района проживания преступника. Criminal Geographic Targeting был запатентован и интегрирован в специализированный программный продукт для анализа преступности под названием Rigel. Данный продукт разработан компанией-разработчиком программного обеспечения Environmental Criminology Research Inc. Другими известными автоматизированными системами географического профилирования являются CrimeStat и Gemini. Входные данные системы – это адреса или координаты места преступления, часто вводимые через географическую информационную систему. Результатом является поверхность опасности (трехмерная поверхность вероятности) или цветной геопрофиль, на котором изображены наиболее вероятные районы проживания преступника или поисковая база. Эти программы помогают криминалистам и следователям более эффективно концентрировать свои ресурсы, выделяя важнейшие географические районы.

Примером успешного применения географического профилирования в раскрытии и расследовании преступлений является дело расследования серийных убийств Анджела Буоно (в рамках расследования данного дела был установлен так называемый эффект угольного мешка (coal-sack effect, англ.), который заключается в том, что у подобных преступников есть тенденция избегать совершения преступления вблизи места своего проживания). В ходе расследования американский криминалист Барретт задокументировал несколько наблюдений правоохранителей относительно связи между местами совершения преступлений и районом проживания преступника. Если места убийства и захоронения тел разные, то убийца, вероятно, живет в том районе или недалеко от него, где было совершено нападение. И наоборот, если жертва была оставлена на месте убийства, то убийца, вероятно, не местный.

Барретт также говорит о том, что если место преступления находится рядом с дорогой общего пользования, это указывает на то, что преступник, возможно, не из этого района, в то время как место преступления вдалеке от дороги предполагает, что преступник местный. Сокрытое тело жертвы может означать, что преступник, вероятно, может повторно использовать место захоронения, в то время как брошенное в открытом месте тело может означать то, что преступник не местный и его не интересует обнаружат ли жертву.

Иным примером успешного использования географического профилирования в раскрытии и расследовании преступлений является расследование серии изнасилований Джона Даффи. Географическое профилирование позволило правоохранителям обнаружить предположительное место проживания преступника на основе расположения известных мест преступления и составления психологического портрета преступника и провести спецоперацию по его задержанию.

Раскрытие и расследование преступлений с использованием географического профилирования в общих чертах может быть разделено на следующие этапы: 1) установление факта совершения преступлений; 2) начало процесса расследования; 3) выявления связи между совершенными преступлениями (установление серийного характера); 4) осуществление психологического профилирования с выявлением психологического портрета преступника; 5) проведение географического профилирования с выявлением географического профиля расследуемой серии преступлений; 6) разработка новых путей и стратегии расследования.

В современных условиях для поддержания правопорядка и привлечения к ответственности лиц, совершивших преступления, правоохранительным органам требуется применять в своей практике новейшие достижения науки и техники, чем являются на данный момент автоматизированные системы географического профилирования. В рамках обеспечения национальной безопасности требуется как можно быстрее выявить и обезвредить преступников, совершающих серийные преступления, в особенности преступления против жизни и здоровья граждан – серийных убийц, насильников, разбойников и террористов. С этой целью обоснованным представляется дальнейшее исследование и усовершенствование географического профилирования на основе автоматизированных программ и разработанных под них алгоритмов в контексте расследования серийных преступлений.

УДК 343.98

О.А. Слащинин

ВИРТУАЛИЗАЦИЯ КРИМИНАЛИСТИЧЕСКИХ ОБРАЗОВ, ПОЛУЧЕННЫХ С ЭЛЕКТРОННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ, ИЗЪЯТЫХ ПО УГОЛОВНОМУ ДЕЛУ

В настоящее время органы уголовного преследования при производстве предварительного следствия, дознания по уголовному делу все чаще сталкиваются с электронными устройствами (далее – устройство) и содержащимися в них электронными носителями информации (далее – носитель). Это связано с непрекращающимся научно-техническим прогрессом, цифровизацией общественных отношений и ростом оборота указанных устройств у потенциальных участников уголовного процесса. Последние, используя в своей жизнедеятельности компьютерную технику, смартфоны и иные устройства, могут аккумулировать в их носителях сведения об обстоятельствах, имеющих значение для правильного раз-

решения уголовного дела. В связи с этим указанные носители должны рассматриваться органами уголовного преследования как возможный источник доказательств в соответствии с ч. 2 ст. 88 и ч. 2 ст. 100 Уголовно-процессуального кодекса Республики Беларусь (УПК) [1].

Получив в свое распоряжение упомянутые устройства с носителями, органы уголовного преследования должны обеспечить извлечение из них всех имеющихся цифровых доказательств. Однако сам порядок сбора и фиксации указанных доказательств в УПК не закреплен, что может вызвать проблемы с их последующей проверкой и оценкой согласно ст. 104 и 105 УПК. В свою очередь, существуют общепринятые стандарты работы с носителями и содержащейся на них компьютерной информацией. Данные стандарты устанавливаются как международными организациями в области компьютерной криминалистики [2, 3], так и отечественными судебными экспертами [4].

Упомянутые стандарты можно кратко изложить в следующих поэтапных положениях, которые могут применяться и в рамках уголовного процесса:

1) безопасное подключение осматриваемого носителя в аппаратном или программном режиме «только-для-чтения», исключающем запись на него новых данных, а также изменение или удаление уже имеющихся;

2) подключение дополнительного очищенного носителя с емкостью памяти, количественно равной или большей осматриваемого носителя;

3) снятие побитовой копии (образа) осматриваемого носителя с возможностью ее верификации посредством проверки контрольной суммы, а также запись копии (образа) на дополнительный носитель (создание отдельного файла-образа или полное клонирование осматриваемого носителя);

4) отключение осматриваемого носителя, его последующая упаковка и опломбирование в целях защиты от несанкционированного доступа к нему;

5) дальнейшее взаимодействие лишь с вышеуказанной побитовой копией (образом), записанной на дополнительном носителе.

Вышеуказанные положения направлены на извлечение максимального объема цифровых доказательств и защиту от их возможной перезаписи или уничтожения самого оригинального носителя. Этот объем может обеспечиваться в результате частичного восстановления ранее удаленной компьютерной информации, а также сохранения целостности и доступности уже зафиксированных данных в самой копии (образе).

Полученный образ носителя монтируется к компьютерной технике органа уголовного преследования, в результате чего появляется возможность осматривать его содержимое с помощью файлового менеджера. Современное программное обеспечение (ПО) позволяет создавать также криминалистические образы различных форматов (например,*.e01, *.001, *.aff), поддерживающих их фрагментацию, сжатие и шифрование. Вышеуказанная копия (образ) полностью реплицирует свойства физического носителя, его логические разделы, каталоги и электронные файлы, в том числе скрытые, зашифрованные и ранее удаленные (фрагментарно).

Компьютерная информация, осматриваемая посредством файлового менеджера без поддержки графического интерфейса самой операционной системы (ОС) и ПО оригинального носителя, не всегда может быть достаточно информативной. В отдельных случаях извлечение необходимых данных возможно только при их осмотре с помощью графического интерфейса ОС и иного ПО в динамике (например, экранные формы и элементы, логика организации взаимодействия пользователя с файловой системой и процессами). Однако запуск оригинального носителя, в том числе посредством изъятых у участника уголовного процесса устройств, неизбежно приведет к изменению содержащейся на нем компьютерной информации. Факт нарушения ее целостности может стать основанием для признания полученных цифровых доказательств недостоверными или недопустимыми в соответствии со ст. 105 УПК. Для решения указанной проблемы компьютерные криминалисты (форензисты) предлагают виртуализировать получаемые образы, что позволяет осматривать компьютерную информацию в ее аутентичной форме, т. е. аналогичной запуску носителя с оригинального устройства участника уголовного процесса [5, 6].

Виртуализация криминалистического образа осуществляется посредством выполнения на компьютерной технике, используемой органом уголовного преследования, следующих последовательных действий:

1) полученный для целей виртуализации образ монтируется с помощью программного эмулятора (например, Arsenal Image Mounter, AccessData FTK Imager) с обязательным созданием временных дифференциальных файлов, препятствующих последующей модификации оригинального образа;

2) эмулированный криминалистический образ посредством гипервизора (например, VMware Workstation, Oracle VM VirtualBox) идентифицируется как физический носитель, подключенный к компьютерной технике;

3) на основе идентифицированного носителя производится создание виртуальной машины и его гибкая настройка в зависимости от свойств устройства, которое было изъято у участника уголовного процесса;

4) осуществляется запуск виртуальной машины, полностью имитирующей содержание и работу первоначального носителя в составе устройства.

Несмотря на имеющиеся практические руководства по виртуализации криминалистических образов, их реализация на практике достигается не всегда. Это зависит от вида виртуализируемой ОС (например, Windows, Linux, Android), емкости и доступности самого носителя, а также характеристик ранее используемого с ним устройства. Невзирая на имеющиеся проблемы, данный подход собирания цифровых доказательств можно признать перспективным для органов уголовного преследования и требующим дальнейшей разработки.

Список использованных источников

1. Уголовно-процессуальный кодекс Республики Беларусь [Электронный ресурс] : 16 июля 1999 г., № 295-З : в ред. Закона Респ. Беларусь от 20.07.2022 г. № 199-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

2. Association of chief police officers – Good Practice Guide for Digital Evidence (March 2012) [Electronic resourse]. – Mode of access: www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf. – Data of access: 08.12.2022.

3. National Institute of Standards and Technology – Guide to Integrating Forensic Techniques into Incident Response (August 2006) [Electronic resourse]. – Mode of access: tsapps.nist.gov/publication/get_pdf.cfm?pub_id=50875. – Data of access: 08.12.2022.

4. Методика исследования компьютерной информации : метод. рекомендации / Гос. ком. судеб. экспертиз Респ. Беларусь. – Минск, 2016.

5. Форум ИБ – Codeby.net: Виртуализация криминалистических образов в Windows [Электронный ресурс]. – Режим доступа: codeby.net/threads/ virtualizecija-kriminalisticheskix-obrazov-v-windows. 64120. – Дата доступа: 08.12.2022.

6. Security is FUN: Booting up evidence E01 image using free tools [Electronic resourse]. – Mode of access: www.securityisfun.net/2014/06/booting-up-evidence-e01-image-using.html. – Data of access: 08.12.2022.

УДК 343.98.06

Е.Н. Соболевский

НЕКОТОРЫЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ СЕТИ ИНТЕРНЕТ В КОНТЕКСТЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Новые тенденции в развитии информационных технологий создают новые риски для информационной безопасности любого государства. Цифровой мир стремительно расширяется, он становится мобильным,

управляет производством и технологическими процессами, охватывает всю среду обитания человека – от бытовых приборов до умных офисов и интеллектуального транспорта. Все больше информации передается через мобильные сервисы, ранее изолированные системы начинают взаимодействовать и обмениваться информацией, лавинообразно нарастает поток данных и объемы хранения. Внедрение новых парадигм организации распределенных крупномасштабных систем, таких как «Интернет вещей» (Internet of Things, IoT), приведет к новым рискам информационной безопасности, когда через сеть станут доступны почти все предметы, окружающие человека.

По мере развития технологий в окружающем человека мире появляется все больше устройств, находящихся под управлением микропроцессоров и программного обеспечения. С ростом числа внедрений решений на базе IoT, как считают эксперты, все больше атак будет направлено не только на программное, но и на аппаратное обеспечение (сетевые карты, USB-устройства), входящее в инфраструктуру «интеллектуального транспорта», «умных домов», автоматизированных систем управления производством и др.

Возможности коммуникаций, которые стали доступны государствам, юридическим и физическим лицам после возникновения глобальной компьютерной сети Интернет, привели к кардинальному преобразованию общества и его экономической реальности. Интернет сегодня – это среда, используемая для всевозможных форм взаимодействия всех субъектов экономики. Высокая степень необходимости интернета как в повседневных практиках общества, так и в деятельности государства и бизнес-сообщества, воздвигает его в ряд необходимых элементов социально-экономического развития общества. По состоянию на текущий год в мире насчитывается более 5 млрд пользователей сети Интернет – это 63 % от общего населения Земли. Об этом свидетельствуют данные отчета April Global Statshot report, подготовленного при участии We Are Social и Hootsuite.

Приоритетную важность представляет собой переход различных государственных отраслей экономики в цифровое пространство – электронное правительство. Предоставление цифровых услуг населению, создание государственных информационных систем и ресурсов, формирование межгосударственных каналов передачи данных сегодня представляют собой повсеместные практики.

На текущий момент 80 % организаций, прошедшие стадию цифровых преобразований (внедрение технологий «Индустрия 4.0»: промышленный Интернет вещей, большие данные, 3D-принтеры и др.), смогли существенно увеличить свою прибыль. Ежегодная прибыль компаний Samsung, LG, Huawei и др. оценивается в десятки млрд дол-