Способы и приемы анализа неправомерных действий в сфере информационных технологий ГИБДД

Мишин Дмитрий Станиславович,
старший преподаватель кафедры информационных технологий в деятельности ОВД Орловского юридического института МВД России, к.ю.н., подполковник полиции

Паньков Сергей Леонидович,
начальник научно-исследовательского и редакционно-издательского отдела Орловского юридического института МВД России, полковник полиции

Современный этап развития общества можно охарактеризовать вступлением в эру новых информационных технологий. Постоянно возрастающие требования к оперативности протекания информационных процессов в различных областях деятельности инициировали развитие и повсеместное использование средств вычислительной техники и телекоммуникационных систем. Кроме того, следует обратить внимание на постоянное создание и совершенствование программных и технических средств обеспечения циркуляции информации, а также методов распределенной обработки данных, реализации доступа к рабочим станциям посредством телекоммуникационных сетей.

Не осталось в стороне от рассматриваемого процесса и отечественное законодательство, в котором дается следующее определение:

Информационно-телекоммуникационная сеть — технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.[1]

В настоящее время с полной уверенностью можно говорить о том, что общественные отношения в сфере использования информационных технологий в России затрагивают многие стороны жизни современного общества. Информационные технологии широко используются в промышленности, торговле, в научно-исследовательской и во многих других сферах деятельности.

В органах внутренних дел процесс внедрения современных информационных технологий и телекоммуникационных сетей идет одновременно с другими структурами Российской Федерации. В настоящее время введена в эксплуатацию и успешно функционирует во всех подразделениях единая информационно-телекоммуникационная система МВД России, которая используется для хранения информационных массивов специализированных учетов и циркуляции информации ограниченного распространения.

В целях повышения эффективности информационного обеспечения подразделений Госавтоинспекции и иных подразделений органов внутренних дел Российской Федерации подписано Положение о системе информационного обеспечения[2]. Данное положение направлено на эффективное использование подразделениями Госавтоинспекции функциональных возможностей федеральной специализированной территориально-распределенной информационной системы.

Следствием создания информационных массивов в подразделениях ГИБДД стала возможность несанкционированных действий, направленных на ознакомление, копирование, удаление или модификацию. Причины этого зачастую кроются в том, что недостаточная эффективность существующих методов и способов защиты компьютерной информации при эксплуатации средств вычислительной техники и информационно-телекоммуникационных систем вызывает повышенный интерес у криминальных элементов, преследующих цель противоправного завладения информацией для совершения различных видов неправомерных действий. Еще одной проблемой является достаточно высокий уровень латентности противоправных деяний в сфере компьютерной информации.

Рассмотрение процедур совершения неправомерного доступа к компьютерной информации следует начинать с определения распространенных способов совершения неправомерных действий в информационно-телекоммуникационных сетях. При этом следует обратить внимание на тот факт, что рассматриваемая проблема характерна практически для всех телекоммуникационных сетей и при ее рассмотрении целесообразно обращать внимание не на какую-то конкретную сеть, а лишь на наиболее характерные для нее процедуры неправомерного доступа.

В первую очередь необходимо классифицировать способы совершения неправомерного доступа к информации в вычислительных и телекоммуникационных сетях. **Наиболее целесообразно их классифицировать, объединив в три основные группы[3]:**

- способы опосредованного доступа;
- способы непосредственного доступа;
- смешанные способы.

Способ опосредованного доступа основан на получении компьютерной информации методом аудиовизуального и электромагнитного перехвата. Этот способ в свою очередь можно разделить на пассивный и активный.

Наиболее простой способ опосредованного пассивного перехвата — это

1 Федеральный закон от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации».

2 Федеральный закон от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации».

3 Приказ МВД России от 03.12.2007г. №1144 «Об утверждении положения о системе информационного обеспечения Госавтоинспекции».

перехват электромагнитного излучения, позволяющий проводить добычу информации без прямого контакта, то есть не привлекая к себе внимания и не оставляя следов. Это объясняется тем, что «всякое электронное устройство, телефон и факс, а также линии связи излучают в открытое пространство высокие уровни поля в диапазоне частот вплоть до 150 МГц»[4] и на определенном расстоянии можно уловить устойчивый сигнал при помощи измерительной установки и записывающей аппаратуры.

Пассивный перехват не оставляет следов неправомерного доступа к компьютерной информации, но при этом требует больших финансовых затрат на закупку оборудования и наем специалистов в соответствующих областях науки и техники. В этом кроется причина того, что этот способ неправомерного доступа в нашей стране применяется довольно редко.

Активный перехват осуществляется путем непосредственного подключения к средствам вычислительной техники или системе передачи данных при помощи различных штатных оперативно-технических или специально разработанных, изготовленных, приспособленных, запрограммированных средств негласного получения информации. Подобный способ неправомерного доступа достаточно опасен для подразделений ГИБДД. Причина этого кроется в том, что оконечные узлы телекоммуникационных систем ГИБДД осуществляют связь не только по проводным линиям, но и посредством использования услуг операторов сотовой связи. В этом случае злоумышленнику не обязательно быть сотрудником подразделения, а достаточно подключиться к каналу передачи данных.

Особенность совершения неправомерного доступа к компьютерной информации при помощи способов непосредственного доступа заключается в том, что для его реализации необходим прямой доступ непосредственно к компьютеру или рабочей станции телекоммуникационной сети, содержащей информацию ограниченного доступа. Осуществить доступ к подобной информации, находящейся в контролируемой зоне, может не только лицо, работающее или имеющее отношение к производству работ с информацией, но и лицо, целенаправленно проникшее в место ее обработки и хранения.

Остановимся более подробно на случаях непосредственного доступа к информации в информационно-телекоммуникационной сети. Способы и приемы противодействия случаям нарушения безопасности информации не достигнут достаточной эффективности без тщательного анализа уже произошедших попыток неправомерного доступа. Подобную работу обычно выполняет эксперт-криминалист либо лицо, являющееся специалистом в области выявления неправомерных действий в сфере компьютерной информации в данном подразделении. Проведение анализа преследует цель определения механизма совершения и поиска следов неправомерного доступа к информации. Представляется, что для повышения эффективности подобного процесса следует разбить его на несколько этапов, которые заключаются в реализации таких фаз, как сохранение системы, поиск следов и реконструкция событий.

На этапе сохранения системы необходимо произвести консервацию места совершения противоправного деяния с минимизацией всех возможных потерь следов, необходимых для проведения последующего анализа.

В процессе перехода к фазе поиска следов и анализа места совершения противоправного действия в сфере компьютерной информации необходимо определить, как этот поиск будет проводиться — на самом носителе информации при помощи «живого анализа» или на специально созданной копии («мертвый анализ»).

При проведении «живого анализа» необходимо завершить или приостановить все подозрительные процессы, происходящие в операционной системе компьютера, при необходимости отключить его от телекоммуникационной сети. В этом случае целесообразно подключить компьютер к отдельному концентратору для предотвращения появления в журнале сообщений о недоступности сети и неверной работы некоторых программ.

Проведение «мертвого анализа» требует завершения всех процессов, протекающих в компьютере, с последующим отключением системы. По окончании данного процесса целесообразно создать резервные копии всех данных, содержащихся на диске.

При любом предложенном виде анализа необходимо определить криптографический хеш-код, который может понадобиться для доказательства целостности данных и отсутствия в процессе проведения экспертных действий следов модификации на носителе информации. Криптографический хеш-код (MD5, SHA-1 или SHA-256)[5] представляет собой очень большое число, вычисляемое по математической формуле для набора входных данных. Изменение хотя бы одного бита во входных данных приводит к заметному изменению выходного числа.

На этапе поиска следов совершенного противоправного деяния осуществляется поиск, необходимый для подтверждения или опровержения выдвинутых на первоначальном этапе гипотез о происшедшем неправомерном доступе. Процесс поиска заключается, в первую очередь, в определении общих характеристик искомого объекта. На основании данных характеристик происходит выделение предмета и объекта поиска. Второй этап должен заключаться в поиске непосредственно в выделенном наборе данных, что позволяет сузить круг и сократить время поиска. Для выполнения подобных задач существует множество программ, используемых при проведении анализа цифровых систем, функции которых в основном сосредоточены в фазах сохранения и поиска следов.

Практика расследования неправомерного доступа в сфере компьютерной информации показывает, что большинство следов находятся в файловой системе. В этом случае к стандартной методике поиска следует отнести поиск ключевой комбинации в названии файла или поиск по шаблонам. Часто необходимо осуществлять поиск определенного слова в содержании файла или по его временным параметрам (время последнего обращения или записи), если анализ проводится по «горячим следам».

В случаях, когда требуется анализ сетевого трафика, возможен поиск всех пакетов, отправленных с некоторого исходного адреса, или всех пакетов, адресованных конкретному порту. Кроме того, при необходимости можно найти все пакеты с заданными ключевыми словами.

При выполнении фазы реконструкции событий на основе найденных следов производится реконструкция событий, происходивших в системе. Для осуществления данной задачи эксперт должен на достаточно высоком уровне работать с операционной системой и приложениями, установленными на данном компьютере, чтобы провести правильную реконструкцию происходивших событий.

На основании предложенного порядка проведения анализа места совершения противоправного деяния в сфере информационных технологий следует привести некоторые общие рекомендации.

В первую очередь целесообразно осуществить сохранение исследуемой системы. Эксперт должен исключить любую вероятность модификации или

4 Организационно-правовые основы противодействия неправомерному доступу к информации криминалистических учетов ОВД / А. Н. Ильяшенко, Д. С. Мишин — Краснодар: КрУ МВД России, 2009 г.

5 Соколов А. В., Степанюк О. М. Методы информационной защиты объектов и компьютерных сетей.— М.: ООО «Фирма «Издательство АСТ»»; СПб: ООО «Издательство «Полигон»», 2000.

уничтожения данных, которые могут послужить следами, то есть изолировать среду анализа от анализируемых данных и внешнего мира. Необходимость выполнения подобных действий объясняется тем, что неизвестны назначение и скрытые задачи исследуемых файлов. Порядок выполнения данной рекомендации зависит от метода проведения анализа. Предлагается различать, как указывалось ранее, два типа: «мертвый анализ» и «живой анализ».

При использовании метода «мертвого анализа» необходимо:

1. Провести копирование важных данных на аналогичный носитель и поместить оригинальный носитель исследуемой информации в надежное место. Исследование копии необходимо для исключения возможности модификации или удаления данных на протяжении всего процесса анализа и наличия сохраненных данных в случае модификации их копии программами с заранее заготовленными сценариями.
2. В процессе проведения исследования необходимо произвести вычисление хеш-кодов при помощи алгоритмов MD5 и SHA для данных, необходимых для проведения анализа.

При использовании метода «живого анализа» необходимо:

1. Воспользоваться устройствами блокирования записи во время любых действий, в особенности способных привести к изменениям данных во время анализа.
2. Свести к минимуму количество файлов, создаваемых в период проведения анализа и способствующих стиранию следов на свободном пространстве диска. По оценкам специалистов, из «хвостовых» кластеров через сутки можно извлечь до 85%, а через десять суток — до 25–40% исходной информации.
3. Проявлять осторожность при открытии файлов, так как данное событие может в свою очередь привести к модификации или удалению необходимых следов.

Рассмотренные материалы позволяют сделать вывод о том, что проведение «живого анализа» является «рискованным предприятием». Эксперту необходимо проверять анализируемые данные по независимым источникам, что снижает риск использования модифицированных данных. Кроме того, документирование всех действий, совершаемых во время проведения анализа, позволяет избежать повтора проводимого исследования и производить учет полученных результатов.

По окончании краткого рассмотрения фаз анализа места совершения противоправного деяния в сфере информационных технологий целесообразно приступить к рассмотрению способов и методике проведения анализа.

Современные базы данных имеют многоуровневую архитектуру, при этом обладая необходимой гибкостью и масштабируемостью для эффективного хранения и обработки информации, циркулирующей в персональных компьютерах и информационно-телекоммуникационных сетях[6]. Воспользуемся для определения типов анализа такой структурой, которая включает в себя две независимые области. Первая основывается на устройствах хранения информации, а вторая — на устройствах обмена данными.

Иерархия последовательности анализа производится на основании архитектуры цифровых данных. После проведения анализа физических носителей информации необходимо переходить к анализу томов и файловой системы с последующим выходом на прикладной уровень. В рамках данной статьи не рассматривается обращение к таким видам анализа, как анализ файлов подкачки, баз данных, анализ ячеек памяти, сетевой анализ.

Анализ физических носителей информации относится к исследованию низкоуровневых данных и требует наличия надежного метода чтения физических носителей (жесткие диски, карты памяти и т.д.). Это объясняется тем, что при необходимости долгосрочного хранения информации она организуется в виде томов, где под томами понимается совокупность ячеек, доступных для обращения и записи со стороны приложений.

Анализ прикладного уровня играет важную роль, так как, основываясь на анализе конфигурации файлов, можно определить программы, выполнявшиеся в системе, и выявить скрытое содержание графических файлов, которое может создаваться при помощи специальных программ.

Немаловажную роль в процессе противодействия правонарушениям в сфере информационных технологий играют способы профилактики неправомерного доступа к компьютерной информации.

Помимо традиционно используемого способа профилактики неправомерного доступа к компьютерной информации, заключающегося в усилении защищенности компьютерных систем от неправомерного вмешательства в их деятельность, рассмотрим ряд способов, применение которых позволит снизить количество правонарушений. К подобным способам относятся:

- пропаганда правовых знаний и широкая огласка ответственности, что позволит ограничить круг лиц, совершающих правонарушения по незнанию, из любопытства или хулиганских побуждений;
- проведение работы по официальной блокировке и закрытию сайтов, размещенных в сети Интернет, на которых осуществляется пропаганда хакерства и крэкерства, а также свободно распространяются программные средства, позволяющие осуществлять неправомерный доступ к компьютерной информации. Кроме того, необходимо исключить издание литературы, содержащей пропаганду хакерства и крэкерства и способы совершения противоправных деяний.

Необходимо отметить, что главная цель любой системы информационной безопасности заключается в обеспечении устойчивого функционирования объекта: предотвращении угроз его безопасности, защите законных интересов владельца информации от противоправных посягательств, в том числе уголовно наказуемых деяний в рассматриваемой сфере отношений, предусмотренных Уголовным кодексом РФ, обеспечении нормальной производственной деятельности всех подразделений объекта. В сложившейся ситуации просматривается глобальная тенденция по совершенствованию систем и средств обнаружения, противодействия и предотвращения попыток неправомерного доступа в информационных сетях любого уровня.

В настоящее время концепция информатизации ОВД и ВВ МВД России предусматривает интеграцию ФИС ГИБДД в ЕИП МВД России, что влечет за собой разработку и внедрение средств информационного взаимодействия с различными службами и компаниями[7]. При этом следует обратить внимание на тот факт, что информационные ресурсы, циркулирующие в телекоммуникационных сетях ГИБДД, зачастую в соответствии с действующим законодательством являются информацией ограниченного распространения. Все это указывает на необходимость создания и использования достаточно эффективных средств обеспечения безопасности информации, которые целесообразно основывать на тщательном анализе неправомерных действий злоумышленников.

6 Carrier, Brian. «Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers». International Journal of Digital Evidence, Winter 2003a. http://www.ijde.org.

7 Приказ МВД России от 04.04.2009г. №1144 «Об утверждении концепции информатизации органов МВД России и ВВ МВД России до 2012 года».