На основе анализа этих определений, а также понятия «тактическая задача» и связанных с ним других категорий криминалистики мы считаем, что тактическую задачу следует рассматривать как результат мыслительной деятельности следователя, обусловленный соотношением между ситуацией расследования и тактической целью, связанный тактическим решением и реализуемый в соответствии с оптимальным правомерным воздействием криминалистическими средствами и методами на объекты, процессы и явления для достижения указанной цели.

Если рассматривать тактическую задачу в логико-психологическом аспекте, она представляет собой преобразование несогласованных или противоречивых информационных процессов (систем), т. е. получение определенной криминалистически значимой информации, связанной с тактическими целями расследования преступлений.

Структурно рассматриваемое понятие включает в себя условие (известная исходная или установленная криминалистически значимая информация, из которой следует исходить при решении тактической задачи) и требование (тактическая цель, к которой следует стремиться в результате решения тактической задачи в соответствии с реализацией тактического решения посредством криминалистических средств и методов).

Исходя из соотношения между ситуацией расследования и тактической целью, условия и требования тактической задачи могут носить характер данных (криминалистически значимой информации) исходных, привлеченных и искомых.

Исходные условия при определении следователем тактической задачи представляют собой известные исходные данные, установленные расследованием преступления. В ситуациях расследования, когда этих данных недостаточно, следователь может предпринять попытки получения дополнительной информации – привлеченных данных, с тем чтобы решить тактическую задачу. Искомые данные (криминалистически значимая информация) – те сведения, которые следователю требуется отыскать в процессе решения тактической задачи.

Понятие тактической задачи и структуру ее решения можно считать прикладными криминалистическими инструментами, которые могут быть использованы следователем в процессе расследования дорожно-транспортных происшествий в ситуациях, когда требуется точное определение такой задачи для достижения соответствующей результатам ее решения цели.

1. Самыгин Л.Д. Расследование преступлений как система деятельности. М., 1989.

2. Полевой Н.С. Криминалистическая кибернетика. 2-е изд. М., 1989.

3. Величкин С.А. О соотношении понятий «тактический прием», тактическая задача», «тактическая операция» // Проблемы укрепления социалистической законности в уголовном судопроизводстве : межвуз. сб. Барнаул, 1985.

4. Солодов Д.А. Процессуальные и тактические решения следователя (сущность, проблемы оптимизации принятия) : учеб. пособие. Воронеж, 2004.

5. Криминалистика : учеб. пособие / А.В. Дулов [и др.] ; под ред. А.В. Дулова. Минск, 1998.

6. Логвиненко Е.А. Мысленное моделирование в тактике следственных действий: дис. … канд. юрид. наук. Краснодар, 2003.

7. Головин М.В. Проблемы целеопределения в расследовании : дис. … канд. юрид наук. Краснодар, 2002.

8. Большая советская энциклопедия : в 50 т. 2-е изд. М., 1950–1957. Т. 36. 1955.

9. Туманов Г.А. Организация управления в сфере охраны общественного порядка. М., 1972.

10. Белкин Р.С. Курс криминалистики : учеб. пособие для вузов. 3-е изд., доп. М., 2001.

11. Цветков С.И. Состояние и перспективы использования данных науки управления в криминалистике : дис. … канд. юрид. наук. М., 1977.

12. Якушин С.Ю. Тактические задачи и средства их решения при расследовании преступлений. Казань, 2014.

13. Головин А.Ю. Системные средства и методы в криминалистической науке : учеб. пособие. Тула, 2013.

УДК 343.58

П.Л. Боровик

КРИМИНАЛИСТИЧЕСКИЙ ПОДХОД К ИССЛЕДОВАНИЮ ОБЪЕКТОВ – НОСИТЕЛЕЙ ВИРТУАЛЬНЫХ СЛЕДОВ ПРЕСТУПЛЕНИЙ ПРОТИВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

На современном этапе при расследовании преступлений против информационной безопасности существенно повышается значимость результатов, получаемых в ходе проведения криминалистического анализа такого компонента операционной системы, как WindowsRegistry (реестр). Это связано с тем, что механизм совершения рассматриваемых деяний предполагает внесение в реестр определенных изменений, являющихся по своей сути виртуальными следами, свидетельствующими о преступном событии. Поскольку для их уничтожения требуются доста-

точно глубокие знания программирования, системный реестр служит важным криминалистическим артефактом, который необходимо исследовать в первую очередь с целью получения объективной тематической и интегративной информации о состоянии информационной системы на момент возникновения исследуемого события.

Значительная же часть иных источников следообразования (например, системные файлы, журналы событий, атрибуты файлов и др.) в информационной среде могут подвергаться корректировке (уничтожению) со стороны злоумышленника с целью сокрытия либо маскировки следов, поскольку имеют относительно простую и незащищенную структуру.

Рассмотрим некоторые возможности криминалистического исследования системного реестра Windows, позволяющие с помощью специальных (в том числе бесплатных) программ для чтения реестра (например, RegOrganizer, RegistryMechanic, Regedit и др.) установить обстоятельства, имеющие значение для раскрытия, расследования и предупреждения преступлений.Так, при наличии определенных навыков работы с реестром можно выявить все процессы и операции, проведенные на исследуемом компьютере за последние 30 дней, с указанием точных даты и времени их проведения.

Изучение показало, что в ряде случаев перед криминалистами ставится задача хронологической реконструкции происшедших событий в системе, прямо либо косвенно указывающих на конкретные обстоятельства совершения преступлений: фактов установки и использования каких-либо программ (в том числе вредоносных), внешних устройств хранения информации (HDD-, SSD-, флеш-накопители) и их содержимого, средств сетевой и мобильной связи (сетевые карты, USB-модемы, виртуальные машины с функцией внешней сетевой карты), времени инициализации и длительности этих событий на компьютере потерпевшего и др.

С целью получения первоначальной объективной информации о происшедших событиях в системе и их хронологической реконструкции необходимо исследовать ключ реестра HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{GUID}\Count, который содержит два подраздела: CEBFF5CD и F4E57C4B.

Первый подраздел указанного ключа содержит детальную информацию о запуске исполняемых программ (имя файла, дата и время последнего запуска, количество запусков), второй – ярлыков файлов. При этом каждый подраздел содержит список системных объектов исследуемой информационной среды (программы, ярлыки и апплеты панели управления), к которым зарегистрированный пользователь обратился.

В ходе криминалистического анализа операционной системы Windows возникает необходимость не только установления времени запуска конкретного файла либо процесса, но и идентификации пользователей (установления сведений об их учетных записях), выполнявших их запуск. Для решения этой задачи рекомендуется осуществить анализ системного файла Ntuser.dat, в котором хранятся следующие значения ветки реестра HKEY_CURRENT_USER: идентификаторы SID, имена пользователей, индексы, имена приложений, количество запусков, сеанс и атрибуты времени последнего запуска.

Для установления последних запущенных приложений и процессов в скомпрометированной компьютерной системе, включая время первого и последнего запуска соответствующей программы, а также для ее изменения, удаления и просмотра ее путей рекомендуется осуществить исследование файла Amcache.hve (%SystemRoot%\AppCompat\Programs\Amcache.hve).

Актуальные данные, параметры и компоненты полного цикла загрузки операционной системы Windows и запуска наиболее часто используемых программ можно получить, исследуя системную папку Prefetch (%windir%\Prefetch). В этой папке хранятся данные о последних 128 исполняемых файлах на операционной системе Windows 7 и последних 1 024 на Windows 8–10 (имя исполняемого файла, список библиотек DLL в формате Unicode, используемых этим исполняемым файлом, счетчик количества запусков исполняемого файла и отметка времени последнего запуска программы).

Криминалистический интерес может вызывать системная служба BackgroundActivityModerator (BAM), контролирующая активность фоновых приложений (появилась в Windows 10 в версии начиная с 1709). Соответствующая ветка реестра, расположенная по адресу HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\{SID}, содержат полный путь к исполняемым файлам, которые были запущены на компьютере, дату и время их последнего запуска, идентификатор учетной записи пользователя.

Информацию о съемных USB-носителях, когда-либо подключавшихся к системе, может предоставить раздел реестра HKLM\System\ControlSet00x\ENUM\USBSTOR. В этой ветке реестра находятся ключи, каждый из которых представляет свой класс устройств. В свою очередь, в таких ключах содержатся подключи, отражающие серийный номер устройства. Для установления времени последнего подключения USB-устройства следует осуществить просмотр временной метки одного из подключей ключа SYSTEM\ControlSet00x\Control\DeviceClasses. Поиск подключа проводится по названию, которое должно содержать серийный номер искомого USB-устройства.

Чтобы доказать факт использования на анализируемом компьютере сетевой карты или устройства, исполняющего роль внешней сетевой карты (например, виртуальной машины, с помощью которой осуществлялись вредоносные атаки), исследователю необходимо изучить содержимое раздела реестра SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkCards. В нем находятся подключи, каждый из которых хранит информацию по всем сетевым устройствам. С учетом того, что эти ключи не обновляются, соответствующей временной меткой можно воспользоваться для установления даты их установки.

Операционная система хранит также подробную информацию о сетевой активности, осуществляемой на исследуемом компьютере. Так, для любой беспроводной сети, к которой было произведено подключение с данного компьютера, создается запись в разделе SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Nla\Wireless. В нем содержится наименование идентификатора сети. Связывая данные идентификаторы с сигнатурами из раздела реестра SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged, а также с профилями, находящимися в записях раздела ProfileGuid по адресу SOFTWARE\Microsoft\WindowsNT\CurrentVersion\NetworkList\Profiles\{ProfileGuid}, можно получить информацию о дате и времени создания сетевого подключения (в том числе последнего), имени профиля и MAC-шлюзе.

Для получения информации об использовании интранет-сетей следует обратиться к разделу реестра SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Nla\Cache\Intranet, просмотреть соответствующие подключи и связать их с записями сетевых профилей (посредством GUID).

Общий список (до 150 записей) последних открытых документов (без группировки по расширению) на исследуемом устройстве хранится внутри корневого ключа реестра HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDoc.

Сведения о запускаемых с помощью диалогового окна «Выполнить» командах содержатся в ключе реестра HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU. В данном ключе хранится до 26 значений с названиями от *a* до *z* и одно значение MRUList, задающее порядок отображения списка последних выполненных команд (и, соответственно, порядок их выполнения пользователем).

В заключение следует отметить, что криминалистическое исследование рассмотренных артефактов реестра Windows необходимо осуществлять комплексно, в контексте изучения механизма следообразования, детерминированного средой протекания системных процессов и участвующих в нем объектов. В этом случае сведения, найденные при

их изучении, позволят построить целостную информационно-следовую картину криминального деяния. Обобщение особенностей представленных характерных объектов – носителей виртуальных следов преступлений против информационной безопасности поможет создать необходимую основу для разработки, внедрения и эффективного применения средств и методов собирания и исследования следовой информации.

УДК 343.98

Ю.В. Варавко

ИНСТРУМЕНТАРИЙ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ СЛЕДОВАТЕЛЯ

Стремительный рост количества данных в информационном пространстве, а также повышение уровня их доступности приводят к существенным изменениям в различных сферах человеческой деятельности, в том числе и в области раскрытия, расследования и предупреждения преступлений. В связи с этим все более востребованной становится аналитическая обработка информации.

Данная тенденция в ходе досудебного уголовного производства находит свое отражение в формировании и развитии такого самостоятельного направления работы следственных органов, как информационно-аналитическая деятельность. Под ней, по нашему мнению, следует понимать целенаправленный и объединенный задачами раскрытия, расследования и предупреждения преступлений процесс сбора, обработки, хранения, систематизации и аналитической интерпретации криминалистически значимой информации в целях получения новых знаний о преступлении и лицах, причастных к его совершению, принятия на основе полученных знаний обоснованных уголовно-правовых, уголовно-процессуальных и тактических решений, а также в целях обеспечения взаимодействия с субъектами, вовлеченными в процедуру расследования преступлений.

Базовым компонентом информационно-аналитической деятельности, определяющим самостоятельность ее существования, а также обеспечивающим ее практикоориентированность, является инструментарий такой деятельности, т. е. арсенал приемов, способов, технологий, методов, методик и подходов обработки криминалистически значимой информации.

Анализ криминалистической литературы и иных источников научных исследований в данной области показывает, что мыслительной