Лекція 4.

Технології захисту інформації

План.
1. Проблеми захисту інформації у сучасних ІС.
2. Види комп'ютерних злочинів. Причини поширення комп'ютерної злочинності.
3. Поняття і класифікація комп'ютерних вірусів.
4. Засоби захисту інформації.

Література.

1. Виявлення та розслідування злочинів, що вичиняються у сфері інформаційних технологій: Наук.-практ.посіб./ За заг.ред.проф. Я.Ю.Кондратьєва. – К., 2004.
2. Ніколаюк С.І., Никифорчук Д.Й., Томма Р.П., Барко В.І. Протидія злочинам у сфері інтелектуальної власності. – К., 2006.
3. К. Мандиа, К. Просис. Защита от вторжений. Расследование компьютерных преступлений.– М., 2005.
4. Луцкер А. Авторское право в цифровых технологиях и СМИ. – М., 2005.

1.

Захист інформації є однією з вічних проблем. Протягом історії людства способи розв'язання цієї проблеми визначались рівнем розвитку технологій. У сучасному інформаційному суспільстві технологія відіграє роль активатора цієї проблеми — комп'ютерні злочини стали характерною ознакою сьогодення.

Комп'ютерними називають **злочини,** пов'язані з втручанням у роботу комп'ютера, і злочини, в яких комп'ютери використовуються як необхідні технічні засоби.

Серед ***причин комп'ютерних злочинів*** і пов'язаних з ними викрадень інформації головними є такі:

- швидкий перехід від традиційної паперової технології зберігання та передавання інформації до електронної за одночасного відставання технологій захисту інформації, зафіксованої на машинних носіях;
- широке використання локальних обчислювальних мереж, створення глобальних мереж і розширення доступу до інформаційних ресурсів;
- постійне ускладнення програмних засобів, що викликає зменшення їх надійності та збільшення кількості уразливих місць.

Сьогодні ніхто не може назвати точну цифру загальних збитків від комп'ютерних злочинів, але експерти погоджуються, що відповідні суми вимірюються мільярдами доларів. Серед основних статей варто виокремити такі:

- збитки, до яких призводить ситуація, коли співробітники організації не можуть виконувати свої обов'язки через непрацездатність системи (мережі);
- вартість викрадених і скомпрометованих даних;
- витрати на відновлення роботи системи, на перевірку її цілісності, на доробку уразливих місць тощо.

Варто також враховувати й морально-психологічні наслідки для користувачів, персоналу і власників ІС та інформації. Що ж до порушення безпеки так званих «критичних» додатків у державному і військовому управлінні, атомній енергетиці, медицині, ракетно-космічній галузі та у фінансовій сфері, то воно може призвести до тяжких наслідків для навколишнього середовища, економіки і безпеки держави, здоров'я і навіть для життя людей.

Економічні та юридичні питання, приватна та комерційна таємниця, національна безпека — усе це зумовлює необхідність захисту інформації та ІС.

Згідно із *Законом України «Про захист інформації в автоматизованих системах»* **захист інформації** — це сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи АС та осіб, які користуються інформацією.

У літературі вживаються також споріднені терміни «безпека інформації» та «безпека інформаційних технологій».

Забезпечення безпеки інформаційних технологій являє собою комплексну проблему, яка охоплює правове регулювання використання ІТ, удосконалення технологій їх розробки, розвиток системи сертифікації, забезпечення відповідних організаційно-технічних умов експлуатації. Розв'язання цієї проблеми потребує значних витрат, тому першочерговим завданням є співвіднесення рівня необхідної безпеки і витрат на її підтримку. Для цього необхідно визначити потенційні загрози, імовірність їх настання та можливі наслідки, вибрати адекватні засоби і побудувати надійну систему захисту.

Базовими **принципами інформаційної безпеки** є забезпечення цілісності інформації, її конфіденційності і водночас доступності для всіх авторизованих користувачів. Із цього погляду **основними випадками порушення безпеки інформації** можна назвати такі:

- несанкціонований доступ — доступ до інформації, що здійснюється з порушенням установлених в 1С правил розмежування доступу;
- витік інформації — результат дій порушника, унаслідок яких інформація стає відомою (доступною) суб'єктам, що не мають права доступу до неї;
- втрата інформації — дія, внаслідок якої інформація в 1С перестає існувати для фізичних або юридичних осіб, які мають право власності на неї в повному чи обмеженому обсязі;
- підробка інформації — навмисні дії, що призводять до перекручення інформації, яка має оброблятися або зберігатися в 1С;
- блокування інформації — дії, наслідком яких є припинення доступу до інформації;
- порушення роботи ІС — дії або обставини, які призводять до спотворення процесу обробки інформації.

Причини настання зазначених випадків такі:

- збої обладнання (збої кабельної системи, перебої в електроживленні, збої серверів, робочих станцій, мережних карт, дискових систем тощо);
- некоректна робота програмного забезпечення (втрата або змінювання даних у разі помилок у ПЗ, втрати даних унаслідок зараження системи комп'ютерними вірусами тощо);
- навмисні дії сторонніх осіб (несанкціоноване копіювання, знищення, підробка або блокування інформації, порушення роботи 1С, спричинення витоку інформації);
- помилки обслуговуючого персоналу та користувачів (випадкове знищення або змінювання даних; некоректне використання програмного та апаратного забезпечення, яке призводить до порушення нормальної роботи системи, виникнення вразливих місць, знищення або змінювання даних, порушення інтересів інших законних користувачів тощо; неефективно організована система захисту; втрата інформації через неправильне зберігання архівних даних тощо);
- навмисні дії обслуговуючого персоналу та користувачів (усе сказане у попередніх двох пунктах, а також ознайомлення сторонніх осіб із конфіденційною інформацією).

Зауважимо, що порушенням безпеки можна вважати і дії, які не призводять безпосередньо до втрати або відпливу інформації, але передбачають втручання в роботу системи.

Приклад

Порушення безпеки IT — несанкціоноване використання ресурсів

За результатами розслідування, яке тривало 6 місяців, Центральне розвідувальне управління США (http://www.cia.gov) звільнило 4 співробітників за створення і використання таємного чата безпосередньо в мережі розвідувального підрозділу. Звільнених було визначено як неблагонадійних, щоб їх не могли прийняти на роботу аналогічні організації. Один із них обіймав високу посаду в американській розвідці. Ще 96 осіб понесли різного роду стягнення.

Чат, який було створено в середині 1980-х років, відвідували близько 160 співробітників, щоб пофліртувати, пожартувати або просто побазікати в обхід систем безпеки. В офіційній заяві ЦРУ цей факт було названо «волаючим порушенням цілісності мережі». Цей скандал ще раз засвідчив не лише існування проблем щодо інформаційної безпеки у ЦРУ, а й серйозне ставлення до них. Можна згадати, що наприкінці 1996 року за зберігання секретних матеріалів на домашньому комп'ютері, підімкненому до Інтернет, було звільнено Джона Дейча, директора Управління.

Основні особливості комп'ютерних злочинів:

- встановлення факту вчинення злочину. На відміну від традиційних, правоохоронець не може виявити труп, відсутність матеріальних цінностей на складі, пошкоджений автомобіль. Всі сліди злочину знаходяться на матеріальних носіях комп'ютера, який може знаходиться на значній відстані від потерпілої особи;
- відсутність міждержавних кордонів для злочинців (якщо злочин вчиняється з використанням глобальної комп'ютерної мережі) та існування декількох місць вчинення злочину (при несанкціонованому доступі до банківських комп'ютерних систем місцем вчинення злочину слід вважати саму банківську систему, що була атакована, так і місце знаходження комп'ютера, з якого здійснювали доступ, а також місце надходження коштів для отримання готівки).

Загалом найбільшу загрозу безпеці інформації становлять люди, тому саме їхні навмисні чи випадкові дії потрібно передбачати, організовуючи систему захисту.

Співробітники служб комп'ютерної безпеки поділяють усіх порушників на чотири групи стосовно жертви: сторонні, які не знають фірму; сторонні, які знають фірму, та колишні співробітники; співробітники-непрограмісти; співробітники-програмісти.

Межа між програмістами та простими користувачами з погляду небезпечності останнім часом стирається. Останні становлять більшість співробітників, звичайно мають базову комп'ютерну підготовку і можуть скористатися спеціальним програмним забезпеченням, яке має дружній інтерфейс і доступне на піратських CD-ROM, у спеціальних розділах BBS і на сайтах Інтернет та FidoNet. За твердженнями експертів, тільки чверть співробітників цілком лояльна, чверть настроєна до фірми вороже і не має моральних обмежень, лояльність решти залежить від обставин. Тому нелояльні співробітники, які мають доступ до комп'ютерів і знайомі з системою, становлять серйозну загрозу ІС. Передусім це організаційна проблема, технологія тут може відігравати тільки допоміжну роль.

Для позначення різних категорій комп'ютерних злочинців використовуються різноманітні терміни: «хакери», «кракери», «пірати», «шкідники».

Хакери (хекери) — це узагальнююча назва людей, які зламують комп'ютерні системи. Часто цей термін застосовується і до «програмістів-маніяків» — за однією з легенд, слово «hack» уперше стало застосовуватись у Массачусетському технологічному інституті для позначення проекту, який не має видимого практичного значення і виконується виключно заради задоволення від самого процесу роботи. У більш вузькому

розумінні слово «хакер» позначає тих, хто одержує неправомочний доступ до ресурсів 1С тільки для самоствердження (див. приклад). Останнє відрізняє хакерів від професійних зламувачів — **кракерів** (або «крекерів», не плутати з печивом!), які є серйозними порушниками безпеки, оскільки не мають жодних моральних обмежень.

Найбільш криміногенною групою є **пірати** — професіонали найвищого ґатунку, які спеціалізуються на крадіжках текстів нових комерційних програмних продуктів, технологічних ноу-хау тощо. Така робота, природно, виконується на замовлення або передбачає реального покупця. За відсутності замовлень пірат може зосередитися на кредитних картках, банківських рахунках, телефонному зв'язку. В усіх випадках мотивація – матеріальні інтереси, а не цікавість чи пустощі.

За даними дослідження корпорації IDG у 88 % випадків розкрадання інформації відбувається через працівників фірм і тільки 12 % — через зовнішні проникнення із застосуванням спеціальних засобів.

ПРИКЛАД

Хакери: погоня за славою, розваги чи самореалізація?

У січні 2001 року на сайт! Xakep.ru з'явилось повідомлення про злом сайта ФБР (www.fbi.gov). За неперевіреними зі зрозумілих причин даними, хакери змінили структуру сайту і стерли директорію «wanted» (список найбільш небезпечних злочинців, яких розшукує ФБР), зробивши дублювальні копії файлів, про що й повідомили адміністратора сайту. Один з авторів зламу, московський програміст galblch, прокоментував свої дії так: «У принципі, злам був дрібницею — там була дірка. Першою ідеєю було просто написати адміну (адміністратору) про дірку без зламу як такого, але у зв'язку з іменитістю відомства, якому належить сайт, вирішили все ж таки розважитись». При цьому galblch вважає, що «писати програми більш цікаво, ніж шукати в них дірки, але й дірки цікаві...»

Шкідники (вандали) намагаються реалізувати у кіберпросторі свої патологічні схильності — вони заражають його вірусами, частково або повністю руйнують комп'ютерні системи. Найчастіше вони завдають шкоди без якої-небудь вигоди для себе (крім морального задоволення). Часто спонукальним мотивом є помста. Іноді шкідника надихає масштаб руйнівних наслідків, значно більший за можливі позитивні успіхи від аналогічних зусиль.

Слід також зупинитись ще на одній групі, яка посідає проміжне місце між хакерами і недосвідченими користувачами (до речі, ненавмисні дії останніх можуть призвести до не менш тяжких наслідків, ніж сплановані атаки професіоналів). Ідеться про **експериментаторів («піонерів»).** Найчастіше це молоді люди, які під час освоєння інструментальних та інформаційних ресурсів Мережі і власного комп'ютера бажають вчитися тільки на власних помилках, відштовхуючись від того, «як не можна». Основну частину цієї групи становлять діти та підлітки. Головною мотивацією у цій групі є гра. З експериментаторів виходять професіонали високого класу, зокрема й законослухняні.

Отже, **одними з основних причин порушення безпеки інформації** є незапитаність творчого потенціалу в поєднанні з неусвідомленням усіх наслідків протиправних дій. Цей фактор існує незалежно від національності або сфери професійної діяльності. Звичайно, жодна з особистих проблем не може стати приводом для протиправної діяльності, але сьогодні суспільство тільки починає виробляти належне ставлення до комп'ютерних злочинців. Стають відомими колосальні збитки від їхньої діяльності. Розвінчується міф про хакера як про комбінацію Гудіні і Фантомаса, адже часто своїми успіхами вони завдячують не своїм навичкам, а банальним пропускам у захисті систем (звідси і нове прізвисько— «ламери»). Поширюється думка про те, що комп'ютерний злочин легше попередити, ніж потім розслідувати. Однак це не вирішує проблему повністю, адже, крім бажання розважитись і самоствердитись існує ще

недбалість, холодний комерційний розрахунок, прояви садизму та хворобливої уяви. Тому комп'ютерні злочини залишаються об'єктом уваги фахівців.

Хакерство — загроза чи невинна гра?

Секретні служби США поінформували комітет з озброєнь сенату про загрозу безпеці США № 1. '(і становив хакер, який близько 200 разів зламав системи безпеки різного рівня і скопіював десятки секретних файлів, включаючи подробиці досліджень і розробок балістичних ракет. На те щоб його піймати, знадобилось 13 місяців. Хакером виявився англійський 16-річний хлопець, комп'ютерні навички котрого шкільний учитель оцінив у 4 бали. У ході судового засідання адвокат стверджував, що неповнолітній хакер не мав злого наміру і перебував під враженням від фільму «Ігри патріотів».

Такі ігри можуть загрожувати виникненням реального військового конфлікту. Комп'ютерна атака на Пентагон у 1998 році збіглась у часі з черговим загостренням американо-іракських відносин у районі Перської затоки. Американське командування вважало, що атаку заподіяв Ірак з метою завадити висадці американських військ. До спеціального розслідування під кодовою назвою «Solar Sunrise» (http://www.sans.org/newlook/resources/IDFAQ/solar_sunrise.htm) було залучено агентів ФБР, представників відділу спеціальних розслідувань Військово-повітряних сил США, Міністерства юстиції, ЦРУ, Агентства національної безпеки та деяких інших урядових структур США. А справжніми винуватцями виявились двоє американських підлітків, якими керував 21-річний ізраїльський хакер.

2.

Проблема комп’ютерної злочинності та розробка механізмів протидії привернула до себе увагу провідних криміналістів ще з часів широкого впровадження комп’ютерної техніки. Статистка таких злочинів велася з 1958 р. Тоді їх розуміли як випадки псування і розкрадання комп’ютерного устакування; крадіжку інформації; несанкціоноване використання комп’ютерів; шахрайство або крадіжку, вчинене за допомогою комп’ютерів. У 1996 р. комп’ютер уперше був використаний як інструмент для пограбування банку (Мінесота).

Нині високотехнологічна злочинність набуває високих темпів. Загалом об'єктами зазіхань можуть бути як технічні засоби (комп'ютери і периферія), так і програмне забезпечення та бази даних, для яких комп'ютер є середовищем. У першому випадку правопорушення можна кваліфікувати за звичайними нормами права (крадіжка, грабіж, розбій і т. ін.). В інших випадках, коли комп'ютер виступає і як інструмент, і як об'єкт, злочин відносять до окремої категорії (див. розділ XVI Кримінального кодексу України).

Найбільш поширені види комп'ютерних злочинів:

1. ***Несанкціонований доступ до інформації, що зберігається у комп'ютері, та її розкрадання***. Розрізнити ці дві категорії дуже важко. Найчастіше присвоєння машинної інформації та програмного забезпечення відбувається копіюванням, що зменшує ймовірність виявлення факту крадіжки. Можливі шляхи здійснення злочину:

* використання чужого імені або пароля («маскарад»). Одержати коди та паролі законних користувачів можна придбанням (звичайно з підкупом персоналу) списку користувачів з необхідними відомостями, знаходженням подібного документа в організаціях, де контроль за їх збереженням недостатній; підслуховуванням через телефонні лінії. Відомі випадки, коли секретна інформація, і не тільки приватного характеру, відпливала через дітей;
* незаконне використання привілейованого доступу;
* «зламування» системи;
* знаходження слабких місць у захисті системи чи недоробок у програмному

забезпеченні;

* використання збоїв системи;
* крадіжка носіїв інформації;
* читання інформації з екрана монітора;
* збирання «сміття»;
* встановлення апаратури підслуховування та запису, підімкненої до каналів передавання даних;
* віддалене підімкнення;
* модифікація програмного забезпечення.

2. ***Підробка комп'ютерної інформації***. Цей злочин можна вважати різновидом несанкціонованого доступу з тією різницею, що скоїти його може і стороння особа, і законний користувач, і розробник 1С. В останньому випадку може підроблятись вихідна інформація з метою імітування роботоздатності 1С і здачі замовнику свідомо несправної продукції. До цього самого виду злочинів можна віднести підтасування результатів виборів, голосувань і т. ін.
3. ***Уведення у програмне забезпечення «логічних бомб»*** — невеликих програм, які спрацьовують з настанням певних умов і можуть призвести до часткового або повного виведення системи з ладу. Різновидом логічної бомби є «часова бомба», яка спрацьовує в певний момент часу. Ще одним способом модифікації програмного забезпечення є таємне введення у програму (чужу або свою) «троянського коня» — команд, які дають можливість зі збереженням працездатності програми виконати додаткові, не задокументовані функції, наприклад переслати інформацію (зокрема паролі), що зберігається на комп'ютері. В останньому випадку «троянській кінь» є засобом реалізації «прихованого каналу». Виявити «троянського коня» дуже важко, оскільки сучасні програми складаються з тисяч і навіть мільйонів команд і мають складну структуру. Завдання ускладнюється, коли у програму вставляється не власне «троянській кінь» (див. вище визначення), а команди, які його формують і після досягнення поставленої мети — знищують. Також можна зазначити, що «троянські коні» можуть перебувати не тільки у програмах, айв інших файлах, наприклад в електронних листах.

ПРИКЛАД

«Троянській кінь» — найкращий засіб попередження порушень авторського права?
Один із перших завантажувальних вірусів для IBM-PC (заражав дискети 360 Kb), який стрімко розповсюдився на Заході, був написаний у Пакистані власниками компанії з продажу програмних продуктів, які хотіли з 'ясувати рівень піратського копіювання у своїй країні. Автори залишили у тілі вірусу текстове повідомлення зі своїми іменами, адресами і навіть номерами телефонів. Незважаючи на появу інших різноманітних методів захисту авторських прав, за минулий час цей приклад неодноразово наслідувався.

4. ***Розробка і поширення комп'ютерних вірусів***. Напевне, сьогодні не має жодного користувача 1С, який у своїй роботі не стикався б із комп'ютерними вірусами. Прояви вірусів можуть бути різноманітними — від появи на екрані точки, що світиться (так званий «італійський стрибунець»), до стирання файлів з жорсткого диска. У будь-якому разі це означає порушення цілісності 1С. Сьогодні фахівці очікують появи вірусів для програмованих мікросхем і мобільних телефонів.
5. ***Злочинна недбалість у розробці, виготовленні й експлуатації комп'ютерної техніки та програмного забезпечення.*** Необережне використання комп'ютерної техніки аналогічне недбалому поводженню з будь-яким іншим видом техніки, транспорту і т. Його особливістю є те, що безпомилкових програм не буває в принципі. Якщо помилка призвела до наслідків, які вимагають покарання винуватців,

про винність розробників свідчать:

• наявність у технічному завданні вказівок на те, що в системі може виникнути ситуація, яка призводить до збою (аварії);

• можливість створення контрольного прикладу з даними, які імітують ситуацію, що призвела до збою (аварії).

Окремим випадком недбалості програмістів є створення і залишення без контролю «люків» («чорних ходів») — прихованих, не задокументованих точок входу у програмний модуль, які часто використовуються для відлагодження програми та її підтримання у процесі використання. Але «люк» може бути використаний і для зламування системи сторонньою особою, і для таємного доступу до програми самим розробником. Для виявлення «люків» слід проводити ретельний аналіз початкових текстів програм.

До тяжких непередбачуваних наслідків можуть призвести й дії користувачів. Визначити їх як халатні можна за таких ознак:

- користувач мав у своєму розпорядженні інформацію про можливі наслідки порушення інструкцій;
- виконати вимоги інструкції було можливо фізично і психологічно.

6. ***Комп'ютерні злочини в мережі Інтернет***. Виокремлення цієї категорії диктується реаліями використання глобальної мережі. По-перше, Інтернет стає інструментом здійснення «звичайних» злочинів. Це ***промисловий шпіонаж, саботаж, поширення дитячої порнографії*** і т. ін. Понад третина користувачів Мережі страждає від ***шахрайств***. Продавці еквадорської нерухомості, нафтових свердловин в Антарктиді і кокосових плантацій в Коста-Ріці, будівельники фінансово-інвестиційних пірамід і брокери, які просувають акції певних фірм і наживають на продажу цих акцій у період ажіотажу, — їхні сайти та розсилки наздоганяють сотні тисяч людей, серед яких не так вже й мало легковірних. Одним із ключових аспектів багатьох «схем» подібного роду є доступ до персональних даних користувача (див. приклад). Заповнивши анкету, людина стає потенційним об'єктом шахрайства в майбутньому, а найбільш довірливі, зокрема ті, хто надає інформацію про свою кредитну картку, страждають відразу. Відомо, що більшість шахрайств пов'язана з використанням пластикових кредитних карток і здійснюється на сайтах, що спеціалізуються на купівлі-продажу товарів.

По-друге, стає все більше злочинів, пов'язаних із самим існуванням Інтернет. Крім ***розповсюдження вірусів та зламування сайтів*** можна назвати такі:

* ***«нюкання»*** (від англійського «nuke», ядерна зброя) -— програмна атака на іншого користувача Інтернет, у результаті якої його комп'ютер втрачає зв'язок з мережею або «зависає»;

* ***«спам»*** (від англійського «spam»1) або «junk mail» (пошта з мотлохом, непотрібна кореспонденція) — варіант багаторівневого маркетингу в мережі. Спаммерів можна поділити на дві групи. Першу становлять новачки, які тільки-но одержали доступ до Мережі та усвідомили, що можуть розсилати повідомлення куди завгодно і кому завгодно. Другу групу утворюють професіонали, які заробляють гроші на заздалегідь неправдивій рекламі типу «Отримай премію...», «Розбагатій...», «Швидко зароби...» і т. ін. Про нечесність таких «бізнесменів» говорить хоча б їх небажання вказати свої справжні ім'я та координати;

* ***«винюхування» («sniffing»)*** — сканування пакетів, які передаються в мережі для одержання інформації про користувача (-ів);

* ***«серверний трикутник»*** **(**Web-spoofing, Web-мистифікація) — зловмисник, який проникає на сайт, змінює механізм пошуку так, що вся інформація, що її запитують користувачі, передається через якийсь інший сайт, де її, до того ж, можуть певним чином «обробити»;

*** мережні атаки**, спрямовані на «зависання» серверів («Denial of service attack», DOS-attack, атака, що спричинює відмову від обслуговування) або уповільнення їхньої роботи різними способами («повені»). Найчастіше для реалізації таких атак використо-

вуються пакети технологічної інформації та самі правила взаємодії серверів за мережними протоколами.

Фактично єдиний спосіб створити систему, абсолютно стійку до зовнішніх впливів, — припинити будь-які її зв'язки із зовнішнім світом. А мінімальним із погляду заходом є заборона доступу до Інтернет не для службових цілей.

Злочини, що вичиняються організованими злочинними угрупуваннями з використанням ІТ:

1) злочини насильницького характеру та інші злочини, які є потенційно небезпечними;

2) злочини ненасильницького характеру (як правило, економічного)ю

Злочини І категорії:

Кібертероризм – тероризм спланований, вчинений чи скоординований в кіберпросторі, тобто в терористичних акціях використовуються новітні досягнення науки і техніки в галузі ІТ.

Загроза фізичної розправи

Дитяча порнографія – за даними менеджера портала системи Яндекс , число запитів із словосполученням «детское порно» становить від 1,5 до 3 тис. в середньому в день, порносайти відвідує в середньому понад 32 млн.громадян. В Інтереті розповсюджується до 75% всієї дитячої порнопродукції. За даними Інтерполу, основними постачальниками таких матеріалів , поряд з Тайванем і В'єтнамом стали Росія і Україна.

Злочини ІІ категорії:

- **«відмивання» грошей**
- **крадіжка грошей з банківських рахунків**
- **шахрайські операції з пластиковими платіжними картками**
- **розповсюдження інформації про наркотики через Інтернет**

3. КОМП'ЮТЕРНІ ВІРУСИ ЯК ЗАГРОЗА ІНФОРМАЦІЙНИМ СИСТЕМАМ

Вважають, що перші прототипи «електронних інфекцій» з'явились наприкінці 1960-х — на початку 1970-х років у вигляді програм-«кроликів», які швидко розмножувались і займали системні ресурси, знижуючи таким чином, продуктивність комп'ютерів. «Кролики» не передавались між системами і були результатом пустощів системних програмістів. Термін «комп'ютерний вірус» уперше вжив американський студент Фред Коен у 1984 році. Він поділив віруси на дві великі групи. До першої він відніс ті, які написані для певних наукових досліджень у галузі інформатики, а до другої — «дикі» віруси, вироблені з метою заподіяння шкоди користувачам.

Сьогодні написання вірусів набуває ознак промислового виробництва, їх кількість вимірюється десятками тисяч, і розуміння цієї загрози має стати необхідною вимогою для кожного користувача.

Комп'ютерний вірус — спеціально написана невелика за розмірами програма, яка може створювати свої копії, впроваджуючи їх у файли, оперативну пам'ять, завантажувальні області і т. ін. (заражати їх), та виконувати різноманітні небажані дії.

Небезпечність вірусу зростає через наявність у нього латентного періоду, коли він не виявляє себе. Для маскування вірус може використовуватися разом з «логічною» або «часовою бомбою».

Кілька ознак зараження ІС вірусами:

- припинення роботи або неправильна робота програм, які раніше функціонували успішно;
- неможливість завантаження операційної системи;

- зменшення вільного обсягу пам'яті;
- уповільнення роботи комп'ютера;
- затримки під час виконання програм, збої в роботі комп’ютера;
- раптове збільшення кількості файлів на диску;
- зникнення файлів і каталогів або перекручування їхнього вмісту;
- незрозумілі зміни у файлах;
- зміни дати і часу модифікації файлів без очевидних причин;
- незрозумілі зміни розмірів файлів;
- видача непередбачених звукових сигналів;
- виведення на екран непередбачених повідомлень або зображень.

Віруси можна класифікувати за різними ознаками.

За середовищем існування розрізняють файлові, завантажувальні, комбіновані (файлово-завантажувальні), пакетні та мережні віруси.

Файлові віруси звичайно заражають файли з розширеннями .com та .exe. Однак, деякі їх різновиди можуть інфікувати файли й інших типів (.dll, .sys, .ovl, .prg, .bat, .mnu), при цьому вони, як правило, втрачають здатність до розмноження.

У свою чергу**, за способом зараження середовища** існування файлові віруси поділяють на резидентні та нерезидентні. Останні починають діяти тільки під час запуску зараженого файла на виконання і залишаються активними обмежений час. Резидентні віруси інсталюють свою копію в оперативній пам'яті, перехоплюють звертання операційної системи до різних об'єктів і заражають їх. Деякі віруси здатні перехоплювати досить багато різних функцій переривань, У результаті чого файли можуть заражатись у процесі перейменування, копіювання, знищення, змінювання атрибутів, перегляду каталогів, виконання, відкривання та здійснення інших операцій. Резидентні віруси зберігають активність весь час до вимикання комп' ютера.

. Порівняно новою групою можна назвати **макровіруси,** які використовують можливості макромов, вбудованих у текстові редактори, електронні таблиці і т. ін. Нині поширені макровіруси у Microsoft Word і Excel. Вони перехоплюють деякі файлові функції в разі відкриття чи закриття зараженого документа і згодом інфікують решту файлів, до яких звертається програма. У певному сенсі такі віруси можна назвати резидентними, оскільки вони активні тільки у своєму середовищі — відповідному додатку.

Окрему категорію файлових вірусів становлять віруси сім'ї DIR, які не впроваджуються у файли, а виконують реорганізацію файлової системи так, що під час запуску будь-якого файла управління передається вірусу.

Завантажувальні віруси відрізняються від файлових резидентних вірусів тим, що вони переносяться із системи в систему через завантажувальні сектори. Комп'ютер заражається таким вірусом після спроби завантаження системи з інфікованого диска, а дискета — при читанні її «змісту».

Комбіновані віруси можуть поширюватись як через завантажувальні сектори, так і через файли.

Пакетні віруси — це порівняно прості і старі віруси, написані мовою управління завданнями операційної системи.

Мережні віруси («черв'яки») розмножуються по комп'ютерній мережі, зменшуючи тим самим її пропускну здатність, уповільнюючи роботу серверів і т. ін. Вони посідають перше місце за швидкістю поширення. Найбільш відомим є так званий «черв'як Морріса». Останні моделі «черв'яків» упроваджуються у різні архіви (arj, zip та ін.) і зменшують вільний простір на диску.

За ступенем деструктивності віруси можна поділити на такі групи:

• порівняно безпечні, нешкідливі — їх вплив обмежується зменшенням вільної пам'яті і графічними або звуковими ефектами. Варто зазначити, що зменшення пам'яті в деяких випадках може призвести до збою системи, а ефекти — відволікти користувача, у

результаті чого він припуститься помилки;

• небезпечні — віруси, які можуть призводити до збійних ситуацій;

- дуже небезпечні — дії вірусів можуть призвести до втрати програм, знищення даних, стирання інформації в системних областях тощо.

За особливостями алгоритму віруси важко класифікувати через їх різноманітність. Можна виокремити найпростіші, **«вульгарні» віруси**, написані єдиним блоком, який можна розпізнати в тексті програми-носія, та віруси «роздроблені» — поділені на частини, що нібито не мають між собою зв'язку, але містять інструкції комп'ютерові, як їх зібрати в єдине ціле і розмножити вірус.

З погляду прийомів маскування розрізняють віруси-невидимки (стелс-віруси, stealth) та поліморфні віруси. Перші перехоплюють функції операційної системи, відповідальні за роботу з файлами, і коригують результати звернень. Механізм «невидимості» в кожному з цих вірусів реалізується по-своєму, однак можна виокремити кілька загальних принципів:

• для приховування збільшення довжини заражених файлів вірус передає програмі перегляду каталогів зменшене значення їхньої довжини;

• для того щоб користувач не виявив код вірусу під час перегляду файла, вірус виліковує його в момент відкриття і заново заражає у процесі закриття;

• для того щоб замаскувати свою присутність у пам'яті комп'ютера, вірус стежить за діями резидентних моніторів пам'яті, у разі спроби перегляду коду вірусу система зависає.

Поліморфними називають віруси, які застосовують різноманітні способи шифрування власного тіла. У разі зараження чергового файла алгоритм шифрування змінюється випадковим чином. При цьому дуже важко виділити **сигнатуру** — характерну послідовність байтів у коді вірусу.

4.

Класифікація засобів захисту інформації

Залежно від можливих порушень у роботі системи та загроз несанкціонованого доступу до інформації численні види захисту можна об'єднати у такі групи: морально-етичні, правові, адміністративні (організаційні), технічні (фізичні), програмні. Зазначимо, що такий поділ є досить умовним. Зокрема, сучасні технології розвиваються в напрямку сполучення програмних та апаратних засобів захисту.

Морально-етичні засоби. До цієї групи належать норми поведінки, які традиційно склались або складаються з поширенням ЕОМ, мереж і т. ін. Ці норми здебільшого не є обов'язковими і не затверджені в законодавчому порядку, але їх невиконання часто призводить до падіння авторитету та престижу людини, групи осіб, організації або країни. Морально-етичні норми бувають як неписаними, так і оформленими в деякий статут. Найбільш характерним прикладом є Кодекс професійної поведінки членів Асоціації користувачів ЕОМ США.

Правові засоби захисту — чинні закони, укази та інші нормативні акти, які регламентують правила користування інформацією і відповідальність за їх порушення, захищають авторські права програмістів та регулюють інші питання використання ІТ.

Перехід до інформаційного суспільства вимагає удосконалення карного і цивільного законодавства, а також судочинства. Сьогодні спеціальні закони ухвалено в усіх розвинених країнах світу та багатьох міжнародних об'єднаннях, і вони постійно доповнюються. Порівняти їх між собою практично неможливо, оскільки кожний закон потрібно розглядати у контексті всього законодавства. Наприклад, на положення про забезпечення секретності впливають закони про інформацію, процесуальне законодавство, кримінальні кодекси та адміністративні розпорядження. До проекту міжнародної угоди про боротьбу з кіберзлочинністю, розробленого комітетом з економічних злочинів Ради Європи (див. матеріали сайту http://www.coe.int), було внесено зміни, оскільки його

розцінили як такий, що суперечить положенням про права людини і надає урядам і поліцейським органам зайві повноваження.

Загальною тенденцією, що її можна простежити, є підвищення жорсткості кримінальних законів щодо комп'ютерних злочинців. Так, уже сьогодні у Гонконгу максимальним покаранням за такий злочин, якщо він призвів до виведення з ладу 1С або Web-сайту, є 10 років позбавлення волі. Для порівняння, у Кримінальному кодексі України незаконне втручання в роботу комп'ютерів та комп'ютерних мереж карається штрафом до сімдесяти неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або обмеженням волі на той самий строк.

Адміністративні (організаційні) засоби захисту інформації регламентують процеси функціонування 1С, використання її ресурсів, діяльність персоналу, а також порядок взаємодії користувачів із системою таким чином, щоб найбільшою мірою ускладнити або не допустити порушень безпеки. Вони охоплюють:

• заходи, які передбачаються під час проектування, будівництва та облаштування об'єктів охорони (врахування впливу стихії, протипожежна безпека, охорона приміщень, пропускний режим, прихований контроль за роботою працівників і т. ін.);

• заходи, що здійснюються під час проектування, розробки, ремонту й модифікації обладнання та програмного забезпечення (сертифікація всіх технічних і програмних засобів, які використовуються; суворе санкціонування, розгляд і затвердження всіх змін тощо);

* заходи, які здійснюються під час добору та підготовки персоналу (перевірка нових співробітників, ознайомлення їх із порядком роботи з конфіденційною інформацією і ступенем відповідальності за його недодержання; створення умов, за яких персоналу було б невигідно або неможливо припускатися зловживань і т. ін.);

• розробку правил обробки та зберігання інформації, а також стратегії її захисту (організація обліку, зберігання, використання і знищення документа і носіїв з конфіденційною інформацією; розмежування доступу до інформації за допомогою паролів, профілів повноважень і т. ін.; розробка адміністративних норм та системи покарань за їх порушення тощо).

Адміністративні засоби є неодмінною частиною захисту інформації, їх значення зумовлюється тим, що вони доступні і здатні доповнити законодавчі норми там, де це потрібно організації (див. приклад), а особливістю є те, що здебільшого вони передбачають застосування інших видів захисту (технічного, програмного) і тільки в такому разі забезпечують достатньо надійний захист. Водночас велика кількість адміністративних правил обтяжує працівників і насправді зменшує надійність захисту (інструкції просто не виконуються).

Засоби фізичного (технічного) захисту інформації — це різного роду механічні, електро- або електронно-механічні пристрої, а також спорудження і матеріали, призначені для захисту від несанкціонованого доступу і викрадень інформації та попередження її втрат у результаті порушення роботоздатності компонентів 1С, стихійних лих, саботажу, диверсій і т. ін. До цієї групи відносять:

* засоби захисту кабельної системи. За даними різних досліджень саме збої кабельної системи спричиняють більш як половину відказів ЛОМ. Найкращим способом попередити подібні збої є побудова структурованої кабельної системи (СКС), в якій використовуються однакові кабелі для організації передавання даних в 1С, сигналів від датчиків пожежної безпеки, відео-інформації від охоронної системи, а також локальної телефонної мережі. Поняття «структурованість» означає, що кабельну систему будинку можна поділити на кілька рівнів залежно від її призначення і розміщення. Для ефективної організації надійної СКС слід додержувати вимог міжнародних стандартів;

* засоби захисту системи електроживлення. Американські дослідники з компанії Best Power1 після п'яти років досліджень проблем електроживлення зробили висновок: на

кожному комп'ютері в середньому 289 раз на рік виникають порушення живлення, тобто частіш ніж один раз протягом кожного робочого дня. Найбільш надійним засобом попередження втрат інформації в разі тимчасових відімкнень електроенергії або стрибків напруги в електромережі є установка джерел безперебійного живлення. Різноманітність технічних і споживацьких характеристик дає можливість вибрати засіб, адекватний вимогам. За умов підвищених вимог до роботоздатності 1С можливе використання аварійного електрогенератора або резервних ліній електроживлення, підімкнених до різних підстанцій;

* засоби архівації та дублювання інформації. За значних обсягів інформації доцільно організовувати виділений спеціалізований сервер для архівації даних. Якщо архівна інформація має велику цінність, її варто зберігати у спеціальному приміщенні, що охороняється. На випадок пожежі або стихійного лиха варто зберігати дублікати найбільш цінних архівів в іншому будинку (можливо, в іншому районі або в іншому місті);

* засоби захисту від відпливу інформації по різних фізичних полях, що виникають під час роботи технічних засобів, — засоби виявлення прослуховувальної апаратури, електромагнітне екранування пристроїв або приміщень, активне радіотехнічне маскування з використанням широкосмугових генераторів шумів тощо.

До цієї самої групи можна віднести матеріали, які забезпечують безпеку зберігання і транспортування носіїв інформації та їх захист від копіювання. Переважно це спеціальні тонкоплівкові матеріали, які мають змінну кольорову гамму або голографічні мітки, що наносяться на документи і предмети (зокрема й на елементи комп'ютерної техніки) і дають змогу ідентифікувати дійсність об'єкта та проконтролювати доступ до нього.

Як було вже сказано, найчастіше технічні засоби захисту реалізуються в поєднанні з програмними.

Програмні засоби захисту забезпечують ідентифікацію та аутентифікацію користувачів (див. підрозд. 3.4.4), розмежування доступу до ресурсів згідно з повноваженнями користувачів, реєстрацію подій в 1С, криптографічний захист інформації, захист від комп'ютерних вірусів тощо (див. докладніше далі).

Розглядаючи програмні засоби захисту, доцільно спинитись на стеганографічних методах. Слово «стеганографія» означає приховане письмо, яке не дає можливості сторонній особі взнати про його існування. Одна з перших згадок про застосування таємнопису датується V століттям до н. е. Сучасним прикладом є випадок роздрукування на ЕОМ контрактів з малопомітними викривленнями обрисів окремих символів тексту — так вносилась шифрована інформація про умови складання контракту.

Комп'ютерна стеганографія базується на двох принципах. По-перше, аудіо- і відеофайли, а також файли з оцифрованими зображеннями можна деякою мірою змінити без втрати функціональності. По-друге, можливості людини розрізняти дрібні зміни кольору або звуку обмежені. Найчастіше стеганографія використовується для створення цифрових водяних знаків. На відміну від звичайних їх можна нанести і відшукати тільки за допомогою спеціального програмного забезпечення — цифрові водяні знаки записуються як псевдовипадкові послідовності шумових сигналів, згенерованих на основі секретних ключів. Такі знаки можуть забезпечити автентичність або недоторканість документа, ідентифікувати автора або власника, перевірити права дистриб'ютора або користувача, навіть якщо файл був оброблений або спотворений.

Щодо впровадження засобів програмно-технічного захисту в 1С, розрізняють два основні його способи:

• додатковий захист — засоби захисту є доповненням до основних програмних і апаратні засобів комп'ютерної системи;

• вбудований захист — механізми захисту реалізуються у вигляді окремих компонентів 1С або розподілені за іншими компонентами системи.

Перший спосіб є більш гнучким, його механізми можна додавати і вилучати за потребою, але під час його реалізації можуть постати проблеми забезпечення сумісності

засобів захисту між собою та з програмно-технічним комплексом 1С. Вмонтований захист вважається більш надійним і оптимальним, але є жорстким, оскільки в нього важко внести зміни. Таким доповненням характеристик способів захисту зумовлюється те, що в реальній системі їх комбінують.

Захист від комп'ютерних вірусів

Для виявлення, знищення та попередження «електронних інфекцій» можна використовувати загальні засоби захисту інформації (копіювання інформації, розмежовування доступу до неї) та профілактичні заходи, які зменшують імовірність зараження. Останніми роками з'являються апаратні пристрої антивірусного захисту, наприклад спеціальні антивіруси! плати, які вставляються у стандартні слоти розширення комп'ютера. Але найбільш поширеним методом залишається використання антивірусних програм — спеціальних програм, призначених для виявлення і знищення комп'ютерних вірусів.

Антивірусні програми поділяють на кілька видів.

Програми-детектори здійснюють пошук сигнатур вірусів. Недоліком детекторів є те, що вони можуть знаходити тільки ті віруси, які відомі їхнім розробникам, а отже, вони швидко застарівають. Деякі програми-детектори можна настроювати на нові типи вірусів, проте неможливо розробити програму, яка могла б виявити будь-який заздалегідь невідомий вірус. Отже, негативний результат перевірки програмою-детектором не гарантує відсутності вірусів. Багато детекторів мають режими лікування або знищення заражених файлів — функції докторів.

Програми-доктори («фаги») не тільки знаходять заражені вірусами файли, а й «лікують» їх (видаляють з файла тіло програ-ми-вірусу), повертаючи їх у початковий стан. Перед лікуванням файлів програма очищує оперативну пам'ять. Серед фагів виокремлюють поліфаги — програми-доктори, призначені для пошуку і знищення великої кількості вірусів. Як і детектори, програми-доктори потребують постійного оновлення.

Програми-ревізори запам'ятовують початковий стан програм, каталогів і системних областей, коли комп'ютер не заражений вірусом, а згодом, періодично або за бажанням користувача, порівнюють поточний стан системи з початковим. Як правило, перевірка здійснюється відразу після завантаження операційної системи — контролюються довжина файла, його контрольна сума, дата і час модифікації та інші параметри. Деякі програми-ревізори можуть при цьому виявляти і стелс-віруси. Гібриди програм-ревізорів і докторів можуть не тільки виявляти зміни, а й повертати файли і системні області до початкового стану. Вони є більш універсальними, оскільки можуть захистити і від вірусу, не відомого на час їх створення, якщо він використовує стандартний механізм зараження.

Програми-фільтри («сторожа», «монітори») — резиденти} програми, призначені для виявлення підозрілих дій при роботі комп'ютера. Після одержання відповідного повідомлення користувач може дозволити або відмінити виконання операції. Деякі програми-фільтри перевіряють програми, які викликаються до виконання, та файли, що копіюються. Недоліком подібних програм є їх «набридливість», можливі конфлікти з іншим програмним забезпеченням, а перевагами — виявлення вірусів на ранній стадії, що мінімізує втрати.

Програми-вакцини («іммунізатори») модифікують програми і диски таким чином, що це не відбивається на роботі програм, але вірус, від якого проводиться вакцинація, вважає їх інфікованими. Це вкрай неефективний спосіб захисту. Вакцини мають обмежене використання — їх можна застосувати тільки проти відомих вірусів.

Жодний з типів антивірусних програм не надає стовідсоткового захисту, тому слід додержувати загальних правил (див. вставки) і користуватись останніми розробками антивірусних лабораторій.

Основні заходи з антивірусного захисту

1. Комплексно використовуйте сучасні антивірусні програми та оновлюйте їх версії.
2. Регулярно перевіряйте комп'ютер (системні області, пам'ять, файли), завантаживши ОС із захищеної від запису дискети (диска).
3. Перевіряйте на наявність вірусів дискети, записані на інших комп'ютерах.
4. Перевіряйте на наявність вірусів файли, що надходять із комп'ютерних мереж.
5. Завжди закривайте свої дискети від запису під час роботи на інших комп'ютерах, якщо на них не записується інформація.
6. Не залишайте у дисководі дискети під час вмикання комп'ютера або перезавантаження комп'ютера чи ОС.
7. Обов'язково робіть архівні копії цінної інформації на змінних носіях.

Чотири правила поведінки при зараженні комп'ютерної системи вірусом

1. Не поспішайте і не приймайте необачних рішень.
2. Слід негайно вимкнути комп'ютер, щоб вірус не продовжував своєї руйнівної дії.
3. Усі дії з виявлення вірусу і лікування системи обоє 'язково слід виконувати після завантаження комп'ютера із захищеної від запису чистої від вірусів дискети (диску) з ОС.
4. Якщо Ви не маєте досить знань і досвіду для лікування комп'ютера, скористайтесь досвідом фахівців.

Надати повну характеристику конкретних антивірусних програм і зробити рекомендації щодо вибору з-поміж них майже неможливо. Швидкість появи нових вірусів (близько 2000 на рік) приводить до постійного оновлення антивірусного програмного забезпечення. Це означає не тільки поповнення антивірусних баз, а й удосконалення евристичних аналізаторів, зміну конфігурації програм і т. ін. Тому для одержання актуальної інформації рекомендується звертатися до фахівців, розробників і періодичних видань. Відповідну інформацію можна також знайти в мережі Інтернет

Найбільшого поширення в Україні набули російськомовні антивірусні програми:

• поліфаг Dr.Web і резидентний сторож SpIDer Guard, розроблені антивірусною лабораторією Ігоря Данилова — http://www. drweb.ru;

• поліфаг Antiviral Toolkit Pro (AVP) Євгена Касперського — http://www.avp.ru;

* антивірусний пакет Norton Antivirus компанії Symantec — http://www.symantec.com.

За прогнозами експертів, у недалекому майбутньому очікується підвищення кількості вірусів, залучення у процесі їх створення нових технологій (див. приклад) та розширення «анти-антивірусних» дій. Прикладом останнього є скандал, який відбувся у 1996 році у зв'язку з наявністю «троянського коня» у фальшивому доповненні до Dr.Web, який знищував файли на дисках. Однією з причин цього є двозначне положення розробників антивірусів — за деякими оцінками, кожний вірус приносить антивірусній індустрії не менш як 15 тис. доларів доходу щорічно протягом багатьох років.

Методи криптографічного захисту

Криптографічний захист (шифрування) інформації - це вид захисту, який реалізується за допомогою перетворень інформації з використанням спеціальних (ключових) даних з метою приховування змісту інформації, підтвердження її справжності, цілісності, авторства тощо. На відміну від тайнопису, яке приховує сам факт передавання повідомлення, зашифровані повідомлення передаються відкрито, приховується їхній зміст.

Методи криптографії поділяють на дві групи — підставлення (заміни) і переставлення. Підстановчний метод передбачає, що кожна літера та цифра повідомлення замінюється за певним правилом на інший символ. Зокрема, для визначення порядку під-

ставлення може використовуватись певне слово або фраза — ключ. У загальному випадку у криптографії ключ — це послідовність бітів, що використовуються для шифрування та розшифрування даних. Наприклад, якщо використати слово ЮРИСТ як ключ за допомогою підстановної таблиці (див. нижче), то слово ЗЛОМ буде виглядати як ГИЙІ.

А	Б	В	г	Д	Е	Є	Ж	З	и	І	ї	Й	к	л	м	н	0
					А	Б	В	г	Д	Е	Є	Ж	З	и	І	ї	й
Ю	Р	И	с	Т													

У разі використання перестановного алгоритму змінюються не символи, а порядок їх розміщення в повідомленні. Залежно від доступності ключів розрізняють:

• **симетричне шифрування** — для шифрування і розшифрування використовується один ключ. Такі системи із закритим ключем реалізовані, наприклад, в архіваторах даних. Це зручно для шифрування приватної інформації, але під час передавання повідомлення по каналах зв'язку слід забезпечити таємне передавання ключа, щоб одержувач міг здійснити розшифрування. У принципі, якщо можна таємно передати ключ, то можна передати і таємну інформацію, тоді відпадає необхідність у шифруванні, а якщо такої можливості немає, шифрування даремне;

* **асиметричне** — для шифрування використовується один, відкритий (публічний, загальнодоступний) ключ, а для дешифрування — інший, закритий (секретний, приватний). Це робить непотрібним таємне передавання ключів між кореспондентами. Відкритий ключ безплідний для дешифрування, і його знання не дає можливості визначити секретний ключ. Єдиним недоліком моделі є необхідність адміністративної роботи — ключі (і відкриті, і закриті) треба десь зберігати і час від часу оновлювати.

Сьогодні існує достатня кількість криптографічних алгоритмів. Найбільш поширеними з них є стандарт шифрування даних DES (Data Encryption Standart) та алгоритм RSA, названий за першими літерами прізвищ розробників (Rivest, Shamir, Adleman), розроблені у 1970-х роках. Обидва алгоритми є державними стандартами США. DES є симетричним алгоритмом, а RSA — асиметричним. Ступінь захищеності під час використання цих алгоритмів прямо залежить від довжини ключа, що застосовується.

Криптографічні алгоритми використовуються як для шифрування повідомлень, так і для створення ***електронних (цифрових) підписів (ЦП)*** — сукупностей даних, які дають змогу підтвердити цілісність електронного документа та ідентифікувати особу, що його підписала.

Звичайно терміни «електронний підпис» і «цифровий підпис» застосовуються як синоніми, але перший з них має ширше значення, оскільки позначає будь-який підпис в електронній формі («оцифрований» не означає «цифровий»). Отже, електронні підписи не обов'язково базуються на криптографічних методах і можуть бути створені, наприклад, за допомогою засобів біометрії (див. п. 3.4.4).

Цифровий підпис передбачає вставляння в повідомлення сторонньої зашифрованої інформації. Поширеним методом є створення ЦП за допомогою асиметричного шифрування. При цьому накладання підпису виконується за допомогою закритого ключа, а перевірка підпису за допомогою відкритого (відмінність створення ЦП від шифрування інформації). Публічний ключ та додаткові відомості (їм я відправника, серійний номер ЦП, назва уповноваженої фірми І ЦП) передається разом з підписом. Таким чином, послати зашифроване повідомлення і перевірити підпис може будь-хто, а розшифрувати або підписати повідомлення — тільки власник відповідного секретного ключа.

Загалом для забезпечення належного рівня захищеності інформації потрібна криптографічна система (криптосистема) сукупність засобів криптографічного захисту, необхідної ключової, нормативної, експлуатаційної, а також іншої документації (зокрема й такої, що визначає заходи безпеки).

Головним обмеженням криптосистем є те, що при одержанні повідомлення зашифрованого парним ключем, не можна взнати напевне, хто саме його відправив (див.

п. 4.3.1).

Останній недолік можна виправити за допомогоюо засобів біометричного захисту (див. наступний пункт) та методцом двофакторної аутентифікації «Я маю» + «Я знаю» (використовується й однофакторна аутентифікація, але вона є менш надійною). Наприклад, користувач повинен мати пластикову карті-ку (картку з магнітною смужкою або смарт-картку) і знати PIN-код.

Отже, розвиток криптосистем і підвищення надійності цифрових підписів створює необхідні передумови для заміняй паперового документообігу електронним і переходу до здійснення електронних операцій.

Біометричний захист інформації ї

Системи біометричного захисту використовують унікальні для кожної людини вимірювані фізіологічні характеристики для перевірки особи індивіда. Цей процес називається електронною аутентифікацією. Його суть — визначити, чи справді індивід є тією особою, якою він або вона себе називає. Це відрізняє аутентифікацію від ідентифікації та авторизації1. Мета ідентифікації — перевірити, чи відомий індивід системі, наприклад перевіркою пароля, а авторизація полягає в наданні користтувачеві доступу до певних ресурсів залежно від його особи.

Біометричні системи забезпечують найбільш точну аутентифікацію, оскільки перевіряють параметри, які дуже: важко або неможливо змінити або підробити, їхні переваги очевидні, оскільки традиційні системи захисту не здатні з'ясувати, наприклад, хто саме вводить код або вставляє смарт-картку.

Слід зазначити, що біометричні технології мають один суттєвий недолік. Вони спрацьовують завдяки тому, що системі відомі унікальні, конфіденційні характеристики кожної конкретної людини. Однак прибічники біометрії стверджують, щез насправді вона забезпечує вищий рівень секретності, оскільки під час аутентифікації не залучається інформація про адресу людинку, домашній телефон, банківський рахунок тощо.

Донедавна біометрія вважалась атрибутом фантастичних романів і військових систем, але сьогодні відповідні технології доросли до загального застосування і далі швидко розвиваються. З удосконаленням біометричних пристроїв можна очікувати їх застосування не тільки у промисловості, а й у приватному секторі — проведення онлайнових операцій, доступ до банкоматів і засобів роздрібної торгівлі, вхід та вихід до будинків та багато іншого.

Протягом тривалого часу здійснювались спроби вибрати різні фізичні характеристики як індивідуальний штамп, що його можна було б постійно розпізнавати з високою точністю. Результати таких спроб втілено в сучасних технологіях:

- розпізнавання відбитків пальців. Основою цієї технології, започаткованої у кримінології в XIX столітті, є сканування візерунку пальців людини і порівняння їх з тими, що були попередньо записані у систему. Засоби захоплення варіюються від стандартних сканерів до складних пристроїв, які вимірюють дрібні заряди між складками шкіри. З огляду на зрілість цієї технології за допомогою подібних пристроїв можна досягнути високої точності. Подальший розвиток технології вимагає врахування можливих змін поверхні шкіри і навіть погодних умов. Для користувачів ця технологія приваблива через її простоту і швидкість;
- розпізнавання голосу. Цей підхід використовує стандартні засоби для запису модуляцій індивідуального мовлення. Рівень точності при цьому дещо нижчий, оскільки залежить від акустичного середовища та якості пристрою аудіозапису;
- аналіз геометрії руки передбачає вимірювання фізичних характеристик руки і пальців користувача. Рівень точності ідентифікації прямо пропорційний до кількості точок у записаному зразку. Новітні пристрої дають можливість створити тривимірну карту руки користувача;

- сканування сітківки ока. Ця технологія передбачає сканування системи кровоносних судин на сітківці. Точність розпізнавання дуже висока, на рівні розпізнавання відбитків пальців;
- сканування райдужної оболонки. Основою цього підходу є порівняння унікальних рисунків райдужної оболонки ока. Сканування виконується за допомогою спеціальної камери. На сьогодні точність ідентифікації не дуже висока, але очікується її збільшення з удосконаленням технології;
- розпізнавання обличчя. Для запису тривимірної геометричної карти обличчя людини застосовується стандартна цифрова камера. Залежно від конкретного варіанта технології рівень точності розпізнавання коливається від низького до середнього;
- розпізнавання динаміки підпису. Під час аналізу підпису, який робиться спеціальною ручкою з перетворювачем прискорення по осях X і Y, враховується не тільки написання літер, а й швидкість і ступінь натискування;
- розпізнавання стилю набирання символів на клавіатурі. Під стилем тут розуміється швидкість натискання на клавіші, ритм ударів і тиск, який здійснюється на клавіши. За даними маркетингових досліджень, користувачі довіряють більше системам розпізнавання відбитків пальців, а не стилю введення даних. Але слід зазначити, що останні будуть готові до масового впровадження значно раніше завдяки своїй дешевизні. Так, у 2001 році на ринку з'явилось біометричне програмне забезпечення для захисту мереж Windows NT — «BioPassword LogOn». Для роботи не потрібне додаткове обладнання. Єдине, що вимагається від користувача, — створити власний шаблон, 15 разів ввівши своє ім'я і пароль. Точність розпізнавання становить 98 %. Початкова вартість пакета — від 20 до 90 дол. залежно від розмірів мережі.

Реальні біометричні системи — досвід США

Проект ФБР «Інтегрована автоматизована система ідентифікації відбитків пальців (Integrated Automated Fingerprint Identification Systems, IAFIS) має на меті заміну карток з відбитками пальців на базу даних з відсканованими зображеннями та супроводжувальною текстовою інформацією, яка буде доступна агентствам забезпечення законності та правопорядку в усьому світі. IAFIS розглядається як наріжний камінь Підрозділу інформаційних послуг кримінальної юстиції (Criminal Justice Information Services Division, CJIS).

Служба імміграції та натуралізації США (U.S. Immigration and Naturalization Service) використовує засоби аналізу геометрії руки для зменшення напруги на обмежувальних переходах. Дубльовані Системи прискореного обслуговування пасажирів (7/vs Passenger Accelerated Service System, INSPASS) встановлюються у найбільших аеропортах США. Мандрівник, інформацію про якого вже записано, вставляє видану йому картку у блок системи, йому ставляться кілька запитань і, нарешті, йому пропонується внести руку у спеціальний зчитувач. Якщо порівняння записаних даних і щойно відсканованих відбувається успішно, особу направляють до митного інспектора, а якщо ні — бо імміграційного. Типовий процес займає 15—20с.

Описані щойно технології можна розбити на дві групи залежно від того, як у них реалізується процес «захоплення» елементів людської анатомії. Технології, які не передбачають будь-якого зіткнення з людиною, наприклад, розпізнавання голосу, більш прийнятні для користувачів, але менш надійні. Але, з огляду на широке поле застосування біометричних технологій, можна передбачити, що всі вони будуть запитані. Швидкість їх поширення залежатиме від темпів удосконалення відповідних пристроїв та програмного забезпечення і зниження їхньої вартості. Також велике значення матиме законодавча підтримка і розробка промислових стандартів.

ОРГАНІЗАЦІЯ ЗАХИСТУ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Захист інформації неможливо регламентувати через різноманітність існуючих 1С та видів інформації, що обробляється. Конкретні заходи визначаються виробничими, фінансовими та іншими можливостями підприємства (організації), обсягом конфіденційної інформації та її значущістю. Можна назвати тільки загальні правила:

• створення та експлуатація системи захисту інформації є складною і відповідальною справою, яку мають робити професіонали;

• не слід намагатись організувати абсолютно надійний захист — такого просто не існує. Система захисту має бути достатньою, надійною, ефективною та керованою. Ефективність захисту інформації вимірюється не витратами на її організацію, а її здатністю адекватно реагувати на всі загрози;

* заходи із захисту інформації повинні мати комплексний характер, об'єднувати різні засоби;

* систему захисту слід будувати, виходячи з того, що основну загрозу становлять співробітники підприємства (організації, установи).

Необхідність залучення кваліфікованих фахівців до організації захисту інформації диктується тим, що тільки вони можуть визначити всі загрози і знайти ефективні засоби протидії. Сьогодні захист інформації стає однією з галузей, для якої розробляються спеціальні інструментальні засоби, призначені для генерації тестів, імітації загроз, аналізу текстів програм. Створюються експертні системи для формування вимог до безпеки ІТ та оцінки рівня їх виконання.

Однак до захисту інформації повинні залучатись і звичайні користувачі, оскільки цю проблему неможливо вирішити тільки технічними і програмними засобами, людський фактор відіграє важливу роль у забезпеченні конфіденційності (див. вставку).

Власники і користувачі інформації можуть якнайкраще оцінити її важливість для визначення адекватних заходів з її захисту. Вони ж мають брати активну участь у виробленні стратегії захисту, оскільки остання має бути частиною внутрішньої політики організації. За приклад можна вважати появу нової посади у штатному розкладі корпорації IBM, — директором з проблем захисту конфіденційної інформації стала ветеран IBM Арієт Пірсон, яка має інженерну та юридичну освіту.

Необхідне розуміння цієї проблеми і на державному рівні. В Україні базовим законом для цього є Закон «Про державну таємницю», який надає таке визначення: державна таємниця (секретна інформація) — вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому Законом України «Про державну таємницю», державною таємницею і підлягають охороні державою. Цей Закон доповнюють інші закони та нормативні акти, однак слід зазначити, що для ефективного захисту інформації потрібне не тільки вдосконалення правової бази, а й комплексні заходи з втілення державної політики в цій галузі в життя (див. вставку).

Боротьба з кіберзлочинністю — справа державна

Наприкінці 2000 року уряд Великобританії (http://www.number-10.gov.uk) повідомив про виділення 25 млн фунтів стерлінгів на створення у 2001 р. спеціального елітного поліцейського підрозділу з боротьби зі злочинністю у сфері високих технологій (National Hi-Tech Crime Unit). До підрозділу запрошені спеціально підготовлені детективи з поліції, митниці, Національного управління з розслідування карних злочинів (National Crime Squad) і Національної кримінальної поліції (NCIS — National Criminal Intelligence Service) — всього 40 осіб у Лондоні і 46 слідчих у підрозділах на місцях. Об'єктами кіберкопів є шахраї, педофіли, хакери, автори вірусів та інші шкідники. На виділені гроші також фінансується цілодобова «гаряча лінія», яка інформує про можливі атаки та інші

загрози.

Федеральне бюро розслідувань США запустило у 2001 році програму попередження комп'ютерних злочинів InfraGuard, розроблену Центром захисту національної інфраструктури (National Infrastructure Protection Center, NIPC, http://www.nipc.gov/). Однією з цілей програми є створення захищеної від вторгнення ззовні мережі для обміну інформацією між компаніями та органами забезпечення правопорядку про здійснені атаки та надання відомостей, які можуть попередити такі зазіхання. Однак деякі експерти вважають, що контроль з боку ФБР спричиняє недоступність інформації іншим учасникам. Це зумовлює появу інших подібних програм. Так, американські комп'ютерні корпорації Miscrosoft, Oracle, AT&T, Intel та 15 інших компаній створили центр обміну інформацією по боротьбі з комп'ютерною злочинністю (Information Technology Information Sharing and Analysis Center).

За твердженнями експертів, з усієї кількості комп'ютерних злочинів бувають своєчасно розкриті і покарані тільки 10— 17 %. У 90 % випадків виявлення злочину завдячує випадковості. Основною причиною такого становища є особливості комп'ютерних злочинів, які ускладнюють їх виявлення та доведення:

• незначні зовнішні прояви злочину — викрадена інформація може залишитись на місці, зчитування інформації може тривати частки секунд, занесення комп'ютерного вірусу списується на недосконаліть антивірусного програмного забезпечення, а втрата даних — на збій технічних засобів;

складність точного визначення втрат та їх оцінювання у грошовому еквіваленті;

• часто розслідування комп'ютерних злочинів є дуже дорогим, що обмежує можливості його проведення. А оскільки виявлені зловмисники часто здобувають легке покарання, потерпілі не бачать сенсу витрачати додаткові кошти на їх розшук;

• небажання постраждалих звертатись до правоохоронних органів, оскільки це може призвести до обнародування секретної інформації, втрати клієнтів, партнерів або акціонерів, конфліктів усередині організації. Деякі постраждалі побоюються, що у процесі розслідування будуть виявлені незаконне ведення ними операцій або інші протиправні дії. Одним з аспектів цієї проблеми є те, що потерпіла особа зазвичай сприймається громадськістю як жадібна і дурна;

• складність доведення злочинного наміру або необережності. Найчастіше злочинець не в змозі передбачити повністю наслідки своїх дій — вони залежать від багатьох суб'єктивних і об'єктивних факторів, зокрема від стану 1С, її захищеності та кількості зв'язків з іншими системами;

• високі вимоги до слідчого, який повинен мати підготовку на рівні професійного програміста або системного адміністратора. Щонайменше слідчий повинен вміти користуватись відповідним програмним забезпеченням, але критичним для нього є розуміння внутрішніх механізмів роботи систем і мереж. Останнє необхідне вже при виконанні таких звичайних слідчих дій, як обшук і збір речових доказів. Інформацію, зчитану або роздруковану з машинних носіїв, можна прийняти як доказ тільки за гарантованої неможливості її змінювання у процесі виконання цієї операції. Таку гарантію може дати використання сертифікованих програмних засобів, перевірених на відсутність незадокументованих можливостей. Але це не вирішує проблему повністю, оскільки залишається питання, хто буде контролювати застосування слідчим подібних програм — запрошені на обшук поняті навряд чи зможуть це зробити. Отже, ці питання потребують додаткових досліджень і детальної регламентації у кримінально-процесуальному законодавстві. Як не парадоксально, допомогти правоохоронним органам можуть і хакери

Роль хакерів у захисті 1С — тестування на проникнення

Тестування на проникнення є заходом, який має на меті перевірку відсутності в 1С простих шляхів обійти механізми захисту для неавторизованого користувача. Для цього можна скористатися професійними засобами тестування. Відповідні програми існують для всіх операційних систем, їх доцільно застосовувати хоча б тому, що вони можуть стати

інструментом справжньої атаки. Недоліком подібних програм є те, що вони аналізують тільки вже відомі вразливі місця.

Кращим способом атестації безпеки системи є надання можливості спеціально запрошеним хакерам зламати її без попередження адміністраторів і користувачів. Результатом має стати конфіденційний звіт з оцінкою рівня доступності інформації та рекомендаціями щодо вдосконалення системи захисту.

Цей метод використовують і виробники програм комп'ютерного захисту. Прикладом є щорічний конкурс хакерів OpenHack, який проводить журнал eWeek. Компанія-розробник пропонує грошові призи у кілька десятків тисяч доларів тим, хто за два тижні зламає систему.

Однак, і тут можна зробити зауваження. Подібний конкурс не можна вважати ідеальною перевіркою. Професійні пірати не будуть рекламувати свої здібності, а залишать їх для «власного користування». OpenHack швидше можна назвати конкурсом молодих талантів, оскільки досвід минулих змагань показав, що серед переможців є особи, надто малі, щоб водити автомобіль.

Проте залучення юних хакерів до суспільно корисної роботи може стати одним із заходів з попередження комп'ютерних злочинів і розкриття вже скоєних. Сьогодні хакерів активно залучають у спеціальні поліцейські підрозділи. Прикладом є індійська національна кібер-поліція (National Cyber Cop Committee), «співробітниками» якої стали у 2000 році 19 хакерів у віці від 14 до 19 років.