



ВЕСТНИКЪ КРИМИНАЛИСТИКИ
BULLETIN OF CRIMINALISTICS
I (85) - 2023

Издается с 1999 г.

*Основатель журнала и его первый ответственный редактор
профессор А.Т. Филиппов*

Ответственный редактор Е.В. Иванова

В журнале

«ВЕСТНИКЪ КРИМИНАЛИСТИКИ ~ BULLETIN OF CRIMINALISTICS»
публикуются статьи по криминалистике, судебной экспертизе, оперативно-розыскной деятельности, представляющие интерес для практикующих работников правоохранительных органов, а также адвокатов, судей, преподавателей и научных работников.

ISSN 2220-847X

Адрес редакции:

author@vestcrim.ru, contact@fact-gsgu.ru

2023



СОДЕРЖАНИЕ

КОРИФЕЙ НАУКИ

СМИРНОВА С.А. Р.С. Белкин – истинный хранитель криминалистических смыслов, камертон судебно-экспертных ценностей и устремлений (Послесловие к 100-летию учёного) 5

АКТУАЛЬНЫЕ ПРОБЛЕМЫ КРИМИНАЛИСТИКИ И СУДЕБНОЙ ЭКСПЕРТИЗЫ

АНТОНОВ О.Ю. Классификация следов преступной деятельности, фиксируемых с помощью информационно-телекоммуникационных технологий, и ее значение для решения экспертных задач..... 14

ДЬЯКОНОВА О.Г. Унификация положений об использовании специальных знаний в судопроизводстве как вектор развития правового макроинститута 21

КОКИН А.В. Правосубъектность искусственного интеллекта в криминалистике и судебной экспертизе..... 46

ЛАВЕЛИНА В.В. Федеральная база данных геномной информации: исторический контекст развития 55

ЛОГВИНЕЦ Е.А., КАТОРГИНА Н.П. О классификации цифровых следов в криминалистике..... 64

ХАТУНЦЕВ Н.А. Электронное обеспечение судебно-экспертной деятельности 78

ЧИСТИЛИНА А.С. Процессы формирования и развития новых родов и видов экспертиз как объекты судебно-экспертного прогнозирования.... 85

ТРЕБОВАНИЯ ДЛЯ АВТОРОВ 91

АКТУАЛЬНЫЕ ПРОБЛЕМЫ КРИМИНАЛИСТИКИ И СУДЕБНОЙ ЭКСПЕРТИЗЫ

КЛАССИФИКАЦИЯ СЛЕДОВ ПРЕСТУПНОЙ ДЕЯТЕЛЬНОСТИ, ФИКСИРУЕМЫХ С ПОМОЩЬЮ ИНФОРМАЦИОННО- ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ, И ЕЕ ЗНАЧЕНИЕ ДЛЯ РЕШЕНИЯ ЭКСПЕРТНЫХ ЗАДАЧ

Антонов О.Ю.

Аннотация. Статья посвящена содержанию и видам следов преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. Цель исследования – формирование новой классификации рассматриваемых следов. Предложенная классификация позволяет выделить диагностическое и идентификационное значение каждого вида следов для последующего исследования. Предложено использовать в науке криминалистике и следственно-судебной практике термин «следы преступной деятельности, фиксируемые с помощью информационно-телекоммуникационных технологий». Обосновано, что такие следы могут быть зафиксированы вне зависимости от воли и желания преступника и, соответственно, отражать определенные знания, умения и навыки лиц, совершающих преступление, либо их признаки внешности или другие обстоятельства совершенного деяния.

Ключевые слова: информационные технологии, преступления, совершенные с использованием информационно-телекоммуникационных технологий, криминалистическая техника, цифровые следы.

Для цитирования: Антонов О.Ю. Классификация следов преступной деятельности, фиксируемых с помощью информационно-телекоммуникационных технологий, и ее значение для решения экспертных задач //Вестник криминалистики. 2023. № 1. С.14-20.

Как обоснованно отмечается в криминалистической литературе, процессы цифровизации в раскрытии и расследовании преступлений проявляются через широкое использование цифровых средств фиксации, сохранения, автоматизированной обработки и исследования доказательственной и ориентирующей информации,

а также через новые виды криминалистические значимой информации, фиксируемой на компьютерных носителях [1, с. 15, 41.].

Действительно, с помощью компьютерных средств и информационно-телекоммуникационных технологий можно фиксировать следы любого вида преступной деятельности.

В рамках развития учения о цифровых следах как источниках криминалистически значимой компьютерной информации, являющегося частью теории информационно-компьютерного обеспечения криминалистической деятельности, разработанной Е.Р. Россинской, А.И. Семикаленовой, И.А. Рядовским и Т.А. Сааковым [1, с. 19], можно предложить свою точку зрения на сущность и виды следов преступной деятельности, фиксируемых с помощью информационно-телекоммуникационных технологий.

Присоединяясь к точки зрения большинства ученых-криминалистов о то, что данные следы имеют материальных характер, поскольку отображаются в массиве памяти компьютерной системы, можно рассмотреть их с точки зрения российского уголовного процесса следующим образом, используя предложенную Е.Р. Россинской, А.И. Семикаленовой, И.А. Рядовским и Т.А. Сааковым классификации цифровых доказательств, подразделяемых на оригинал, его дубликат и копию.

Само компьютерное средство (персональный компьютер, мобильное устройство), содержащее носители данных (микросхемы памяти), выступает в качестве вещественного доказательства, а находящиеся в его памяти информационные объекты – оригинальными доказательствами. Компьютерное средство, на котором информация сохраняется пользователем путем удаленного доступа – удаленный сервер, облачное хранилище – может выступать в качестве вещественного доказательства только в случае его непосредственного изъятия, что практически невозможно.

Энергонезависимые носители данных (магнитные и лазерные диски, флэш-карты, портативные жесткие диски и др.), хранящие точную цифровую репродукцию информационных объектов, полученную путем копирования в ходе следственных действий, в том числе из удаленного сервера или облачного хранилища, являются дубликатом доказательств, выступая в уголовном процессе в качестве вещественного доказательства.

Распечатки информации, содержащейся памяти компьютерных средств и носителей цифровых данных, и распечатанные скриншоты информации, отображенной на экране компьютерного средства, имеют непосредственное доказательственное значение в качестве иных документов, поскольку содержат копию (репродукцию) информации, хранящейся в том числе в режиме удаленного доступа.

Развивая позицию А.Г. Себякина, подразделяющего электронно-цифровые следы на непосредственные и опосредованные [2, с. 22-23, 27], можно предложить классифицировать следы преступлений, фиксируемые с помощью информационно-телекоммуникационных технологий, по двум основаниям: степень опосредованности воздействия пользователя на компьютерную систему и результат этого воздействия – следующим образом:

– под непосредственно-пользовательскими следами будут подразумеваться цифровые следы, имеющие прямую (непосредственную) связь с причиной (целью) воздействия пользователя на компьютерную систему, по результатам которого пользователем создается новая компьютерная информация. В качестве таких следов выступают компьютерные данные, образованные пользователем посредством устройств ввода (клавиатура, микрофон, светочувствительная матрица и пр.), в результате чего создаются новые файлы или программное обеспечение, хранящиеся в памяти компьютерной системы или в режиме удаленного доступа;

– непосредственно-коммуникационные – это цифровые следы, имеющие прямую (непосредственную) связь с причиной (целью) воздействия, но образуемые программным обеспечением, фиксирующим действия пользователя по поиску или передаче компьютерной информации: скопированные (перемещённые) файлы, почтовые отправления, переписка с использованием мессенджеров, история запросов Интернет-браузера, журнал вызовов, записи в прикладных базах данных и пр. Указанные следы также могут быть как локальными (то есть находящимися непосредственно на носителе, который может быть изъят и подвержен исследованию), так и удалёнными (находящимися на ресурсе, доступ к которому обеспечивается с применением средств телекоммуникации, т.е. канала связи);

– в качестве опосредованных следов будут рассматриваться цифровые следы, не имеющие прямой связи с причиной (целью) воздействия пользователя на компьютерную систему, но инициированные этим воздействием, обусловленные особенностями функционирования системного программного обеспечения, стандартами форматов файлов и протоколов передачи данных. К таким следам будут

относиться находящиеся на используемой компьютерной системе записи в файлах журналирования системных событий, файлах реестра операционной системы, метаданные пользовательских файлов, записи служебных баз данных, таблиц размещения файлов и пр.;

– внешними электронными следами можно считать следы деятельности участников преступления, не связанной с воздействием на конкретную компьютерную систему, но инициированные различными компьютерными или информационно-телекоммуникационными системами, направленными на сбор информации, подпадающей под сферу их функционирования (камеры видеонаблюдения, базовые станции операторов связи, телематические системы автомобиля и т.п.), и отображаемые в устройствах памяти, как установленных в технических средствах участников преступления (например, электронных блоков управления или мультимедийных устройствах автомобиля), так и в указанных внешних системах.

При этом, непосредственные следы в виде созданных пользователей файлов или программного обеспечения, например, вирусной программы, а также опосредованные следы могут быть объектами компьютерно-технической судебной экспертизы, в том числе первые – в целях идентификации пользователя, их создавшего. Содержание данных файлов в печатном виде может стать объектом соответствующего вида судебной экспертизы, например, судебно-бухгалтерской по исследованию документов, выгруженных из информационной базы «1С: Предприятие».

Непосредственно-коммуникационные и внешние следы могут выступать в качестве традиционных объектов различных видов судебных экспертиз, отображенные в электронно-цифровом виде. Например, файлы, содержащие электронные сообщения, отправленные в любом мессенджере (непосредственно-коммуникационный след), могут исследоваться в рамках судебных речеведческих экспертиз, в том числе в целях идентификации их автора, а видеозапись камеры наружного наблюдения (внешний след) – стать объектом судебно-портретной экспертизы, в том числе в целях идентификации запечатленного на ней лица.

Что касается внешних цифровых следов, то они фиксируют факт регистрации (нахождения, подключения) на объекте (территории) их обслуживания какого-либо средства, как электронного (например, транспортная карта или карт-пропуск), так и иного, например, автотранспорта по его регистрационному номеру.

В случае большого объема информации, отображенной в опосредованных и внешних цифровых следах (Big Data) на носителе данных, она может стать объектом нового вида судебных экспертиз – информационно-аналитическая [см., подр.: 3] или анализироваться с помощью аппаратно-программных комплексов в ходе осмотра цифровых носителей информации.

На основании изложенного, более оптимальным предлагается использовать в науке криминалистике и следственно-судебной практике термин «следы преступной деятельности, фиксируемые с помощью информационно-телекоммуникационных технологий» и описанную классификацию данных следов, большая часть из которых может являться объектом различного вида судебных экспертиз. Представляется, что понятие «преступная деятельность» наиболее четко отражает систему действий, выполняемых субъектом преступления в рамках замышления, подготовки, реализации и маскировки преступного замысла. При этом в предлагаемой дефиниции такие действия могут быть зафиксированы при помощи информационных технологий вне зависимости от воли и желания преступника и, соответственно, отражать определенные знания, умения и навыки лиц, совершающих преступление, либо их признаки внешности или другие обстоятельства совершенного деяния.

Библиографический список:

1. Теория информационно-компьютерного обеспечения криминалистической деятельности: монография / под ред. Е.Р. Россинской. М.: Проспект, 2022. 256 с.
2. Себякин А.Г. Тактика использования знаний в области компьютерной техники. М.: Юрлинформ, 2023. Сер. Библиотека криминалиста. 200 с.
3. Антонов О.Ю. Международные и национальные тенденции и перспективы развития информационно-аналитической судебной экспертизы // Международные и национальные тенденции и перспективы развития судебной экспертизы: сборник докладов II Международной научной конференции, г. Нижний Новгород, 21–22 мая 2020 г. Нижний Новгород: ННГУ, 2020. С. 30-37.

References:

1. Theory of information and computer support of criminalistic activity: monograph / edited by E.R. Rossinskaya. M.: Prospect, 2022. 256 p. (In Russ.)

2. Sebyakin A.G. Tactics of using knowledge in the field of computer technology. M.: Yurlitinform, 2023. Ser. Criminalist Library. 200 p. (In Russ.)

3. Antonov O.Yu. International and national trends and prospects for the development of information and analytical forensic examination // International and national trends and prospects for the development of forensic examination: Collection of reports of the II International Scientific Conference, Nizhny Novgorod, May 21-22, 2020 Nizhny Novgorod: UNN, 2020. Pp. 30-37. (In Russ.)

Oleg Yu. Antonov

CLASSIFICATION OF TRACES OF CRIMINAL ACTIVITY RECORDED WITH THE USE OF INFORMATION AND TELECOMMUNICATION TECHNOLOGIES AND ITS SIGNIFICANCE FOR SOLVING EXPERT TASKS

Abstract. The article deals with the content and types of traces of crimes committed with the use of information and telecommunication technologies. The purpose of the study is to form a new classification of the traces under consideration. The proposed classification allows to determine diagnostic and identification meaning of each trace type for further investigations. It is proposed to use the term “traces of criminal activity, recorded by means of information and telecommunication technologies” in forensic science and investigative and judicial practice. It is proved that such traces can be recorded irrespective of the will and desire of the criminal and consequently reflect certain knowledge, abilities and skills of persons committing a crime or their signs of appearance or other circumstances of the committed act.

Keywords: information technologies, crimes committed with the use of information and telecommunication technologies, forensic techniques, digital traces.

Сведения об авторе:

Антонов Олег Юрьевич – доктор юридических наук, доцент, полковник юстиции, декан факультета подготовки криминалистов, ФГКОУ ВО «Московская академия Следственного комитета Российской Федерации»

Адрес электронной почты: antonov@udm.ru

АНТОНОВ О.Ю.

About the author:

Oleg Yu. Antonov – Doctor of Sciences (Law), Assistant Professor, Colonel of Justice, Dean of Criminalists Training Faculty, the Moscow Academy of the Investigative Committee of the Russian Federation

E-mail: antonov@udm.ru

© Антонов О.Ю., 2023