В. В. Бондаренко, В. В. Серпухов (Самара, СамГУ)**. Некоторые методы расследования компьютерных преступлений.**

Расследование компьютерных преступлений — относительно новое явление. В зарубежной литературе [4] используется несколько терминов: «цифровая экспертиза», «анализ носителей информации» и т. д. В последнее время стало очевидно, что цифровые устройства, и в первую очередь компьютеры, могут служить ценным источником улик в широком спектре расследований. Например, в 2003 году Американское общество директоров криминалистических лабораторий (ASCLD) признал поиск цифровых улик полноценной отраслью криминологической экспертизы.

Цифровым расследованием называется процесс разработки и проверки гипотез, отвечающих на вопросы о цифровых событиях. Задача должна решаться научными методами: эксперт строит гипотезы на основе найденных улик, а затем проверяет их поиском дополнительных улик, которые бы доказывали или опровергали высказанную гипотезу. **Цифровой уликой** называется цифровой объект, содержащий информацию, подтверждающую или опровергающую выдвинутую гипотезу.

Объектом цифрового расследования является некоторое цифровое устройство, задействованное в инциденте или преступлении. Цифровое устройство могло использоваться при совершении физического преступления или могло стать источником события, нарушившего закон. Примером первого случая служит сбор в Интернете информации для подготовки преступления; ко второму случаю относят получение несанкционированного доступа к компьютеру, загрузку незаконного материала по сети. После выявления факта нарушения начинается собственно расследование компьютерного преступления.

К сожалению, на сегодняшний день не существует единого подхода к расследованию компьютерных преступлений. Подход, используемый в работе [1], основан на процессе анализа места физического преступления. Следует помнить, что в данном случае имеет место цифровое преступление, к которому относится цифровое окружение, создаваемое программами и оборудованием.

Процесс анализа места компьютерного преступления состоит из трех основных фаз [4]: консервация системы, поиск улик и реконструкция событий. При этом эти фазы не обязательно должны следовать одна за другой. Общая схема процесса показана на рис.

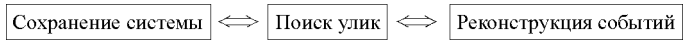

Рис. Основные фазы анализа места компьютерного преступления

Процесс применяется при проведении расследований как в «живых», так и в «мертвых» системах. «**Живой**» **анализ** происходит при поиске улик с использованием операционной системы (ОС) и других ресурсов анализируемого компьютера. «**Мертвый**» **анализ** происходит при использовании доверенных приложений в доверенной ОС. Ясно, что при «живом» анализе существует риск получения ложной информации (программное обеспечение преступника может намеренно скрывать или искажать данные), а «мертвый» анализ надежнее, но не всегда доступен.

К задачам **идентификации** применительно к экспертизе носителей и систем относятся [3]:

• идентификация продукции (носителей, упаковки) — по аналогии с ГОСТ Р 51293-99 «Идентификация продукции» — выявляются признаки контрафактности, т.е. внешние отличия по сравнению с оригинальными (эталонными) образцами либо их описанием;

• идентификация программных и информационных объектов — определение тождественности или различий файлов, записей, файловых структур и других форм организации информации. Данный тип исследований позволяет выяснить, что на носителе действительно записан определенный объект авторского права (например, компьютерная игра, в том числе в модифицированной форме).

К **диагностическим** задачам относятся:

• определение основных характеристик ПО; выявление и исследование функциональных свойств и настроек ПО, времени его инсталляции, модификации и последнего использования; определение фактического состояния программного объекта; диагностирование алгоритма программного продукта, видов использованных при его разработке или модификации инструментальных средств, определение целей и условий изменения свойств и состояния ПО (программно-компьютерная экспертиза);

• установление свойств и вида представленной информации (не программ) в компьютерной системе, установление первоначального состояния информации на носителе данных (восстановление); определение времени, хронологической последовательности воздействия на информацию; определение условий создания и изменения свойств исследуемой информации (информационно-компьютерная экспертиза).

Основной целью **фазы сохранения системы** является сведение к минимуму возможных потерь улик в ходе расследования. Этот процесс продолжается после снятия данных с исследуемой системы. Так как снятые данные необходимо сохранить для будущего анализа, основным методом является создание полной копии жесткого диска. В этой фазе эксперт пытается законсервировать состояние системы — места компьютерного преступления. Выполняемые действия зависят от юридических требований к расследованию. Например, эксперт может отключить систему от сети и создать полную копию всех данных. К крайним случаям можно отнести ситуации, связанные с заражением вредоносными программами — в таких случаях сохранение не выполняется [4].

Изъятие носителей информации должно осуществляться с привлечением компетентного специалиста, который может обеспечить элементарные меры по консервации системы и данных, находящихся на жестком диске. Приведем реальный пример о выполнении процедуры изъятия ПК сотрудниками милиции, не обладающими специальными познаниями. В ходе проверки одной из крупных фирм г. Самара (в эксплуатации ЛВС около 50 компьютеров), сотрудники милиции обнаружили внешние признаки контрафактности программного обеспечения фирм «1С» и корпорации «Майкрософт», а так же следы использования вредоносного программного обеспечения, т. е. признаки преступлений предусмотренных ст.ст. 146, 273 УК РФ. В ходе проверки сотрудниками милиции не было произведено отключение ЛВС, а так же другого блокирования информации. В результате, сотрудник милиции, переходя от одного рабочего места к другому, составляет протокол осмотра программного обеспечения, а неустановленное лицо из другого помещения, используя удаленный доступ к ЛВС, форматирует винчестеры уже осмотренных, но не отключенных от ЛВС и электропитания ПК. В итоге на экспертизу поступают ПК, что называется «пустые как барабан» — исследовать нечего.

Так как фаза сохранения системы направлена на минимизацию потерь улик, необходимо ограничить количество процессов, способных записывать данные на носители информации. При проведении «мертвого» анализа эксперт завершает все процессы, отключает систему, создает резервные копии всех данных. Для предотвращения потери улик также могут применяться блокировщики записи. При «живом» анализе необходимо завершить или приостановить все подозрительные процессы. Компьютер необходимо отключить от сети (возможно подключив систему к пустому концентратору/коммутатору, чтобы предотвратить появление в журнале сообщений о недоступности сети) или установить сетевые фильтры, чтобы злоумышленник не смог подключиться из удаленной системы и уничтожить данные. Важные данные копируются на случай возможной потери в процессе поиска. Например, если необходимо читать файлы, то следует сохранить временные метки всех файлов, чтобы у эксперта была эталонная копия времени последнего обращения, ибо чтение из файла приведет к обновлению отметок времени. При сохранении важных данных в процессе «живого» или «мертвого» анализа для обеспечения целостности и аутентичности данных

рекомендуется вычислить криптографические хеш-значения данных [2]. Позднее они помогут доказать, что данные не изменялись.

Фаза поиска улик обычно начинается с изучения стандартных мест, зависящих от типа инцидента (если он известен). С ходом расследования эксперт строит гипотезы и ищет улики, которые подтвердили бы или опровергли их. Важно, чтобы эксперт искал и опровергающие улики, не ограничиваясь только подтверждающими. Теория процесса поиска проста: сначала следует определить общие характеристики искомого объекта и затем произвести поиск этого объекта в наборе данных, и, как правило, состоит из двух ключевых шагов — определение того, что нужно найти, и тех мест, где должен производиться поиск. Большинство улик находится в файловой системе и файлах. Стандартная методика поиска заключается в поиске файлов по именам или шаблонам. Также часто требуется найти файл по ключевым словам, присутствующим в их содержимом. Возможен вариант поиска файлов по временным данным, например, дата последнего обращения или записи. Иногда поиск известных файлов проводится путем сравнения хеш-значений содержимого файлов, вычисленных по алгоритму MD5 или SHA-1, с базой данных хеш-значений, например, National Software Reference Library (NSRL, http://www.nsrl.nist.gov). Базы данных хеш-значений применяются при поиске вредоносных фалов. Другой распространенный метод поиска основан на сигнатурах, присутствующих в содержимом. По сигнатурам часто можно найти все файлы заданного типа, даже если они были переименованы. При анализе сетевого трафика возможен поиск всех пакетов, отправленных с некоторого исходного адреса, или всех пакетов, адресованных конкретному порту, или зафиксировать все пакеты с заданным ключевым словом.

Одним из примеров поиска, является поиск и сравнение «эталонных» и «модифицированных» кодов программного обеспечение. Например, в прикладном программном обеспечении фирмы «1С» такой модификацией является изменение, устранение или блокирование из оригинального кода программы процедуры обращения к аппаратному ключу защиты от несанкционированного копирования и распространения, предусмотренного производителем. В программном обеспечение корпорации «Microsoft» устранение или модификация процедуры обязательной регистрации (активации) программного обеспечения. Такая модификация является одним из существенных признаков контрафактности, исследованного ПО.

В последней фазе — **фазе реконструкции событий** — расследования на базе найденных улик определяются события, происходившие в системе. Иногда после фазы реконструкции цифровых событий удается связать эти цифровые события с физическими. Для реконструкции событий эксперт должен хорошо знать приложения и ОС, установленные на компьютере, чтобы строить гипотезы на основании их возможностей. Например, цифровые события в Windows9x отличаются от событий в Windows XP.

Существует ряд процессуальных и юридических проблем доказывания, например, периода времени в течении которого эксплуатировалась та или иная прикладная или операционная система, имеющая признаки контрафактности. Связано это с тем, что устройство стандартного ПК на аппаратном уровне можно сравнить с наручными часами: какую дату и время задаст пользователь, такое и будет регистрироваться в системе. Другими словами, время установки файлов операционной системы нельзя принимать за абсолютную истину, об этом времени можно судить лишь предположительно. Однако существуют косвенные свидетельства, по которым можно связать время, установленное на ПК с реальным временем. Например, в прикладных бухгалтерских системах, создаются, регистрируются и, как правило, имеют свои печатные формы, различные документы, обеспечивающие хозяйственную деятельность предприятия-нарушителя, использующего контрафактное программное обеспечение. Одним из этих документом является платежное поручение (ПП), имеющее печатную форму, которая регистрируется банком и на бумажной копии ПП имеется отметка

банка о принятии данного ПП к исполнению. Таким образом, путем сравнения оригиналов ПП и их электронных копий, можно сделать достоверный вывод о времени и сроке эксплуатации прикладного программного обеспечения, а постольку-поскольку прикладное программное обеспечение функционирует под управлением какой либо ОС, то и вывод о сроке эксплуатации данной ОС.

В заключение сформулируем ряд правил, которым следует придерживаться при проведении расследований компьютерных преступлений.

1. **Сохранение исследуемой системы**. Эксперт должен исключить любые модификации данных, которые могут послужить уликами.

2. **Изоляция среды** анализа как от анализируемых данных, так и от внешнего мира. Для изоляции возможно применять аппарат виртуальных машин.

3. **Проверка данных** по другим независимым источникам. Тем самым снижается риск использования ложных данных.

4. **Документирование всех действий**. При проведении «живого» анализа или применении методов, которые могут привести к модификации данных, важно документировать все проводимые действия. Позднее это позволит описать, какие изменения были внесены экспертом в систему. В любом случае документирование действий поможет определить, какой поиск еще не проводился и какие результаты были получены ранее.

СПИСОК ЛИТЕРАТУРЫ

1. *Carrier B.*, *Eugene H.* Spafford Getting Physical with the Digital Investigation Process. — International Journal of Digital Evidence, Fall 2003. http://www.ijde.org.
2. *Алферов А. П.*, *Зубов А. Ю.*, *Кузьмин А. С.*, *Черемушкин А. В.* Основы криптографии: учебное пособие. М.: Гелиос АРВ, 2002, 480 с.
3. Компьютерное пиратство: методы и средства борьбы. Разработка Некоммерческого Партнерства Поставщиков Программных Продуктов, совместно с Департаментом экономической безопасности, Департаментом охраны общественного порядка и управлением «К» БСТМ МВД России, двенадцатое издание, Москва, 2007.
4. *Кэрриэ Б.* Криминалистический анализ файловых систем. СПб.: Питер, 2007, 480 с.