Миру угрожают электронные гангстеры

Правоохранительные органы стран "большой восьмерки" утвердили план совместной борьбы с киберпреступностью. Документ предусматривает безоговорочную выдачу компьютерных взломщиков в руки правосудия тех стран, на территории которых было совершено преступление. И вскоре США был передан гражданин России Владимир Левин, арестованный еще в 1995 году и находившийся в лондонской тюрьме. Ему было предъявлено обвинение в… похищении 10 млн.долл. со счетов клиентов одного из самых надежных банков Северной Америки — Сити-банка. Сидя в своей квартире в Питере, компьютерный "медвежатник" внедрялся в сеть банка, снимал со счетов клиентов деньги и направлял их "тихой скоростью" в разные города и страны. А затем через подставных лиц пытался собрать дань. Случай был воспринят как сенсация. А между тем, Владимир Левин — вовсе не первый электронный гангстер. Киберпреступность заявила о себе еще 30 лет назад и с тех пор приобрела такие масштабы, что, по мнению ученых, сравнялась с ядерной, химической и бактериологической опасностью. И это совсем не преувеличение…

…Не спасли банк ни бронированные двери, ни специальные запоры, ни вооруженная охрана. В денежное хранилище никто не входил. На сейфовых замках не осталось ни царапины, ни отпечатка пальца. Однако 123 тыс. долл. исчезли бесследно. Это таинственное похищение произошло в одном из столичных филиалов крупнейшего российского банка. Доллары испарились в буквальном смысле со скоростью света. Сыщикам стоило немалого труда обнаружить преступника (точнее, преступницу). Дело в том, что некто В. Виноградова совершила грабеж, не покидая своего служебного кабинета. Она проникла в денежное хранилище … по проводам, используя вместо традиционной для банковских грабителей отмычки клавиатуру компьютера. Несколько нажатий на клавиши, и электрические сигналы переместили немалое состояние со служебного счета Инкомбанка на частные счета друзей "взломщицы".

На этот раз злоумышленник был обнаружен. Но в целом криминальное использование современных информационных технологий делает компьютерную преступность не только весьма прибыльным, но и достаточно безопасным делом. И не зря подкомитет ООН по преступности ставит эту проблему в один ряд с терроризмом и наркобизнесом. В одном из банков Великобритании с помощью компьютера в одно мгновение был похищен миллиард долларов. Чем не преступление века? А всего (по самым скромным подсчетам) ежегодные потери от компьютерной преступности в Европе и Америке составляют десятки миллиардов долларов!

В 90% случаев сыщикам даже не удается выйти на след преступников. И это в Америке, где первое подобное правонарушение было зафиксировано еще в 1966 году и полиция уже накопила некоторый опыт в этой области. В России же подразделение по борьбе с хищениями, совершаемыми с использованием электронных средств, создано лишь в январе 1996 года. С тех пор возбуждено уже немало уголовных дел, но нет уверенности, что все они будут доведены до суда. Дела разваливаются, так как выявить личность преступника порой просто невозможно. Так, еще в 1993 году в компьютерную сеть Центробанка неизвестным лицом была введена команда о переводе более 68 млрд. руб. на другие счета. Преступники не найдены. В начале 1995 года злоумышленники через компьютерную сеть одного из московских банков фиктивно перевели на его счет 2 млрд.руб., попытавшись потом перевести эту сумму на другие счета. Преступление было предотвращено. Но уголовное дело приостановлено "за неустановлением виновных лиц"…

Прокомментировать ситуацию согласился программист одной из московских фирм, который, правда, попросил не называть его имени.

— Проблема даже не в том, что наши сыщики плохо работают или российские банки экономят на защите своих компьютерных сетей. Уверен, что при желании сумел бы безнаказанно проникнуть сквозь любую защиту. Не верите? Вспомните про американского школьника, который буквально поставил на уши ЦРУ, шутки ради проникнув в сверхсекретные файлы. А там защитные коды не чета нашим банковским. Не сложно написать и "мерцающую программу", которая через модемную связь произвольно включалась бы в счета разных предприятий, организуя денежные переводы за какие-либо "услуги", скажем, за маркетинг. Как поймать такого воришку, если сигналы легко перебрасываются через спутник и могут поступать в тот же Центробанк хоть из Зимбабве, хоть с Берега Слоновой Кости? А если компьютер-взломщик и найдется, то выяснится, что он работает в автономном режиме в каком-нибудь ничейном сарае… Деньги прокручиваются через несколько банков, и если их след все же обнаружится, конечный получатель только пожмет плечами: мол сам удивляюсь, откуда они, — и ничего с ним никто не сделает. Уверен, что при тотальной криминализации нашего общества компьютерная преступность не стала еще в России национальным бедствием лишь из-за не менее тотальной технической отсталости.

Компьютерная преступность — это не только хищения денег. Это и "шалости" с электронными вирусами, которые приводят порой к весьма плачевным последствиям. Америка уже накопила немалый печальный опыт в этой области. В 1988 году электронный вирус, неведомым образом попавший в компьютер Мичиганского госпиталя, перепутал в электронной памяти фамилии пациентов, их диагнозы и назначенное лечение, поставив под угрозу жизнь многих больных… В том же году молодой лоботряс Корнелл Морисс заразил вирусом крупнейшую компьютерную сеть Internet, что вывело из строя 6 тыс. компьютеров в 700 университетах, фирмах, федеральных агентствах. Ущерб составил 100 млн.долл. Исследовательскому центру НАСА пришлось на два дня закрыть свою сеть, чтобы восстановить нормальное обслуживание 52 тыс. пользователей. Сегодня, когда сеть Internet стала поистине всемирной, последствия подобной "шалости" трудно предугадать.

В России проблемой компьютерных вирусов занимается группа специалистов ФСБ, у которых нам, к сожалению, не удалось получить информацию о масштабах этого явления в нашей стране. Но программисты утверждают, что сейчас по компьютерам кочует около 5 тыс. разных вирусов и каждую неделю появляются пять новых. По их мнению, большая часть этой "инфекции" создается в границах бывшего СССР. Оценить степень ее опасности можно на примере уголовного дела, возбужденного прокуратурой Литвы в 1992 году. Тогда "электронная зараза" попала в компьютер Игналинской атомной электростанции, что привело к выводу из строя ее защитной системы. Еще чуть-чуть, и был бы второй Чернобыль…

Компьютеризация России — естественный, неизбежный и очень важный для страны процесс. Но надо помнить, что принесет он, к сожалению, не только благо. Уже сегодня киберманьяку вполне по силам оставить часть страны без света и телефонной связи или парализовать работу аэропортов и железных дорог. Самое неприятное, что весьма непросто отличить мелкое компьютерное хулиганство от серьезных попыток преднамеренного взлома сетей стратегических объектов. Поэтому вполне понятно, что с ростом зависимости страны от компьютеров компьютерные сети необходимо включить в число объектов стратегического назначения со всеми вытекающими отсюда последствиями. Если этого не сделать, в недалеком будущем с помощью телекоммуникационных средств злоумышленники, не вставая с дивана, смогут легко совершать террористические акты и даже небольшие государственные перевороты "в отдельно взятой стране". И все это легким нажатием кнопки "мыши"…

И. Царев