

**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ
СПРАВ**

Сумська філія

Кафедра соціально-економічних дисциплін

ТЕКСТ ЛЕКЦІЇ

з навчальної дисципліни «Інформаційне забезпечення професійної діяльності»
обов'язкових компонент
освітньої програми першого (бакалаврського) рівня вищої освіти

262 Правоохоронна діяльність (правоохоронна діяльність)

**за темою – «Захист даних у мережі. Електронний підпис. Основи
інформаційної безпеки»**

Суми 2023

ЗАТВЕРДЖЕНО

Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 30.08.2023 р № 7

СХВАЛЕНО

Вченою радою Сумської філії
Харківського національного
університету внутрішніх справ
Протокол від 29.08.2023 р № 8

ПОГОДЖЕНО

Секцією Науково-методичної ради
ХНУВС з технічних дисциплін
Протокол від 29.08.2023 р № 7

Розглянуто на засіданні кафедри соціально-економічних дисциплін Протокол
від 29.08.2023 р № 2

Розробники:

Доцент кафедри соціально-економічних дисциплін Сумської філії ХНУВС,
канд.екон.наук, доцент Виганяйло Світлана Миколаївна

Рецензенти:

1. Доцент кафедри протидії кіберзлочинності, факультету № 4 (кіберполіції)
Харківського національного університету внутрішніх справ, канд.пед.наук,
доцент Тетяна Петрівна Колісник
2. Доцент кафедри кібернетики та інформатики СНАУ, канд.екон.наук, доцент
Олександр Борисович В'юнєнко

План лекції

1. Проблеми захисту інформації в сучасних ІС
2. Основні види комп'ютерних злочинів.
3. Комп'ютерні віруси як загроза інформаційним системам.
4. Засоби захисту інформації.
5. Класифікація засобів захисту інформації
6. Захист від комп'ютерних вірусів
7. Методи криптографічного захисту
8. Біометричний захист інформації
9. Організація захисту комп'ютерних ІС.

Рекомендована література:

Основна

1. Виганяйло С. М. Інформаційне забезпечення професійної діяльності: навч. посіб. Харків: ХНУВС, 2021. 110 с.
<http://dspace.univd.edu.ua/xmlui/handle/123456789/11258>
2. Клімушин, П. С. Інформаційні системи та технології в економіці : навчальний посібник / П. С. Клімушин, О. В. Орлов, А. О. Серенок; Нац. акад. держ. управління при Президентові України, Харк. регіон. ін-т держ. управління. - Харків : Вид-во ХарPI НАДУ "Магістр", 2011. - 448 с.
<http://dspace.univd.edu.ua/xmlui/handle/123456789/4730>
3. Сезонова, І. К. Інформатика для правоохоронців: навч. посіб. / І. К. Сезонова; МВС України, Харк. нац. ун-т внутр. справ. - Харків, 2015. – 182 с. <http://dspace.univd.edu.ua/xmlui/handle/123456789/1311>

Допоміжна

1. Застосування інформаційних технологій у діяльності правоохоронних органів : зб. матеріалів кругл. столу (м. Харків, 9 груд. 2020 р.) / МВС України, Харків. нац. ун-т внутр. справ. – Харків : ХНУВС, 2020. – 132 с.
2. Методичні рекомендації щодо використання комп'ютерної програми «Навчальний ЄРДР» (для ролі «курсант») / [Розроб. Коршенко В. А., Демидов З. Г., Колмик О. О., Абламський С. Є.]; МВС України, Харків. нац. ун-т внутр. справ, Наук.-досл. лаб. з проблем розвитку інформац. технологій, Каф. крим. процесу та організації досуд. слідства ф-ту № 1. - Харків: ХНУВС, 2019. - 30 с.

Текст лекції

1. Проблеми захисту інформації в сучасних ІС

В усьому світі злочини в сфері електронних засобів інформації вважаються одними із най розповсюджених. Останнім часом і в Україні почала створюватись нормативна база для запобігання цим злочинам.

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

Комп'ютерні злочини – протизаконні дії, знаряддям або об'єктом яких є електронна обробка інформації.

Наприклад, до категорії комп'ютерних злочинів належить шахрайство з магнітними кредитними картками, злочини в сфері телекомунікацій тощо.

Більшість спеціалістів з правових питань поділяють комп'ютерні злочини на два види:

1. Злочини, об'єктом скоєння яких є комп'ютер:

- знищення або заміна даних, програмного забезпечення і обладнання;
- економічне шпигунство і розголошення інформації, що є державною або комерційною таємницею;
- інші подібні злочини.

2. Протизаконні дії, для скоєння яких комп'ютер використовується, як знаряддя:

- комп'ютерний саботаж;
- вимагання і шантаж;
- розтрата;
- розкрадання грошових коштів;
- обман споживачів, інвесторів або користувачів;
- інші злочини (зокрема, несанкціоноване використання комп'ютерів в особистих цілях).

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 втрат варто виокремити такі:

- збитки, до яких призводить ситуація, коли співробітники організації не можуть виконувати свої обов'язки через нероботоздатність 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**» (<http://zakon3.rada.gov.ua/laws/show/80/94-вр>)

захист інформації — це сукупність організаційно-технічних заходів і правових норм для запобігання заподіяння шкоди інтересам власника інформації чи АС та осіб, які користуються інформацією.

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 ІС 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 ІС перестає існувати для фізичних або юридичних осіб, які мають право власності на неї в повному чи обмеженому обсязі;
- **підrobка інформації** — навмисні дії, що призводять до перекручення інформації, яка має оброблятися або зберігатися в ІС;
- **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, підrobка або блокування інформації, порушення роботи ІС, 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).

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.

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 ІС 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 зосередитись на кредитних картках (таких називають «кардерами»), банківських рахунках, телефонному зв'язку (так звані «фрікери», «частотники») і т. ін., але в усякому разі його мотивацією є матеріальні інтереси, а не цікавість чи пустощі.

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.

2. Основні види комп'ютерних злочинів

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. Далі описано найбільш поширені види комп'ютерних злочинів.

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;
- 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.

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 ІС. В останньому випадку може підроблятися вихідна інформація з метою імітування роботоздатності ІС і здачі замовнику свідомо несправної продукції. До цього самого виду злочинів можна віднести підтасування результатів виборів, голосувань і т. ін.

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 роботоздатності 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».

Розробка і поширення комп'ютерних вірусів. Прояви вірусів можуть бути різноманітними — від появи на екрані точки, що світиться, до стирання файлів

з жорсткого диска. У будь-якому разі це означає порушення цілісності ІС. Сьогодні фахівці очікують появи вірусів для програмованих мікросхем і мобільних телефонів.

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. ін. Його особливістю є те, що безпомилкових програм не буває у 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.

Комп'ютерні злочини в мережі Інтернет. Виокремлення цієї категорії диктується реаліями використання глобальної мережі. По-перше, Інтернет стає інструментом здійснення «звичайних» злочинів. Це промисловий шпідіаж, саботаж, поширення дитячої порнографії і т. ін. Понад третина користувачів мережі страждає від шахрайств. Одним із ключових аспектів багатьох «схем» шахрайства є доступ до персональних даних користувача. 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-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 (атака, що спричинює відмову від обслуговування) або уповільнення їхньої роботи різними способами («повені»). Найчастіше для реалізації таких атак використовуються пакети технологічної інформації та самі правила взаємодії серверів за мережними протоколами. Конкретні назви атак з'являються за назвами програм, що їх реалізують («persi»), позначеннями пакетів технологічної інформації («SYN», «UDP»).

3. Комп'ютерні віруси як загроза інформаційним системам

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.

Варто враховувати, що зазначені явища можуть бути наслідком й інших причин.

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, 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 файлу на виконання і залишаються активними обмежений час. Резидентні віруси інсталиують 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 DDK**, які не впроваджуються у файли, а виконують реорганізацію файлової системи так, що під час запуску будь-якого файлу 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 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'ютерів, як їх зібрати в єдине ціле і розмножити вірус.

З погляду **прийомів маскування** розрізняють віруси-невидимки 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. Засоби захисту інформації

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.

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.

5. Класифікація засобів захисту інформації

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. (Кодекс професійної поведінки членів Асоціації користувачів ЕОМ).

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.

Адміністративні (організаційні) засоби захисту інформації регламентують процеси функціонування ІС, 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 не вигідно 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 ІС, 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 ІС, сигналів від датчиків пожежної безпеки, відеоінформації 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 дотримуватися вимог міжнародних стандартів;

- **засоби захисту системи електроживлення.** Американські дослідники з компанії Best Power 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 ІС 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 впливу 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, розмежування доступу до ресурсів згідно з повноваженнями користувачів, реєстрацію подій в ІС, криптографічний захист інформації, захист від комп'ютерних вірусів тощо.

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 тайнопису датується V століттям до н. е. Сучасним прикладом є випадок роздрукування на ЕОМ контрактів з малопомітними викривленнями обрисів окремих символів тексту — так вносились 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. Методи стеганографії дають можливість замінити несуттєві частки даних на конфіденційну інформацію. Сімейна* цифрова фотографія може містити комерційну інформацію, а файл із записом сонати Гайдна — приватний лист.

Але 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 ІС, 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 ІС 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 ІС. 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.

6. 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 антивірусні 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 налаштовувати 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 «клікують» їх (видаляють з файла тіло програми-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 («імунізатори») 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.

Як видно з наведеного опису, жодний з типів антивірусних програм не надає стовідсоткового захисту, тому слід дотримувати 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 свої руйнівні дії.
3. Усі дії з виявлення вірусу і лікування системи обов'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.

Нині 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 та розширення «антиантивірусних» дій.

7. 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. Підстановний метод передбачає, що кожна літера та цифра повідомлення замінюється за певним правилом на інший символ. Зокрема, для визначення порядку підставлення 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	Й	І	Ї	Ї	К	Л	М	Н	О
					А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й
Ю	Р	И	С	Т													

Подібний шифр дуже швидко можна розкрити, вивчивши повторюваність символів та короткі слова «і», «або», «за» і т. ін.

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.

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.

Цифровий підпис передбачає вставляння в повідомлення сторонньої зашифрованої Інформації. При цьому, якщо не застосовується додаткове шифрування, сама інформація, що передається, ніяк не захищається. Сторонньою інформацією може бути **контрольна сума** (циклічний надлишковий код) — значення, яке автоматичне обчислюється за певним алгоритмом і широко використовується для перевірки цілісності інформації. Вимогою до відповідного алгоритму є неможливість створення відмінних текстів з однаковою сумою.

Більш 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 (ім'я відправника, серійний номер ЦП, назва уповноваженої фірми та її 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.

Криптографічний захист може бути організований як програмне, так і з використанням апаратно-програмних і апаратних засобів. Сьогодні фактичним стандартом для електронного листування в усьому світі завдяки своїй популярності й безплатному поширенню стала програма Філіпа Циммермана «**Pretty Good Privacy**» (PGP). У PGP застосовується так звана модель рівної довіри — відправник знає одержувача і довіряє йому ключ шифру, звідки і пішла назва «pretty good» (у буквальному перекладі — досить гарна). Перевагами PGP є висока надійність (єдиний метод зламування — «лобова атака»), потужний механізм обробки ключів, велика швидкодія. PGP можна інтегрувати в усі популярні поштові програми.

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).

Уразливість криптографічних систем пов'язана з тим, що вони базуються на задачах, які визнані умовно нерозв'язуваними — для жодної з них не знайдено ефективного розв'язання, але й не доведено, що воно не існує. Від добору ключа методом перебирання криптосистема захищена поки що недостатнім рівнем швидкодії комп'ютерів. А численність типів можливих атак на криптографічні системи («на спосіб реалізації», «на паролі», «на користувача», «на моделі довіри» і т. ін.) підтверджує той факт, що захист є надійним і безпечним доти, доки не розпочинаються спроби його зламування.

І нарешті, головним обмеженням криптосистем є те, що при одержанні повідомлення зашифрованого парним ключем, не можна взнати напевне, хто саме його відправив.

Останній недолік можна виправити за допомогою засобів біометричного захисту та **методом двофакторної аутентифікації** «Я маю» + «Я знаю»

(використовується й однофакторна аутентифікація, але вона є менш надійною). Наприклад, користувач повинен мати пластикову картку (картку з магнітною смужкою або смарт-картку) і знати РІМ-код.

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

8. Біометричний захист інформації

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 авторизації. Мета **ідентифікації** — перевірити, чи відомий індивід системі, наприклад перевіркою пароля, а **авторизація** полягає в наданні користувачеві 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, що насправді вона забезпечує вищий рівень секретності, оскільки під час аутентифікації не залучається інформація про адресу людини, 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 онлайн-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 ХІХ 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 клавіші. 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'явилося 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.

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.

9. Організація захисту комп'ютерних інформаційних систем

Захист інформації неможливо регламентувати через різноманітність існуючих ІС 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**» <http://zakon2.rada.gov.ua/laws/show/3855-12>, 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.

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 недосконалість 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 витратити 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 ІС, 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.

Контрольні питання і завдання

1. Назвіть основні шляхи порушення безпеки інформації.
2. Які основні види комп'ютерних злочинів?
3. Назвіть основні джерелами загрози для інформації.
4. Прокласифікуйте комп'ютерні віруси за відомими Вам ознаками.
5. У чому полягає відмінність між симетричними та асиметричними системами криптографії?
6. У чому полягає відмінність процесу створення цифрового підпису від шифрування інформації?
7. Які технології біометричної аутентифікації Ви знаєте?