К ВОПРОСУ О РОЛИ ЦИФРОВОЙ КРИМИНАЛИСТИКИ В УСЛОВИЯХ КОМПЬЮТЕРИЗАЦИИ СОВРЕМЕННОГО ОБЩЕСТВА

К.Д. Борченко, *студент*
Е.С. Антилова, *студент*
Научный руководитель: *М.А. Яворский, канд. юрид. наук, доцент*
Самарский государственный экономический университет
(Россия, г. Самара)

DOI: 10.24411/2500-1000-2020-11434

Аннотация. *В данной работе авторами поднимается вопрос необходимости использования и усовершенствования методов цифровой криминалистики при расследовании различного рода компьютерных преступлений. Рассматриваются цели и особенности цифровой криминалистики, а также выделяются специальные оперативно-розыскные мероприятия, которые связаны со спецификой технического оборудования и необходимы при расследовании компьютерных преступлений.*

Ключевые слова: *цифровая криминалистика, компьютеризация, цифровые следы, компьютерные технологии, цифровые преступления.*

В современном мире трудно представить человека без мобильного телефона, компьютера, цифрового фотоаппарата или интернета. Цифровые информационные технологии плотно вошли в жизнь каждого и являются неотъемлемым элементом работы или учебы. Однако и преступники используют информационные технологии для совершения противозаконной деятельности, совершая квалифицированные преступления удаленным способом. Чтобы пресекать такого рода преступную деятельность, государству необходимо совершенствовать способы раскрытия, расследования и предотвращения информационных преступлений, учитывая возможности информационных систем.

Основным элементом для выработки новых методов и возможностей сбора и анализа доказательств такого рода преступлений является новая подотрасль криминалистических знаний – «цифровая криминалистика», которая представляет собой совокупность (систему) знаний, умений и навыков, обеспечивающих деятельность по выявлению информационных преступлений, криминалистическому исследованию электронной доказательственной базы, а также включает регистрирование и дальнейшее использование цифровых следов в раскрытии и расследовании преступлений [1].

Цифровая криминалистика ставит перед собой следующие цели: обнаружение данных, их восстановление и криминалистический анализ, а также собирание доказательственной базы с использованием цифровых технологий. Стоит отметить, что область распространения цифровой криминалистики достаточно обширна, она охватывает не только современные компьютерные технологии, но и так же их программное обеспечение, электронное хранилище данных, средства мобильной связи и т.д.

Особенность цифровой криминалистики заключается в специфичности обнаружения, фиксации и изъятии цифровых следов. Такие следы могут находиться на электронных носителях, либо передаваться по специальным каналам связи, однако на практике цифровые следы, оставленные преступниками довольно сложно отследить. Поэтому для полноценного и своевременного раскрытия преступления в цифровой сфере необходимо специализированное оборудование и лица, обладающие достаточными знаниями и навыками в данной области. Помимо этого, следует отметить, что в качестве вещественных доказательств в уголовном процессе, принято считать материальный носитель электронной информации (ноутбук, телефон, флеш-карта, диск и т.д.), а информация,

содержащаяся на этом носителе, становится доказательством по делу только после ее исследования экспертом и при наличии соответствующего заключения [2]. Когда как, например, бумажный документ вместе со всей информацией, изложенной в нем, считается самостоятельным доказательством, не требующим проведения экспертизы. Таким образом, вышеизложенное можно считать еще одной особенностью цифровой криминалистики.

Если обращаться к статистическим данным за январь-июль 2020 г., то можно заметить насколько сильно возросли показатели информационных преступлений по сравнению с предыдущими годами и в соотношении с другими совершаемыми преступлениями [3].

Рис. Статистика отдельных видов преступлений

Практически на треть в стране возросли различного рода мошенничества с использованием сети «Интернет», средств мобильной связи, компьютерной техники или других информационных технологий – 188,5 тыс. Всего совершается более 67,6% «цифровых» мошенничеств (127,4 тыс.) и их число продолжает увеличиваться (+ 80,3%).

В 2 раза больше выявлено мошенничеств с использованием электронных средств платежа – 17,7 тыс. Увеличение таких деяний в разной степени зафиксировано в 77 регионах, наибольшие число выявлено в Саратовской (1801, + 94,7%), Омской (1394, + 136,3 %) областях и г. Москве (1166, + 113,6%).

В целом каждое четвертое из выявленных преступлений за период с января по июль 2020 года совершено в области компьютерной информации либо при помощи информационных технологий. По сравнению с предыдущими годами число таких преступлений увеличилось практический вдвое и достигло свыше 272 тысяч преступлений.

При использовании сети «Интернет» совершается больше половины всех «киберпреступлений» (155,7 тыс.), а с использованием мобильной связи – больше 40% (116 тыс.). Так же стоит отметить, что при помощи сети «Интернет» довольно часто совершаются преступления экстремисткой направленности, а именно 55%, при чем каждое второе такое преступления является призывом к осуществлению экстремисткой деятельности.

Именно благодаря вышеуказанным статистическим данным можно оценить необходимость усовершенствования методов и способов использования цифровой криминалистики.

При раскрытии цифровых преступлений, как и преступлений, совершенных стандартным способом, так же используется комплекс следственных действий и оперативно-розыскных мероприятий. Однако, в отличии от доказательств, имеющих материальное обозначение, цифровые доказательства (какая-либо информация, особенно зашифрованная) намного сложнее зафиксировать и изъять.

Поэтому для цифровой криминалистики характеры и специальные оперативно-розыскные мероприятия, «представляющие собой совокупность действий по перехвату и исследованию данных трафика, установление логов веб и мейл-серверов, системных логов, доменов, принадлежности адреса электронной почты, исследование кейлогеров» [4].

К специальным ОРМ в борьбе с цифровыми преступлениями можно отнести:

– восстановление удаленных файлов, в т.ч. электронных писем;

– определение источника (компьютера, др. устройство) вредоносного программного обеспечения или атак;

– установление IP-адреса источника;

– установление устройства, на котором был сделан снимок, видео или аудиозапись, а также определение даты, времени и местоположения;

– установление информации, находящейся на устройстве: контакты, пропущенные/исходящие/входящие звонки, сообщения SMS или iMessage;

– отслеживание местоположения устройства, при наличии GPS системы или без нее;

– установления времени создания или изменения файла;

– взламывание паролей на заблокированных/зашифрованных телефонах, компьютерах, жестких дисках или файлах;

– отслеживание истории посещения веб-сайтов лица и установление скаченных файлов;

– установление лица, взломавшего беспроводную сеть или лица, не авторизированного, как пользователь и т.п. [5].

В современном мире цифровые и компьютерные технологии заняли прочные позиции практически в каждой сфере жизнедеятельности человека, и следствием этого стало развитие цифровой криминалистики, как специализированной отрасли криминалистики. Еще несколько лет назад считались латентными преступления в сфере высоких технологий, т. е. такие преступления при подготовке и совершении которых использовались компьютерные технологии и цифровая информация. А это означало, что своевременного выявления лиц и раскрытие дела ждать не следовало. Такая ситуация оправдывалась многими факторами: отсутствием специальной техники, позволяющий обнаружить, зафиксировать и исследовать цифровые следы; недостаточное развитие методики расследования таких преступлений; а самое главное – отсутствие лиц, обладающих достаточными знаниям и навыками в данной сфере.

На сегодняшний день специалисты обладают современным оборудованием, которое позволяет осуществить поиск и фиксацию следов «цифровых» преступлений. Так же достаточно изучен механизм следообразования в различных информационных системах – все это позволяет сделать расследование преступлений в цифровой сфере эффективнее.

Библиографический список

1. Русанова Д.Ю. Цифровая криминалистика: возможности и перспективы развития // Международный журнал гуманитарных и естественных наук. – 2019. – №12-4 (39). – С. 142-145.

2. Соловьева С.М. Применение цифровых технологий в криминалистике // Молодой ученый. – 2019. – № 51 (289). – С. 161-164.

3. Статистический сборник «Состояние преступности в России за июль 2020 г.» // сайт Генеральной Прокуратуры Российской Федерации. – [Электронный ресурс] – Режим доступа: https://genproc.gov.ru/stat/data/1888262/ (дата обращения: 14.10.2020).

4. Афанасьев А.Ю., Репин М.Е. Некоторые особенности расследования компьютерных преступлений // Студенческие южно-уральские криминалистические чтения: Сборник материалов всероссийской заочной научно-практической конференции. Выпуск 3 // Под. ред. И.А. Макаренко. – Уфа: РИЦ БашГУ. – 2015. – С. 27.

5. Репин М.Е. Преступления в сфере компьютерной информации: проблемы выявления и раскрытия / М.Е. Репин, А.Ю. Афанасьев // Молодой ученый. – 2015. – №15 (95). – С. 460-463.

TO THE QUESTION ABOUT THE ROLE OF DIGITAL FORENSICS IN CONDITIONS OF COMPUTERIZATION OF MODERN SOCIETY

K.D. Borchenko, *Student*
E.S. Antilova, *Student*
Scientific supervisor: *M.A. Yavorsky,* *Candidate of Legal Sciences, Associate Professor*
Samara State University of Economics
(Russia, Samara)

Abstract*. In this work, the authors raise the question of the need to use and improve the methods of digital forensics in the investigation of various types of computer crimes. The goals and features of digital forensics are considered, and special operational-search measures are highlighted that are associated with the specifics of technical equipment and are necessary in the investigation of computer crimes.*

Keywords: *digital criminalistics, computerization, digital traces, computer technologies, digital crimes.*