УДК 343.985.7
DOI 10.33184/pravgos-2020.4.22

ПОРЯДОК ОБНАРУЖЕНИЯ, ИЗЪЯТИЯ И ФИКСАЦИИ ЦИФРОВЫХ СЛЕДОВ ПРЕСТУПЛЕНИЯ

ГАЛИМХАНОВ Азат Булатович
кандидат юридических наук, доцент кафедры криминалистики Института права Башкирского государственного университета, г. Уфа, Россия.
E-mail: alflaw@mail.ru

ХАЛИУЛЛИНА Айгуль Фаатовна
кандидат юридических наук, доцент кафедры криминалистики Института права Башкирского государственного университета, г. Уфа, Россия.
E-mail: aigul229@mail.ru

Активное использование информационно-коммуникационных технологий привело не только к изменениям во всех сферах человеческой деятельности, но и обусловило появление новых возможностей для преступной деятельности. С помощью цифровых технологий совершаются сегодня преступления в сфере компьютерной информации, против жизни и здоровья человека, против собственности и др. В этой связи возникают вопросы, связанные с выявлением, фиксацией и исследованием цифровых следов, которые образуются в результате совершения противоправных деяний. Для большинства практических работников работа с цифровыми следами вызывает большую сложность, поскольку отсутствует четкий алгоритм действий и рекомендаций по рассматриваемому вопросу. **Цель:** анализ действующего законодательства в области применения цифровых технологий и разработка тактических рекомендаций для обнаружения, изъятия и фиксации цифровых следов. **Методы:** в работе использованы общенаучные методы, сравнительно-правовой, а также такие логические приемы, как анализ и синтез. **Результаты:** исследование позволило разработать тактические рекомендации по обнаружению, изъятию и фиксации цифровых следов преступления.

Ключевые слова: цифровые технологии; следы; обнаружение следов; фиксация; цифровизация.

Криминалистическое изучение следов занимает центральное место в системе науки криминалистики.

С позиции теории отображения каждый объект материального мира всегда вызывает изменения в окружающей среде. Следы, образующиеся в процессе подготовки, совершения и сокрытия противоправных деяний, являются отражением совершенного преступления. При этом свойство отражения присуще всем видам и формам материи.

С наступлением эпохи цифровизации изменилось отношение к понятию и классификации следов. Сегодня в оборот теории и практики повсеместно входят «цифровые следы» [1, с. 35], «виртуальные следы» [2, с. 112], «электронные следы» [3, с. 79] и т. д. Не вдаваясь подробно в анализ этих понятий, отметим лишь, что мы разделяем позицию Е.Р. Россинской и считаем, что следы, образованные при совершении преступлений с использованием компьютерных технологий, уместно называть цифровыми.

Обнаружение, изъятие и фиксация цифровых следов имеют свои особенности и требуют научно обоснованных рекомендаций и методов. Поскольку такие следы быстро трансформируются и легко уничтожаются, промедление или неосторожные действия при их выявлении в ходе производства следственных действий могут привести к необратимым последствиям.

Опрос практических работников показал, что в процессе расследования компьютерных преступлений они практически всегда привлекают специалистов. Однако стоит отметить, что не все специалисты обладают должной компетенцией, поэтому следователю самому важно знать и умело руководить следственным действием. При производстве обыска или осмотра в ходе расследования преступлений могут быть обнаружены не только цифровые следы, но и следы рук, микрообъекты, следы ДНК и пр. Исходя из этого, на наш взгляд, стоит придерживаться следующего алгоритма действий в ходе осмотра места происшествия при расследовании компьютерных преступлений:

1) статическая стадия осмотра:

– определить местоположение компьютерной техники и подробно описать его в протоколе следственного действия;

– осмотреть все внешние устройства, которые подключены к ПК (клавиатура, мышь, веб-камера и др.);

– обратить пристальное внимание на индивидуальные особенности всей компьютерной техники (системного блока, клавиатуры, монитора и пр.);

2) динамическая стадия осмотра:

– с помощью криминалистической техники обнаружить на поверхности внешних устройств материальные следы преступления (микрообъекты, следы пальцев рук);

– изучить аппаратное обеспечение (координатные устройства, устройства для ввода текста, устройства ввода изображений и видео и т. п.);

– определить операционную систему;

– установить IP-адрес;

– посмотреть данные о пользователе с помощью браузера. При этом стоит отметить, что, работая с браузером, не следует закрывать открытые вкладки, а переходить по гиперссылкам необходимо в режиме новой вкладки;

– изучить историю просмотра веб-страниц;

– изучить электронную почту;

– определить, имеются ли у пользователя средства анонимизации;

– исследовать средства синхронизации данных;

– использовать программы для поиска и восстановления недавно удаленных файлов (Recuva, Hetman Partition Recovery, EaseUS Data Recovery и др.).

На заключительной стадии осмотра, если следователь принимает решение изъять компьютерную технику, следует позаботиться о том, чтобы компьютер был переведен в «спящий» режим, поскольку это позволит сохранить информацию с жесткого диска и с запущенных приложений. Далее, соблюдая все требования уголовно-процессуального законодательства, необходимо изъять электронные носители информации и упаковать их должным образом. После чего с соблюдением уголовно-процессуальных требований необходимо упаковать осмотренный объект.

В заключение хотелось бы отметить, что процесс цифровизации должен существенно изменить и порядок подготовки практических работников. К сожалению, рабочие программы высших учебных заведений не предусматривают нужного количества часов и информации, посвященной этой тематике, что наводит нас на мысль о необходимости концептуальных изменений образовательного процесса. А действующие сотрудники правоохранительных органов должны постоянно повышать свою квалификацию в области расследования преступлений, совершаемых с использованием информационных технологий.

Библиографический список

1. Россинская Е.Р. Проблемы использования специальных знаний в судебном исследовании компьютерных преступлений в условиях цифровизации // Вестник Ун-та им. О.Е. Кутафина (МГЮА). 2019. № 5. С. 31–44.
2. Мещеряков В.А. Основы методики расследования преступлений в сфере компьютерной информации : дис. ... д-ра юрид. наук. Воронеж, 2001. 387 с.
3. Электронные доказательства в уголовном судопроизводстве : учеб. пособие для вузов / отв. ред. С.В. Зуев. М. : Юрайт, 2020. 193 с.

Дата поступления: 28.10.2020

PROCEDURE FOR DETECTING, SEIZING AND RECORDING DIGITAL TRACES OF CRIME

GALIMKHANOV Azat Bulatovich
Candidate of Sciences (Law), Assistant Professor of the Chair of Forensics, Bashkir State University, Ufa, Russia
E-mail: alflaw@mail.ru

HALIULLINA Aigul Faatovna
Candidate of Sciences (Law), Assistant Professor of the Chair of Forensics, Bashkir State University, Ufa, Russia
E-mail: aigul229@mail.ru

The active use of information and communication technologies has led to changes in all spheres of human activity. However, this has also affected the emergence of new opportunities for criminal activity. Digital crime today is computer-related, it is committed against human life and health, against property, etc. This raises issues related to detecting, recording and researching digital crime traces of unlawful acts. Working with digital traces is very difficult for most practitioners, because there is no clear algorithm of actions and recommendations on the issue under consideration. **Purpose:** to analyze the current legislation in the field of digital technologies and develop tactical recommendations for detecting, seizing and recording digital traces. **Methods:** the authors use general scientific methods, comparative law method, as well as logical techniques such as analysis and synthesis.

Results: the study allows us to develop tactical recommendations for detecting, seizing and recording digital traces of crime.
Keywords: digital technologies; traces; trace detection; recording; digitalization.

References

1. Rossinskaya E.R. Problems of using special knowledge in forensic investigation of computer crimes in the context of digitalization. *Vestnik Universiteta im. O.E. Kutafina (MGYUA) = Courier of the Kutafin Moscow State Law University (MSAL)*, 2019, no. 5, pp. 31–44. (In Russian).

2. Meshcheryakov V.A. *Osnovy metodiki rassledovaniya prestuplenij v sfere komp'yuternoj informacii. Dokt. Diss.* [Fundamentals of methods for investigating computer-related crimes Doct. Diss.]. Voronezh, 2001. 387 p.

3. Zuev S.V. (ed.). *Elektronnye dokazatel'stva v ugolovnom sudoproizvodstve* [Electronic evidence in criminal proceedings]. Moscow, YUrajt Publ., 2020. 193 p.

Received: 28.10.2020