ВВЕДЕНИЕ

В настоящее время киберпреступления (преступления, связанные с хищением, разрушением, нарушением целостности компьютерной информацией) занимают лидирующее положение по числу совершенных преступлений и сумме ущерба, принесенного юридическим и физическим лицам. Так, согласно данным информационного ресурса «Ведомости», только за 2014 год правоохранительными органами было зарегистрировано более 11000 компьютерных преступлений в Российской Федерации. По данным Group-IB, ущерб от компьютерных преступлений в РФ увеличивается с каждым годом — в 2015 году ущерб увеличился на 2,649 млрд рублей по сравнению с 2014 годом, а в 2016 году — на 3,811 млрд рублей по сравнению с 2015 годом [1]. В 2017 году ущерб составил более 6 млрд рублей.

Принципиально меняется характер, стиль и методы компьютерных преступлений. С расширением спектра информационных и сетевых услуг, развитием киберфизических систем, интернета вещей возникают и новые виды преступлений. Хорошо организованные преступные группы и сообщества для достижения корыстных целей активно и высокопрофессионально применяют в своей деятельности новые методы, подходы, специальные программно-аппаратные средства и технику. При этом преступные группировки не имеют национальности и принадлежности к какой-либо стране, часто работая в разных странах и имея в своем арсенале не только широкий спектр инструментов для планирования преступления, взлома информационного ресурса и сокрытия (уничтожения) цифровых следов преступлений, но и пользуются при взаимодействии собственными системами скрытой связи. В связи со значительным ростом криминального профессионализма увеличивается и сложность расследования преступлений. Мы не планируем приводить примеры удачно осуществленных кибератак, поскольку в современных СМИ таких фактов превеликое множество.

К сожалению, киберпреступления имеют очень высокую степень латентности (скрытности) — большая часть преступлений остается даже не зарегистрированной. По имеющимся у авторов сведениям, кибератакам подвергаются практически все финансовые структуры и банки. Ряд компьютерных атак завершаются успехом и наносят значительные убытки. Часто коммерческие структуры (финансовые, банковские, кредитные и др.) стремятся не афишировать успешные атаки злоумышленников с целью сохранения бизнеса и нежелательного массового оттока клиентов. Раскрываемость компьютерных преступлений составляет не более 5 % (по данным «Лаборатории Касперского»*). В связи с этим особое значение имеет компьютерно-техническая экспертиза (КТЭ). Ее целью является получение ответа на вызовы и вопросы, требующие специальных познаний в области форензики.

Форензика (forensic science или, сокращенно, forensics — судебная наука) — компьютерная криминалистика, расследование киберпреступлений — совокупность знаний о методах поиска, исследования и закрепления цифровых доказательств по киберпреступлениям. Иными словами, это поиск цифровых доказательств по совершенным киберпреступлениям. Следует отметить, что форензика, находясь на стадии развития, не имеет пока достаточных и развитых теоретических подходов, классификации, методологических основ.

Форензика, производство КТЭ и использование ее результатов являются неотъемлемыми частями комплексной деятельности по обеспечению информационной безопасности, включая выявление, идентификацию и классификацию угроз нарушения информационной безопасности, противодействие угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет, а также формирование политики обеспечения информационной безопасности.

Многие исследователи уделяют внимание только частным подходам: особенностям экспертизы систем на сетевом уровне,

---

* Лаборатории Касперского — компания, работающая в сфере информационной безопасности, и входящая в четверку ведущих мировых производителей программных решений для защиты конечных устройств (Endpoint Protection). В основу рейтинга легли данные о выручке от продаж решений класса Endpoint Security в 2012 году.

созданию корректного образа взломанной системы для ее дальнейшего исследования и др., не затрагивая при этом общих принципов и подходов к проведению расследования компьютерных преступлений.

Весомый вклад в развитие этого направления работ внесли ученые Е.Р. Россинская, А.И. Усов, Н.Н. Федотов, К. Мандиа, К. Проспис [2, 10, 13, 14, 30], сотрудники компании Group-IB [https://www.group-ib.ru], «Лаборатории Касперского» [https://www.kaspersky.ru] и другие. Научной школой профессора А.А. Шелупанова в Томском государственном университете систем управления и радиоэлектроники накоплен значительный опыт по теоретическому обоснованию подходов и методов в области форензики, а также практической деятельности [48–53, 55, 56, 110–123].

В настоящее время темпы развития науки и техники в области компьютерной криминалистики значительно опережают появление экспертного теоретического и методического обеспечения. В результате расследование киберпреступлений, производство экспертиз по ним осложняется тем, что с постоянным развитием информационных технологий появляются новые объекты исследования, которых ранее просто не было. Постоянно изменяются, модифицируются механизмы и методы совершения ранее известных видов преступлений, появляются абсолютно новые виды преступлений. Экспертам КТЭ для дачи полного достоверного научно обоснованного заключения необходимо постоянное повышение квалификации, совершенствование навыков, обновление имеющихся теоретических, практических знаний и использование соответствующей современному состоянию научной и методической литературы. КТЭ обладает существенными особенностями и отличиями от многих видов традиционной экспертизы (например, почерковедческой, дактилоскопической), где для дачи полного достоверного научно обоснованного заключения возможно использование методического обеспечения (экспертных методик) двадцатилетней давности, что неприменимо для КТЭ. Под экспертной методикой принято понимать совокупность методов, используемых при производстве экспертизы.

В основе требований, предъявляемых к экспертным методикам, лежат процессуальные нормы, изложенные в УПК РФ

и Федеральном законе № 73 от 31.05.2001 (ред. 08.03.2015) «О государственной судебно-экспертной деятельности в Российской Федерации».

Так, методы, используемые экспертами при производстве экспертизы, должны удовлетворять перечню требований, выдвигаемому отечественным судопроизводством: законности; обоснованности; достоверности получаемых результатов; безопасности; эффективности; экономичности; этичности и допустимости. Наиболее важным параметром при выборе метода исследования является допустимость. Определяющим фактором при оценке того или иного метода на допустимость является научная обоснованность и удовлетворение метода новейшим достижениям области современных научных технологий [2].

На основе проведенного критического анализа отечественных и зарубежных методических рекомендаций, находящихся в свободном доступе, ранее выполненных исследований по данной тематике установлено, что методическое обеспечение, полностью удовлетворяющее вышеописанным процессуальным нормам, положениям и требованиям, отсутствует.

Потребность в экспертных методиках испытывают не только коммерческие учреждения, но и государственные организации, занимающиеся производством компьютерно-технических, компьютерных экспертиз [3]. В настоящее время из-за отсутствия должных методик, проводя экспертизу, давая заключение, эксперт напрямую зависит от личного опыта. Выбор метода в основном определяется исходя из личных знаний, а не из методических рекомендаций, что, несомненно, порождает большое число экспертных ошибок в заключениях начинающих экспертов. Область производства КТЭ с каждым годом требует все более сложных технических подходов и средств поддержки.

При использовании устаревшей методики возможно увеличение сроков производства экспертизы, ее стоимости, трудозатрат, а также получение недостоверных результатов и заключения, не пригодного в качестве доказательства.

Наличие алгоритмического обеспечения производства КТЭ позволит сократить число экспертных ошибок и сроки производства экспертизы путем разработки с их помощью в дальнейшем системы поддержки.

В соответствии с Доктриной информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646) одним из основных направлений обеспечения информационной безопасности в области государственной и общественной безопасности является «повышение эффективности профилактики правонарушений, совершаемых с использованием информационных технологий, и противодействия таким правонарушениям».

В программе «Цифровая экономика», принятой Правительством РФ в 2018 г., большое внимание уделено направлению информационная безопасность: «достижение состояния защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет и устойчивое социально-экономическое развитие Российской Федерации».

В результате КТЭ, проводимой при расследовании преступлений, связанных с нарушением информационной безопасности в открытых компьютерных сетях, хищением (разрушением, модификацией) информации и нарушением информационной безопасности, формируется информация об уязвимости процессов переработки информации в информационных системах. Эти результаты могут быть использованы специалистами по информационной безопасности для совершенствования средств защиты информации и обеспечения информационной безопасности.

Таким образом, необходимы современная методика, алгоритмы производства КТЭ, способствующие обеспечению информационной безопасности объектов различных сфер деятельности (государственной, в том числе политической, оборонной, социально-экономической и культурной сфер и т. д.) от внешних и внутренних угроз хищения/разрушения/модификации информации.

Наличие актуального методического и алгоритмического обеспечения производства КТЭ, применимого при решении широкого круга вопросов, для производства экспертиз в соответствии с текущими требованиями законодательства позволяет су-

щественно повысить общесистемные уровни обеспечения информационных ресурсов, включая критически важные объекты.

Многолетний практический опыт проведения значительного числа КТЭ в интересах различных государственных и коммерческих структур, муниципальных и региональных органов власти позволил авторам провести систематизацию имеющихся в настоящее время подходов и инструментов производства КТЭ и предложить свой подход, позволивший проводить КТЭ высокого качества. В частности, представленные результаты по всем проведенным КТЭ были учтены судами и не получали ни одной рекламации или направление на проведение повторной экспертизы.