Matchanov Alimjan Atabaevich
O'zbekiston Respublikasi IIV Akademiyasi Tashkiliy-shtab faoliyati bo'limi boshlig'i, yuridik fanlar doktori, professor, polkovnik
E-manzil: alimjan.matchanov@gmail.com

KIBERFIRIBGARLIKNI TERGOV QILISHDA RAQAMLI DALILLARNI QAYD ETISHDA AXBOROT-KOMMUNIKATSIYA TEXNOLOGIYALARIDAN FOYDALANISHNING O'ZIGA XOS XUSUSIYATLARI

Matchanov Alimzhan Atabaevich
Head of the Department of Organizational and Staff Activities of the Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan, Doctor of Law, professor, colonel
E-mail: alimjan.matchanov@gmail.com

FEATURES OF THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES IN FIXING DIGITAL EVIDENCE IN THE INVESTIGATION OF CYBER FRAUD

Матчанов Алимжан Атабаевич
Начальник кафедры организационно-штабной деятельности Академии МВД Республики Узбекистан, доктор юридических наук, профессор, полковник
Эл-почта: alimjan.matchanov@gmail.com

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В ФИКСАЦИИ ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ В РАССЛЕДОВАНИИ КИБЕРМОШЕННИЧЕСТВА

Информационно-коммуникационные технологий (ИКТ) оказывают положительное влияние на эффективность собирания и закрепления доказательств и соответственно на результаты раскрытия и расследования общественно-опасных деяний, среди которых особое место занимают киберпреступления и ее разновидность – кибермошенничество. Методика их расследования и криминалистическая тактика проведения следственных действий и оперативно-розыскных мероприятий имеет актуальный характер в современных условиях развития информационных технологий.

Термин «киберпреступления» можно воспринимать как общественно-опасные деяния, связанные с совершением преступлений, в сфере информационно-коммуникационных технологий, где сама электронная информация, техника или ресурсы, с помощью которой совершаются преступления, составляют признаки этих противоправных деяний.

Неотвратимость уголовной ответственности за совершения киберпреступлений, по мнению А.К. Расулева зависит от повышения эффективности борьбы с преступлениями в сфере информационных технологий. При этом он выделяет такое приоритетное направление как обеспечение принципа неотвратимости ответственности за киберпреступления в сфере экономики путем раскрытия их юридической природы[1].

Органы, осуществляющие доследственную проверку, дознаватели, следователи раскрывают и расследуют кибермошенничество посредством процессуальных, следственных и оперативно-розыскных действий, которые могут оформляться в процессуальной и не процессуальной формах. При этом они применяют инновационные информационно-коммуникационные технологии, позволяющие значительно расширить диапазон возможностей криминалистической методики и тактики проведения следственных и оперативно-розыскных действий.

Понятие мошенничества в киберпространстве сегодня приобрело весьма широкий смысл. Согласно Конвенции о киберпреступности это – лишение другого лица собственности посредством любого ввода, изменения, удаления или блокирования компьютерных данных, а также любого вмешательства в функционирование компьютерной системы с намерением неправомерного извлечения экономической выгоды для себя или для третьих лиц.

Кибермошенничество имеет следующие виды: QFC – мошенничество с банкоматами; QFF – компьютерная подделка; QFG – мошенничество с игровыми автоматами; QFM – манипуляции с программами ввода вывода; QFP – мошенничества с платежными средствами; QFT – телефонное мошенничество; QFZ – прочие мошенничества в виртуальном пространстве.

Процесс развития и совершенствования ИКТ и распространения в глобальном, международном пространстве посредством информационной интеграции, создал благоприятные условия для совершения киберпреступлений. Это потребовало от органов внутренних дел и других правоохранительных структур создать и оптимизировать методику расследования этих преступлений и тактику проведения следственных действий и оперативно-розыскных мероприятий направленных на получение доказательств, которые имеют несколько специфическую, электронную форму. Так, Н.А. Нугманов среди проблем связанных с применением информационных технологий выделят создание правовых условий для электронного документа в качестве доказательств[2].

В методике расследования кибермошенничества особое место уделяется тактическим приемам получения доказательств посредством информационных технологий, которые создали предпосылки для

возникновения таких специфических форм как цифровые или электронные доказательства.

Относительно этого Е.С. Ермакова отмечает, что «электронные доказательства легко подвергаются изменениям и мгновенному уничтожению. При этом он выделяет следующие особенности фиксации электронных доказательств: 1) Оперативность; 2) Участие специалиста; 3) Наличие специальных устройств для их записи, сохранения и воспроизведения»[3].

На наш взгляд эти особенности в методике расследования кибермошенничества наиболее полно отражают криминалистическую тактику их получения. При этом следует помнить, об особенностях присущих только этому источнику доказательств, а именно факт формирования цифровых сигналов в виртуальном пространстве.

Опыт методики расследования кибермошенничества в такой развитой информационно-коммуникационной сфере как США показывает, что для получения цифровых доказательств были созданы специальные технические группы по их исследованию – Technical Working Group on Digital Evidence (TWGDE), которые впоследствии были преобразованы в единую Scientific Working Group on Digital Evidence (SWGDE)[4].

По мнению Н.А. Иванова, под цифровыми доказательствами понимаются фактические сведения, полученные с помощью информационно-коммуникационных технологий дискретных сигналов, содержащихся или зафиксированных на компьютерных или иных машинных носителях, изъятую, переданную участниками процесса или полученную иным способом в соответствии с действующим уголовно-процессуальным законодательством[5].

Одним из основных приемов криминалистической тактики расследования кибермошенничества является изъятие электронных носителей при проведении следственного осмотра. В этом отношении В.А. Мещеряков, В.В. Трухачев установили особую важность данной криминалистической тактики отметив, что «арсенал имеющихся процессуальных действий достаточно велик, он все же, с одной стороны, ограничен, исчерпывающим списком, а с другой – в рассматриваемых нами целях фактически сводится к одному единственному следственному действию – осмотру»[6]. Это связано с тем, что осмотр является универсальным следственным действием, в котором восприятие цифровой информации предусматривает наличие определенных технических средств и необходимого программного обеспечения, позволяющего понять сущность информации, выраженной в цифровой форме.

Органы, ответственные за расследование преступлений, не всегда имеют дело непосредственно с физическим электронным носителем информации. Особенность информационных, телекоммуникационных систем выражается в том, чтобы получить соответствующие цифровые доказательства, имеющие значение в методике расследования, не имея

физического доступа к месту нахождения информационного носителя. При этом цифровая информация фиксируется в составляемом протоколе осмотра с использованием доступных для пользователей открытых источников, но только в том случае, когда данные размещены на общедоступных машинных, компьютерных или иных информационных носителях[7].

Тактические приемы проведения данных следственных действий выражаются в непосредственном проникновением в помещение, где находятся их машинные, электронные и иные информационные носители. При этом, вышеуказанный вид доказательств может быть зафиксирован на любом материальном носителе, в том числе, полученном в результате применения и использования информационно-телекоммуникационных технологий. В сущности, они материализуются как вещественные доказательства или электронный документ посредством ИКТ, как сведения, представленные в форме цифровых сигналов материальным, машинным (электронным) носителем, независимо от средств их хранения, обработки и передачи. Это могут быть аппаратные и программные средства микропроцессорной техники. При этом доказательственную базу составляет информация, зафиксированная на машинных носителях или на CD-дисках, DVD-дисках, флешнакопителях (переносимые носители), а также встроенных в средства микропроцессорной, компьютерной или иной инновационной техники.

Таким образом, на основании вышеизложенного, можно сделать вывод, что тактические приемы получение и фиксация цифровых доказательств в расследовании киберпреступлений представляет собой процедуру, сочетающую в себе комплекс мероприятий, связанных с криминалистической методикой и тактикой обнаружения, получения и оценки этих доказательств. Знание и умение на практике применить оптимальную криминалистическую тактику работы с цифровыми доказательствами позволит создать наиболее эффективную и оптимальную методику расследования киберпреступлений.

Библиографические ссылки:

1. Расулев А.К. Совершенствование уголовно-правовых и криминалистических мер борьбы с преступлениями в сфере информационных технологий и безопасности: Автореф. дис. …д-ра юрид. наук (DSc). – Т., 2018. – С. 74. (С. 37)

2. Нугманов Н.А. Теоретико-практические особенности формирования международного информационного права: Автореф. дис. …док. юрид. наук (DSc). – Т., 2018. – С. 59. (С. 42).

3. Ермакова Е.С. Электронные доказательства как новое направление в практике расследования преступлений / Е.С. Ермакова, Д.М. Джумангалиева. – Текст: непосредственный // Молодой ученый. –

2018. – № 23 (209). – С. 85-87. – URL: https://moluch.ru/archive/209/51196/ (дата обращения: 05.10.2021).

4. http ://ncfs.org/swgde/.

5. Иванов Н.А. О понятии «цифровые доказательства» // Вестник Омского юридического института, 2006. – № 2 (5), – С. 77–78.

6. Мещеряков В.А., Трухачев В.В. Формирование доказательств на основе электронной цифровой информации // Вестник Воронежского института МВД России. 2012. – № 2. – С. 108–110.

7. Карташов И.И. Нетрадиционные источники оперативной информации // Актуальные проблемы деятельности подразделений УИС: сборник материалов открытой научно-практической конференции / ФГОУ ВПО Воронежский институт ФСИН России. – Воронеж: Научная книга, 2010. – С. 169–174. – С. 171.