УДК 343

СОВЕРШЕНСТВОВАНИЕ ТЕХНИКО-КРИМИНАЛИСТИЧЕСКИХ МЕТОДОВ В СИСТЕМЕ ОБЕСПЕЧЕНИЯ НАИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Пахритдинова Адема Шамилевна
Adema.96@mail.ru
Магистрантка 2-го курса кафедры уголовно-правовых дисциплин ЕНУ им. Л.Н.Гумилева, Нур-Султан, Казахстан
Научный руководитель – Б.Р. Сембекова

Цифровая криминалистика является быстро развивающейся областью. В цифровой криминалистике существует множество проблем, .как связанных с технологическим обеспечением так и с процессуальными недостатками.

Согласно ст. 34 ЗРК «О судебно-экспертной деятельности» срок производства судебной экспертизы не должен превыщать 30 суток со дня получения псотановления о проведения судебной экспертизы [1]. Но в настоящее время на одном цифровом носителе например, телефон может иметь 1 терабайт данных, что составляет 78 миллионов документов, или страницы информации на одном мобильном устройстве, и это просто физически невозможно для следователя просматривать, раскрывать, анализировать, извлекать и прочитайть всю эту информацию и современные технологии в области цифровой криминалистики не соответствуют требованиям законодательства относительно сроков. Поэтому искусственный интеллект и эксперт должны обучаться и работать в коллаборации. На данный момент в Республике не имеются технологии, которые бы соответствовали критериям научности и в сроки давали результаты, и были бы просты в использовании экспертам. Проблема в слабой обеспеченности технологии существует даже в Великобритании: «Существует мало исследований в области методов для просеивания и анализа данных, с помощью искусственного интеллекта и машинного обучения» - Пол Хакетт, Управляющий директор Key Forensic Services Ltd сказал: «Кто продвигает технология в искусственном интеллекте в цифровой криминалистике в Великобритании?... Никто» [2].

Проблема цифровой криминалистики состоит не только в слабом техническом обеспечении, но так же в неполноте законодательной базы, что затрудняет международное сотрудничество, что и является краеугольным камнем в обеспечении национальной безопасности страны. Согласно ст. 121 УПК РК Доказывание состоит в собирании, исследовании, оценке и использовании доказательств с целью установления обстоятельств, имеющих значение для законного, обоснованного и справедливого разрешения дела. Международная организация по стандартизации (ИСО, международная неправительственная организация) и Международная электротехническая комиссия (МЭК, международная некоммерческая организация) разрабатывают и публикуют международные стандарты для унификации практики, используемой в разных странах. В 2012 году Международная организация по стандартизации (ИСО) и Международная электротехническая комиссия (МЭК) опубликовали международные стандарты, касающиеся обращения с цифровыми доказательствами (ISO/IEC 27037 Руководство по 13 идентификации, сбору, получению и сохранению свидетельств, представленных в цифровой форме). Это руководство охватывает только начальный процесс обращения с цифровыми доказательствами. Предлагаются следующие четыре этапа обращения с цифровыми доказательствами:

1. Идентификация. Этот этап включает в себя поиск и распознавание соответствующих доказательств, а также их документирование. На этом этапе приоритетные задачи сбора доказательств определяются на основе ценности и изменчивости доказательств.
2. Сбор. Этот этап предполагает сбор всех цифровых устройств, которые могут содержать данные, имеющие доказательную ценность. Эти устройства затем транспортируются в лабораторию судебной экспертизы или другое учреждение для сбора и анализа цифровых доказательств. Этот процесс именуется сбором данных в статическом режиме. Однако бывают случаи, когда сбор данных в статическом режиме является практически неосуществимым. В таких ситуациях осуществляется сбор данных в реальном времени. Рассмотрим, к примеру, системы критически важных объектов инфраструктуры (например, системы управления производственными процессами). Эти системы не могут быть отключены от питания, поскольку они предоставляют критически важные услуги. Поэтому в этих случаях осуществляется сбор данных в реальном времени, когда изменчивые и неизменчивые данные извлекаются из систем, работающих в реальном времени. Однако такой сбор данных в реальном времени может мешать нормальному функционированию систем управления производственными процессами (например, замедлять их работу).

Однако следует помнить, прежде чем приступить к сбору данных в реальном времени, следует определить приоритеты сбора данных с точки зрения их доступности, а также их ценности и изменчивости.

3. Получение. Цифровые доказательства необходимо получать без ущерба для целостности данных. Национальный совет начальников полиции Соединенного Королевства (NPCC), ранее известный как Ассоциация руководителей полицейских служб Соединенного Королевства, придает этому требованию большое значение и выделяет его в качестве важного принципа в практике цифровой криминалистики (принцип №.1: «Никакие действия, предпринимаемые правоохранительными органами, лицами, работающими в этих органах, или их представителями, не должны приводить к изменению данных, которые впоследствии могут использоваться в суде»). [3] Такое получение данных без их изменения осуществляется путем создания копии содержимого цифрового устройства (процесс, известный как создание неискаженного образа) с использованием устройства (блокировщика записи), которое предназначено для предотвращения изменения данных в процессе копирования. Для того чтобы определить, является ли дубликат точной копией оригинала, значение хэшфункции рассчитывается с использованием математических вычислений; здесь для получения значения хэш-функции используется криптографическая хэш-функция. Если значения хэш-функции для оригинала и копии совпадают, то содержимое копии является точно таким же, что и в оригинале. Признавая возможность существования определенных «обстоятельств, при которых какое-либо лицо считает необходимым получить доступ к исходным данным (т.е. осуществить сбор данных в реальном времени)», Национальный совет начальников полиции Соединенного Королевства отмечает, что «лицо, (получающее доступ к этим данным), должно быть компетентным для таких действий и быть в состоянии представить доказательства, объясняющие целесообразность своих действий и их последствия» [4].

4. Сохранение. Целостность цифровых устройств и цифровых доказательств может быть обеспечена с использованием системы охраны доказательств, которая определяется как «процесс, при помощи которого следователи обеспечивают охрану места преступления (или происшествия) и сохранность доказательств на протяжении всего периода производства по делу. В журнал регистрации записывают информацию о том, кто осуществлял сбор доказательств, где и каким образом они были собраны, какие лица получили эти доказательства, и когда они их получили» [5] (Maras, 2014, p. 377). Тщательное документирование процесса цифровой судебной экспертизы на каждом этапе имеет важное значение для обеспечения допустимости доказательств в суде).

Остальные этапы процесса цифровой судебной экспертизы (анализ и отчетность) не включены в руководство ISO/IEC 27037. Этап анализа (или исследования) требует использования надлежащих инструментов и методов цифровой криминалистики для обнаружения цифровых данных. На рынке доступно большое количество инструментов самого разного качества для проведения цифровой судебной экспертизы. Примеры инструментов для цифровой криминалистической экспертизы включают в себя программы EnCase, FTK, и X-Ways Forensics. Выбор типа инструмента зависит от типа проводимой цифровой судебной экспертизы (например, для криминалистической экспертизы мобильных устройств и облачных сервисов на мобильных устройствах можно использовать программу Oxygen Forensics Suite; для сетевой криминалистики в качестве инструмента можно использовать программу Wireshark). Существующие инструменты цифровой криминалистики (например, EnCase, FTK и NUIX) предназначены для работы с традиционными вычислительными устройствами. Специализированные инструменты цифровой криминалистики необходимы, например, для экспертизы сетей, интерфейсов и операционных систем критически важных объектов инфраструктуры.

Массовое использование интеллектуальных транспортных средств с функциями выхода в Интернет (и разработка автономных транспортных средств) придали дополнительный импульс усилиям по созданию процедур, стандартов и инструментов

проведения криминалистической экспертизы интеллектуальных транспортных средств, которые могли бы обеспечить возможность проведения надежной с точки зрения криминалистики цифровой экспертизы таких средств. Эти транспортные средства могут обеспечить получение большого количества информации (например, о маршрутах поездок и часто посещаемых местах, домашних и рабочих адресах, набранных номерах телефонов, принятых звонках и т.д.), которая может использоваться при расследовании преступлений, совершенных в отношении интеллектуальных или автономных транспортных средств (например, взлома), или других преступлений, когда информация, полученная из этих транспортных средств, может быть использована в качестве доказательства совершения преступления.

Используемые инструменты должны быть надежными с точки зрения криминалистики. При этом процесс «сбора и последующего анализа… [цифровых] данных» с помощью этих инструментов должен быть в состоянии сохранить «данные в том состоянии, в котором они были впервые обнаружены», и «никоим образом не уменьшать доказательную ценность электронных данных из-за технических или процедурных ошибок либо ошибок в интерпретации».

Проще говоря, полученные данные не должны быть каким-либо образом изменены, то есть их целостность должна быть сохранена. В рамках Программы тестирования инструментов компьютерной криминалистики Национального института стандартов и технологий США была принята методология тестирования программных средств компьютерно-технической экспертизы на основе разработки общих спецификаций инструментов, процедур испытаний, критериев испытаний, наборов тестов и оборудования для тестирования. Тестирование дает возможность получить информацию, которая необходима разработчикам для совершенствования разрабатываемых инструментов, позволяет пользователям делать осознанный выбор в отношении приобретения и использования инструментов компьютерно-технической экспертизы и способствует пониманию возможностей инструментов всеми заинтересованными сторонами.

Целью этапа анализа является определение значимости и доказательственной силы свидетельств. Это делается, например, путем определения того, имеет ли рассматриваемое доказательство «тенденцию делать существование любого факта, имеющего значение для разрешения дела, более или менее вероятным, чем это было бы без этого доказательства». Этап отчетности включает в себя подробное описание шагов, предпринятых на протяжении всего процесса цифровой судебной экспертизы, обнаруженных цифровых доказательств и выводов, сделанных на основе результатов цифровой судебной экспертизы и обнаруженных доказательств. Искусственный интеллект может использоваться для получения достоверных результатов. Однако использование искусственного интеллекта может создавать проблемы на этапах анализа и представления данных процесса цифровой судебной экспертизы, поскольку эксперты могут быть не в состоянии объяснить, как были получены эти результаты. ИСО/МЭК опубликовали дополнительные руководства по процессу цифровой криминалистики, которые охватывают: достоверность и надёжность инструментов и методов цифровой судебной экспертизы. Эти стандарты не предназначены для нетрадиционных вычислительных систем, таких как облачные вычисления. Тем не менее, Cloud Security Alliance (Альянс безопасности в облаке) опубликовал документ под названием «Привязка криминалистического стандарта ISO/IEC 27037 к облачным вычислениям» с целью «нового истолкования руководства ISO 27037 для облачного контекста» [5].

В настоящее время доступны руководства по передовой практике для определения и популяризации обоснованных и надежных процессов и результатов цифровой судебной экспертизы. В качестве примеров можно привести руководство по передовой практике, разработанное в США Научной рабочей группой по цифровым доказательствам, для компьютерно-технической судебной экспертизы, сбора цифровых доказательств и сбора данных для компьютерно-технической экспертизы, а также руководство по передовой практике Европейской Сети судебно-экспертных учреждений для судебной экспертизы

цифровых технологий. Эти стандарты и передовые практические методы используются с целью установления обоснованности и достоверности результатов цифровой судебной экспертизы. Во-первых, для того они были допустимыми, инструменты и методы, используемые в процессе цифровой судебной экспертизы, должны быть «научно обоснованными», то есть путем эмпирического тестирования должно быть доказано, что они дают точные результаты. Во-вторых, результаты цифровой судебной экспертизы должны быть достоверными, то есть одни и те же результаты должны быть получены в разных случаях с использованием одних и тех же данных, инструментов и методов. В частности, результаты должны быть повторяемыми и воспроизводимыми. Результаты являются повторяемыми, когда одни и те же результаты цифровой судебной экспертизы получаются с использованием одних и тех же тестируемых предметов, оборудования, лаборатории и оператора. Результаты являются воспроизводимыми, когда одни и те же результаты цифровой судебной экспертизы получаются с использованием одних и тех же тестируемых предметов, но с использованием разных видов оборудования, лабораторий и операторов. Как отметил Национальный совет начальников полиции Соединенного Королевства, важным принципом практики цифровой криминалистики является способность «независимой третьей стороны… изучать эти процессы и достигать того же результата».

Цифровая криминалистика включает в себя процессы идентификации, получения, сохранения, анализа и представления цифровых доказательств. Цифровые доказательства должны быть аутентифицированы, чтобы обеспечить их допустимость в суде. В конечном счете артефакты для судебно-экспертного анализа и используемые криминалистические методы (например, сбор данных в статическом режиме или в реальном времени) зависят от устройства, его операционной системы и его средств защиты. Реальность такова, что каждая страна следует своим собственным стандартам, протоколам и процедурам в области цифровой криминалистики и ее объектам и методам доказывания. Однако различия в этих процессах служат препятствием для осуществления международного сотрудничества в проведении расследований правоохранительными органами. Необходима их стандартизация для повышения качества работы органов преследования и дознания.

Список использованных источников:

13. ЗРК «О судебно-экспертной деятельности РК» от 18.04.2017г. adilet.gov
14. Paul Hackett, House of Lords, Science and Technology Select Committee Corrected oral evidence: forensic science, Q78.
15. UK Association of Police Chiefs. (2012). ACPO Good Practice Guide for Digital Evidence.https://www.digitaldetective.net/digitalforensicsdocuments/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf.
16. Vijayan, Jaikumar. (2017). Researchers from Google, CTI Break SHA-1 Hash Encryption Function. eWeek, 23 February 2017. http://www.eweek.com/security/researchers-from-google-cti-breaksha-1-hash-encryption-function .
17. U.S. National Institute of Justice. (2008). Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition. Second Edition. https://www.ncjrs.gov/pdffiles1/nij/219941.pdf