УДК 34.096

Гундерич Галина Альбертовна, кандидат технических наук, доцент кафедры уголовного процесса, криминалистики и участия прокурора в уголовном судопроизводстве, кандидат технических наук, Крымский юридический институт (филиал) Академии Генеральной прокуратуры Российской Федерации, Россия, г. Симферополь

e-mail: gunderich@mail.ru

ВОПРОСЫ КРИМИНАЛИСТИЧЕСКОЙ ТАКТИКИ ПРИ РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ

Аннотация. В данной статье освещаются некоторые вопросы криминалистической тактики, используемые при исследование цифровых данных с любого устройства, способного обрабатывать, хранить или передавать данные в любой форме. Перечислены основные принципы использованные при расследовании компьютерных преступлений

Ключевые слова: киберпреступность, компьютерные преступления, цифровые данные, цифровые устройства.

Gunderich Galina Albertovna, Candidate of Technical Sciences, Associate Professor of the Department of State and Legal Disciplines of the Crimean Institute of Law (branch) of the University of the Prosecutor's Office of the Russian Federation, Simferopol, Republic of Crimea, Russian Federation.

e-mail: gunderich@mail.ru

FORENSIC TACTICS IN CYBERCRIME INVESTIGATIONS

Annotation. The following article highlights some of the issues of forensic tactics used in the study of digital data from any device capable of processing, storing

or transmitting data in any form. Basic principles that are used in the investigation of computer crimes are enumerated.

Keywords: cybercrime, computer crimes, digital data, digital devices.

Криминалистическая тактика определяет структурированное исследование цифровых данных с любого устройства, способного обрабатывать, хранить или передавать данные в любой форме. Тактика расследования компьютерных преступлений имеет много общего с тактикой производства следственных действий по делам, по которым искомые следы имеют материальную природу. Тем не менее, существует отличие, которое должно учитываться: доказательства по компьютерным преступлениям являются цифровыми. В связи с этим традиционная криминалистическая тактика не всегда отвечает требованиям собирания доказательств, подтверждающих гипотезу о преступлении или инциденте. Криминалистическая тактика при расследовании данного вида преступления должна гарантировать, что независимо от того, какие цифровые доказательства обнаружены, их необходимо надлежащим образом сохранить, зафиксировать и идентифицировать, чтобы использовать в процессе доказывания. Рекомендации по тактике исследования цифровых доказательств имеют общий характер в том плане, что они могут использоваться при расследовании любых преступлений с использованием цифровых устройств, в том числе компьютерных устройств, мобильных устройств, Интернет-ресурсов и даже будущих цифровых технологий [1]. Электронные устройства подозреваемых в разбойном нападении, экстремизме и иных преступлениях могут быть подвергнуты криминалистическому экспертному исследованию в ходе расследования для обнаружения и фиксации доказательств по делу. Такие доказательства могут дать ответы на основные вопросы: кто совершил преступление, где соучастники преступления были в тот момент, когда подозреваемый получал или отправлял текстовое сообщение, каковы обстоятельства преступления, когда, почему и как оно было совершено. Цифровые доказательства можно

обнаружить в разных местах, например в истории сообщений или других цифровых журналах (логах) [2]. Надо при этом учитывать, что лишь малое количество киберпреступлений предполагает только исследование электронных устройств, поэтому тактика расследования киберпреступлений включает и традиционные наработки. При расследовании компьютерных преступлений необходимо следовать распространенным и хорошо зарекомендовавшим себя криминалистическим принципам:

- в целостности доказательства – оно должно быть сохранено и зафиксировано в первоначальном виде.

- все действия по исследованию доказательства должны быть соответствующим образом процессуально закреплены.

Понятие цифрового доказательства не закреплено в уголовном процессе, но можно определить как любые цифровые данные, удовлетворяющие требованиям достоверности, относимости и допустимости, которые поддерживают или опровергают гипотезу о преступлении [3]. В поисках цифровых доказательств эксперты исследуют электронные устройства, при этом если установлено, что электронное устройство имеет отношение к расследованию и получено процессуальным путем, то оно считается физическим носителем доказательства. Тактика расследования киберпреступлений включает традиционные этапы криминалистического исследования: осмотр исследуемого объекта, в ходе которого изучаются все объекты (идентифицируемые, идентифицирующие), а также образцы для сравнительного исследования (свободные, условно свободные и экспериментальные); раздельное, детальное исследование объекта с целью выявления максимального количества общих и частных признаков, характеризующих объект идентификации. Эта стадия может сопровождаться проведением эксперимента; сопоставление признаков сравниваемых объектов. На данном этапе осуществляется выявление совпадающих признаков и признаков различия; оценка признаков объекта и формирование выводов о наличии или об отсутствии тождества. Выводы могут быть утвердительные или

отрицательные, достоверные или вероятные. Тактика первичного осмотра места преступления при расследовании киберпреступлений имеет некоторые особенности. Как правило, первым на место происшествия прибывает сотрудник полиции, который отвечает за сохранность потенциальных доказательств, включая электронные устройства. Цифровые данные, обнаруженные на одном устройстве, могут быть не единственным источником доказательств, поэтому следует обеспечить сохранность всех имеющихся на месте преступления электронных устройств. Должны быть предусмотрены актуальные должностные инструкции для обеспечения целостности доказательств. Местом совершения киберпреступления чаще всего является помещение или участок местности (или несколько помещений или участков). Если это квартира или частный дом, необходимо учитывать все имеющиеся устройства, на которых может содержаться цифровая информация[4]. Многие из них подключены к беспроводным сетям, к которым могут иметь доступ устройства вне квартиры или жилого помещения. Кроме того, преступники могут также получить доступ к сети, особенно там, где отсутствует адекватный контроль. Устройства могут быть подключены к сетевым хранилищам цифровых данных (облачное хранилище, общие почтовые службы). Если местом преступления выступает помещение небольшой фирмы (организации), необходимо иметь в виду, что цифровые устройства обычно в некоторой степени управляются и учитываются. Поскольку предприятия работают с отдельными компьютерами, смартфонами и назначенными приложениями, сетью и доступом к услугам и устройства зарегистрированы в общей топологии сети и документах инвентаризации, идентифицировать потенциальные источники доказательств проще. Крупные предприятия обычно практикуют более строгий контроль за цифровыми устройствами и оборудованием, в них часто есть ИТ-отделы. Они могут иметь системы безопасности, а также службы безопасности, которые могут помочь в выявлении потенциальных источников цифровых доказательств. Журналы (логи) – основной источник доказательств, поэтому в первую очередь необходимо обеспечить их

сохранность, обратившись к лицу, ответственному за их мониторирование [4]. В ходе расследования может возникнуть конфликт между следственно-оперативной группой и службой безопасности предприятия, подвергшегося кибератаке. Излишняя секретность может помешать расследованию, поэтому следователь должен использовать психологические приемы убеждения в беседах с сотрудниками, имеющими доступ к искомой информации. После осмотра и возможного опроса лиц следует определить круг электронных устройств, относящихся к расследуемому делу. Собирание доказательств начинается с момента получения доступа к электронному устройству (устройствам), содержащему(им) нетронутые цифровые данные, которые относятся к совершенному преступлению.

Список источников:

1. Аверьянова Т.В. Судебная экспертиза: курс общей теории: монография. М.: Норма; ИНФРА-М, 2015.

2. Бикмиев Р.Г., Бурганов Р.С. Собирание электронных доказательств в уголовном судопроизводстве // Информ. право. 2015. № 3.

3. Оконенко Р.И. Электронные доказательства как новое направление совершенствования российского уголовно-процессуального права // Актуал. проблемы рос. права. 2015. - № 3.

4. Теория судебной экспертизы (судебная экспертология): учебник / Е.Р. Россинская, Е.И. Галяшина, А.М. Зинин; под ред. Е.Р. Россинской. 2-е изд., перераб и доп. М.: Норма; ИНФРА-М, 2018.