**Способы совершения преступления в сфере компьютерной информации**

Под способом совершения преступления понимается система объединенных единым замыслом действий преступника (и связанных с ними лиц) по подготовке, совершению и сокрытию преступления, детерминированных объективными и субъективными факторами и сопряженных с использованием соответствующих орудий и средств.

На сегодняшний день в криминалистике нет единой классификации способов совершения преступлений в сфере компьютерной информации. Одна из классификаций предложена А.Н. Родионовым и А.В. Кузнецовым. Согласно ей, способы совершения компьютерных преступлений можно подразделить:

1) на «изъятие средств компьютерной техники;

2) неправомерный доступ к компьютерной информации: преступления, совершенные в отношении компьютерной информации, находящейся в глобальных компьютерных сетях; преступления, совершенные в отношении компьютерной информации, находящейся в ЭВМ, не являющихся компьютером в классическом понимании этого слова (пейджер, сотовый телефон, кассовый аппарат и т.п.);

3) изготовление или распространение вредоносных программ (вирусы, программы – взломщики и т.п.);

4) перехват информации: электромагнитный; непосредственный;

5) нарушение авторских прав (компьютерное пиратство);

6) комплексные методы.

Данная классификация не лишена недостатков.

Во-первых, фактически авторами за основу классификации взят непосредственный объект преступного посягательства, а не способ совершения преступления.

Во-вторых, неправомерный доступ к компьютерной информации, как показано нами выше, совершается гораздо большим количеством способов, чем отметили авторы (в частности, ими не отмечены непосредственные способы).

В-третьих, способы перехвата информации относятся к способам неправомерного доступа к ней, и выделение их в качестве самостоятельной группы необоснованно.

И в-четвертых, изъятие средств компьютерной техники представляет собой преступление против собственности, а не в сфере компьютерной информации.

Способы совершения неправомерного доступа компьютерной информации можно объединить в три основные группы.

Первая группа – это способы непосредственного доступа. При их реализации информация уничтожается, блокируется, модифицируется, копируется, а также может нарушаться работа ЭВМ, системы ЭВМ или их сети путем отдачи соответствующих команд с компьютера, на котором информация находится.

Непосредственный доступ может осуществляться как лицами, работающими с информацией (имеющими отношение к этой работе), так и лицами, специально проникающими в закрытые зоны и помещения, где производится обработка информации. Например, человек, имеющий умысел на противоправный доступ к компьютерной информации, держа в руках определенные предметы, указывающие на его «принадлежность» к работе на компьютере (дискеты, распечатки и пр.), прохаживается около запертой двери помещения, где расположен терминал. Дождавшись, когда в названное помещение войдет работающий в нем сотрудник, он входит туда вслед за ним, а потом через определенный промежуток времени при благоприятной для этого обстановке совершает неправомерный доступ к компьютерной информации.

Необходимо отметить, что описанный способ в настоящее время менее распространен по причине децентрализации обработки информации. Практика показывает, что преступники компьютерную информацию чаще перехватывают при ее передаче по телекоммуникационным каналам и компьютерным сетям. Сделать это им и проще, и безопаснее, чем при непосредственном проникновении в помещение. Примером совершения неправомерного доступа к компьютерной информации может являться дело по обвинению К. по ч. 1 ст. 272 УК РФ. В ходе расследования было установлено, что он, находясь на работе в качестве электромеханика Переяславского районного узла электрической связи, на принесенную с собой дискету скопировал с компьютера готовящийся к изданию телефонный справочник района им. Лазо. Эту дискету он принес домой и скопировал полученную информацию на жесткий диск своего компьютера, а затем на принтере отпечатал 4 экземпляра названного справочника. Таким образом, К. умышленно, незаконно скопировал информацию, хранившуюся в электронно-вычислительной машине.

Другой способ непосредственного доступа к компьютерной информации заключается в неправомочном использовании преступником технических отходов информационного процесса, оставленных пользователем после работы с компьютерной техникой. Он осуществляется в двух формах: физической и электронной.

Физический поиск отходов сводится к обследованию рабочих мест программистов, содержимого мусорных баков, емкостей для технологических отходов для сбора оставленных или выброшенных физических носителей информации, а также обследованию различной документации, оставленной на рабочем месте: ежедневников, книг рабочих записей, перекидных календарей и т.п. в целях поиска черновых записей, паролей доступа в систему и пр.

Электронный вариант требует просмотра и последующего исследования данных, находящихся в памяти компьютера. Он основан на некоторых технологических особенностях функционирования средств компьютерной техники. Например, данные, записанные в последний момент работы, не всегда стираются из оперативной памяти компьютерной системы.

В названных целях могут просматриваться и восстанавливаться стертые файлы. В данном случае предполагается обязательное использование в качестве орудия преступления различных программных средств специального назначения. Одним из них является программный комплекс PC Tools Deluxe, содержащий универсальную программу восстановления стертых файлов.

Вторая группа способов совершения рассматриваемого преступления включает способы опосредованного (удаленного) доступа к компьютерной информации. При этом неправомерный доступ к определенному компьютеру и находящейся на нем информации осуществляется с другого компьютера, находящегося на определенном расстоянии, через компьютерные сети. Способы опосредованного доступа к компьютерной информации, в свою очередь, можно разделить на две подгруппы: способы преодоления парольной а также иной программной или технической защиты и последующего подключения к чужой системе; способы перехвата информации.

К способам первой подгруппы относятся:

1. Подключение к линии связи законного пользователя (например, к телефонной линии) и получение тем самым доступа к его системе. Подключившись, преступник дожидается сигнала, означающего окончание работы, перехватывает его «на себя», а потом, когда законный пользователь закончил сеанс работы, осуществляет доступ к его системе. Данный способ сравним с работой двух параллельных телефонных аппаратов, подключенных к одному абонентскому номеру: если один телефон находится в активном режиме (ведется разговор с абонентом) и на другом аппарате поднимается трубка, то когда разговор по первому телефону закончен и трубка положена, он может быть продолжен по второму.

2. Проникновение в чужие информационные сети путем автоматического перебора абонентских номеров с последующим соединением с тем или иным компьютером (перебор осуществляется до тех пор, пока на другом конце линии не «отзовется чужой» компьютер). Поскольку в подобном случае один несанкционированный пользователь может быть легко обнаружен, подобный «электронный взлом» осуществляется одновременно с нескольких рабочих мест: в заданное время несколько (более десяти) персональных компьютеров одновременно предпринимают попытку несанкционированного доступа. Это может привести к тому, что несколько «атакующих» компьютеров отсекаются системой защиты, а остальные получают требуемый доступ. Один из «прорвавшихся» компьютеров блокирует систему статистики сети, которая фиксирует все попытки доступа. В результате этого другие «прорвавшиеся» компьютеры не могут быть обнаружены и зафиксированы. Часть из них приступает к «взлому» нужного сектора сети, а остальные занимаются фиктивными операциями в целях дезорганизации работы предприятия, организации, учреждения и сокрытия преступления.

3. Проникновение в компьютерную систему с использованием чужих паролей, выдавая себя за законного пользователя. При подобном способе незаконный пользователь осуществляет подбор пароля для доступа к чужому компьютеру. Подбор паролей может осуществляться двумя методами.

Первый: подбор паролей путем простого перебора всех возможных сочетаний символов до тех пор, пока не будет установлена нужная комбинация. Для реализации такого подбора существуют уже специально разработанные программы, которые можно приобрести на «черном» компьютерном рынке. Алгоритм их действия основан на использовании быстродействия современных компьютеров при переборе всех возможных комбинаций букв, цифр и автоматического соединения специальных символов, имеющихся на стандартной клавиатуре персонального компьютера, и в случае совпадения комбинации символов с оригиналом произведения.

Второй: «интеллектуальный» подбор паролей на основе имеющихся «словарей» наиболее распространенных паролей, систематизированных по определенным тематическим группам. Практика показывает, что данным методом вручную вскрываются более 40% паролей. При этом наиболее распространенными тематическими группами паролей являются следующие: имена, фамилии и производные от них (22%); последовательность клавиш компьютера, повтор символов (14%); даты рождения пользователя и его близких, а также их комбинации (12%); интересы, хобби (9,5%); адрес, место рождения (5%); номера телефонов или документов: паспортов, удостоверений личности и пр. (3,5%).

Подобрав необходимый пароль (для подбора восьмизначного пароля требуется несколько часов), незаконный пользователь получает доступ к компьютерной информации и может проводить с ней любые действия под видом законного пользователя: копировать ее, модифицировать, удалять, заставлять программы производить требуемые операции, например, по переводу денежных средств на свои счета, фальсификации платежных документов и пр.

4. Разновидностью способа получения пароля для последующего незаконного вхождения в компьютерную систему является так называемый социальный инжиниринг («обратный социальный инжиниринг»). Это метод основан на недостаточной бдительности пользователей, когда информация получается в процессе беседы (телефонной, посредством обмена электронными сообщениями) правонарушителями с пользователями системы. При этом способе правонарушитель представляется либо системным администратором, либо сотрудником обслуживающей компьютерной фирмы, либо сотрудником, вновь поступившим на работу, и запрашивает у собеседника данные о паролях доступа к системе. Данный способ широко применяется для получения данных (имя, пароль) в целях подключения к компьютерной сети Интернет за счет законных пользователей.

Интересен пример из зарубежной практики: преступник, являющийся законным пользователем компьютерной сети, с рабочей станции передал сообщение всем пользователям сервера о том, что его номер якобы изменен. В качестве нового номера был назван номер собственного персонального компьютера преступника, запрограммированный таким образом, чтобы ответить аналогично серверу. Пользователи, посылавшие вызов, набирали при этом свой личный код, что позволило преступнику получить исчерпывающий список личных кодов пользователей.

Ко второй подгруппе способов опосредованного (удаленного) доступа к компьютерной информации относятся способы ее непосредственного, электромагнитного и других видов перехвата.

Непосредственный перехват осуществляется либо прямо через внешние коммуникационные каналы системы, либо путем непосредственного подключения к линиям периферийных устройств. При этом объектами непосредственного «подслушивания» являются кабельные и проводные системы, наземные микроволновые системы, системы спутниковой связи, а также специальные системы правительственной связи.

Современные технические средства позволяют получить информацию без непосредственного подключения к компьютерной системе: за счет перехвата излучений центрального процессора, дисплея, коммуникационных каналов, принтера и т.д. Все это можно осуществить, находясь на достаточном удалении от объекта перехвата. Например, используя специальную аппаратуру, можно «снимать» информацию с компьютера, расположенного в соседнем помещении, здании.

Впервые дистанционный перехват информации с монитора компьютера был открыто продемонстрирован в марте 1995 г. в Каннах на международном конгрессе по вопросам безопасности ЭВМ. Сотрудник голландской телекоммуникационной РТТ Вим Ван Эк шокировал специалистов тем, что с помощью разработанного им устройства из своего автомобиля, находящегося на улице, «снял» данные с экрана монитора персонального компьютера, установленного на 8-м этаже здания, расположенного в 100 м. от автомобиля.

Отечественным примером совершения неправомерного доступа к компьютерной информации подобным способом является дело по обвинению Л. и М. по п. «а» ч. 2 ст. 272 УК РФ. В ходе расследования было установлено, что М. собственноручно у себя дома произвел демонтаж и переоборудовал заранее приобретенные им сотовые телефоны фирмы «Моторолла» под микропроцессоры со специальной программой. Изготовив таким образом два аппарата с режимом автосканирования и шесть аппаратов с возможностями ввода с клавиатуры скопированных номеров в электронные записные книжки, он осуществлял неправомерный доступ к сети ЭВМ компании сотовой телефонной связи «Вотек-Мобайл». Путем модернизации телефонного аппарата «Моторолла» гр. М. была получена возможность фиксации в радиусе до 200 м. абонентского и серийного номера аппарата законного пользователя сотовой телефонной сети с последующим занесением его в память электронной записной книжки. Это позволяло производить телефонные звонки с переделанных таким образом сотовых телефонных аппаратов бесплатно, за счет законных клиентов сотовой сети.

К методам перехвата информации относится также аудиоперехват и видеооптический перехват.

Аудиоперехват, или снятие информации по вибро-акустическому каналу, имеет две разновидности: заходовую (заносную) и беззаходовую.

Первая заключается в установке инфинитивного телефона (подслушивающего устройства – «таблетки», «клопа», «жучка» и т.п.) в аппаратуру средств обработки информации: в различные технические устройства, на проводные коммуникационные линии (радио, телефон, телевизионный кабель, кабель охранно-пожарной сигнализации или электросеть и т.п.), а также в различные конструкции инженерно-технических сооружений и бытовых приборов, находящихся на объекте. Делается все это в целях перехвата разговоров работающего персонала и звуковых сигналов технических устройств (определение номера вызываемого абонента АТС и т.п.).

Установка «клопа» или иной разведывательной аппаратуры на объект возможна тремя способами.

При первом необходимо скрытное или легендированное проникновение в помещение, при втором требуется радиопередающая и звукозаписывающая аппаратура, которая устанавливается во время постройки или ремонта помещения, при третьем – специальная техника приобретается или заносится самой потерпевшей стороной, даже не подозревающей об этом, например монтируется в приобретаемые предметы.

К специальной технике, используемой для этого, относятся: спецмикрофоны с возможным дистанционным управлением, диктофоны с длительной записью, цифровые адаптивные фильтры типа АО-512, ОАС-256 и ОАС-1024, позволяющие проводить обработку зашумленных речевых сигналов.

Обнаружить аппаратуру съема информации крайне трудно, так как она обычно очень хорошо камуфлируется преступником (под микросхему, зажигалку, булавочную головку и т.д.).

Вторая разновидность аудиоперехвата – беззаходовая – наиболее опасна. Заключается она в следующем. Акустические и вибрационные датчики съема информации устанавливают на инженерно-технические конструкции, находящиеся за пределами охраняемого помещения, из которого необходимо принимать речевые сигналы. Выделяют следующие типовые конструкции инженерно-технических сооружений: несущие стены зданий, перегородки, перекрытия, окна, оконные рамы, двери и дверные коробки, вентиляционные воздуховоды, трубопроводы. При этом необязательно проникать в помещение, достаточно приблизиться к нему снаружи. Датчик устанавливается либо непосредственно, либо дистанционно. В последнем случае используются различные выстреливающие устройства, предназначенные для дистанционного снятия речевой информации через открытые окна, двери и т.п.

Видеооптический перехват заключается в действиях преступника, направленных на получение информации путем использования различной видеооптической техники. Этот способ осуществляется как физически, так и электронно. Физически перехват информации производится с помощью применения преступником различной бытовой видеооптической аппаратуры – например подзорной трубы, бинокля, прибора ночного видения, оптического прицела и т.п. При этом преступник проводит отдаленное наблюдение за объектом (жертвой) в целях получения необходимой информации, которую в отдельных случаях фиксирует на физический носитель. В рассматриваемом случае орудие преступления находится непосредственно в руках преступника.

Электронный процесс получения информации осуществляется с использованием преступником специальной техники. В данном случае передающее устройство находится непосредственно на объекте наблюдения, а приемное – в руках преступника Может использоваться следующая спецтехника: спецвидеомагнитофоны с длительной записью; оборудование для скрытой видеосъемки; цифровые электронные видеокамеры; приборы ночного видения и т.п.

Третью группу способов совершения анализируемого преступления составляют смешанные способы, которые могут осуществляться как путем непосредственного, так и опосредованного (удаленного) доступа. К числу таких способов относятся:

1. Тайное введение в чужую программу таких команд, которые помогают ей осуществить новые, незапланированные разработчиком функции при одновременном сохранении прежней ее работоспособности. Данный способ может иметь две разновидности. В первом случае программные модули-фрагменты, которые создают так называемого троянского коня, то есть не запланированного разработчиком программного блока, самоликвидируются по окончании исполнения своей задачи. Найти после этого данные программные модули практически невозможно. Во втором случае в алгоритм программы, наряду с ее основными функциями, закладывается алгоритм действий, осуществляющих саморазмножение, автоматическое самовоспроизводство указанного «троянского коня». В результате подобные «программы-черви» автоматически копируют себя в памяти одного или нескольких компьютеров (при наличии компьютерной сети). Из зарубежной следственной практики интересен факт использования «троянского коня» одним американским программистом. Он вставил в программное обеспечение персонального компьютера по месту своей работы команды, которые позволяли не отражать в итоговом отчете определенные поступления денежных средств. Эти суммы особым образом шифровались и циркулировали только в информационной среде компьютера. Похитив бланки выдачи денег, преступник заполнял их с указанием своего шифра, а затем проставлял в них определенные суммы денег. Поскольку соответствующие операции по их выдаче также не отражались в отчетности, то они не могли быть подвергнуты документальной ревизии.

Модификация программ путем тайного встраивания в программу набора команд, которые должны сработать при определенных условиях через определенное время. Например, как только программа незаконно перечислит денежные средства на так называемый подставной счет, она самоуничтожится и при этом уничтожит всю информацию о проделанной операции.

Осуществление доступа к базам данных и файлам законного пользователя путем нахождения слабых мест в системах защиты. При их обнаружении появляется возможность читать и анализировать содержащуюся в системе информацию, копировать ее, возвращаться к ней по мере необходимости. Таким образом, можно обращаться к базам данных конкурирующей фирмы с тем, чтобы не только иметь возможность анализировать ее финансовое положение, но и получать упреждающую информацию о перспективах ее развития. Получение такой информации дает несомненное преимущество в конкурентной борьбе.

Использование ошибок в логике построения программы и обнаружение «брешей». При этом программа «разрывается» и в нее вводится необходимое число определенных команд, которые помогают ей осуществлять новые, незапланированные функции при одновременном сохранении прежней ее работоспособности. Именно таким образом можно переводить деньги на подставные счета, получать информацию о недвижимости, о персональных данных личности и пр.

Если первая и вторая группа способов более характерна исключительно для неправомерного доступа к компьютерной информации, то третья группа способов может быть характерна и для создания, использования и распространения вредоносных программ для ЭВМ.

Преступники могут получить пароли, коды и идентифицирующие шифры законных пользователей (путем получения списка пользователей со всей необходимой информацией, обнаружение документа в организациях, где не налажен контроль за их хранением, прослушивание телефонных переговоров) и проникнуть в компьютерную систему, выдавая себя за законного пользователя. Особенно уязвимы в этом отношении системы, которые не обладают средствами аутентичной идентификации (например, по физиологическим характеристикам: по отпечаткам пальцев, по рисунку сетчатки глаза, голосу и т.п.).

Также следует отметить, что неправомерный доступ к компьютерной информации может быть связан и с насилием над личностью либо угрозой его применения в целях получения преступниками сведений о способах преодоления средств защиты компьютерной информации и иных данных.