УДК 343.9

АНАЛИЗ ВЫСОКОТЕХНОЛОГИЧНЫХ СПОСОБОВ НЕПРАВОМЕРНОГО УДАЛЕННОГО ДОСТУПА К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

В.В. Поляков*, С.М. Слободян

*Алтайский государственный университет, г. Барнаул
Томский государственный университет систем управления и радиоэлектроники
E-mail: polyakovvv@rambler.ru

Проведен анализ высокотехнологических способов совершения преступлений в сфере обращения компьютерной информации, практически осуществленных с удаленно расположенных ЭВМ. Выявлены виртуальные следы, оставляемые при реализации таких способов. Разработаны конкретные предложения по расследованию и предотвращению данного вида компьютерного проникновения.

На протяжении последних лет прослеживается все возрастающая тенденция развития способов неправомерного, с точки зрения законодательства РФ, и административно несанкционированного доступа к компьютерной информации с использованием сетевых технологий, основанных на удаленном доступе потребителей к информационным базам данных. Одним из основных факторов, способствующих этому процессу, является наличие в сфере обращения компьютерной информации новых программно-аппаратных средств, обладающих широкими высокотехнологическими возможностями, освоение и применение которых позволяет находить нестандартные решения для осуществления неправомерного доступа [1]. В таких ситуациях неправомерный доступ бывает достаточно специфичен, а виртуальные следы для правоохранительных органов остаются скрытыми. Данные обстоятельства серьезным образом сказываются на латентности преступлений в сфере компьютерной информации, которая достигает 90 %. Подчеркнем, что в современной криминалистике следы осуществления такого вида преступлений практически не изучены [2]. Таким образом, актуальной задачей является изучение закономерностей проявления механизма «практики» подготовки, совершения и сокрытия преступлений в сфере компьютерной информации.

Наиболее профессионально опытные нарушители действуют таким образом, чтобы следы компьютерного проникновения были максимально скрыты или достоверно не указывали на лицо, их оставившее [3]. Более того, в этих случаях зачастую используют такие способы проникновения, чтобы логические пути расследования в еще большей степени осложнили работу правоохранительных органов. Проблема объясняется недостаточным уровнем специальных знаний о компьютерной технике и информационных технологиях у расследующих эти преступления сотрудников правоохранительных органов. В таких условиях значительную помощь при проведении следствия должны оказать четкие представления о том, какие следы остаются при высокотехнологичных способах неправомерного доступа в сфере компьютерной информации. В этой предметной области особенно сложными и важными нарушениями являются основанные на высокотехнологичных способах несанкционированного доступа к компьютерной информации и совершенные путем использования информационной сети с удаленно расположенных ЭВМ.

Следует отметить, что для неправомерного удаленного доступа характерно нахождение следов в разных местах одновременно и на большом расстоянии друг от друга. Так, они могут быть оставлены не только на рабочем месте, но и в месте хранения или резервирования информации [4]. Следы также могут быть обнаружены на местах подготовки к доступу (например, там, где разрабатывались или тестировались программы для неправомерного доступа), использования инструментов, устройств и средств, предназначенных для операций неправомерного доступа, а также в месте использования информации [5]. Указанные обстоятельства требуют проверки всех предполагаемых мест, где могут находиться виртуальные следы. Важно отметить, что только полученные и оформленные с соблюдением уголовно-процессуального законодательства следы могут быть приобщены к уголовному делу и станут рассматриваться в качестве доказательств.

Рассмотрим некоторые основные особенности высокотехнологичных способов неправомерного доступа к компьютерной информации.

1. Использование чужих регистрационных адресов в локальной сети, имеющей выход в Интернет

Компьютеры, подключенные к локальной сети с выходом в Интернет, как правило, имеют два адреса: логический адрес сетевого уровня (IP-адрес) и физический адрес сетевой интерфейсной карты (MAC-адрес) [6]. При отправке пакетов за пределы локальной сети эти адреса будут зафиксированы, следовательно, можно будет найти ЭВМ, с которой был совершен неправомерный доступ, что в дальнейшем позволит отыскать соответствующие традиционные и виртуальные следы. Однако лица, обладающие специальными знаниями, могут самостоятельно прописать чужой IP-адрес, чтобы запутать следствие. В случае, когда имеются основания полагать, что произошла именно такая ситуация, следует обратить внимание на MAC-адрес сетевой

карты. Как правило, все сетевые карты имеют свой уникальный номер, который сложно изменить или уничтожить. Данный номер может быть также зафиксирован при сетевом соединении. Таким образом, доказательством того, что нарушитель использовал чужой IP-адрес, будет служить несоответствие MAC-адреса сетевой карты компьютера тому MAC-адресу, который был указан при подключении. Для расследования подобных нарушений негативную роль оказывает то обстоятельство, что в продаже имеются сетевые карты, позволяющие изменять MAC-адреса программным способом. В таком случае можно без особого труда использовать не только чужой IP-адрес, но и MAC-адрес. Если будет установлено, что во время неправомерного доступа за компьютером, на который указывают прописанные преступником IP и MAC-адреса, работал конкретный человек, то подозрение падет именно на него. Более того, вполне возможна ситуация, когда на данный компьютер затем будет подброшена похищенная информация. Подобные действия являются крайне опасными, так как при недостаточно умелой следственной работе может быть привлечен невиновный человек.

Чаще всего, на сервере провайдера могут храниться учетные данные его клиентов. Большинство этих данных используются правоохранительными органами в качестве доказательств совершения преступления с конкретного компьютера. В то же время анализ показывает, что контроля, указывающего на того, кто именно работал на компьютере в период совершения с него неправомерного доступа, практически не бывает [7]. Например, рассмотрим ситуацию, когда доступ совершался с домашнего компьютера. Лицо, которому он принадлежит, может в своих показаниях заявить, что в период совершения доступа у него дома находились посторонние люди. Если в подобной ситуации подозреваемый договорится с кем-либо из них о том, чтобы они подтвердили данные обстоятельства, установить, кто совершил доступ, будет крайне затруднительно.

2. Использование беспроводного (Wi-Fi) соединения

Для несанкционированного доступа может быть использован ноутбук, сотовый телефон или иное портативное устройство вблизи пункта, предоставляющего доступ в Интернет по беспроводной технологии, например, в «Интернет-кафе». В такой ситуации на сервере провайдера останутся следующие следы:

- учетные данные нарушителя, например, логин и пароль;
- настройки, которыми пользовался нарушитель, в частности его IP-адрес, выделенный для определенного сеанса связи;
- информация о пакетах, которые были отправлены либо получены на адрес клиента, в частности время отправки/приема, размер, тип, IP-адрес получателя или отправителя и т. д.;
- в некоторых случаях данные о конфигурации компьютера злоумышленника.

В то же время следствие, даже располагая этими данными, не сможет выделить конкретное лицо и устройство, с которого был осуществлен неправомерный доступ. Под подозрением может оказаться неопределенный круг лиц, которыми мог быть уловлен сигнал на тот момент, когда был совершен доступ. Например, это могут быть лица с ноутбуками, находящиеся в кафе или в припаркованных автомобилях, жители близлежащих домов, использующие специальные улавливающие слабый сигнал устройства. Оперативные мероприятия по обыску перечисленных лиц с целью обнаружения и осмотра их компьютеров представляются маловероятными с точки зрения их эффективности.

3. Использование чужого телефонного номера

Органы следствия при поиске, как правило, исходят из данных, полученных от фирмы провайдера, в первую очередь касающихся телефонного номера, с которого осуществлялся неправомерный доступ при использовании модемного соединения [8]. Анализ ряда уголовных дел показал, что доказывание совершения проникновения строится на базе главного доказательства – телефонного номера, с которого происходило соединение с сервером провайдера [9]. Представляется, что подобное обстоятельство нельзя рассматривать в качестве универсального доказательства. Это подтверждается тем, что практически к телефонным кабелям имеется открытый доступ, распространены технические сбои на автоматической телефонной станции (АТС), а также возможно соучастие работников АТС в совершении неправомерного доступа. Все это создает благоприятную ситуацию для того, чтобы злоумышленники воспользовались описанными вариантами. Так, с помощью ноутбука можно подсоединиться к линии телефонной сети в многоквартирном доме и тем самым осуществить выход в сеть Интернет с чужого телефонного номера, в том числе воспользовавшись картой доступа в Интернет. Доказать факт подключения нарушителя к чужому телефонному кабелю будет крайне сложно. Отметим, что случаев использования чужих телефонных линий связи для осуществления междугородних звонков современная российская практика знает достаточно. Данное обстоятельство свидетельствует о потенциально возможном росте совершения действий, связанных с неправомерным доступом по подобной схеме. Для предотвращения следственной ошибки и обвинения невиновного необходимо воспользоваться помощью специалистов или экспертов, задачей которых являлось бы установление совершения проникновения с иного компьютера [10]. Выявление данного обстоятельства возможно путем исследования программно-аппаратного обеспечения этого компьютера и сравнения имеющихся в нем данных с информацией, предоставленной провайдером.

4. Использование чужого компьютера в качестве средства неправомерного доступа путем кратковременного удаленного соединения с ним

Для неправомерного доступа может быть использовано кратковременное удаленное соединение с чужим компьютером в случае, когда подключение к линии телефонной связи потерпевшего отсутствует. Например, распространенным является подключение к чужому компьютеру дистанционным образом с помощью программы вирусного типа «троянский конь». Установить такую программу можно с помощью электронной почты, Wi-Fi соединения или путем неправомерного подключения, т. к. защита компьютеров у большинства пользователей крайне низкая. В такой ситуации на зараженном компьютере останется вся информация о неправомерном подключении, и подозрение ляжет на владельца этого компьютера.

При расследовании такого способа совершения доступа можно предложить следующие рекомендации по обнаружению следов. В случае самоликвидации вредоносной программы можно проанализировать системный реестр на наличие характерных команд и их реквизитов и обнаружить данные, позволяющие предположить, что на компьютере был подобный вирус. Для доказательства наличия вируса можно попытаться использовать также стандартные программы по восстановлению удаленных данных. Такая операция не будет успешна, если в ячейки памяти, зарезервированные под вирус, затем записывалась другая информация. Кроме того, во многих случаях доступ в Интернет осуществляется посредством использования прокси-сервера, который фиксирует всю информацию, касающуюся сетевых соединений [11]. По данным прокси-сервера можно установить факт соединения компьютера, с которого предположительно совершалось преступление, с компьютером злоумышленника.

5. Использование услуг провайдера, не фиксирующего данные о своих пользователях

В настоящее время появляется все большее количество провайдеров, которые не фиксируют у себя информацию о пользователях. Это делается с целью повышения анонимности, чтобы не было известно, какие сайты посещают клиенты провайдера. При использовании таких услуг на сервере провайдера не останется следов доступа, что значительно затруднит расследование. Кроме этого, для неправомерного доступа могут быть использованы и так называемые анонимные прокси-сервера, доступные в сети Интернет.

6. Возможные пути предотвращения попыток неправомерного доступа

Необходимость совершенствования комплекса мер по защите компьютерных систем и информационных баз данных, в частности, автоматизированных средств контроля использования специальной информации в различных областях деятельности человека, существует давно. Потребность в защите информации от неправомерного доступа вызвана компьютеризацией многих экономических и политических отраслей функционирования государственных структур как средства повышения эффективности обработки информации для ускорения принятия решений и управления.

Компьютеризация резко увеличила объем потока информации и емкость баз данных. Более того, непрерывно возрастает уровень профессиональной подготовки специалистов высокой квалификации в области компьютерных средств, темп и интенсивность использования этих средств. Это приводит к, вытекающей отсюда, логической необходимости осуществления разработки, создания новых и совершенствования существующих компьютерных систем и средств, причем не только для защиты, но и для оценки надежности защиты и сохранения компьютерной информации от несанкционированного к ней доступа. Существует также ряд факторов экономического, политического, социального, психофизиологического, медицинского, геополитического и т. п. характера (их анализ выходит за рамки предмета исследования), которые приводят к росту попыток несанкционированного доступа к компьютерной информации, включая возросшую практику проникновения через сетевые структуры в информационные базы данных с удаленных ЭВМ. Такая практика несанкционированного проникновения в базы данных с удаленных ЭВМ основана на использовании развивающихся сетевых технологий и усовершенствования средств приема и передачи компьютерной информации.

Наиболее простой и достаточно эффективный путь – введение некоторого порога защиты информации и сохранения неприкосновенности баз данных состоит в априорном принятии мер, заключающихся, например, в установке в компьютер известных программных средств, предназначенных для ограничения свободного доступа, предотвращения и предупреждения попыток неправомерного использования данного компьютера и, хранящейся в нем, компьютерной информации [6]. Такие средства обеспечивают поддержание минимального (нижнего) уровня мер защиты информации в компьютерных средствах коллективного пользования. Установленная в них, система производит защиту информации от несанкционированного доступа таким образом, чтобы право и возможность использования, хранящихся в компьютерах, данных, производства с ними операций по их модификации получал только пользователь индивидуально распознаваемый данной системой.

Подобный вариант обеспечения защиты информации от неправомерного к ней доступа может быть выполнен путем использования стандартных программных средств, предусмотренных библиоте-

кой пакета Microsoft Access. Применение Microsoft Access не позволяет нескольким пользователям одновременно корректировать или изменять одни и те же информационные данные, т. е. вводит ранжирование на доступ к информации по приоритетам, которые установлены администратором системы. При этом Microsoft Access автоматически обеспечивает защиту данных от одновременного их изменения разными пользователями (разнесение по времени и приоритетам доступа к данным).

В Microsoft Access предусмотрены надежные, с точки зрения удовлетворения требований нижнего уровня защиты интересов широкого круга пользователей, меры защиты целостности данных разделением доступа к информации по рангам и приоритетам. Причем, если пользователям с наивысшим приоритетом предоставляется право доступа к основным информационным и программным средствам, то другим, не включенных в список администратором, разрешена работа только с дубликатами выделенных фрагментов информации или фреймов базы данных. Это дает возможность создать дополнительный порог доступа, помимо предусмотренных в самом пакете Microsoft Access, к логическим правилам защиты информации и обеспечения повышения надежности защиты баз данных от попыток неправомерного доступа.

Конечно, профессионально освоивший программный продукт Microsoft Access пользователь может найти пути обхода защитных барьеров доступа к информационным ресурсам и базе данных. Но, в последнем случае, он получает доступ только к фрагментам дубликата, а не к основным ресурсам. Принципиально возможны и другие логические правила установления барьеров доступа. Например, усложнение порядка идентификации признаков, отражающих подлинность пользователя, на предоставление ему права доступа даже к дубликату или к системе с удаленного терминала.

Еще одной мерой защиты является учет того фактора, что включение высокопрофессиональных специалистов в процесс использования высоких технологий неизбежно требует установления соответствующих этому фактору и мер контроля. Необходима также и оценка «прозрачности» порядка соблюдения установленных законодательством или инструктивными материалами, правил и требований при использовании разрешенных данному пользователю тех фрагментов информации, которые в той или иной мере затрагивают сферу безопасности компании, организации, государства или личных и других прав граждан. Возможны и другие, основанные на идентификации личности, принципы ранжирования приоритетов доступа и оценки необходимого уровня информационной безопасности доступа данному пользователю к информационным ресурсам.

7. Заключение

Проводя анализ и обобщение выше изложенного, можно придти к следующим заключениям:

1. Разработка мер, программных и аппаратных средств противодействия попыткам несанкционированного доступа к компьютерной информации должна быть тесно увязана с изучением методов, подходов к решению и принципов высоких технологий осуществления на практике таких попыток. Анализ существующих «практик» неправомерного проникновения к компьютерной информации важен для понимания сущности и формирования в последующем решений проблемы, которые смогут предотвратить проведение таких действий в принципе. Предпочтительнее предотвратить их еще на стадии планирования и подготовки возможности осуществления такой попытки, т. е. важно показать неосуществимость проведения неправомерных действий в плане достижения цели проникновения. В рамках массового обследования, по вполне понятным причинам, обусловленных определенной мотивацией таких «пользователей» и закрытостью подобной информации, анализ и исследование подобных «практик» провести затруднительно, скорее невозможно.
2. Разработка мер предотвращения неправомерного доступа к компьютерной информации на основе обобщения и анализа, имевших место на практике, реально рассмотренных или подлежащих предметному и обстоятельному изучению, разных аспектов путей подхода и мотивации осуществления деятельности по неправомерному, в том числе удаленному, доступу к компьютерной информации является актуальной. Следует признать, что принятие и выработка прогнозных решений на основе анализа рассмотренных реальных «практик» неправомерного проникновения к компьютерной информации, а также их обобщение крайне затруднены. Действительно, в таких случаях исследователь имеет «дело» с многоальтернативной мотивацией особого рода «пользователя». Получаемый при этом, фактический материал для исследования представляет собой выборку малой размерности с признаками, которые характерны для юридической, социологической, психологической и правовой практик.
3. В рассматриваемой предметной области важно исследовать мотивационные аспекты и технологические пути осуществления подобного рода «практик». Необходимо изучить закономерности статистики явления. Другими словами, выявить все возможные направления подобной деятельности; определить, как и каким образом возникают и устанавливаются несанкционированные компьютерные связи; исследовать фак-

ты любого неправомерного доступа; оценить, что способствует, а что может препятствовать неправомерному доступу, включая доступ с удаленных ЭВМ.

Выводы

В настоящей работе проведен, хотя и ограниченный, анализ методов и способов, реально осуществленных, высокотехнологичных противоправных, по действующему законодательству РФ, действий путем несанкционированного доступа к компьютерной информации с удаленных терминалов.

Проанализированы особенности следов преступлений, связанных с применением нарушителями высокотехнологичных способов неправомерного доступа к компьютерной информации, и предложены способы выявления этих следов. Результаты исследования, проведенного в настоящей работе, свидетельствуют о том, что, в свете усиливающегося противодействия следствию от современной криминалистики требуется дальнейшее изучение закономерностей и механизмов подготовки, совершения и сокрытия рассматриваемого вида преступлений.

На наш взгляд, только всестороннее изучение всех аспектов имеющейся проблемы даст возможность найти оптимальное решение для формирования прогноза возникновения подобных ситуаций и определения возможных направлений их осуществления. На основе найденных решений при анализе можно сформировать направление действий по предотвращению подготовки неправомерных попыток высокотехнологичного проникновения в компьютерные системы.

Краткое описание изложенных выше реальных фактов неправомерного доступа позволяет выявить скрытые логические закономерности формирования «виртуальных» следов неправомерных действий в исследуемой предметной области. Логические закономерности являются существенными для построения базы знаний о методах неправомерного доступа, формирование которой потребует ввода новых понятий и осмысления множества фрагментов знаний в данной области.

Рассмотренные подходы, способы и методы выявления «виртуальных» следов «взлома» – неправомерного доступа к компьютерной информации могут дополняться или замещаться другими методами поиска скрытых закономерностей осуществления несанкционированного доступа. Это потребует пересмотра процедуры анализа реальных фактов доступа или действий получаемых другим способом проникновения.

СПИСОК ЛИТЕРАТУРЫ

1. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000. – 452 с.
2. Мещеряков В.А. Преступления в сфере компьютерной информации: правовой и криминалистический анализ. – Воронеж: Воронежский государственный университет, 2001. – 176 с.
3. Полещук О.В., Шаповалова Г.М. Криминалистическое исследование следов при расследовании компьютерных преступлений. – Владивосток: Изд-во Дальневосточного ун-та, 2006. – 157 с.
4. Гаврилов М., Иванов А. Следственный осмотр при расследовании преступлений в сфере компьютерной информации // Законность. – 2001. – № 4. – С. 11–14.
5. Никонов В. Панасюк А. Нетрадиционные способы собирания и закрепления доказательств // Законность. – 2001. – №4. – С. 19–24.
6. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2006. – 960 с.
7. Гавло В.К., Поляков В.В. Некоторые особенности расследования преступлений, связанных с неправомерным доступом к компьютерной информации // Известия Алтайского государственного университета. – 2006. – № 2. – С. 44–48.
8. Архив Октябрьского районного суда г. Барнаула. Дело № 1-705/ 04.
9. Архив Индустриального районного суда г. Барнаула. Дело № 1-51/05.
10. Россинская Е.Р. Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе. – М.: Норма, 2005. – 656 с.
11. Архив Центрального районного суда г. Барнаула. Дело № 1-537/03.

Поступила 26.10.2006 г.