовой защите подлежит любая информация, неправомерное обращение с которой может нанести ущерб ее собственнику (владельцу, пользователю). Закрепление предложенных определений в базовом для этой сферы законодательстве, например в Федеральном законе от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о за-

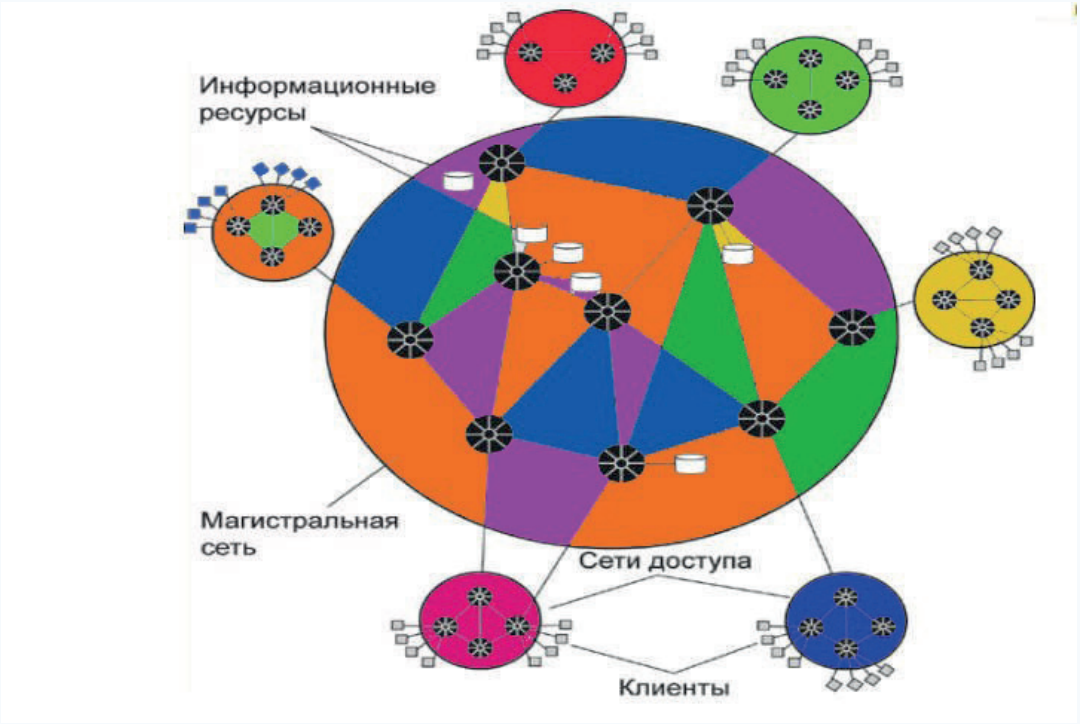

Рис. 2. Телекоммуникационная сеть

щите информации», позволит, на наш взгляд, существенно сократить ошибки в правовом применении рассматриваемых уголовно-правовых норм [1, с. 32].

В настоящее время одними из современных видов совершаемых преступлений являются преступления в сфере телекоммуникаций и компьютерной информации.

Телекоммуникационные системы и компьютерная информация внедряются во все сферы жизнедеятельности человека, представляют собой сеть развитых технических средств по сбору, передаче, обработке и хранению информации, поэтому они наиболее часто подвержены пристальному вниманию со стороны преступников.

Преступления, совершаемые в сфере телекоммуникаций и компьютерной информации, являются одной из разновидностей преступлений, входящих в гл. 28 УК РФ «Преступления в сфере компьютерной информации», а некоторые из них могут тесно взаимодействовать с иными видами преступлений, которые входят в другие главы УК РФ (например, ст. 242.1 УК РФ «Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних», ст. 242.2 УК РФ «Использование несовершеннолетнего в целях изготовления порнографических материалов или предметов», которые входят в гл. 25 УК РФ «Преступления против здоровья населения и общественной нравственности»).

Следует отметить, что сотрудниками Бюро специальных технических мероприятий МВД России постоянно проводятся комплексы мероприятий, направ-

ленных на осуществление как оперативно-поисковых, оперативно-розыскных мер, так и на выявление, пресечение и раскрытие преступлений, предусмотренных ст. 132 УК РФ «Насильственные действия сексуального характера», ст. 135 УК РФ «Развратные действия», ст. 242.2 УК РФ «Использование несовершеннолетнего в целях изготовления порнографических материалов или предметов».

Рассматриваемые виды преступлений обладают следующими криминалистическими особенностями.

1. Компьютерная информация достаточно просто и быстро преобразуется из одной объектной формы в другую, копируется (размножается) на различные виды машинных носителей и пересылается на любые расстояния, ограниченные только радиусом действия современных средств телекоммуникационных сетей.

2. При изъятии (копировании) информации, зафиксированной в телекоммуникационных сетях, а также любого вида компьютерной информации (в отличие от изъятия материального предмета) она может сохраниться в первоисточнике.

3. В большинстве случаев информация, в том числе и телекоммуникационная, становится продуктом общественных отношений, имеет определенную цену и является предметом купли-продажи [2, с. 69].

Такого рода общественные отношения закреплены в Федеральном законе от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». В связи с этим новые информационные технологии не только дали толчок в плане прогресса общества, но и стимулировали возникновение и развитие новых форм преступности. Прогресс в области компьютерной техники и телекоммуникационной среде предоставил злоумышленникам широкие возможности неправомерного доступа к новым техническим средствам и дальнейшему их использованию в противоправных целях.

Как нам известно, виды преступлений в сфере компьютерной информации представлены в гл. 28 УК РФ, а именно:

– ст. 272 УК РФ «Неправомерный доступ к компьютерной информации»;

– ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ»;

– ст. 274 УК РФ «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей»;

– ст. 274.1 УК РФ Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации».

В связи с тем, что преступления, совершаемые в телекоммуникационных сетях, являются новой разновидностью сферы компьютерных преступлений, законодатель ввел новые нормы неизвестных ранее составов преступлений, что

вызвало необходимость установления уголовной ответственности за причинение вреда в связи с использованием той или иной информации во многих сферах деятельности.

В свое время И.Г. Чекунов говорил о том, что все большее количество государств ставит перед собой в качестве приоритетной цели создание информационного общества на основе широкого внедрения телекоммуникационных технологий. Одной из определяющих задач на этом пути является формирование комплексной инфраструктуры для оказания электронных услуг населению. Постановка этой задачи в России вполне оправданна, поскольку сегодня компьютеры, мобильные средства связи, программное обеспечение, телекоммуникационные системы охватывают практически все сферы жизнедеятельности человека, общества и государства [4, с. 9]. Однако выстроенные глобальные информационные сети, востребованные современным цивилизованным обществом, все чаще используются и лицами, склонными к совершению различного рода преступлений, и, к нашему сожалению, статистические данные говорят, что такое незаконное использование сферы телекоммуникаций и компьютерной информации из года в год растет (рис. 3) [4, с. 10].

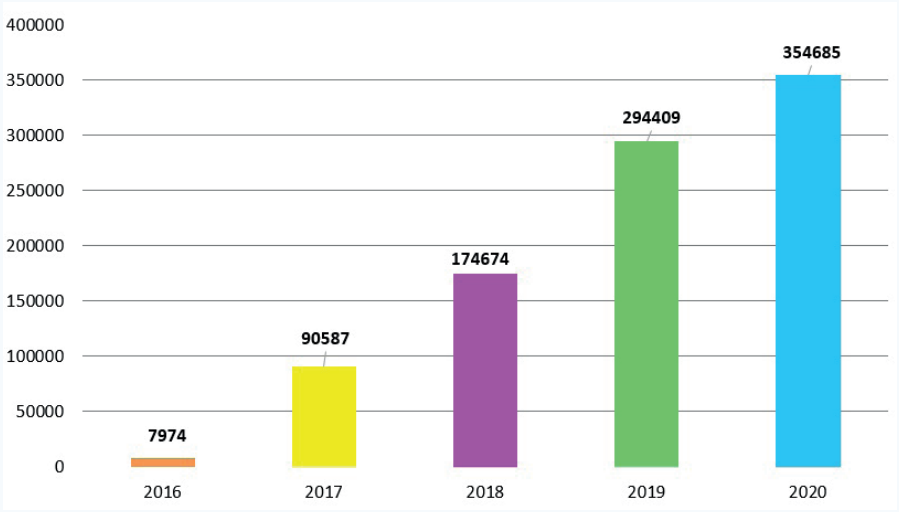

Рис. 3. Сведения о количестве зарегистрированных преступлений в сфере телекоммуникаций и компьютерной информации

Существенно то, что предметом данных преступлений является информация, находящаяся в телекоммуникационных сетях. По данным компании «Лаборатория Касперского», ежедневно злоумышленники создают и используют новые способы заражения компьютерными вирусами и обходят установленные, не отвечающие современным требованиям, способы защиты информации, хранящейся на ПЭВМ. Известно, что количество созданных вредоносных программ ежедневно составляет от 250 до 300 тысяч.

Кроме того, предметом компьютерных преступлений является и оборудование, обеспечивающее информационно-телекоммуникационные процессы.

Непосредственным объектом данных преступных деяний является безопасность информационно-телекоммуникационных систем, базирующихся на использовании ИТКС.

Объективная сторона компьютерных преступлений, и в частности преступлений, совершаемых в телекоммуникационных сетях, характеризуется как действием, так и бездействием. Действие (бездействие) сопряжено с нарушением прав и интересов по поводу пользования информацией, находящейся в телекоммуникационной сети.

Компьютерные преступления имеют материальные составы. Действие (бездействие) должно причинить значительный вред правам и интересам личности, общества или государства (исключением является преступление с формальным составом, предусмотренное ч. 1 ст. 273 УК РФ «Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации». Преступные последствия конкретизируются в законе применительно к конкретным видам компьютерных преступлений. Между деянием и последствиями обязательно должна быть установлена причинная связь, относящаяся к элементам криминалистически значимой информации.

Субъективная сторона компьютерных преступлений, а также преступлений, совершаемых в телекоммуникационных сетях, характеризуется умышленной виной. Деяние, совершенное по неосторожности, признается преступлением только тогда, когда это специально предусмотрено соответствующей статьей Особенной части УК РФ. Неосторожная форма вины названа в Особенной части лишь применительно к квалифицированным видам компьютерных преступлений, предусмотренных ч. 2 ст. 273 УК РФ и ч. 2 ст. 274 УК РФ.

Субъект компьютерного преступления общий – лицо, достигшее 16 лет. В ст. 274 УК РФ «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» и ч. 2 ст. 272 УК РФ формулируются признаки специального субъекта – лицо, имеющее доступ к ЭВМ, системе ЭВМ или их сети.

Однако необходимо заметить, что перечисленные статьи гл. 28 УК РФ в зависимости от создаваемой криминогенной обстановки и появления новых способов совершения преступлений иногда требуют существенных исследований и новых дополнений.

Предлагаем рассмотреть некоторые виды преступлений, совершаемых с использованием ЭВМ (преступления, в которых компьютер является средством достижения цели):

– разработка сложных математических моделей, которые в последующем будут использованы при осуществлении преступного замысла злоумышленника;

– создание «логических бомб» – программ, которые срабатывают при выполнении определенных условий и частично или полностью выводят из строя программное обеспечение компьютерной системы;

– ввод в программное обеспечение «логических бомб»;

– совершение преступления с общим названием «воздушный змей».

Рассмотрим пример данного вида преступления. Злоумышленники в нескольких банках открывают небольшие счета, и деньги «перегоняются» из одного банка в другой и обратно с естественной процентной надбавкой. Цель данной финансовой махинации направлена на то, чтобы информация о сумме перевода в первый банк доставлялась быстрее, чем поступающее платежное поручение из другого банка, до того, как будет обнаружено, что перевод не обеспечен необходимой денежной суммой. Данные денежные манипуляции осуществляются неоднократно, с каждым разом увеличивая конечную сумму, пока процентная ставка денежных переводов не будет устраивать мошенников и их преступный замысел не будет удовлетворен. В результате достижения преступной цели деньги с конечного счета присваиваются преступниками, которые впоследствии скрываются. В данной афере чем больше банков задействовано, тем больше и быстрее накапливается желаемая денежная сумма. Такой вид совершения преступления возможен при осуществлении операций при помощи компьютера.

Библиографический список

1. Алескеров, В.И. Информация как основной элемент, характеризующий преступления в телекоммуникационной сети / В.И. Алескеров, Ф.А. Куц // Вестник Всероссийского института повышения квалификации сотрудников МВД России. – Домодедово : ВИПК МВД России. – 2013. – № 2(26). – С. 32-37.

2. Алескеров, В.И. К вопросу о преступлениях, совершаемых в телекоммуникационных сетях / В.И. Алескеров, Ф.А. Куц // Вестник Всероссийского института повышения квалификации сотрудников МВД России. – Домодедово : ВИПК МВД России. – 2012. – № 3(23). – С. 67-69.

3. Ворошилова, Т.В. Социальная и психологическая характеристика личности компьютерного преступника / Т.В. Ворошилова. – М., 2009.

4. Чекунов, И.Г. Современные киберугрозы. Уголовно-правовая и криминологическая классификация и квалификация киберпреступлений / И.Г. Чекунов // Право и кибербезопасность. – 2012. – № 1. – С. 9-10.