

1. Тишутина, И.В. Преодоление противодействия расследованию организованной преступной деятельности (организационные, правовые и тактические основы) : дис. ... д-ра юрид. наук : 12.00.12 / И.В. Тишутина. – М., 2013. – 488 л.

2. Матюк, А.В. Взаимодействие правоохранительных органов Республики Беларусь в преодолении противодействия раскрытию и расследованию преступлений против порядка осуществления экономической деятельности / А.В. Матюк // Аграр. и земел. право. – 2019. – № 4. – С. 136–140.

3. Архив суда Центрального района г. Минска за 2016 год. – Уголов. дело № 16121090986. – Арх. № 1-549/16.

4. Судебно-экономическая экспертиза в уголовном процессе : учеб. пособие для вузов / под ред. Э.Ф. Мусина. – М. : Юрайт, 2017. – 273 с.

УДК 343.98

Г.Ю. Миронов

ПРОБЛЕМЫ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ КРАЖИ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Развитие общественных отношений, переход их на новый, более современный, необходимый и отвечающий требованиям прогрессирующего общества, уровень, приводит к появлению новых форм частной собственности, например, таких как интеллектуальная собственность.

Появляются новые технологии, большинство из которых в настоящее время находится на таком надежном устройстве, как электронный носитель. Причем он может быть совершенно разным и, порой, настолько непохожим на исходный, проверенный вариант, как компьютер, что понять его работу невероятно трудно. Многие ученые, технологи, программисты и профессора, рассматривая современный мир через призму информационного общества, многократно уверялись в необходимости надежной защиты информации, содержащейся в сети Интернет. Именно в этом и заключается основная проблема – защита сети от кражи.

Известно множество случаев, когда система защиты, считавшейся самой верной, практичной и устойчивой, давала сбои или же хакеры, преступники в сфере компьютерных технологий, находили определенный код доступа, что позволяло им достать некогда засекреченную информацию. Так, в сентябре 2021 г. стало известно, что хакеры взломали компьютерную сеть ООН. После чего с сети Организации Объединенных Наций была похищена ценная информация, которая может быть использована в дальнейшем для атак ведомства в составе НАТО (<https://www.securitylab.ru/news/524272.php>). И это далеко не единственный случай взлома сети как

коммерческих, так и государственных организаций, в результате которых были понесены колоссальных размеров убытки, возместить которые, порой, преступнику не представляется возможным.

Современное состояние преступности в сфере информационных и компьютерных технологий свидетельствует о непрекращаемом росте правонарушений в данной сфере. Сотрудники органов внутренних дел, осуществляющие непосредственную охрану прав частной, интеллектуальной и информационной собственности, порой не справляются с поставленной задачей. Несоответствие необходимым требованиям обусловливается неэффективностью расследования преступления в сфере информационной безопасности сотрудниками органов внутренних дел. Именно поэтому многие криминалисты, ученые и другие представители органов внутренних дел настаивают на разработке и введении определенной новой комплексной и полноценной методики расследования преступлений в сфере информационной безопасности.

Следует отметить, что правонарушители в своих противоправных действиях используют различные новые способы и средства, которые позволяют им наиболее незаметно совершать кражи компьютерной информации, мошенничество в сети Интернет и др. Именно поэтому российское законодательство максимально дифференцирует подход к определению уголовной ответственности за киберпреступления. Так, основные положения, в которых говорится об уголовной ответственности, содержатся в гл. 28 «Преступления в сфере компьютерной информации» Уголовного кодекса Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 24 сентября 2022 г.). Однако принятие подобных мер вызвало у многих правоприменителей возмущение.

При расследовании преступлений в сфере краж компьютерной информации сотрудники правоохранительных органов должны квалифицировать преступные деяния, а это означает, что сотрудники должны обладать специальными знаниями для более точного применения той или иной нормы права. Существует также множество нюансов, которые следует учитывать при проведении расследования. Например, изъятие носителя – особая процедура, которая является необходимой для дальнейшего расследования информационных преступлений. Но изъятие носителя должно проходить строго в соответствии с регламентом, который предусматривается в Уголовно-процессуальном кодексе Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (ред. от 7 октября 2022 г.).

После возникает необходимость в проведении информационных и технологических экспертиз. Еще одной проблематичной особенностью расследования преступлений в подобной сфере является то, что чаще

всего кодификаторы уничтожают, зашифровывают программы, файлы, документы и другие носители информации, что ведет к потере улик.

Следователь при осмотре места происшествия должен быть предельно аккуратен, чтобы не навредить технике, ее работоспособности. Поэтому необходимо создание специальных инструкций, которые позволят эффективно разбираться в особенностях данного вида преступлений и дадут криминалистический анализ деяний. Таким образом, российским криминалистам еще предстоит подробно изучить киберпространство, разработать эффективные тактические подходы к выявлению и расследованию киберпреступлений, которые в условиях глобального масштабирования более чем актуальны.

Актуальность преступлений информационного характера обуславливается сразу несколькими факторами. Популярность глобальной компьютерной сети Интернет, простота в использовании, анонимность – один из самых простых и желанных способов незаконного заработка для преступников. Частные компании нередко пренебрегают покупкой дорогих устройств, защищающих информацию от третьих лиц, результатом чего нередко являются денежные потери и «утечка» информации. Единичные киберпреступления преобразовались всего лишь за несколько лет в транснациональную киберпреступность.

Еще одной проблемой при расследовании преступлений в сфере кражи компьютерной информации стало то, что нет определенного закрепления понятия «киберпреступность» в законодательстве или же на международном уровне. Это вызвано постоянно изменяющимися способами совершения преступления, что затрудняет квалификацию преступных деяний. Так, В.А. Дуленко (учебное пособие «Использование высоких технологий криминальной средой. Борьба с преступлениями в сфере компьютерной информации», 2007), Р.Р. Мамлеев, В.А. Пестриков считают, что «киберпреступность» – это любое преступление, совершенное с помощью компьютерной сети, т. е. любое преступление, совершенное в электронной среде.

Раскрываемость преступлений в сфере компьютерной кражи на данный момент в России довольно низкая. Основной причиной такого показателя является неспособность правоохранительных органов качественно раскрыть преступления. Одним из факторов этой проблемы является то, что сотрудники органов внутренних дел с такими преступлениями встречаются очень редко, поэтому опыт работы практически отсутствует, либо полученных практических знаний оказывается недостаточно. В связи с этим разработка определенного плана расследования таких преступлений – необходимость.

О СТРУКТУРЕ КРИМИНАЛИСТИЧЕСКОГО УЧЕНИЯ О ПОТЕРПЕВШЕМ

В криминалистической науке взаимосвязь потерпевшего и подозреваемого при расследовании преступлений рассматривалась задолго до возникновения научно обоснованных данных в качестве направления для установления обстоятельств совершения преступления. Так, Г. Гросс отмечал, что «следователь не должен стесняться ни хорошей репутацией, ни положением «потерпевшего» в обществе, ни удачной обстановкой происшествия, ни вообще подобными условиями. В этих случаях важно не столько изобличение лживости жалобы, сколько ограждение невиновных, на которых может пасть подозрение благодаря таким недостойным проделкам» [1, с. 33]. Подобная позиция основоположника криминалистики является ярким свидетельством того, что он выступал за всестороннее изучение потерпевшего, в том числе, и при приеме заявлений о совершении преступлений, анализ которых позволяет получить представление о содержащихся в них сведениях (оценить их на предмет достоверности).

В криминалистической литературе длительное время внимание акцентировалось на таких аспектах личности потерпевшего, как его поведение, установление взаимосвязи с другими участниками преступления [2, с. 16–17], что и в настоящее время достаточно активно используется как при характеристике участников уголовного судопроизводства при расследовании конкретных преступлений, так и при формировании частных криминалистических учений, в том числе, и учения о жертве преступления.

Развивая данные постулаты, Е.Е. Центров полагает, что: «Криминалистическое учение о жертве преступления – это опирающаяся на положения уголовного и уголовно-процессуального закона динамическая система криминалистических теоретических построений и фактических знаний о жертве преступления, ее криминалистически значимых особенностях личности, поведения, связей, взаимодействия и взаимоотношений с лицом, совершившим преступление, и другими лицами и объектами, имеющая целью разработку и совершенствование технических средств, тактических приемов расследования и предупреждения преступлений» [3, с. 46]. В рассматриваемом определении автором