УДК 343.9

Е.В. Кирилюк

РАССЛЕДОВАНИЕ ПРЕСТУПЛЕНИЙ В КОМПЬЮТЕРНОЙ СФЕРЕ

Преступления в компьютерной сфере являются довольно новым видом преступлений, расследование которых производится с 1991 г., когда традиционные виды преступлений имели место быть и до принятия нового уголовного законодательства. Преступления в компьютерной сфере являются наболевшей темой современного общества и заслуживают внимания органов внутренних дел. Компьютерная сфера включает в себя многочисленные программы и сеть Интернет, которая, в свою очередь, из-за большого объема информации и большого количества пользователей является легкой наживой для преступных элементов. В профессиональной среде компьютерную сферу называют информационными технологиями (ИТ). Понятие «информационные технологии» пришло в обыденную среду людей довольно таки недавно, в XX в., когда процесс информатизации начал набирать обороты. ИТ возникли в связи с развитием науки «Информатика» [1, с. 66].

С развитием компьютерных технологий развивается и преступность, которая начала распространяться на такой объект общественных отношений, который направлен на защиту компьютерной информации.

В современном мире почти каждый человек, у которого имеется техническое устройство в виде персонального компьютера, ноутбука, смартфона, планшета и иных источников информационных технологий, в какой-либо мере имеет компьютерную информацию, которая может по-разному выражаться.

Информационные технологии закрепились в уже устоявшемся информационном обществе. Они помогают обществу развиваться и быстро получать нужную ему информацию.

Не секрет, что именно компьютерные преступления в современном обществе занимают одну из лидирующих позиций среди всех нарушений уголовного законодательства. Особенно это было распространено в период обострения эпидемиологической обстановки по COVID-19 во всем мире, в том числе и в России.

Люди были изолированными от общества в связи с введением ограниченного правового режима, при котором не были доступны многие сферы жизнедеятельности, в том числе остались без работы и средств для жизни. Для заработка многие начали использовать все возможности

информационных систем и средств заработка дистанционным путем, используя компьютер.

Уголовное законодательство Российской Федерации выделяет целую главу, посвященную компьютерным преступлениям, в которой закреплены следующие виды преступлений:

1) неправомерный доступ к компьютерной информации;

2) создание, использование и распространение вредоносных компьютерных программ;

3) нарушение правил эксплуатации средств хранения, обработки и передачи компьютерной информации и информационно-телекоммуникационных сетей;

4) неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации;

5) нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети Интернет и сети связи общего пользования [2].

Наиболее распространенным средством неправомерного использования компьютерной информации, ответственность за которую предусмотрена ст. 272 Уголовного кодекса Российской Федерации (УК РФ), является фишинг. Он не является самостоятельным преступлением, а лишь средством, которым достигается преступный результат для копирования чужой информации. Фишинг подразумевает собой кражу личных данных, например, логина и пароля от почтовых сервисов или социальных сетей, номеров телефона, и наиболее распространенным является кража данных банковских платежных карточек.

Хищение данных с банковских платежных карточек, как правило, является первоначальным этапом совершения такого преступления, ответственность за которое предусмотрена п. «г» ч. 3 ст. 158 УК РФ, а именно: кража, совершенная с банковского счета, а равно в отношении электронных денежных средств.

Денежные средства, хранящиеся на банковских платежных карточках, являются электронными. Подавляющее большинство населения в современном обществе имеет при себе как минимум одну банковскую платежную карточку. Организации выплачивают заработные платы, премии, проводят иные денежные операции в электронном виде, путем зачисления их на банковские платежные карточки сотрудников. Поэтому, даже если человек привык к традиционному способу оплаты наличными, он не защищен на 100 % от совершения в отношении его противо-

правных действий, поскольку периода, который будет проходить от момента зачисления заработной платы до снятия ее, переведя в наличные средства, хватит, чтобы осуществить факт кражи.

При расследовании данного вида преступления следует установить, в какое точное время было совершено в отношении их противоправное деяние, после каких действий это произошло (путем мошеннических звонков-сбросов или же СМС).

При создании, использовании и распространении вредоносных компьютерных программ, которые были направлены на копирование, уничтожение, блокирование или модификацию компьютерной информации, либо же для взлома или уничтожения средств защиты этой информации, следует устанавливать, каким путем данные вредоносные программы попали на устройство потерпевшего.

Варианты попадания вредоносных программ на компьютер потерпевшего:

1) фишинговые сайты, на которых заведомо размещены файлы, содержащие в себе программы, предназначенные для совершения противоправных действий;

2) проверенные сайты, но по каким-либо причинам распространяющие файлы, содержащие в себе программы, предназначенные для совершения противоправных действий;

3) заведомая передача файлов по электронной почте, мессенджерам и иным средствам электронной передачи данных;

4) заражение компьютера путем физического воздействия на компьютер, которое выражается в непосредственном участии преступника, его действии, направленном на перенос файла с флеш-носителя, диска и иных портативных источников, на компьютер потерпевшего.

Вредоносные программы могут не только работать с компьютерной информацией, но и замедлять, а в некоторых случаях и полностью останавливать работу компьютера.

Поэтому при расследовании данного вида преступления следует устанавливать, на какие сайты в последнее время заходил потерпевший, скачивал ли он какие-либо файлы, получал ли сообщения от знакомых или незнакомых лиц посредством электронной почты или мессенджеров, кто имел, кроме него самого, доступ к компьютеру.

Преступления, совершаемые посредством нарушения правил эксплуатации средств обработки, хранения и передачи компьютерной информации, заключаются в самом деянии, вытекающем из ст. 274 УК РФ.

К средствам обработки, хранения и передачи компьютерной информации относят различные технические предметы: компьютеры, смартфоны, ноутбуки, банкоматы, флеш-носители, карты памяти и т. д.

Естественно, что лицо, нарушающее правила, должно быть ознакомлено с ними. Как правило, это указывается в должностной инструкции либо в договоре [3, с. 89].

Таким образом, при расследовании преступления данного вида следует в первую очередь установить лицо, которому был доверен носитель с компьютерной информацией, а после принимать меры к доказыванию его причастности к данной утере путем проведения оперативно-розыскных мероприятий и следственных действий.

Под неправомерным воздействием на критическую информационную инфраструктуру Российской Федерации подразумевают такое воздействие, которое может нанести ущерб системам управления в стратегических отраслях экономики и государственного управления, которые осуществляют свою деятельность посредством использования информационных технологий.

Как правило, субъектом данного преступления, ответственность за которое предусмотрена ст. 274 УК РФ, являются государственные органы, предприятия, учреждения и индивидуальные предприниматели, которым вверена в управление компьютерная информация стратегического назначения.

Для расследования такого преступления органам, осуществляющим расследование, нужно установить лиц, которые на правах организации осуществляют деятельность по защите данной информации, а также лиц, которые имеют к ней допуск. Как правило, такими лицами является IT-персонал, деятельность которого непосредственно связана с обеспечением безопасности критической информации.

Под нарушением правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети понимаются преступления, тем или иным образом связанные с экстремизмом или терроризмом.

Для расследования подобного преступления требуется много усилий для собирания доказательств по факту противоправного деяния, установления субъекта и в дальнейшем для принятия мер по восстановлению причиненного вреда Российской Федерации.

Таким образом, можно подытожить, что расследование преступлений в компьютерной сфере отличается от расследования традиционных видов преступлений, поскольку работа идет с использованием ИТ и IT-сферы.

1. Володченко, В.С. Понятие и классификация информационных технологий / В.С. Володченко, Д.С. Ланцова, Т.А. Миронова // Достижения науки и образования. – 2020. – № 12. – С. 66.

2. Уголовный кодекс Российской Федерации [Электронный ресурс] : 13 июня 1996 г., № 63-ФЗ : в ред. от 24.09.2022 г. / ЗАО «КонсультантПлюс». Россия. – М., 2022.

3. Стяжкина, С.А. Уголовно-правовые особенности квалификации нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (статья 274 УК РФ) / С.А. Стяжкина // Вестн. Удмурт. ун-та. Серия «Экономика и право». – 2021. – № 3. – С. 89.

УДК 343.98

Я.А. Климова

ЛИЧНОСТЬ НЕСОВЕРШЕННОЛЕТНЕГО ПРЕСТУПНИКА КАК ЭЛЕМЕНТ КРИМИНАЛИСТИЧЕСКОЙ ХАРАКТЕРИСТИКИ: НЕГАТИВНЫЕ ФАКТОРЫ ФОРМИРОВАНИЯ

Приоритетной задачей на протяжении нескольких десятилетий является борьба с преступностью несовершеннолетних. Эта проблема вызывает серьезную обеспокоенность государства, общества и всех граждан в силу своей масштабности, комплексности и негативного характера социальных последствий. В течение длительного времени удельный вес преступлений, совершенных несовершеннолетними или при их участии, остается на высоком уровне. Данная тенденция продолжает усиливаться, во многом приобретая новое качественное содержание.

В соответствии с законодательством Российской Федерации несовершеннолетним признается лицо, которому на момент совершения преступления исполнилось четырнадцать, но не исполнилось восемнадцати лет.

Безусловно, широкий спектр преступлений, совершаемых несовершеннолетними, предопределяет определенную специфику расследования каждого из них. В этой связи ключевым элементом криминалистической характеристики рассматриваемых преступлений является личность несовершеннолетнего преступника.

Анализ уголовных дел позволил выделить типичную психологическую черту, характерную для личности несовершеннолетнего преступника, – это агрессивность, чрезмерная жестокость, дерзость, садизм. Характерной чертой таких преступлений является то, что они сопровождаются бессмысленной жестокостью в отношении потерпевших (мно-

жественные телесные повреждения, вплоть до смертельных). Другим трендом современности стало фиксирование совершения насильственных преступлений посредством снятия видеоматериалов в прямом эфире («стримы»), либо путем дальнейшего их опубликования в социальных сетях или рассылку видео через мессенджеры.

В большинстве случаев это обусловливается тем, что формирование личности несовершеннолетнего происходило под влиянием негативных факторов, таких как неблагоприятный климат в семье и окружении, стрессовые ситуации в жизни, бытовое насилие.

Проблема бытового насилия в отношении несовершеннолетних существует на протяжении длительного времени. Об актуальности проблемы свидетельствует законодательное закрепление ответственности родителей (законных представителей). Так, ст. 65 Семейного кодекса Российской Федерации содержит правовую норму, согласно которой при осуществлении родительских прав родители не вправе причинять вред физическому и психическому здоровью детей, их нравственному развитию. Способы воспитания детей должны исключать пренебрежительное, жестокое, грубое, унижающее человеческое достоинство обращение, оскорбление или эксплуатацию детей. Кроме того, ст. 156 Уголовного кодекса Российской Федерации предусмотрена уголовная ответственность за неисполнение обязанностей по воспитанию несовершеннолетних.

Согласно анализу уголовных дел в 55 % случаев в отношении несовершеннолетнего применяются различные формы физического насилия. Кроме того, жестоким обращением с несовершеннолетними суды признают содержание детей в антисанитарных условиях (31 % случаев), плохое питание (52 % приговоров), отсутствие заботы о здоровье, необращение за медицинской помощью и ненадлежащий уход за больным ребенком (32 % приговоров), а также длительное оставление несовершеннолетнего без присмотра (22 % случаев) [1, 2].

Таким образом, на законодательном уровне выделяются три вида бытового насилия в отношении несовершеннолетних: физическое, эмоциональное, отсутствие заботы.

Согласимся с выводами исследования, проведенного А.А. Усачевым, Л.Н. Котляровой, согласно которым криминалистическая характеристика несовершеннолетнего преступника – жертвы бытового насилия, отражая основные черты общей характеристики несовершеннолетнего преступника, обладает при этом комплексом специфических черт, свойственных только ей: отставание по уровню образования, определенного формальным числом оконченных классов; большая