тно-структурный анализ организованой преступности в сфере частиых инвестиций (кол. авторов). М.;, 1997. 4. Волобуєв А.Ф., Золотухін І.І., Літвінов О.В. Характеристика розкрадань майна, що вчиняються в небанківських фінансових установах // Вісник Луганського інституту внутрішніх справ МВС України. 1998. 5. Трасти: за ошуканство доведеться відповідати // Урядовий кур'єр. 1997. 6 червня. 6. За матеріалами слідчого управління УМВС України в Дніпропетровській області за 1999 р. 7. За матеріалами УМВС України в Сумській області за 2000 р. 8. За матеріалами Слідчого управління ХГУ УМВС України в Харківській області за 1999 р. 9. За матеріалами УБОЗ УМВС України в м. Києві за 1999 р. 10. За матеріалами УБОЗ УМВС України в Закарпатській області за 1999 р. 11. Факты. 2000. 11 февраля. 12. За матеріалами УМВС України в Луганській області за 2000 р. 13. Факты . 24 ноября. 1999. 24 ноября

Надійшла до редколегії 10.06.2000

А.В. Тимченко, канд. психол. наук, доцент Ун-та внутр. дел,
В.Е. Христенко, канд. психол. наук, доц. Ун-та внутр. дел

ИНФОРМАЦИОННЫЙ ТЕРРОРИЗМ КАК ФОРМА ТРАНСНАЦИОНАЛЬНОЙ ПРЕСТУПНОСТИ

В последние годы мы наблюдаем не только за экономическим и территориальным переделом в области сфер влияния организованных преступных групп. Главная ставка в этой борьбе все чаще делается на лингвистику и психологию, разработку теорий воздействия средств массовой информации на аудиторию, восприятия журналистской информации и основы ее моделирования, психологии массовой коммуникации. При определенных допущениях, многие из них экстраполируются на пользователей киберпространства.

На сегодняшний день США обладают 42% мировых компьютерных ресурсов и 60% ресурсов Интернет, в то время как Китай – 1%, а Россия. Украина и Белоруссия вместе взятые – менее 1%. Современная всемирная экономика во многом базируется на информации и наукоемких технологиях. Перекрой доступ к этим знаниям – и страны обречены на прозябание почище последствий бомбардировок. Чем больше государств преодолевают индустриальный барьер развития, тем значимее становятся контроль за глобальными коммуникациями и угроза экономической разновидности информационных войн.

Аналитики предсказывают бум торговли по глобальной сети Интернет. То есть еще больше возрастет влияние информационных технологий на экономику. Цивилизованные страны начнут отказываться от бумажной валюты в пользу цифровой. Для государств могут возникнуть дополнительные трудности в области, которую государства контролируют – налогообложение.

Наиболее наглядно выглядит война хакеров и угроза информационного терроризма уничтожить чьи-либо наборы данных или обнародовать украденную сугубо личную информацию.

Результаты последнего исследования, проведенного Институтом компьютерной безопасности (ИКБ) Сан-Франциско, свидетельствуют, что

большинство американских организаций не готовы противодействовать компьютерной преступности. В ходе опроса 428 организаций (включая корпорации, финансовые учреждения, государственные органы и учебные заведения) подтвердили, что их информационные системы находятся в осадном положении. Выяснилось, что в 1999 году 41% организаций из числа опрошенных испытали вторжение в той или иной форме или иное несанкционированное использование своих компьютерных систем. Более половины вторжений или попыток проникновения в системы приписываются сотрудникам организаций, причем большинство атак на компьютерные системы происходило преимущественно из отдаленных источников по телефонным линиям или в результате подключений к Интернет. Двадцать две организации заявили, что подверглись 10 и более «нападениям» на свои системы на протяжении прошлого года. Основными лазутчиками единодушно названы независимые хакеры и обиженные сотрудники: помимо «подслушивания и подсматривания», они устраивают мистификации, то есть фальсифицируют обратный адрес, чтобы получить доступ к той или иной компьютерной системе.

Нельзя сбрасывать со счетов и конкурирующие фирмы и организации – они тоже способны на компьютерные диверсии. Представители ИКБ и ФБР заявили, что результаты этого исследования, впервые столь дотошного, помогут лучше разобраться в ситуации и эффективно противостоять компьютерной преступности. Постоянные изменения в технологии и растущий спрос на компьютерную технику означают, что и преступность этого рода будет расти до тех пор, пока предприятия в срочном порядке не пересмотрят подход к проблемам безопасности и не усовершенствуют меры защиты. Компьютерная преступность – противоправная деятельность образованных людей и, следовательно, наиболее опасна для общества.

Финансовые учреждения лондонского Сити уже выплатили астрономические суммы международным бандам изощренных «кибертеррористов», которые собрали по всему миру около 400 миллионов фунтов, и угрожали вывести из строя компьютерные системы. Американские банки, брокерские конторы и инвестиционные фирмы также тайно выплачивают дань, чтобы избежать дорогостоящих компьютерных разрушений и утраты доверия со стороны клиентов. В ходе конфиденциального расследования было установлено, что британские и американские органы в настоящее время изучают более 40 «наездов» на финансовые учреждения в Нью-Йорке, Лондоне и других европейских банковских центрах за последние два года. Жертвам приходилось выплачивать вплоть до 13 миллионов фунтов единовременно, когда шантажисты демонстрировали свои способности немедленно остановить все сделки, пользуясь современными методами ведения «информационных боевых действий».

По мнению Агентства национальной безопасности США, гангстеры проникают в компьютерные системы, применяя «логические бомбы», вирусы, «троянских коней», электромагнитные импульсы и «радиочастотные пушки высокой мощности», которые учиняют опустошительную электронную «бурю» в компьютерной системе. После этих безобразий преступники

оставляют зашифрованные угрозы для руководства банков: «Теперь вы верите в то, что мы можем уничтожить ваши компьютеры?». Так демонстрируется внедрение в святая святых коммерческого банка, в самое сердце системы безопасности – парольно – ключевую систему. Очень неприятно, наверное, получить от шантажиста подтверждение самых худших предположений о слабости защиты своего банка.

В Америке ФБР образовало три самостоятельных подразделения для расследования случаев компьютерного вымогательства. Агентство национальной безопасности считает, что в мире существует четыре основных группы кибергангстеров, и что как минимум одна из них обосновалась в России. В настоящее время Агентство до сих пор расследует четыре эпизода вымогательства, имевших место в Лондоне:

– 6 января 1993 года деятельность одной из брокерских контор была полностью парализована после угрозы вымогателей и созданной ими аварийной ситуации в компьютерной системе. Выкуп в размере 10 млн фунтов был переведен на счет в Цюрихе;

– 14 января 1993 года один из первоклассных банков выплатил вымогателям 12,5 миллионов фунтов;

– 29 января 1993 года одной из брокерских контор пришлось заплатить 10 миллионов фунтов отступного после аналогичных угроз;

– 17 марта 1995 года одна оборонная фирма была вынуждена откупиться 10 миллионами фунтов стерлингов.

Во всех четырех случаях гангстеры угрожали высшим руководителям и демонстрировали имеющиеся у них возможности разрушить компьютерную систему. Все жертвы уступали требованиям вымогателей через несколько часов и переводили деньги на счета банков, располагающихся в офшорных зонах, откуда гангстеры снимали их в считанные минуты. Методы варьировались. В Лондоне, действуя под видом маркетинговых фирм, преступники тщательно изучали систему, выбранную объектом шантажа, опрашивая руководителей отделов информационных технологий. В некоторых случаях ничего не подозревающим руководителям даже вручали анкеты. Вооруженные полученной информацией, преступники могли взламывать системы безопасности и оставлять зашифрованные записки с обещаниями больших неприятностей.

Факты компьютерных преступлений не ограничиваются рамками хищений крупных денежных средств. Куда более опасны случаи шантажа кибертеррористов, взламывающих секретные коды компьютерных сетей ядерных и военных объектов. Так:

– Правительственная проверка компьютеров, установленных в Госдепартаменте США и Федеральной авиационной администрации, дала неутешительные результаты. Практически к любому из компьютеров этих ведомств, управляющим воздушным движением, можно получить доступ из Интернета через модем и скопировать любые данные или прервать их нормальную работу.

– Агентство MSNBC сообщило, что к нам попал внутренний отчет Министерства энергетики США, в котором говорится, что тысячи сетей

этой организации, хранящих секретную информацию, в частности результаты ядерных исследований, практически не защищены от доступа к ним из Интернета.

– Группа хакеров Milw0rm, в которую входят подростки от 15 до 18 лет, утверждает, что проникла в секретную сеть ядерного исследовательского центра Индии и скопировала оттуда 5 Мб информации — документацию, служебную переписку и т. д. Она также пробралась в государственные компьютерные сети Пакистана. Эта группа известна неоднократным взломом государственных и военных сетей США и Англии.

– В США практически закончена разработка системы создания так называемых профилей различных военных и политических деятелей для выявления скрытых тенденций и закономерностей в их поведении, для анализа реакции руководителей министерств обороны разных стран на те или иные политические события и т. п. Эта система воплотит в себе достижения теории когнитивной психологии. Она будет автоматически анализировать массивы текстов выступлений, цифровых фотографий, видео клипов, звуковых записей, трехмерных изображений известных личностей. Закономерности поведения, не улавливаемые профессиональными психоаналитиками, будут обнаруживаться с помощью компьютеров.

Все эти факты свидетельствуют о том, что современные технологии все чаще используются транснациональными преступными группами, раскрывая новые возможности хищений, шпионажа или подрывной деятельности без риска оказаться в руках правосудия.

Крайне тяжелое положение в информационной безопасностью в политических, финансовых и силовых структурах практически всех стран мира приводит к неспособности противостоять возможным атакам на информационные системы. Вот почему сегодня необходимо рассматривать сотрудничество государств и их правоохранительных органов в деле информационной безопасности.

Надійшла до редколегії 17.04.2000

Н.М. Дяпленко, наук. співроб. Дніпропетровського юрид. ін-ту МВС України

ГОСПОДАРСЬКО-ПРАВОВІ ЗАХОДИ ПОПЕРЕДЖЕННЯ ТРАНСНАЦІОНАЛЬНОЇ ЗЛОЧИННОСТІ ЩОДО УХИЛЕНЬ ВІД СПЛАТИ ПОДАТКІВ

Транснаціональна злочинність у сфері економіки має складний комплексний характер. Такого роду злочини, з точки зору правоохоронних органів, належать до найбільш важких щодо їх розкриття. По-перше, через те, що злочинці розробляють схеми, які охоплюють декілька сфер діяльності, і обов'язково банківсько-фінансову та зовнішньоекономічну. По-друге, «інфраструктура» транснаціональної злочинності у сфері економіки досить розгалужена: іноземні фірми, представництва іноземних фірм, суб'єкти господарювання різних форм власності в Україні, фінансово-кредитні установи тощо. По-третє, виникають певні ускладнення під час проведення зустрічних перевірок при розкритті транснаціональних злочинів.