«Україні загрожує... кібертероризм»

Комп'ютерна епоха призвела до появи дуже небезпечного й маловивченого явища – кіберзлочинності. Про новий вид загрози для людства розповідає полковник міліції у відставці, директор Центру дослідження комп'ютерної злочинності, доцент кафедри кримінального права і правосуддя Запорізького національного університету Володимир ГОЛУБЄВ:

– Найпоширенішими злочинами в комп'ютерній сфері насамперед є інтернет-шахрайства, пов`язані з так званими лотереями. Організатор цієї акції засипає поштові скриньки користувачів захопленими повідомленнями про лотерейні виграші, в яких вони ніколи не брали участі. Найпопулярніші «розіграші» ноутбуків і путівок. Усе, що потрібно для цього зробити, – відвідати відповідний сайт і ввести номер свого рахунка та ПІН-код картки, яка нібито потрібна для оплати послуг доставки.

«Аукціони» – на цей вид шахрайства припадає майже 75% усіх скарг ошуканих споживачів, зареєстрованих у мережі *Internet Fraud Complaint Center (IFCC)*. Розплатившись за обіцяний товар, клієнт нічого не отримує, а шахрай відразу зникає. Такі «аукціони» розраховані на любителів «халяви»: для них створюють віртуальні інтернет-магазини, в яких постійно відбувається «розпродаж». Скажімо, телевізор із плазмовим екраном за $300 або *MP*3-плеєр за $30. Розплачуватися треба не готівкою, а лише за пластиковою карткою. Довірливі люди віддають свої кошти і... марно чекають на свою покупку.

Фішинг – від англійського слова *«fishing»* (риболовля). Це порівняно новий вид шахрайства, метою якого є виманювання в довірливих користувачів інтернету персональних даних клієнтів. Шахраї розсилають силу-силенну листів, замаскованих під офіційні бланки фінансових установ із посиланнями на сайти-пастки, що візуально копіюють сайти банків, казино й крамниць. Зловмисники використовують схожі домени та web-дизайни. Головна мета – виманювати в людей їхні кредитні дані й паролі банківських рахунків. Щоб цього не сталося, треба пам'ятати про безкоштовний сир у мишоловці, користуватися антивірусними програмами та не відвідувати підозрілих сайтів із «халявами».

– Володимире Олександровичу, чи можливо розв'язати ці проблеми на законодавчому рівні?

– Не тільки можливо, а й необхідно. Нещодавно уряд розробив законопроект № 9575 «Про кіберзлочинність». Ідеться про вдосконалення норм кримінального права, що стосуються злочинів, пов'язаних із комп'ютерними системами. На думку авторів, Кримінальний кодекс України потрібно доповнити, зокрема, статтею 362-3 (відповідальність за спам-розсилання). Таке покарання вже на часі. Про що може сказати навіть звичайний користувач електронної пошти, котрий щодня одержує кілобайти спаму.

– Змалюйте, будь ласка, портрет сучасного інтернет-шахрая.

– Це, як правило, творча особистість, здатна йти на технічні ризики. Дослідження в нашому центрі свідчать, що вік 33% зловмисників не перевищує 20 років, 54% – від 20 до 40 років, 13% – старші за 40 років. Отже, ми спростували стереотип про те, що хакери – підлітки від 12 років. Правопорушення у сфері використання комп'ютерних технологій здійснюються чоловіками вп'ятеро частіше, ніж жінками. Більшість зловмисників мають вищу або незакінчену вищу, а також спеціальну освіту.

Найчисленнішими є хакери-аматори. На їхню частку припадає до 80% усіх комп'ютерних атак. Цю категорію цікавить не якась мета, а лише сам процес атаки. Вони відчувають задоволення від подолання систем захисту. Їхні дії вдається легко припинити, бо хакери-аматори воліють не ризикувати й не вступати в конфлікт із законом.

Найнебезпечнішу групу становлять професійні кіберзлочинці з яскраво вираженою корисливою метою. Наприклад, розкрадання грошових коштів із банківських рахунків. Це висококваліфіковані фахівці. Вони не тільки чудово знають тонкощі інтернет-технологій, а й декілька мов програмування. Зламавши систему захисту, не залишають слідів.

– Ваш центр кіберзлочинці часом не бояться чіпати?

– Раніше вони організовували *DDOS*-атаки на один із наших ресурсів, вимагаючи зняти статтю про кардера – злочинця, який викрадав номери банківських кредитних карток, щоб заволодіти чужими коштами. Проте цю загрозу системний адміністратор протягом доби мінімізував. І, звісно, статтю ми не зняли. Були й інші спроби *DDOS*-атак, але не такі чутливі, як вищезгадана.

– Як вважаєте, слід обмежитися лише боротьбою з кіберзлочинністю чи все-таки зробити акцент на протидії новому явищу – кібертероризму?

– Тут потрібно не обмежуватися чи розмежуватися, а показувати від-

Досьє

Володимир ГОЛУБЄВ – кандидат юридичних наук. 1999 року захистив кандидатську дисертацію «Правові та організаційні аспекти захисту інформації в банківських автоматизованих системах» (спеціальність – інформаційна безпека держави). У 2000–2001 роках працював за програмою американо-українського наукового співробітництва між Академією правових наук України та Національним інститутом юстиції США. Наукові дослідження присвячені запобіганню та розслідуванню транснаціональних комп'ютерних злочинів. Доцент кафедри кримінального права і правосуддя Запорізького національного університету. Засновник і директор Центру дослідження комп'ютерної злочинності. Незалежний експерт і член Міжнародної наукової ради програми ООН «Запобігання злочинності та кримінального правосуддя» *(ISPAC)*. Керівник департаменту аналізу інформації та стратегічних оцінок Міжнародного антикримінального і антитерористичного комітету (МААК). Автор і співавтор майже 170 наукових праць і монографій. Керівник науково-дослідної роботи «Розробка концепції організації і тактики діяльності органів внутрішніх справ України із запобігання транснаціональним комп'ютерним злочинам». Фахівець у галузі запобігання та розслідування комп'ютерних злочинів.

мінність цих явищ як на законодавчому рівні, так і на рівні технічного захисту. Нагадаю, кіберзлочинці використовують інформаційні технології для злочинного посягання на комп`ютерні системи. А кібертероризм – це вид терористичної діяльності, який полягає в навмисній комплексній атаці на комп`ютерну інформацію, включаючи захоплення, виведення з ладу й руйнування об'єктів, що створює загрозу виникнення надзвичайної ситуації в телекомунікаційних мережах, заподіяння значної майнової шкоди чи настання інших суспільно небезпечних наслідків. Таке вчиняють із метою порушення громадської безпеки, залякування населення, провокацій військового конфлікту, ускладнення міжнародних відносин, здійснення впливу на органи влади або привернення уваги громадськості до певних політичних, релігійних чи інших організацій. Характерною відмінністю кібертероризму від кіберзлочинності є його відкритість, коли вимоги терориста широко сповіщаються.

– Наскільки кібертерор небезпечний?

– На відміну від звичайного терориста, озброєного вибухівкою чи «стволом», кібертерорист використовує сучасні інформаційні технології, комп'ютерні системи, спеціальне програмне забезпечення (для несанкціонованого проникнення в чужу мережу з метою організації віддаленої атаки на інформаційні ресурси жертви). Аналіз світових тенденцій свідчить, що Україні загрожує... кібертероризм. Це явище треба не просто вивчати. Нам потрібно бути готовими до протидії та мінімізації збитків з погляду національної безпеки.

– Невже наші правоохоронні органи не здатні приборкати такого спрута?

– У МВС і СБУ для цього є спеціальні підрозділи. Те, як ефективно вони працюють (це і перевірка комп`ютерних клубів, і пошук украдених мобільних телефонів, і припинення транснаціональних комп`ютерних інцидентів, і виконання інших завдань), – питання досить актуальне. Погодьтеся, заходи контролю в інтернет-середовищі можуть використовуватися по-різному: з одного боку, для припинення протиправної діяльності, з другого – для обмеження доступу до певних ресурсів, що визнані, наприклад, шкідливими. А це вже на межі порушення законних прав громадян на вільний доступ до інформації.

– За якою статтею КК України «комп`ютерні» справи порушуються найчастіше?

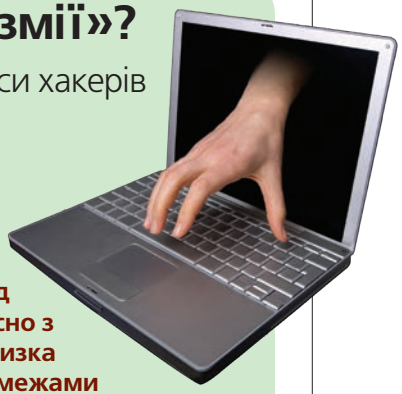
– За статтею 361: несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. За такі злочини передбачено штрафи від 600 до 1000 неоподатковуваних мінімумів доходів громадян, а також позбавлення волі на строк від трьох до шести років.

Розмову вів
Валентин КОВАЛЬСЬКИЙ.

Куди летять «повітряні змії»?

Молодь потребує захисту від спокуси хакерів

Валентин КОВАЛЬСЬКИЙ



Використання новітніх інформаційних технологій створює можливості доступу до різноманітних баз даних, установлення телекомунікаційного зв'язку незалежно від годин доби і державних кордонів. Одночасно з перевагами комп'ютеризації постає ціла низка проблем, розв'язання яких ще й досі поза межами українських законів.

Особливістю комп'ютерної сфери є те, що безпомилкових програм у ній не буває. Якщо в іншій галузі будь-який проект можна виконати з великим запасом надійності, то в інформаційних технологіях і програмах така надійність дуже умовна, а в багатьох випадках майже недосяжна. Це, у свою чергу, призвело до появи нового виду правопорушень – комп'ютерної злочинності. Йдеться про феномен, породжений можливостями майже безкарного вчинення протиправних дій у сфері, наглухо закритій для необізнаних людей.

Сам термін «комп'ютерна злочинність» з'явився в зарубіжній пресі ще півсотні років тому, коли виявили перші порушення з використанням електронно-обчислювальних машин (ЕОМ). Сьогодні це явище посилюється не тільки в локальному (національному), а й навіть у планетарному масштабі. На думку вітчизняних кримінологів, ЕОМ – багатообіцяльне знаряддя для вчинених антизаконних дій насамперед у банківській сфері. Економічні збитки від таких злочинів уже зрівнялися з перевагами, отриманими від утілення досягнень ЕОМ у життя. А соціальні й моральні втрати взагалі не піддаються оцінці.

Прикрі факти промовляють самі за себе. Наприклад, у такій інформаційно розвиненій країні, як США, щорічні матеріальні збитки від комп'ютерної злочинності вже давно перевищують десятки мільярдів(!) доларів. Звісно, в Україні цифри набагато менші. Але в нас цей вид злочинності має досить високу латентність: правоохоронцям відомо лише 10–15 відсотків схожих випадків, оскільки потерпілі неохоче надають інформацію (це може зашкодити їхній репутації або спричинити повторні злочини).

Зрозуміло, що загроза інформаційному ресурсу держави – загроза національній безпеці. На жаль, законодавчі норми й положення в цій сфері ще й досі чітко не визначені. Причина загальновідома: розвиток науково-технічного прогресу створює благодатне підґрунтя для крадіжки грошей з електронних систем взаєморозрахунків, несанкціонованого використання ЕОМ (для отримання власності або послуг), пошкодження або знищення комп'ютерних мереж і програм, проникнення до чужих баз даних, незаконного копіювання чи фальсифікації даних, шантажу, інформблокади, шпіонажу тощо.

Один із найпоширеніших комп'ютерних злочинів – так званий повітряний змій. Для цього потрібно лише відкрити у двох банках по невеличкому рахунку. Далі гроші переводяться із одного банку до другого і навпаки (з сумами, що поступово збільшуються). Хитрість полягає ось у чому: ще перед тим, як банкіри з`ясують, що перерахунки не забезпечені необхідною сумою, до них надходить повідомлення про перекази (до того ж сума першого переказу менша за наступну). Цей цикл повторюється багато разів. «Повітряний змій» піднімається вище й вище, доки на рахунку не з'явиться досить пристойна сума: фактично вона постійно «перескакує» з одного рахунка на інший, штучно збільшуючи свої віртуальні розміри. Потім гроші швидко знімають, а власник рахунка відразу зникає.

На практиці до такої гри залучають велику кількість банків. Тоді сума накопичується швидше і кількість доручень про переказ не досягає підозрілої частоти. Можна уявити такого собі комп'ютерного шпигуна, який залучається до банківської мережі, проводить розвідку, генерує всілякі запити, фіксує й аналізує отримані відповіді. Поставити перепону такому хакеру практично неможливо.

Боротися з цими злочинами покликані фахівці СБУ, МВС і Державної служби України з питань технічного захисту інформації. Свої дії вони завершують на стадії встановлення кримінальної відповідальності за конкретне порушення. Проте цього замало. На рівні держави необхідно, по-перше, якомога тісніше співпрацювати з міжнародними структурами й правоохоронцями інших країн. По-друге, не можна забувати про правове виховання молодого покоління, яке тільки починає опановувати комп'ютерні ази. Інакше наша молодь поповнюватиме лави хакерів та електронних піратів, які запускають віруси (наприклад, «троянського коня»), щоб перевести на свій рахунок певну суму з різних фінансових операцій.