УДК 343,98

Островский О.А.
ФГБОУ ВО «Алтайский государственный университет», Томск,
e-mail: ostrovskii_80@mail.ru

АСПЕКТЫ СОВРЕМЕННЫХ ПРОБЛЕМ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С ИЗЪЯТИЕМ ЦИФРОВЫХ СЛЕДОВ И ПРЕДОСТАВЛЕНИЕМ СООТВЕТСТВУЮЩИХ ДОКАЗАТЕЛЬСТВ

Ключевые слова: киберпреступления, цифровые следы, расследования преступлений, доказательства, криминалистика.

В статье рассматриваются аспекты современных проблем расследования киберпреступлений, связанные с изъятием цифровых следов и предоставлением соответствующих доказательств, представлены некоторые междисциплинарные стратегии решения текущих проблем. Целью исследования явилось рассмотрение научных взглядов на обозначенную проблематику. Приведена основная модель наблюдателя, которая описывает точку зрения судебной экспертизы. Аргументы в статье основаны на конкретных примерах и относятся к установленным процедурам. Существует огромное количество нерешенных вопросов в процессе расследования преступлений, основанных на исследовании цифровых следов, их рост обуславливается стремительным развитием цифровых технологий. Сотрудники правоохранительных органов часто встречаются с процедурными проблемами, такими как получение своевременного доступа к данным на зашифрованных устройствах или в облаке. При выполнении работы использовались методы фиксации фактов, условия и обстоятельства, выдвигаемые версии расследуемого события, наблюдение, измерение, описание, сравнение, эксперимент, моделирование, математико-кибернетические и эвристические методы. Результаты работы могут использоваться в области криминалистики при решении задач судебно-экспертной и оперативно-розыскной деятельности в рамках расследования преступления в сфере компьютерной информации и киберпреступности на основе анализа информационных следов различного спектра.

Ostrovskiy O.A.
Altai State University, Tomsk, e-mail: ostrovskii_80@mail.ru

ASPECTS OF MODERN PROBLEMS OF THE INVESTIGATION OF CRIMES RELATED TO THE ELIMINATION OF DIGITAL TRACES AND THE PROVISION OF RELEVANT EVIDENCE

Keywords: cybercrime, digital traces, crime investigation, evidence, forensics.

The article discusses aspects of contemporary problems of investigating cybercrime related to the seizure of digital traces and the provision of relevant evidence, presents some interdisciplinary strategies for solving current problems. The purpose of the study was to review scientific views on the designated issues. The main model of the observer, which describes the point of view of forensic examination, is given. Arguments in the article are based on specific examples and refer to the established procedures. There are a huge number of unresolved issues in the process of investigating crimes based on the study of digital traces, their growth is due to the rapid development of digital technologies. Law enforcement officers often encounter procedural problems, such as getting timely access to data on encrypted devices or in the cloud. In carrying out the work, the methods of fixing facts, conditions and circumstances, put forward versions of the investigated event, observation, measurement, description, comparison, experiment, simulation, mathematics-cybernetic and heuristic methods were used. The results of the work can be used in the field of forensics in solving the tasks of forensic and operational and investigative activities in the framework of investigating computer crime and cybercrime based on the analysis of information traces of a different spectrum.

Расследования преступлений в сфере киберпреступности имеют много аспектов, и являются одним из важнейших элементов в области криминалистики. Существует огромное количество нерешенных вопросов в процессе расследования преступлений, основанных на исследовании цифровых следов, их рост обуславливается стремительным развитием цифровых технологий.

Сотрудники правоохранительных органов часто встречаются с процедурными проблемами, такими как получение своевременного доступа к данным на зашифрованных устройствах или в облаке. Эти технические проблемы также включают в себя такие понятия как: обратная инженерия и большой анализ данных. Необходимо постоянно устанавливать связи между виртуальными и физическими носителями информационных следов, и оценивать вероятность получения доказательств по одной теории в сравнении с альтернативными. Криминалистам приходится постоянно разрабатывать более широкие стратегии борьбы с киберпреступностью. Бизнес-менеджеры сталкиваются с проблемами управления рисками, в том числе кражу данных и связанные с этим меры регулирования. Аналитики разведки сталкиваются с проблемами в обеспечении национальной безопасности. Не мало важными являются проблемы защиты частной информации от несанкционированного доступа [1,2].

Этот широкий круг проблем подчеркивает необходимость решения междисциплинарных проблем, которые должны по своей сути удовлетворять различным интересам и рискам. Цифровые доказательства широко используются в суде, но до сих пор являются актуальными вопросы о достоверности результатов судебных экспертиз. Это всё создает технические и юридические барьеры для доступа к данным. Несмотря на то, что в течение последних двух десятилетий криминалисты в области цифрового расследования добились значительного прогресса, появляются всё новые и новые вызовы, которые мы должны решать. Существует сильное сообщество исследователей и практиков, работающих над поиском эффективных решений на благо общества.

Цифровые исследования становятся все более дорогостоящими и сложными, что делает их недостижимыми для менее финансируемых исследователей и практиков, разработчиков программного обеспечения с открытым исходным кодом, даже в развитых странах мира. Эти препятствия частично обусловлены отдельно взятыми лицензиями на собственные программные решения, вопросов доступа к заблокированным устройствам, использованием передовых методов, требующими специализированного оборудования и опыта [3]. Использование «сильных» криптографических методов, а также циклов быстрого развития ограничивает информацию, доступную для использования в цифровых исследованиях. Кроме того, производители цифровых устройств добавляют в свои разработки специальные протоколы безопасности, которые делают цифровые исследования более сложными [4]. Например, недавно Apple объявила о планах отключить доступ через USB на устройствах, заблокированных в течение одной недели. Такие улучшения безопасности подогревают текущую дискуссию о том, следует ли потребовать от производителей добавлять альтернативные методы доступа для законного использования.

Для правительства более безопасно разрабатывать свои собственные узко направленные методы извлечения данных с заблокированных мобильных устройств. Другие утверждают, что текущая модель для извлечения цифровых данных из встроенных систем, таких как мобильные устройства, должна коренным образом измениться. Существующие методы извлечения основаны на бессистемном взломе этих устройств. Тот, кто имеет лучших «хакеров» в своем распоряжении, получает лучшее доказательство. Со временем эти уязвимости в мобильным системах исправляются официальными разработчиками и компаниями-производителями, а методы извлечения данных, успешно использующихся ранее, больше не работают.

Этот процесс является слишком ненадежным и имеет риски уничтожения или модификации доказательств [5].

Криминалисты в области исследования цифровых следов не взламывают учетные записи электронной почты, чтобы получить доступ к доказательствам электронной почты. Юридический запрос направляется почтовому прокси-серверу. Криминалисты не взламывают веб-сайты или облачные среды, чтобы

получить доказательства содержания, а юридический запрос делается на хостконтент. Также возможно доставить мобильное устройство непосредственно производителю и подать юридический запрос на изъятие доказательств, а не требовать взлома. Озабоченность по поводу несанкционированного доступа с помощью альтернативных методов доступа, безусловно, актуальна и должна быть решена. Однако такие проблемы аналогичны тем, которые связаны с несанкционированным доступом через уязвимости. В обоих случаях риски несанкционированного доступа могут (и должны) быть смягчены с помощью обновлений программного обеспечения при обнаружении производителем.

Теперь рассмотрим возможности и риски более свободного доступа к цифровым данным, включая сотрудников правоохранительных органов на месте преступления, сотрудников службы безопасности в компании, авторитарных режимов, отдельных хакеров, организованных преступников.

В зависимости от контекста и использования возможности цифрового исследования могут использоваться в качестве полезных инструментов или вредных инструментов [6]. Цифровые возможности исследования используются для поддержания безопасности общества, борьбы с киберпреступностью и террористическими атаками. С другой стороны, люди, которые не имеют надлежащего управления, злоупотребляют цифровыми возможностями расследования, выходящими за рамки их должностных полномочий, тем самым нарушая закон [7].

Эти возможности и риски усугубляются растущим числом постоянно наблюдаемых, всегда прослушивающих устройств, распространяющихся по всему цифровому обществу, которые чувствуют действия и генерируют связанные с ними следы (например, умные помощники, умные очки, широко распространенные системы видеонаблюдения, интеллектуальные автомобильные камеры). В некоторых случаях остаются свидетели.

Для этих сложных задач нет простого средства защиты. Развивающиеся страны имеют ограниченные ресурсы для проведения цифровых расследований, ограничивая их способность бороться с коррупцией и насилием, что может способствовать политической и экономической нестабильности. Кроме того, даже высокозащищенный централизованный контроль не является отказоустойчивым. Для поддержки цифровых исследований, к примеру, правительство США разработало новые способы использования уязвимостей в операционных системах Microsoft, но информация была украдена и впоследствии использована в незаконных атаках [8].

Важно избегать ошибок, упущенных возможностей, неправильных толкований и искажений данных, т.к. постоянная проблема в цифровых исследованиях – обеспечение достоверности доказательств.

Для повышения качества и надежности результатов судебных экспертиз разрабатываются и поддерживаются различные практические руководства во всем мире. Кроме того, внедряются стандарты ISO и ASTM для обеспечения гарантии качества и надежности судебных результатов.

Еще одна проблема заключается в том, что данные телеметрии, собранные поставщиками услуг, уже используются в судебных расследованиях, но могут не иметь достаточной надежности и достоверности. Например, когда исследование с целью изучения местоположения связано с использованием анализа сайта или геолокации с мобильных устройств, важно учитывать возможные ошибки. Кроме того, криминалисты в цифровой области должны уметь четко оценить и выразить свои результаты исследований и соответствующие выводы, чтобы эти выводы не могли восприниматься двояко судом.

Еще одна проблема заключается в оценке достоверности результатов, полученных различными формами искусственного интеллекта, которые применяются для анализа данных, собранных во время цифровых исследований. На-

пример, машинное обучение может давать надежные результаты, но у экспертов часто возникают трудности с объяснением того, как были получены результаты. Этот вопрос дополнительно усугубляется, когда извлечение и корреляция признаков полностью выполняются алгоритмами с использованием методов глубокого обучения.

В дополнение к извлечению данных с отдельных устройств, собирается огромное количество информации с компьютеров и систем связи, чтобы получить глубокое понимание деятельности и поведения людей, создания возможностей для проведения цифровых расследований. В большем числе преступлений люди, снимающие видео с мобильных устройств, предоставили ценные цифровые данные. В будущем толпа людей с умными очками может быть использована в качестве коллективного источника доказательств.

Тщательный анализ большого количества данных может улучшить понимание мотивов преступника, позволяя проводить более целенаправленное расследование, например, где можно найти дополнительные доказательства, что заслуживает более глубокой проверки, и даже там, где можно избежать значительных усилий и времени. Растущий объем информации, собираемой в ходе цифровых расследований, также может быть использован для получения более широкого понимания преступности, преступников, жертв и уязвимостей. Объединение информации из нескольких преступлений может связывать преступления, совершенные одним и тем же преступником (-ами), может выявлять тенденции в преступной деятельности и может помочь в разработке более эффективных стратегий расследования и превентивных действий. С другой стороны, организации, обладающие достаточными деньгами, властью или знаниями, могут использовать эти источники данных, используя большой анализ данных для целевых лиц с определенными целями. Кроме того, существует риск получения преступниками несанкционированного доступа к огромному количеству конфиденциальной информации [9].

Цифровая конфиденциальность играет центральную роль в современном обществе. Грамотно проработанные цифровые исследования помогают устранять злоупотребления личной информацией. Законодательство должно одновременно защищать личные данные и допускать законные расследования преступной деятельности. Кроме того, необходимы упорядоченные судебные процессы, чтобы помочь криминалистам объединить информацию из нескольких преступлений, бороться с международной или организованной преступностью и разработать более широкие стратегии борьбы с преступностью.

В вопросах киберпреступности необходимо прорабатывать стратегии международного сотрудничества, что в свою очередь увеличивает шансы быстрого расследования преступлений. Но, некоторые аспекты и процессы взаимной правовой помощи могут быть неэффективны для многих расследований, и действующие законы в одной стране могут противоречить законам в другой.

Блокировка устройств, зашифрованное хранилище и зашифрованный трафик продолжают оставаться существенным препятствием для доступа к цифровым доказательствам. Стандарты шифрования, основанного на идентификации в 5G, только разрабатываются, и это будет создавать дополнительные барьеры, если нет исключений для правоохранительных органов. Эта проблема должна решаться либо законодательством, либо добровольным сотрудничеством со стороной промышленности, либо увеличением инвестиций в НИОКР.

Анализ носящих приспособлений, медицинских устройств (имплантатов) и других личных устройств Интернет-вещей (IoT) станет более важным. Следы на устройствах IoT могут помочь определить точное время смерти или присутствие человека в доме в момент совершения преступления. Промышленные системы управления (SCADA и т.д.), спутниковые системы, интеллектуальные здания, автомобили и другая интеллектуальная физическая инфраструктура нуждаются в некоторых стан-

дартизированных процессах судебной составляющей.

Дополнительные данные перемещаются в облачные среды, которые контролируются третьими лицами. Данные телеметрии, полученные каждой операционной системы, приложением и устройством (и отправленные на многочисленные серверы или облака), собираются различными организациями и становятся основным источником доказательств. Преимущество централизованного сбора таких данных телеметрии заключается в том, что ее можно получить с помощью ордера правоохранительными органами. В настоящее время личная информация о большинстве облачных систем зашифрована, но поставщики услуг все еще могут получить доступ к личной информации пользователей для поддержки своих маркетинговых услуг. Тем не менее, Apple планирует перейти на нулевую облачную систему знаний, чтобы вся информация была доступна только пользователю и могла, настраивается индивидуально по желанию пользователя.

Многие серверные хранилища уже переместились в облако, а настольные компьютеры – в инфраструктуру виртуального рабочего стола (VDI), и нуждаются в дальнейшем анализе. Корпорации полностью переходят в инфраструктуру VDI, а существующие судебные методы недостаточно развиты.

Разработки и усилия по борьбе с киберпреступностью изо всех сил стараются не отставать от растущего количества онлайн-мошенников, финансового мошенничества, кражи личных данных, нарушений данных, заражения вредоносными программами, вымогательства и других преступлений.

В результате стоит выделить несколько целей для решения задач цифрового расследования:

1) Более тесное сотрудничество между промышленностью и правительством;

2) Больше централизации исследований, разработки и администрирования передовых технологий цифрового исследования;

3) Упорядоченные механизмы обмена информацией о цифровом расследовании между организациями и странами;

4) Расширение доступности знаний о цифровых исследованиях и расширенных возможностей при централизованном надзоре для неспециалистов, работающих в децентрализованных средах.

Объединение этих целей в эффективную междисциплинарную стратегию для решения многих задач расследования преступлений в сфере киберпреступности предполагает укрепление сотрудничества между промышленностью и правительствами различных стран. А также балансирование развертывания децентрализации с централизованными исследованиями и разработками и обеспечение надежного доступа к цифровым доказательствам при строгом юридическом контроле и процедурном надзоре для предотвращения злоупотреблений, обеспечения гарантии качества и обеспечения равного доступа к уполномоченным организациям.

Для решения возникающих проблем цифрового расследования необходима централизация исследований, разработок и администрирования. Исследования и разработки для получения доступа к данным на цифровых устройствах являются дорогостоящими, требующими специализированной экспертизы и существенных инвестиций времени и ресурсов. Анализ аппаратной части, в том числе чипов и изменение аппаратных схем требуют специализации и значительного инвестирования ресурсов. Проведение большого анализа данных по цифровым доказательствам требует специализации и дорогостоящей инфраструктуры, чтобы находить ценную информацию, обнаруживать повторения в преступной деятельности и формировать специальные стратегии для уменьшения социального вреда. В этих областях действуют компании и правительственные учреждения, и здесь необходимы совместные, централизованные усилия, которые делают это всё экономически эффективным и поддерживают качество судебных процессов и результатов.

В конечном счете, единые усилия по решению задач цифрового расследования создают большие возможности для достижения общих целей всех заинтересованных сторон для поддержания безопасного и стабильного общества.

Библиографический список

1. Багутдинов Р.А. Классификационная характеристика для задач обработки разнородных данных // International Journal of Open Information Technologies. – 2018. – Т. 6. – № 8. – С. 14-18.

2. Год небезопасности: крупнейшие хакерские атаки. – URL: https://www.gazeta.ru/tech/2017/12/30/11529068/hackerattacks_2017.shtml (дата обращение 14.10.2018).

3. Островский О.А. Алгоритмы проведения осмотров цифровых носителей информации для предотвращения компьютерных преступлений // Военно-юридический журнал. – 2017. – № 11. – С. 3-6.

4. Островский О.А. Дефиницальный анализ корреляционной зависимости информационной модели и криминалистической характеристики преступления в сфере компьютерной информации // Евразийский юридический журнал. – 2017. – № 7 (110). – С. 221-225.

5. Пастухов П.С., Лосавио М. Использование информационных технологий для обеспечения безопасности личности, общества и государства // Вестник Пермского университета. Юридические науки. – 2017. – Вып. 36. – С. 231–236.

6. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 03.10.2018). Статья 286. Превышение должностных полномочий.

7. Федеральный закон от 6 июля 2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности».

8. Федеральный закон от 6 июля 2016 г. № 375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности».

9. Bagutdinov R.A., Zaharova A.A. The task adaptation method for determining the optical flow problem of interactive objects recognition in real time // Journal of Physics: Conference Series. – 2017. – Т. 803. – № 1.

10. Bagutdinov R.A. The processing of heterogeneous data for multisensor systems of technical vision on the example of analysis of temperature and gas concentration // National Research Tomsk Polytechnic University. – 2018. – С. 25-26.

11. Багутдинов Р.А. Гносеологические аспекты к определению назначения и состава стз в задачах проектирования и разработки робототехнических комплексов // Программные системы и вычислительные методы. – 2017. – №1. – С. 39-45.

12. Островский О.А. Принцип объектной декомпозиции в систематизации идентификационных кодов, характеризующих преступления в сфере компьютерной информации // Полицейская деятельность. – 2017. – № 3. – С. 10-18.

13. Островский О.А. Криминалистический анализ, описывающий состояние детерминированного конечного автомата в модели наблюдателя при расследовании преступлений в сфере компьютерной информации // Евразийский юридический журнал. – 2018. – № 3(118). – С. 294-296.

14. Островский О.А. Алгоритм мероприятий по анализу ситуации при подозрении в совершении преступлений в сфере компьютерной информации с учетом специфики источников данных этой информации // Право и политика. – 2018. – №10. – С. 32-37.