Міністерство освіти і науки України
Львівський національний університет імені Івана Франка

Л. С. Монастирський

СИСТЕМИ І МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

Навчальний посібник

Львів – 2013

УДК 004.056.5(075.8)
ББК 3811-053Я73
М 77

Рецензенти:
д-р техн. наук, проф. **М.Є. Шелест**
(Державний університет інформаційно-комунікаційних технологій, м. Київ);
д-р фіз.-мат. наук, проф. **В.Ф. Чекурін**
(Інститут прикладних проблем механаніки і математики НАН України, м. Львів);
д-р техн. наук, проф. **В.А. Ромака**
(Національний університет "Львівська Політехніка", м. Львів)

Друкується за ухвалою Вченої Ради
Львівського національного університету імені Івана Франка
Протокол № __ від

М77 **Монастирський Л.С.**

Системи і методи захисту інформації: навч. посібник / Л. С. Монастирський. – Львів: Львівський національний університет ім. І. Франка, 2013. – 172 с.

ISBN

У посібнику викладено основи інформаційного захисту, зокрема наведено базові принципи криптографічного та стеганографічного методів захисту інформації, безпеки даних у комп'ютерних мережах, основи фізико-технічних систем і методів захисту інформації та телеохорони. Кожен метод детально проаналізований з математичної та фізичної точок зору і підсилений, для поглиблення знань студента, лабораторною роботою з описом суті, мети, завдання та ходом її виконання. Наведені приклади програмної реалізації криптоалгоритмів з відповідним текстом комп'ютерних програм.

Рекомендований для студентів вищих навчальних закладів, які навчаються за спеціальностями напрямів "Комп'ютерні науки", "Прикладна фізика", "Мікро- та наноелектроніка".

ISBN 978-617-10-0040-7

ЗМІСТ

ВСТУП

Визначальною особливістю сучасності є потреба вирішення складних багатоаспектних завдань, що супроводжуються розширенням інформаційного обміну про найновітніші досягнення науки, сприянням впровадженню їхніх результатів у життя.

Інформаційна епоха зумовила докорінні зміни у способі виконання функціональних обов'язків для численних професій. Сьогодні нетехнічний фахівець середнього рівня може виконувати роботу, яку раніше здійснював висококваліфікований програміст. Службовець у своєму розпорядженні ще ніколи не мав стільки точної й оперативної інформації, як тепер.

Водночас використання комп'ютерів і автоматизованих технологій спричиняє появу низки проблем для керівництва організацією. Доступ до величезної кількості найрізноманітніших даних надають комп'ютери, часто об'єднані в мережі. Тому, дбаючи про безпеку інформації, важливо усвідомлювати наявність ризику, зумовленого автоматизацією і наданням щораз більшого доступу до конфіденційних, персональних чи інших даних. Збільшується кількість комп'ютерних злочинів, що врешті-решт може призвести до економічних втрат. Відтак очевидно, що інформація – це ресурс, який треба захищати. Те, що в 60-х роках минулого століття називали комп'ютерною безпекою, а в 90-х – безпекою даних, тепер точніше називають інформаційною безпекою. Інформаційна безпека зумовлена важливістю інформації в сучасному суспільстві, розумінням того, що інформація – це коштовний ресурс – щось більше, ніж окремі елементи даних.

Інформаційною безпекою називають заходи для захисту інформації від неавторизованого доступу, руйнування, модифікації, розкриття і затримок у доступі.

Інформаційна безпека гарантує досягнення таких цілей:

- конфіденційність критичної інформації;
- цілісність інформації і пов'язаних з нею процесів (створення, введення, оброблення, виведення);
- доступність до інформації у разі потреби;
- облік усіх процесів, пов'язаних з інформацією.

Деякі технології з захисту системи і забезпечення обліку всіх подій вбудовані в самий комп'ютер, інші – в програми. Деякі виконуються людьми і є реалізацією вказівок, що містяться у відповідних керівних документах.

Використання технологій, пов'язані з поняттям інформаційної безпеки, – запорука успішної діяльності будь-якої організації і її управлінської ланки.

Інформаційні процеси і діяльність, зумовлена ними, регламентовані стандартизованими нормами. Для спрощення обміну інформацією, захисту комерційної таємниці й авторських прав, статистичного аналізу, планування та ефективного керування на всіх ієрархічних рівнях глобальної інформаційної системи країни необхідне законодавче регулювання інформаційної діяльності організацій.

Щодо захисту інформації, то хоча розглянуті нами засоби не завжди надійні, оскільки сьогодні швидкими темпами розвивається не тільки техніка (у нашому випадку – комп'ютерна), але й методи, що дають змогу цю інформацію здобувати, цими засобами не слід нехтувати. Нашу епоху часто називають інформаційною, і вона несе величезні можливості, пов'язані з економічним зростом, технологічними нововведеннями. Володіння електронними даними, що стають найбільшою цінністю інформаційної ери, зобов'язує власників дотримуватися прав і обов'язків з контролю за їхнім використанням. Файли і повідомлення, збережені на дисках, і ті, що пересилаються каналами зв'язку, мають іноді більшу цінність, ніж самі комп'ютери, диски. З огляду на це перспективи інформаційного століття можуть бути реалізовані тільки в тому випадку, якщо окремі особи, підприємства й інші підрозділи, які володіють інформацією, що дедалі частіше має конфіденційний характер чи є особливо важливою, зможуть належно захистити свою власність від будь-яких погроз, вибрати такий рівень захисту, що відповідатиме їхнім вимогам безпеки.

Розділ 1

КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ

1.1. Елементи теорії криптографічних систем

Проблемою захисту інформації шляхом її математичного перетворення займається криптологія (від kryptos – таємний, logos – наука). У криптології виділяють два напрями – *криптографію* і *криптоаналіз*. Суть цих напрямів протилежна.

Криптографія займається пошуком та дослідженням математичних методів перетворення інформації.

Сфера інтересів *криптоаналізу* – дослідження можливості розшифровування інформації без знання ключів.

Криптографічна система є сімейством T_k перетворень відкритого тексту. Членів цього сімейства індексують, або позначають символом k, параметр k є ключем. Простір ключів K – це набір можливих значень ключа. Звичайно ключем є послідовний ряд букв алфавіту.

Криптосистеми поділяють на *симетричні* та з *відкритим ключем*.

У *симетричних* криптосистемах і для шифрування, і для дешифрування використовують один і той самий ключ.

У системах з *відкритим* ключем використовують два ключі – відкритий і закритий, які математично пов'язані один з одним. Інформацію шифрують за допомогою відкритого ключа, який доступний усім бажаючим, а розшифровують за допомогою закритого ключа, відомого тільки одержувачу повідомлення.

Терміни розподілу ключів та управління ключами відносять до процесів системи оброблення інформації, змістом яких є створення і розподіл ключів між користувачами.

Електронним (цифровим) *підписом* називають приєднане до тексту його криптографічне перетворення, яке дає змогу в разі одержання тексту іншим користувачем перевірити авторство і достовірність повідомлення.

Криптостійкістю називають характеристику шифру, яка визначає його стійкість до дешифрування без знання ключа (тобто криптоаналізу).

Криптосистему визначають абстрактно – як деяку множину відображень одного простору (множини можливих повідомлень) в інший простір (множини можливих криптограм). Кожне конкретне відображення з цієї множини відповідає способу шифрування за допомогою конкретного ключа.

Передбачають, що відображення є взаємооднозначне, отже, якщо відомий ключ, то внаслідок процесу розшифровування можлива лише єдина змістовна відповідь.

Унаслідок розгляду криптосистем, які можуть бути подані як сукупність відображень однієї множини елементів в іншу, виникають дві природні операції комбінування, які з двох цих систем виробляють третю. Першу операцію комбінування називають операцією *множення* (добутком) і вона відповідає зашифруванню повідомлення за допомогою системи R з дальшим шифруванням одержаної криптограми за допомогою системи S, причому ключі R і S вибирають незалежно. Повний результат цієї операції становить собою криптосистему, відображення якої складаються з усіх добутків у звичайному значенні R на відображення з S. Імовірності результуючих відображень є добутками ймовірностей двох початкових відображень.

Друга операція комбінування є *зваженим складанням*:

$$T=pR+qS,\ \ p+q=1.$$

Вона полягає ось у чому. Спочатку вибирають, яку з систем R або S буде використано, причому систему R вибирають з імовірністю p, а систему S з імовірністю q. Потім вибрану систему використовують описаним способом.

Секретні системи з цими двома операціями комбінування створюють, по суті, “лінійну асоціативну алгебру” з одиницею, – алгебраїчний об’єкт детально вивчений математикою.

Щоб розпочати математичний аналіз криптографії, треба ввести задовільну ідеалізацію і визначити математично прийнятним способом, що розуміють під терміном *секретна система*. Схематична структура секретної системи показана на рисунку.

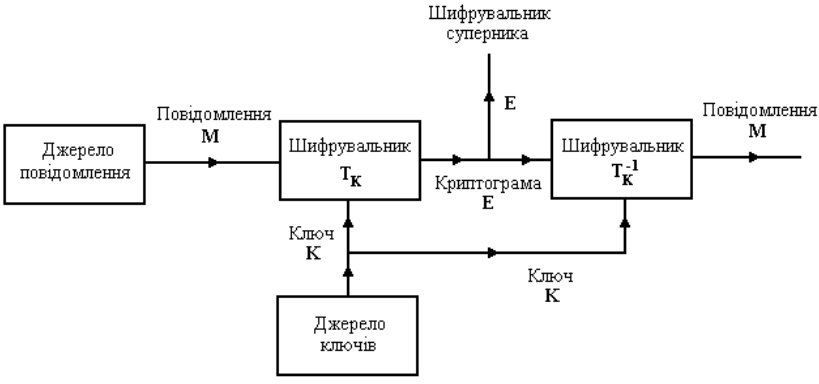


Рис. 1.1. Типова схема криптосистеми

На передавальному кінці є два джерела інформації – джерело повідомлень і джерело ключів. Джерело ключів відбирає конкретний ключ серед усіх можливих ключів цієї системи. Цей ключ передається певним способом на приймальний кінець, причому передбачають, що його не можна перехопити (наприклад, ключ передано посильним). Джерело повідомлень формує певне повідомлення (незашифроване), яке потім зашифровують, і готову криптограму передають на приймальний кінець, причому вона може бути перехоплена (наприклад, пересилається по радіо чи електронною поштою). На приймальному кінці шифрувальник за допомогою ключа за криптограмою відновлює початкове повідомлення.

Очевидно, шифрувальник на передавальному кінці виконує певну функціональну операцію. Якщо M – повідомлення, K – ключ і E – зашифроване повідомлення (криптограма), то маємо:

$$E = f(M, K),$$

тобто E є функцією від M і K, хоча зручніше розуміти E не як функцію двох змінних, а як однопараметричне сімейство операцій або відображень, і записувати його у вигляді $E = T_i M$.

Відображення T_i, застосоване до повідомлення M, дає криптограму E. Індекс i відповідає конкретному ключу.

Вважатимемо, що є лише кінцеве число можливих ключів, кожному з яких відповідає ймовірність p_i. Отже, джерело ключів є статистичним процесом або пристроєм, який вибирає одне з безлічі відображень $T_1,\ldots, T_m$ з імовірностями $p_1,\ldots, p_m$ відповідно. Вва-

жатимемо також, що число можливих повідомлень скінчене, і ці повідомлення $M_1,\ldots, M_n$ мають апріорні ймовірності $q_1,\ldots, q_n$. Наприклад, можливими повідомленнями могли б бути будь-які послідовності англійських букв, що вміщують по N букв кожна, а відповідними ймовірностями тоді були б відносні частоти появи таких букв у нормативному англійському тексті.

Якщо відомі E і K, на приймальному кінці, буде можливість відновлювати M_n. Тому відображення T_i з нашого сімейства мусить мати єдине зворотне відображення T_i^{-1}, тому що $T_i\ T_i^{-1}=I$, де I – тотожне відображення. Отже, $M=T_i^{-1}E$. Принаймні, це зворотне відображення T_i^{-1} має існувати і бути єдиним для кожного E, яке можна одержати з M за допомогою ключа i. Звідси сформулюємо таке визначення: *секретна система* – це сімейство однозначно оборотних відображень T_i безлічі можливих повідомлень у безліч криптограм, причому відображення T_i має ймовірність p_i. Безліч можливих повідомлень для зручності назвемо "простором повідомлень", а безліч можливих криптограм – "простором криптограм".

Дві криптографічні системи збігаються, якщо вони утворені однією і тією ж безліччю відображень T_i, й однаковими просторами повідомлень та криптограм, причому ймовірності ключів у цих системах також збігаються.

Криптографічну систему уявляємо як деяку машину з одним або більш перемикальними пристроями. Послідовність букв (повідомлення) надходить на вхід машини, а на виході її маємо вже іншу послідовність. Конкретне положення перемикальних пристроїв відповідає конкретному використовуваному ключу. Для вибору ключа з безлічі можливих мають бути задані деякі статистичні методи.

Щоб цю проблему можна було розглянути математично, передбачимо, що противнику відома система. Іншими словами, він знає сімейство відображень T_i, і ймовірності вибору різних ключів.

1.2. Класичні криптосистеми

Шифр простого підставляння. У такому шифрі замінюють кожну букву повідомлення на деякий певний символ (зазвичай також на букву). Отже, повідомлення

$$M=m_1m_2m_3m_4\ldots,$$

де m_1, m_2,... – послідовні букви, переходить в

$$E = e_1e_2e_3e_4\ldots = f(m_1)f(m_2)f(m_3)f(m_4)\ \ldots,$$

причому функція $f(m)$ має зворотну функцію. Ключ є простим переставлянням алфавіту (якщо букви замінюють на букви), наприклад:

XGUACDTBFHRSLMQVYZWIEJOKNP.

Перша буква – X замінює букву A, G – B і т.д.

Транспозиція з фіксованим періодом d. У цьому випадку повідомлення ділять на групи символів довжини d і до кожної групи застосовують одне і те ж саме переставляння. Таке переставляння є ключем і може бути задане деяким переставлянням перших d цілих чисел.

Отже, для d = 5 як переставляння візьмемо 23154. Це означатиме, що

$$m_1\ m_2\ m_3\ m_4\ m_5\ m_6\ m_7\ m_8\ m_9\ m_{10}\ldots$$

переходить у

$$m_2\ m_3\ m_1\ m_5\ m_4\ m_7\ m_8\ m_6\ m_{10}\ m_9\ldots$$

Послідовне застосування двох або більше транспозицій матиме назву складної транспозиції. Якщо періоди цих транспозицій різні $d_1,\ldots, d_s$, то, очевидно, в результаті одержимо транспозицію періоду d, де d – найменше спільне кратне $d_1,\ldots, d_s$.

Шифр Віженера і його варіанти. У шифрі Віженера ключ задано набором з d букв. Такі набори підписують з повторенням під повідомленням, а одержані дві послідовності складають за модулем 26 (кожну букву алфавіту, що її розглядають, нумерують від A = 0 до Z = 25).

Звідси $e_i = m_i+k_i$ (*mod 26*), де k_i – буква ключа, одержана шляхом складання числа m_i та k_i за модулем 26. Наприклад, за допомогою ключа GAH маємо:

Повідомлення	N	O	W	I	S	T	H	E
Ключ повторюєть-	G	A	H	G	A	H	G	A
Криптогр.	T	O	D	O	S	A	N	E

Шифр Віженера з періодом *1* названо шифром Цезаря. Це просте підставляння, де кожну букву повідомлення M зсувають вперед на фіксоване число місць алфавіту. Таке число і є ключем, воно

може бути яким завгодно – від 0 до 25. Так званий шифр Бофора (Beaufort) і видозмінений шифр Бофора подібні до шифру Віженера. У них повідомлення зашифровують за допомогою рівностей:

$$e_i = k_i - m_i \ (mod\ 26),$$
$$e_i = m_i - k_i \ (mod\ 26)$$

відповідно. Шифр Бофора з періодом *1* має назву *зворотний шифр Цезаря*.

Повторне застосування двох або більше шифрів Віженера називають *складним шифром Віженера*. Він описується рівнянням:

$$e_i = m_i + k_i + l_i + ... + s_i \ (mod\ 26),$$

де $k_i, l_i, ..., s_i$ мають різні періоди. Період їхньої суми $k_i + l_i + ... + s_i$, як і в складовій транспозиції, є найменшим спільним кратним окремих періодів.

Якщо використовують шифр Віженера з необмеженим ключем, що не повторюється, то це шифр Вернама, в якому

$$e_i = m_i + k_i \ (mod\ 26)$$

і k_i вибирають випадково та незалежно серед чисел 0, 1,..., 25.

Диграмне, триграмне і n-грамне підставляння. Замість підставляння однієї букви можна використовувати підставляння диграм, триграм і т.д. Для диграмного підставляння в загальному вигляді потрібний ключ, що складається з переставляння 262 диграм. Опишемо його за допомогою таблиці, в якій ряд відповідає першій букві диграми, а стовпець – другій букві, причому клітини таблиці заповнені замінювальними символами (звичайно також диграмами).

Шифр Віженера з одноразово перемішаним алфавітом. Такий шифр є простим підставлянням з подальшим застосуванням шифру Віженера:

$$e_i = f(m_i) + k_i \ ,$$
$$m_i = f - 1(e_i - k_i) \ .$$

"Оберненим" до такого шифру є шифр Віженера з дальшим простим підставлянням:

$$e_i = g(m_i + k_i) \ ,$$
$$m_i = g - 1(e_i) - k_i \ .$$

Матрична система. Метод підставляння *n*-грам полягає в застосуванні до послідовних *n*-грам деякої матриці, що має обернену. Передбачено, що букви пронумеровані від 0 до 25 і їх розглядають як елементи деякого алгебраїчного кільця. Якщо до *n*-грами повідомлення застосувати матрицю a_{ij}, то вийде *n*-грама криптограми.

Матриця a_{ij} є ключем, і розшифрування виконують за допомогою оберненої матриці. Обернена матриця існуватиме тоді і тільки тоді, коли визначник $[a_{ij}]$ має обернений елемент у нашому кільці.

Шифр Плейфера. Цей шифр є частковим випадком диграмного підставляння, який проводять за допомогою перемішаного алфавіту з 25 букв, записаних у вигляді квадрата 5×5, (букву *J* при криптографічній роботі часто пропускають, оскільки вона трапляється зрідка, а якщо й трапляється, то її замінюють буквою *I*). Ключовий квадрат записують так:

L	Z	Q	C	P
A	G	N	O	U
R	D	M	I	F
K	Y	H	V	S
X	Y	T	E	W

У цьому випадку диграму AC, наприклад, замінюють на пару букв, розміщених у протилежних кутах прямокутника, що визначається буквами A і C, тобто на LU, причому L береться першою, оскільки вона вище за A. Якщо букви диграми розміщені на одній горизонталі, то використовують ті, що стоять праворуч від них. Отже, RI замінюють на DF, RF – на DR. Якщо букви розміщені на одній вертикалі, то використовують букви, що стоять під ними. Отже, PS замінюють на UW. Якщо обидві букви диграми збігаються, то для їхнього розділення використовують нуль або ж одну з букв пропускають.

Перемішування алфавіту за допомогою багаторазового підставляння. У цьому шифрі використовують послідовно *d* простих підставлянь. Так, якщо $d=4$, то $m_1m_2m_3m_4m_5m_6...$ замінюють на $f(m_1)f(m_2)f(m_3)f(m_4)f(m_5)f(m_6)...$.

Шифр з автоключем. Шифр типу Віженера, в якому або саме повідомлення, або результуючу криптограму використовують як "ключ", називають *шифром з автоключем*. Шифрування почина-

ють за допомогою “первинного ключа” (який є справжнім ключем у нашому значенні) і продовжують за допомогою повідомлення або криптограми, зміщеної на довжину первинного ключа, як у вказаному нижче прикладі, де первинним ключем є набір букв COMET. Як “ключ” використовують повідомлення:

Повідомлення	S	E	N	D	S	U	P	P	L	I	E	S	…
Ключ	C	O	M	E	T	S	E	N	D	S	U	P	…
Криптограма	U	S	Z	H	L	M	T	C	O	A	Y	H	…

Якщо як “ключ” використати криптограму, то вийде:

Повідомлення	S	E	N	D	S	U	P	P	L	I	E	S	…
Ключ	C	O	M	E	T	U	S	Z	H	L	O	H	…
Криптограма	U	S	Z	H	L	O	H	O	S	T	T	S	...

Дробові шифри. У цих шифрах кожну букву спочатку зашифровують у дві (або більше) букви або в два (або більше) числа, потім одержані символи певним способом перемішують (наприклад, за допомогою транспозицій), після чого їх можна знову перевести в первинний алфавіт. Отже, використовуючи як ключ перемішаний 25-буквовий алфавіт, переводимо букви у двозначні числа за допомогою таблиці:

	0	1	2	3	4
0	L	Z	Q	S	P
1	A	G	N	O	U
2	R	D	M	I	F
3	K	Y	H	V	S
4	X	B	T	E	W

Наприклад, букві B відповідає число 41. Після того як одержаний ряд чисел буде піддано деякому переставлянню, його можна знову розділити на пари чисел і перейти до букв.

Гамування. Гамування є також широко застосовуваним криптографічним перетворенням. Насправді межа між гамуванням і використанням нескінченних ключів і шифрів Віженера досить умовна.

Принцип шифрування гамуванням полягає в генеруванні гами шифру за допомогою генератора псевдовипадкових чисел і накла-

данні одержаної гами на відкриті дані, наприклад, використовуючи додавання за модулем *2*.

Процес дешифрування даних зводять до повторного генерування гами шифру при відомому ключі і накладанні такої гами на зашифровані дані.

Одержаний зашифрований текст є досить складним для розкриття в тому випадку, якщо гама шифру не містить повторюваних бітових послідовностей. По суті, гама шифру має змінюватися випадковим способом для кожного слова, яке шифрують. Фактично, якщо період гами перевищує довжину всього зашифрованого тексту і невідома жодна частина вихідного тексту, то шифр розкривають тільки прямим перебором. Криптостійкість у цьому випадку визначають за розміром ключа.

Генератори псевдовипадкових чисел (ПВЧ). Для того, щоб одержати лінійні послідовності елементів гами, довжина яких перевищує розмір шифрованих даних, використовують генератори ПВЧ. На основі теорії груп були розроблені декілька типів таких пристроїв.

Сьогодні найдоступнішими і найефективнішими є конгруентні генератори ПВЧ. Для цього класу генераторів зроблені математично строгі висновки щодо того, якими властивостями володіють вихідні сигнали цих генераторів з погляду періодичності та випадковості.

Одним з ефективних конгруентних генераторів є лінійний конгруентний генератор ПВЧ. Він виробляє послідовності псевдовипадкових чисел $T(i)$, які описують виразом

$$T(i+1)=(A*T(i)+C)\bmod m,$$

де A і C – константи, $T(0)$ – вихідна величина, вибрана як число, що породжує послідовність цих чисел. Очевидно, що ці три величини й утворюють ключ.

Такий пристрій ПВЧ генерує псевдовипадкові числа з визначеним періодом повторення, який залежить від вибраних значень A і C. Значення m звичайно встановлюють $2n$, де n – довжина машинного слова в бітах. Генератор має максимальний період M до того, як, генеруючи послідовність, почне повторюватися. Тому необхідно вибирати числа A і C такими, щоб період M був максимальним. Як доведено Д. Кнутом, лінійний конгруентний генератор ПВЧ має максимальну довжину M тоді і тільки тоді , коли C – непарне, і $A \bmod 4=1$.

Шифрування за допомогою генератора ПВЧ є досить поширеним криптографічним методом. Якість шифру, побудованого на основі генератора ПВЧ, визначають не тільки і не стільки за характеристиками генератора, скільки за алгоритмом одержання гами. Один з фундаментальних принципів криптологічної практики свідчить, що навіть складні шифри можуть бути дуже чутливими до простих впливів.

Лабораторна робота № 1.1. Програмна реалізація алгоритму шифрування за методом Цезаря

Мета роботи. Реалізувати на практиці алгоритм шифрування текстової інформації за методом Цезаря, використовуючи мову програмування Turbo Pascal 7.0.

Хід виконання роботи. Створена за допомогою мови програмування Pascal програма шифрування текстової інформації працює за таким алгоритмом:

- спочатку користувач отримує запит про дію, яку він хоче виконати: шифрувати чи розшифровувати інформацію;
- відбувається прив'язка до двох файлів: 1 – файл, що містить інформацію, яку необхідно зашифрувати; 2 – файл, куди записано інформацію вже в зашифрованому вигляді (адреси цих файлів користувач програми повинен сам увести з клавіатури, коли буде відповідний запит);
- користувач отримує запит про довжину ключа (ключ – це кількість символів, на які буде зсунуто ASCII-код кожного з символів);
- програма зчитує початковий файл з текстом, розбиває кожний прочитаний рядок на символи, перетворює їх в ASCII-коди, додає до ASCII кодів довжину ключа, перетворює утворені ASCII-коди назад у символи і записує їх у файл у зашифрованому тексті.

Під час розшифрування все відбувається аналогічно, лише з однією відмінністю: замість додавання ключа до ASCII-коду програма віднімає його. Внаслідок цього ми одержуємо вихідний текст у розшифрованому вигляді.

Приклад тексту програми

```
uses crt, graph;
const
n=200;
var
    choise, i, key : integer;
    information, encrypt : text;
    symbol : char;
    ss, adres, adres_encrypt : string;
begin
clrscr;
writeln;
    writeln('Program for encription and description');
    writeln;
    writeln('for encription enter 1');
    writeln('for description enter 2');
    readln(choise);
    i:=l;
    if choise=l  then
    begin
    Writeln('Enter file address');
    Readln(adres);
    Writeln;
    Writeln('Enter encrypted file address');
    Readln(adres_encrypt);
    assign (information,adres);
    assign(encrypt,adres_encrypt);
    Reset(information);
    Rewrite(encrypt);
    Writeln('enter the lenght of key');
    Readln(key);
    while not eof(information) do
    begin
    Readln(information, ss);
    For i:=l to length (ss)  do
    Begin
    Write(encrypt, chr(Ord(ss[i])+key));
    end;
    Writeln(encrypt);
```

```
end;
Writeln('Coding procces is allredy complited');
Writeln;
Writeln('for exit push <Enter>');
readln;
end;
if choise=2 then
begin
Writeln('Enter encrypted file address1);
Readln(adres_encrypt);
Writeln('Enter descrypted file address');
Readln(adres);
Writeln;
assign (mformation,adres);
assign(encrypt,adres_encrypt);
Rewrite(information);
Reset(encrypt);
Writeln('enter the lenght of key1);
Readln(key);
while not eof(encrypt) do
begin
Readln(encrypt, ss);
For i:=l to length (ss) do
begin
Write(information,chr(Ord(ss[i]) – key));
end;
end;
Writeln('Decoding procces is allredy complited');
Writeln;
Writeln('for exit push <Enter>');
readln;
close(information);
close(encrypt);
end;
end.
```

1.3. Сучасні блочна та асиметрична криптографії. Стандарт шифрування даних ГОСТ 28147–89

Важливим завданням у справі створення умов для гарантійної безпеки в інформаційній системі (ІС) є розроблення і використання стандартних алгоритмів шифрування даних. Першим серед подібних стандартів був американський DES – послідовне використання замін і переставлянь.

Ефективнішим є стандарт шифрування даних ГОСТ, який рекомендовано для використання і для захисту даних у вигляді двійкового коду, хоч допустимі й інші методи шифрування. Цей стандарт формувався з урахуванням світового досвіду, а саме: були прийняті до уваги недоліки і нереалізовані можливості алгоритму DES, тому використання стандарту ГОСТ має перевагу. Алгоритм досить складний. Опишемо його концепцію.

Введемо асоціативну операцію конкатенації, використовуючи для неї мультиплікативний запис. Крім того, використаємо такі операції додавання:

A⊕B – побітове додавання за модулем 2;

A[+]B – додавання за модулем 2^{32};

A{+}B – додавання за модулем $2^{32} - 1$.

У алгоритмі криптографічного перетворення передбачено декілька режимів роботи. В усіх режимах використано ключ W завдовжки 256 бітів, який поданий у вигляді восьми 32-розрядних чисел x(i).

$$W=X(7)X(6)X(5)X(4)X(3)X(2)X(1)X(0)$$

Для дешифрування використовують той самий ключ, проте процес дешифрування є інверсним до вихідного. Найпростіший з можливих режимів – заміна.

Нехай відкриті блоки розбиті на блоки по 64 біти у кожному. Позначимо їх $T(j)$.

Чергова послідовність бітів $T(j)$ розділена на дві послідовності – $B(0)$ і $A(0)$ по 32 біти (правий і лівий блоки). Далі виконуємо ітераційний процес шифрування, що описуємо за такими формулами (вигляд його залежить від i):

Для $i=1,2,\ldots,24$, $j=(i-1) \bmod 8$;

$$A(i)=f(A(i-1)[+]x(j))\oplus B(i-1),$$
$$B(i)=A(i-1).$$

Для i=25,26,...,31, j=32 – i;

$$A(i)=f(A(i-1)[+]x(j))\oplus B(i-1),$$

$$B(i)=A(i-1).$$

Для i=32

$$A(32)=A(31)$$

$$B(32)=f(A(31)[+]x(0))\oplus B(31),$$

де i – номер ітерації, f – функція шифрування.

Функція шифрування охоплює дві операції над 32-розрядним аргументом.

Перша операція є підставлянням K. Блок підставляння K складається з восьми вузлів заміни $K(1)...K(8)$ з пам'яттю 64 біти кожний. 32-розрядний вектор, який надходить на блок підставляння, розбивають на вісім послідовних чотирирозрядних вектори, кожен з яких перетворюється в чотирирозрядний вектор відповідним вузлом заміни, що є таблицею з 16 цілих чисел у діапазоні 0–15. Вхідний вектор визначає адресу рядка в таблиці, число з якої є вихідним вектором. Потім чотирирозрядні вектори послідовно об'єднують у 32-розрядний вихідний.

Друга операція – циклічне зміщення ліворуч 32-розрядного вектора, одержаного в результаті підставляння K. 64-розрядний блок зашифрованих даних T записуємо у вигляді

$$T=A(32)B(32).$$

Інші блоки відкритих даних у режимі простої заміни зашифровуємо аналогічно. Треба враховувати, що такий режим шифрування має обмежену криптостійкість.

Інший режим шифрування названо *режимом гамування*.

Відкриті дані, розбиті на 64-розрядні блоки $T(i)$ ($i=1,2,...,m$) (m визначають за об'ємом шифрованих даних), зашифровують у режимі гамування шляхом порозрядного додавання за модулем 2 з гамою шифру $Г_ш$, яка виробляється блоками по 64 біти, тобто

$$Г_ш=(Г(1),Г(2),...,Г(m)).$$

Рівняння шифрування даних у режимі гамування опишемо у вигляді

$$Ш(i)=A(Y(i-1)\oplus C2,Z(i-1))\ \{+\}\ C(1)\ \oplus T(i)=Г(i)\ \oplus T(i).$$

У цьому рівнянні $Ш(i)$ позначає 64-розрядний блок зашифрованого тексту; A – функцію шифрування в режимі простої заміни (аргументами цієї функції є два 32-розрядні числа); $C1$ і $C2$ – конс-

танти, які задані за ГОСТом 28147–89. Величини $y(i)$ і $Z(i)$ визначають ітераційно, відповідно до формування гами:

$$(Y(0),Z(0))=A(S),\ S - \text{64-розрядна двійкова послідовність},$$
$$(Y(i),Z(i))=(Y(i-1)[+]C2,\ Z(i-1)\{+\}C(1)),\ I=1,2,\ldots,m.$$

64-розрядна послідовність, що названа *синхропосиланням*, не є секретним елементом шифру, проте його наявність необхідна як на передавальній, так і на приймальній сторонах.

Режим гамування зі зворотним зв'язком дуже подібний до режиму гамування: як і в режимі гамування відкриті дані, розбиті на 64-розрядні блоки $T(i)$, зашифровують шляхом порозрядного додавання за модулем 2 з гамою шифру $Г_ш$, яка виробляється блоками по 64 бітів:

$$Г_ш=(Г(1),Г(2),\ldots,Г(m)).$$

Рівняння шифрування даних у режимі гамування зі зворотним зв'язком має вигляд:

$$Ш(1)=A(S)\ \oplus T(1)=Г(1)\oplus T(1),$$
$$Ш(i)=A(Ш(i-1))\oplus T(i)=Г(i)\ \oplus T(i),\ i=2,3,\ldots,m.$$

За ГОСТом 28147–89 визначають процес створення імітовставки, який одинаковий для всіх режимів шифрування. *Імітовставка* – це блок з p бітів (імітовставка I_p), який виробляється або перед шифруванням усього повідомлення, або паралельно з шифруванням блоками. Параметр p вибирають відповідно до необхідного рівня імітозахищеності.

Для одержання імітовставки відкриті дані подають також у вигляді блоків по 64 біти. Перший блок відкритих даних $T(1)$ підлягає перетворенню, що відповідає першим 16 циклам алгоритму режиму простої заміни. Як ключ використовують той самий ключ, що і для шифрування даних. Одержане 64-розрядне число сумують з відкритим блоком $T(2)$ і сума знову підлягає 16 циклам шифрування для режиму простої заміни. Цю процедуру повторюють для всіх m блоків повідомлення. З одержаного64-розрядного числа вибирають відрізок I_p довжиною p бітів.

Імітовставку передають по каналу зв'язку після зашифрованих даних. На приймальній стороні аналогічним способом з прийнятого повідомлення виділяють імітовставку і порівнюють з одержаною. У випадку незбіжності імітовставок повідомлення вважають неправдивим.

Лабораторна робота № 1.2. Блочні криптосистеми типу DES

Мета роботи. Вивчити принципи роботи програм DESX та DES100. Дослідити вплив зміни пароля, розміру ключа та типу шифрованого файла.

Хід виконання роботи. Програми DES100 та DESX призначені для шифрування та дешифрування файлів.

DESlOO.exe – шифрувальник – дешифрувальник на основі DES (Data Encryption Standard). Довжина ключа змінна, обмежена ресурсами пам'яті, проте може бути задана жорстко через опцію —k. Можна спочатку на фіксовану довжину ключа запросити дамп таблиць (– td) (таблиці *_s.dmp), а потім підставити свої таблиці (– tl). Таблиці генеруються генератором псевдовипадкових чисел з використанням заданого пароля (якщо пароль заданий – h'aaa.exe', то паролем вважають файл aaa.exe).

Опції:

– *c* кодування,

– *d* розкодовування,

– *k* встановлення ключа фіксованої довжини,

– *p* введення пароля,

– *td* запитують дамп таблиць,

– *tl* підставляють свої таблиці.

Для того щоб зашифрувати файл DES100, потрібно ввести у командну стрічку:

deslOO – *c* – *p*[пароль] [назва файла, що його шифруватимуть (з розширенням)] [назва шифрованого файла (також з розширенням)].

Наприклад: deslOO – *c* -ppass myfile.txt myfile.cod.

Для того щоб зашифрувати файл у DESX, потрібно ввести у командний рядок:

desx – *e* "пароль" [назва файла, що його шифруватимуть (з розширенням)] [назва шифрованого файла (також з розширенням)].

Наприклад: desx – e "parol" myfile.txt myfile.cod.

Для розшифрування: desx – *d* "paro" myfile.cod myfile.txt

Система DES ґрунтується на 16-кратному застосуванні одного і того ж самого алгоритму. Ця система є блочним алгоритмом шифрування з довжиною ключа 64 біти.

Кожну букву в алфавіті, починаючи з нуля, зіставляємо з числом. Своєю чергою, кожну цифру у двійковій системі числення подаємо у вигляді шестирозрядної послідовності нулів та одиничок.

Шифрування інформації ґрунтується на цифровому вираженні інформації і відбувається у двійковій формі. Це операція, пов'язана з додаванням символів за модулем числа *2*. Відкритий текст подаємо у вигляді співвідношення: M=M 1M2M3...

У результаті певного перетворення за формулою C=ЃC1C2C3... одержуємо криптотекст. Для одержання блоку зашифрованого тексту необхідно 16 раундів.

Лабораторна робота № 1.3. Криптопакет KRYPTON

Мета роботи. Ознайомитися з принципами роботи програми KRYPTON.

Хід виконання роботи.

KRYPTON дає змогу шифрувати трьома різними способами, а саме:

1. NORMAL,
2. KEYBOOK,
3. PASS PHRASE.

Щоб зашифрувати файл (або групу файлів), необхідно його виділити й натиснути F2 і вибрати один з методів шифрування.

Метод *normal* шифрує файл і автоматично створює для нього ключ. Цей метод найпростіший.

Метод *keybook* для шифрування потребує вказати інший файл, за допомогою якого буде створений ключ.

У разі шифрування методом *pass phrase* треба ввести пароль (не більше як чотири символи).

Опис параметрів командного рядка:

Запускають програму з параметром.

Krypton a myenc filel.txt file2.zz fileS.

Команда шифрує "filel.txt", "filel.zz", "file3" звичайним методом OTP – One – Time – Pad – одноразовий блокнот (OTP) у файли "myenc.enc" і "myenc.key" (файли даних і ключа практично однаково захищені, однак в ".enc" файлі містяться ще і координатно-іменні незашифровані дані).

Krypton akb myenc mykblO filel.txt file2.zz fileS.

Те ж саме, але за методом Кодова книжка з використанням спецфайла "mykblO.kyb", який має бути в тій самій директорії. Після закінчення шифрування програма виведе число "Key Id#", без якого розшифрування неможливе.

Krypton gkb curkb.

Ця команда генерує нову кодову книжку "curkb.kyb". Програма запросить довжину одного ключа та їхню загальну кількість.

Krypton a myenc.

Ця команда розшифрує всі файли з шифровки (OTP) "myenc.enc" за ключем "myenc.key". Також цими параметрами можуть бути конкретні імена файлів.

Алгоритм RSA. Незважаючи на досить велику кількість різних асиметричних шифросистем, найпопулярніша криптосистема RSA, розроблена в 1977 р., була названа на честь Рона Рівеста, Аді Шаміра і Леонарда Ейдельмана.

Систему побудовано на факті, що добуток великих простих чисел здійснюється легко, проте розкладання на множники добутку двох таких чисел практично неможливе. Доведено (теорема Рабіна), що розкриття шифру RSA еквівалентно такому розкладанню, а тому для довільної довжини ключа використовують нижню оцінку кількості операцій для розкриття шифру, а з урахуванням продуктивності сучасних комп'ютерів можна оцінити необхідний для цього час.

Можливість гарантовано оцінити захищеність алгоритму RSA стала однією з причин популярності цієї криптосистеми на фоні десятків інших схем. Тому алгоритм RSA використовують у банківських комп'ютерних мережах, особливо для роботи з віддаленими клієнтами (обслуговування кредитних карток).

Сьогодні алгоритм RSA використовують у багатьох стандартах, серед яких SSL, S – HHTP, S – MIME, S/WAN, STT і PCT.

Розглянемо математичні результати, закладені в основу цього алгоритму.

Теорема 1. (*Мала теорема Ферма*).

Якщо p – просте число, то

$$x^{p-1} = 1 \pmod{p}$$

для будь-якого x, простого щодо p, і

$$x^p = x \pmod p$$

для будь-якого x.

Визначення. Функцією Ейлера $\varphi(n)$ називається число додатних цілих, менших від n і простих відносно n.

N	2	3	4	5	6	7	8	9	10	11	12
$\varphi(n)$	1	2	2	3	2	6	4	6	4	10	4

Теорема 2.

Якщо $n=p\cdot q$ (p і q – відмінні одне від одного прості числа), то

$$\varphi(n)=(p-1)(q-1).$$

Теорема 3.

Якщо $n=p\cdot q$ (p і q – відмінні один від одного прості числа), x – просте щодо p і q, то

$$x^{\varphi(n)}=1 \pmod n.$$

Наслідок. Якщо $n=p\cdot q$, (p і q – відмінні одне від одного прості числа), e – просте щодо $\varphi(n)$, то відображення

$$E_{e,n}: x \to x^e \pmod n$$

буде взаємно однозначним.

Очевидний і той факт, що коли e – просте щодо $\varphi(n)$, то є ціле d – таке, що

$$ed = 1 \pmod{\varphi(n)}.$$

На цих математичних фактах і заснований популярний алгоритм RSA.

Нехай $n=p\cdot q$, де p і q – відмінні прості числа. Якщо e і d задовольняють рівняння $ed = 1 \pmod{\varphi(n)}$, то відображення $E_{e,n}$ і $E_{d,n}$ будуть інверсіями $E_{d,n}$ і $E_{e,n}$ і їх легко обчислити, якщо відомі e,d,p,q. Якщо відомі e і n, а p і q невідомі, то $E_{e,n}$ є односторонньою функцією і знаходження $E_{d,n}$ за заданим n рівнозначно розкладанню n. Якщо p і q – достатньо великі прості, то розкладання n практично нездійсненне. Це і закладено в основу системи шифрування RSA.

Користувач i вибирає пару різних простих p_i і q_i та розраховує пару цілих (e_i, d_i), які є простими щодо $\varphi(n)$, де $n_i=p_iq_i$. Довідкова таблиця містить ключі $\{(e_i,n_i)\}$. Припустимо, що вихідний текст

$$x=(x_0,x_1,\ldots,x_{n-1}),\ x \in Z_n,\ 0 \le i < n.$$

Користувач i зашифровує текст при передаванні його користувачу j, застосовуючи до n відображення $E_{di,ni}$:

$$N \rightarrow E_{di,ni}\ n=n'.$$

Користувач j проводить дешифрування n', застосувавши $E_{ei,ni}$:

$$N' \rightarrow E_{ei,ni}\ n' = E_{ei,ni}\, E_{di,ni}\ n=n.$$

Очевидно, що для того, щоб знайти інверсію $E_{di,ni}$ до $E_{ei,ni}$, потрібно знати множники $n=p_iq_i$. Час виконання найкращих з відомих алгоритмів розкладання при $n=10^{100}$ на сьогодні виходить за межі реальних технічних можливостей.

Застосування алгоритму RSA.

Приклад. Зашифруємо повідомлення CAB. Для простоти використаємо маленькі числа (на практиці застосовують значно більші).

1. Виберемо $p=3$ і $q=11$.
2. Визначимо $n=3\cdot11=33$.
3. Знайдемо $(p-1)(q-1)=20$, а d візьмемо взаємно просте з 20, наприклад $d=3$.
4. Виберемо число e. В ролі такого числа виступає будь-яке число, для якого задовольняється співвідношення $(e\cdot3)\ (\mathrm{mod}\ 20)=1$, наприклад 7.
5. Запишемо шифроване повідомлення як послідовність цілих чисел за допомогою відображення: A→1, B→2, C→3. Тоді повідомлення набуде вигляду (3,1,2). Зашифруємо за допомогою ключа {7,33}:

   ШТ1=$(3^7)(\mathrm{mod}\ 33)=2\ 187(\mathrm{mod}\ 33)=9$,
   ШТ2=$(1^7)\ (\mathrm{mod}\ 33)=1(\mathrm{mod}\ 33)=1$,
   ШТ3=$(2^7)\ (\mathrm{mod}\ 33)=128(\mathrm{mod}\ 33)=29$.

6. Розшифруємо одержане зашифроване повідомлення (9,1,29) на основі закритого ключа {3,33}:

   ВТ1=$(9^3)(\mathrm{mod}\ 33)=729(\mathrm{mod}33)=3$,
   ВТ2=$(1^3)(\mathrm{mod}\ 33)=1(\mathrm{mod}33)=1$,
   ВТ1=$(29^3)(\mathrm{mod}\ 33)=24\ 389(\mathrm{mod}33)=2$.

Отже, в реальних системах алгоритм RSA реалізують у такий спосіб: кожен користувач вибирає два великі прості числа p і q та, відповідно до описаного алгоритму, вибирає два прості числа e і d. Як результат добутку перших двох чисел (p і q) встановлюють n.

Відкритий ключ утворює $\{e,n\}$, а $\{d,n\}$ – закритий (хоч можна і навпаки). Відкритий ключ публікують і він доступний кожному бажаючому надіслати власнику ключа повідомлення, яке зашифроване цим алгоритмом. Після шифрування повідомлення неможливо розкрити за допомогою відкритого ключа. Власник закритого ключа має можливість розшифрувати прийняте повідомлення.

Система Ель – Гамаля. Ця система є альтернативою до RSA і при однаковому значенні довжини ключа забезпечує таку ж криптостійкість.

На відміну від RSA метод Ель – Гамаля заснований на проблемі дискретного логарифма. Цим він подібний до алгоритму Діффі – Хелмана. Якщо підносити число до ступеня в скінченному полі досить легко, то відновити аргумент за значенням ступеня (знайти логарифм) досить складно.

Основу системи становлять параметри p і g – числа, перше з яких – просте, а друге – ціле.

Наприклад, два абоненти Аліса та Борис: Аліса генерує секретний ключ a і обчислює відкритий ключ $y=g^a \bmod p$, Борис хоче надіслати Алісі повідомлення m і він вибирає випадкове число k, менше, ніж p, і обчислює

$$y_1=g^k \bmod p \quad \text{та}$$
$$y_2=m \oplus y^k,$$

де $\oplus$ означає побітове додавання за модулем 2. Потім Борис надсилає (y_1,y_2) Алісі.

Аліса, одержавши зашифроване повідомлення, відновлює його:

$$m=(y_1^a \bmod p) \oplus y_2.$$

Електронний підпис на основі алгоритму RSA. Найпростішим і найпоширенішим інструментом електронного підпису є вже знайомий алгоритм RSA. Крім того, відомі десятки інших схем цифрового підпису.

Припустимо, що d, p, q – секретні, а e, $n = pq$ – відкриті. Нехай DATA – повідомлення, яке передає Аліса Борису. Аліса підписує DATA для Бориса при передаванні:

$$E_{eB,nB}\{E_{dA,nA}\{DATA\}\}.$$

З цією метою використано:

- закритий ключ $E_{dA,nA}$ Аліси,
- відкритий ключ $E_{eB,nB}$ Бориса.

Борис може читати це підписане повідомлення спочатку за допомогою свого закритого ключа $E_{dB,nB}$, щоб одержати

$$E_{dA,nA}\{DATA\}= E_{dB,nB}\{ E_{eB,nB} \{ E_{dA,nA}\{DATA\}\}\},$$

і потім – відкритого ключа $E_{eA,nA}$ Аліси

$$DATA= E_{eA,nA} \{E_{dA,nA} \{DATA\}\}.$$

Отже, у Бориса з'явиться повідомлення DATA, надіслане йому Алісою.

Очевидно, що ця схема дає змогу захиститися від декількох видів порушень.

Аліса не може відмовитися від свого повідомлення, якщо вона визнає, що секретний ключ відомий тільки їй.

Порушник без знання секретного ключа не може ні сформувати, ні зробити осмислену зміну повідомлення, яке передається по лінії зв'язку.

Ця схема дає можливість у вирішенні багатьох конфліктних ситуацій обходитися без посередників.

Деколи немає потреби зашифровувати передавальне повідомлення, але потрібно закріпити його електронним підписом. У такому випадку текст шифрують закритим ключем відправника і одержаний ланцюжок символів прикріплюють до документа. Одержувач за допомогою відкритого ключа відправника розшифровує підпис і порівнює з текстом.

У 1991р. Національний інститут стандартів і технології (NIST) запропонував для алгоритму цифрового підпису DSA (Digital Signature Algorithm) стандарт DSS (Digital Signature Standard), в основу якого покладено алгоритми Ель – Гамаля і RSA.

Цифрова сигнатура. Часто виникають ситуації, коли одержувач повинен вміти довести достовірність повідомлення зовнішній особі. Щоб мати таку можливість, до передавальних повідомлень мають бути приписані т. зв. цифрові сигнатури.

Цифрова сигнатура – це рядок символів, який залежить як від індентифікатора відправника, так і від змісту повідомлення.

Під час використання цифрової сигнатури передбачено застосування деяких функцій шифрування:

$$S=H(k,T),$$

де S – сигнатура, k – ключ, T – вихідний текст.

Функція $H(k,T)$ – є хеш-функція, якщо вона задовольняє таким умовам:

- вихідний текст може бути довільної довжини;
- саме значення $H(k,T)$ має фіксовану довжину;
- значення функції $H(k,T)$ легко обчислюють для довільного аргументу;
- відновити аргумент за значенням функції практично неможливо;
- функція $H(k,T)$ – однозначна.

З визначення випливає, що для будь-якої хеш-функції є тексти-близнюки, які мають однакове значення хеш-функції, оскільки потужність множини аргументів необмежено більша від потужності множини значень. Наявність такого факту названо *ефектом дня народження*.

Найвідоміші з хеш-функцій – MD2, MD4, MD5 і SHA.

Три алгоритми серії MD розроблені Рівестом у 1989, 1990, 1991 роках відповідно. Всі вони перетворюють текст будь-якої довжини в 128-бітну сигнатуру.

В алгоритмі MD2 передбачено:
- доповнення тексту до довжини, кратної 128 бітам;
- визначення 16-бітної контрольної суми (старші розряди відкидають);
- додавання контрольної суми до тексту;
- повторне визначення контрольної суми.

В алгоритмі MD4 передбачено:
- доповнення тексту до довжини, рівної 448 бітам за модулем 512;
- додавання довжини тексту в 64-бітному вираженні;
- 512-бітні блоки піддають процедурі Damgard – Merkle, для чого кожен блок задіюють у трьох різних циклах.

В алгоритмі MD4 доволі швидко були знайдені “дірки”, тому він був замінений алгоритмом MD5, в якому кожний блок задіюють не в трьох, а в чотирьох різних циклах.

Алгоритм SHA (Secure Hash Algorithm), розроблений NIST (National Institute of Standard and Technology), повторює ідеї серії MD. В SHA використовують тексти 2^{64} бітів, які закриваються сигнатурою завдовжки 160 бітів. Такий алгоритм передбачають використовувати в програмі Capstone.

Лабораторна робота № 1.4. Асиметричні криптосистеми

Мета роботи. Освоїти основні принципи роботи з пакетами програм PGP, PGPfone.

Хід виконання роботи. PGP – досить проста у використанні програма, хоча за її допомогою реалізують надзвичайно складні математичні алгоритми шифрування даних.

Розглянемо роботу програми.

- Start (Пуск) > Programs (Програми) > PGP > PGP/keys.
- Вказати власне ім'я (Full name) і адресу електронної пошти (Email address), не забуваючи, що саме ці дані будуть асоційовані програмою з вашими ключами.
- Вибір типу ключа (Key Pair Type): ключ RSA архаїчніший і повільніший від Diffie – Hellman/DSS, однак, якщо серед ваших кореспондентів є користувачі більш ранніх версій, ніж PGP 5.0, доведеться використовувати ключ RSA.
- Вибір довжини загального ключа (Key Pair Size): за замовчуванням (при використанні методу Diffie – Hellman/DSS) пропонують вибрати 2048 – розрядний ключ.
- Встановити термін, до якого певні ключі можуть бути використані.
- Формується додатковий ключ для розшифровування даних (Additional Decryption Key). Він належить до т. зв. "рятівних ключів" (Recovery Keys), необхідних для відновлення зашифрованих даних у випадку втрати особистого ключа.
- Генерування корпоративного ключа (Corporate Signing Key), яким буде користуватись адміністратор сервера для автоматичного підпису і встановлення довіри стосовно ваших повідомлень.
- Для адміністратора також формують ключ для анулювання ключа користувача (Designated Revocation Key).
- Створюємо ключову фразу (passphrase), в якій має бути не менше восьми символів. Можна використовувати будь-які регістри, спеціальні символи, пробіли, будь-яку мову. Якщо подобається набір наосліп, забирають позначку "Приховати надруковане" (Hide Typing), і тоді текст не відображатиметься.
- До чергового натискання кнопки "Далі" (Next) доведеться почекати: процедура генерування ключів може тривати кілька хвилин.

- Коли ключі згенеровані, треба ввійти в Internet і відіслати відкритий ключ на сервер, де вже складені ключі інших користувачів програми.

Програма PGP потребує відповідального підходу, тому вікно "PGPkeys" вдається закрити не відразу.

Можна діяти інакше: занести свій відкритий ключ на деякий сервер і в підпису свого листа вказати його адресу.

Остання комбінація <Ox5DC10B44> – це ідентифікатор ключа. Він записаний у розділі Key Properties (у вікні PGPkeys після правого кліку мишкою в рядку вибрати Key Properties), вікно ID, розділ General.

Для того, щоб підписати свій ключ, після правого кліку на особистому рядку вибирають меню Sign. Відкриється вікно POP Sign Key з необхідним рядком. Після натискання на OK у новому вікні вказують ключову фразу. Наступний клік на OK, і ключ підписано.

PGPkeys. Вибравши цей рядок, отримують доступ до таблиці особистих і загальних ключів, а також відкритих ключів кореспондентів. Якщо ключі не згенеровані, вибирають PGPkeys і створюють їх.

Верхній рядок меню в таблиці PGPkeys надає додаткові можливості. Наприклад, можна додати нові пункти в опис ключів (View):

- ідентифікатор ключа (Key ID),
- рівень довіри,
- дату створення (Creation Date),
- дату знищення (Expiration Date),
- асоційованість з додатковим ключем (ADK).

PGPtools. Активізує таблицю інструментів PGP.

Отже, програма PGP інстальована, пара ключів згенерована, відкритий ключ відіслано. Коли прийде відповідь на послання, яка містить відкритий ключ абонента, виділяють мишкою відкритий блок від BEGIN PGP до END PGP, запам'ятовують його в буфері, клікаючи на іконку з замочком, вибирають Add Key from Clipboard і натискають на Import. Ми одержали відкритий ключ. Маючи від абонента зашифроване повідомлення або файл, розшифровують його через буфер обміну (Decrypt & Verify) або після правого клікання по файлу.

PGPfone (Pretty Good Privacy Phone) – програма, яка дає змогу перетворити комп'ютер чи ноутбук у секретний телефон. У програмі використано компресію аудіоданих і потужні криптографічні протоколи, є можливість безпечно проводити розмови в режимі реального часу. PGPfone приймає голос, використовуючи мікрофон, оциф-

ровує та шифрує сигнал і передає його через модем на інший комп'ютер, на якому також працює програма PGPfone. Всі криптографічні та компресійні протоколи працюють швидко і непомітно, забезпечуючи простий користувальний інтерфейс; передбачена робота з модемом та в мережі Internet.

Зашифрована інформація передається в діапазоні 4 410–11 025 Гц. Під час шифрування голосової інформації є можливість вибору трьох алгоритмів шифрування (Cast, Blowfish, та потрійний DES) та їхніх комбінацій. Також користувачу надана можливість вибору величини ключа для шифрування (768–4096 біт). Схема з'єднання двох користувачів є простою: один із співрозмовників робить дзвінок, а інший приймає виклик.

Вимоги до конфігурації ПК для нормальної роботи PGPfone:

- мультимедійний ПК з ОС типу Windows;
- процесор – не нижче 486 МГц (Pentium рекомендовано);
- звукова карта, мікрофон, акустична система або навушники.

Перед запуском програми потрібно перевірити мікрофон та навушники (це можна зробити, використовуючи стандартні Windows – програми типу "Звукозапис"). Після перевірки потрібно запустити PGPfone, вибрати тип з'єднання (Internet, modem) та встановити зв'язок, увівши у відповідне поле IP-адресу (якщо тип з'єднання – Internet). Окрім цього, можна вибрати ступінь компресії, алгоритм шифрування (CAST, Blowfish, TripleDES, або жодний), ступінь шифрування. Залежно від вибраних параметрів змінюватиметься якість зв'язку (зі збільшенням значення частоти дискретизації якість сигналу покращується) та час затримки (залежить від вибраного алгоритму та ступеня криптування).

1.4. Прикладні застосування криптографічних методів

Криптографічний захист інформації в телефонії. Найефективнішим способом захисту телефонних повідомлень є їхнє криптографічне перетворення. Таке перетворення застосовують до самого повідомлення $X(t)$ чи до його амплітудно–частотного спектра $S(t)$. Найпростішим способом криптографічного перетворення аналогових телефонних повідомлень є розділення $X(t)$ на частини і передання цих частин у визначеному порядку в каналі зв'язку (тимчасові переставляння частин повідомлення $X(t)$). Такий спосіб

застосовують, коли інформація не має особливої цінності. Більш високого захисту досягають перемішуванням частотних смуг або шляхом об'єднання розглянутих способів. Пристрої, що реалізують розглянуті способи, називають *скремблерами*.

Сучасний цифровий телефонний зв'язок передбачає перетворення повідомлення $X(t)$ у послідовність вузьких імпульсів, до яких застосовують відомі криптографічні перетворення і алгоритми DES, ГОСТ–28147–89.

Перетворюють нотбук (ПК) у захищений у реальному часі телефон з ідентифікацією за допомогою пакета PGP Fone, користуючись як телефонними лініями, так і каналами Internet. Звук голосу, прийнятий через мікрофон, PGP Fone послідовно оцифровує, стискує, шифрує і відсилає абонентові, який теж використовує PGP Fone. Всі криптографічні протоколи вибирають динамічно, інтерфейс подібний до звичайного телефону. Вибирають ключ для шифрування за алгоритмом PGP, отож, спеціального каналу для передання секретного ключа не потрібно. Для аутентифікації обміну ключами використовують біометричний підпис (голос), для шифрування мови – DES, Cast, Blofwish, для стискання мови – алгоритм GSM.

Криптографічний захист у стільниковій телефонії. Значним досягненням технологій безкабельних комунікацій є стільниковий телефонний зв'язок та система GPS, яка дає можливість визначати місце перебування окремої особи чи об'єкта, спостерігати за роботою обладнання на відстані.

Стільникові телефони (80% світового ринку) працюють у стандарті GSM (Global System for Mobile communication). Цифрову ситему GSM проектували як захищену систему від перехоплення, прослуховування і шахрайства. Розробляли системи захисту спецслужби країн НАТО. В основу безпеки GSM закладено три секретні алгоритми: A3 – алгоритм аутентифікації, що захищає телефон від клонування; A8 – алгоритм генерування криптоключа (важкооборотна функція, яка на основі фрагмента виходу A3 створює сеансовий ключ для алгоритму A5); A5 – алгоритм шифрування оцифрованої мови для забезпечення конфіденційності.

Як модуль ідентифікації абонента SIM (Subscriber Identity Module) – картка зберігає ідентифікаційний номер мобільного абонента IMSI (International Modul Subscriber Identity) і становить собою номер рахунку, який пізнають за допомогою конфіденційного

(PIN) коду власника. Разом з номером IMSI оператор записує на SIM-картку секретний ключ, який зберігатиметься в центрі аутентифікації.

На практиці, коли потрібно провести аутентифікацію SIM-картки, центр аутентифікації генерує випадкове число RND завдовжки 316 байтів. Центр аутентифікацій виконує алгоритм А3 за цим числом з ключем, що відповідає ідентифікаційному номеру IMSI SIM-картки, одночасно передаючи RND на стільниковий телефон. З телефону відгук передають у центр і порівнюють з попередньо обчисленим, щоб мати доступ до мережі.

Стільникові телефони мають старт-карту, що містить алгоритми А3 і А6, а в самому телефоні є чіп з алгоритмом А5. Базові станції теж мають чіп з А5 і центр аутентифікації, що використовує алгоритми А3–А8 для ідентифікації мобільного абонента і генерування сеансового ключа. З криптографічного погляду А5 реалізує потоковий шифр на основі трьох регістрів зсуву з нерівномірним рухом. Довжини регістрів становлять відповідно 19, 22, 23, що дає в сумі 64-бітний сеансовий ключ шифрування. Асоціація GSM застосовує різні за стійкістю алгоритми шифрування А5: А5/1, А5/2, А5/3, останній з яких тільки починають застосовувати. Важливим є поміщення web-сервера у SIM-картку стільникового телефону, що передбачає нові способи грошової оплати через стільниковий Internet.

Компактний сервер WebCamSIM дає змогу передавати тексти в інші стільникові телефони, а також у комп'ютери. Повідомлення відсилають через шлюз SMS (Shost Message Service). Однак вважають, за захист WebCamSIM є слабким. У нових телефонних мережах застосовуватимуться 128-бітні ключі, а не 40-бітні, як тепер.

У стандарті GSM працює, зокрема, супутникова навігаційна система GPS NAVSTAR. Вона забезпечує високоточними координатами і часом користувачів усього світу протягом 24 год/добу і є найсучаснішою радіонавігаційною системою. Система GPS MONITOR призначена для моніторингу і керування транспортними засобами з використанням супутників систем GPS і мережі GSM для передавання даних на диспетчерський центр.

Америка, Японія розвивають свої цифрові системи зв'язку.

Криптографічний захист інформації в оптичному діапазоні частот. Захищають інформацію в оптичному діапазоні частот

шляхом спектрального розділення каналів, що збільшує смугу пропускання на кілька порядків за рахунок модуляції світла частотою порядку 10^{10} Гц, тобто зміни несучого каналу (одного з чотирьох можливих) за випадковим законом. Відтак ускладнюється можливий несанкціонований аналіз побічного випромінювання.

Можливий також захист інформації за рахунок зашумлення в оптичному діапазоні і методами квантової криптографії, яка ґрунтується на доведенні теореми про неможливість клонування (копіювання) квантових станів, наприклад поляризації окремих фотонів. Спроба перехоплення (прослуховування) ключа, що передається по "квантовому каналу" (оптоволокну), неодмінно буде зареєстрована, оскільки з погляду квантової механіки вимірювання неможливо виконати, не зруйнувавши квантово-механічного стану (поляризації фотона). Отже, передавання секретного ключа абонентам стає цілком надійним, що дотепер було слабким місцем криптографії.

Нещодавно французькі вчені продемонстрували комерційну криптографічну систему, що працює на основі генератора поодиноких фотонів, передаючи секретну інформацію оптоволокном на відстань 67 км. Уперше ідею застосування квантових станів (фотонів) у криптографії запропонували в 1984 р. Ч. Веннет, Ж. Брассард (ситема ВВ84). Перспективність квантового криптоаналізу різко зросте в результаті прогресу в створенні квантових комп'ютерів. Доведено, що традиційні системи RSA та інші системи на основі квантового алгоритму будуть "зламані" за реальні часові проміжки.

Криптографічний захист комп'ютерних операційних систем. Головним і найефективнішим засобом захисту операційної системи Windows NT та інших ОС є система аутентифікації. Клієнти Windows NT обмінюються зашифрованим ідентифікатором користувача (ID) і паролями. Наприкінці 80-х років минулого століття була розроблена система мережевої ідентифікації користувачів під назвою Kerberos. Основна її мета – цілковите унеможливлення пересилання паролів мережею. Користувач уводить пароль тільки один раз, після чого йому виділяють на кілька годин квиток, що зберігається у файлі у зашифрованому вигляді. Квиток містить інформацію про користувача, час видачі, адресу машини і випадково згенерований ключ для дальшого обміну ідентифікаційною інформацією. Початковий квиток використовують для придбання

вторинних квитків, за якими може бути згаданий певний мережевий сервіс.

Криптографічний захист інформації в пластикових картках. Пластикові картки поділяють на дві головні групи – магнітні та електронні. Електронні картки з мікросхемами перспективніші: мікросхеми пам'яті (memory), лічильники (counters), мікропроцесори (smart chips).

Картки пам'яті використовують незалежну електронну перепрограмовувану пам'ять (EEPRom), яка дає можливість записувати, зберігати та зчитувати дані. Для захисту пам'яті від несанкціонованого запису в структуру кристала додають спеціальну секретну логіку, яка при правильному введенні пароля, перемикає комірку з заблокованого стану в дозволений. Картки- лічильники проектують за схемою однократного використання. Захист їхній аналогічний до попереднього. Найуніверсальніші старт-картки, що становлять собою мінікомп'ютер і можуть бути використані як електронний гаманець (e – cash), засіб зберігання електронного підпису з вбудованими елементами шифрування. Кристал такої картки складається з центрального процесора (CPU), однократно програмованої пам'яті (ROM), оперативної пам'яті (RAM), енергонезалежної перепрограмованої пам'яті (EEPROM), секретної логіки (Security Logic), інтерфейсів вводу/виводу інформації (I/O). Мікропроцесор забезпечує керування всіма елементами периферії, виконує обчислювальні операції та криптографічні перетворення. Зокрема, в чіпах таких карток розміщують криптопроцесори RSA та Triple DES.

Мікропроцесорний чіп має декілька рівнів захисту від несанкціонованого доступу до інформації, що в ньому зберігається: програмний, апаратний і технологічний.

Криптографічний захист інформації в супутниковому телебаченні. Телевізійні сигнали зі супутника приймаються будь-ким у межах великих територій, незалежно від бажання передавальної сторони.

Найширше застосовуваний метод обмеження доступу до приймання телеінформації – це неможливість приймання без спеціального декодера, що надається власником програм.

Декодер містить ключ чи спеціальну карту, які захищені від копіювання. Найпростіший захист – перекручування синхросигна-

лу, коли інформація на екрані з'являється у вигляді окремих сегментів. Декодер відновлює стандартні синхроімпульси.

Більш високої надійності шифрування досягають додаванням та інвертуванням частини сигналу. Ще складніший спосіб – зміщення в часі окремих рядків зображення, розсічення рядків і переставляння місцями розсічених частин чи рядків. Типовий спосіб шифрування – Videocrypt. На північноамериканському континенті декодери працюють в інтерактивному режимі й активізуються тільки з одержанням команди з центру керування по телефонних лініях. Такий спосіб практично унеможливлює використання "піратських" декодерів.

Принцип шифрування декодерів комерційних супутникових телеканалів полягає в створенні імпульсів синхронізації чи розгортання самого відеосигналу. У першому випадку пристрій синхронізації телеприймача не може знайти початок синхроімпульсів за рядками і полями. Для фахівців у галузі несанкціонованого доступу відновлення перекручених сигналів не становило труднощів. Це зумовило застосування цифрового оброблення відеосигналу за допомогою АЦП відповідно до алгоритму шифрування.

1.5. Комплексне застосування криптографічних перетворень, кодування і стискування інформації

Комплексне застосування трьох видів перетворення інформації дає змогу ефективніше використовувати канали зв'язку для надійного захисту інформації, що передається. Зокрема, застосування стискання інформації за алгоритмом RLL, Хоффмана, Лемпеля – Зіва та JPEC і MPEG з погляду криптографії змінює статистику вхідного тексту в бік її вирівнювання: всі символи мають однакові частотні характеристики, що суттєво утруднює криптоаналіз навіть для простих криптосистем.

Ці перетворення інформації застосовують з різною метою, зокрема: шифрування – для передавання конфіденційної інформації (зазвичай об'єм інформації не змінюється); кодування – для захисту від спотворення перешкодами в каналах зв'язку (об'єм збільшується); стискання – для зменшення об'єму даних, що їх передають чи зберігають (об'єм зменшується).

Контрольні запитання до розділу 1

1. Що таке криптографія та криптоаналіз?
2. Які Ви знаєте типи криптографічних систем?
3. Означити криптостійкість та електронний підпис.
4. Описати типову схему криптосистем.
5. Навести приклади класичних криптосистем.
6. Шифр Віженера та програмна реалізація алгоритму на прикладі шифрування за методом Цезаря.
7. Порівняти блочну та асиметричну криптографії.
8. Описати алгоритм DES.
9. Математичні основи асиметричних криптосистем. Важкооборотні функції.
10. Які основні означення дискретного аналізу та алгоритму Евкліда?
11. Алгоритм RSA.
12. Електронний підпис на основі асиметричного алгоритму.
13. Описати роботу з пакетом PGP.
14. Прикладні застосування криптографічних методів.

Розділ 2

БЕЗПЕКА ДАНИХ У КОМП'ЮТЕРНИХ МЕРЕЖАХ

Однією з головних проблем, що виникають під час проектування, встановлення та експлуатації комп'ютерної мережі, є безпека даних, оскільки перевагою мережі є доступ до спільних даних та пристроїв, а це зумовлює можливість несанкціонованого доступу до них.

Безпека даних – це захист ресурсів мережі від руйнування та захист даних від випадкового чи навмисного розголошення, а також від неправочинних змін.

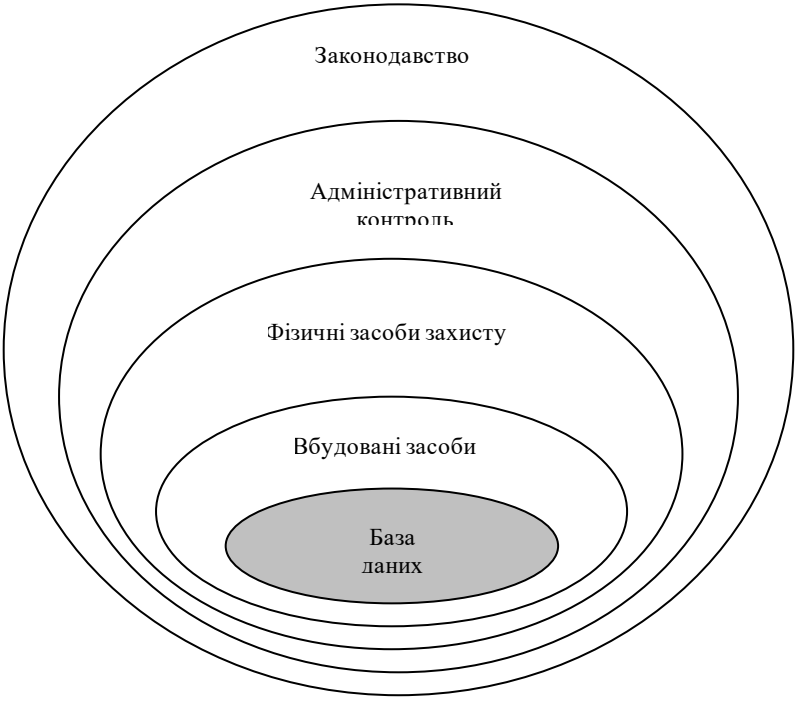


Рис. 2.1. Рівні безпеки даних

У сучасних системах захист даних реалізується на багатьох рівнях (рис. 2.1):

- вбудовані засоби захисту – програмно-системні (паролі, права доступу та ін.);
- фізичні засоби захисту – замки, двері, охорона, сигналізація тощо;
- адміністративний контроль – організаційні заходи, накази адміністрації;
- законодавство та соціальне оточення – соціальний клімат колективу, нетерпимість до несанкціонованого використання чужої інформації, комп'ютерного "піратства", закони про захист авторських та майнових прав.

У кожній інформаційній системі можна виділити найслабші з погляду безпеки місця. На них адміністратор повинен звернути увагу передусім. До таких місць зазвичай належать: сховища даних, адміністративна система, кабельна система, доступ з зовнішніх мереж.

Долають труднощі, пов'язані з безпекою даних, одночасно у трьох напрямках:

- профілактика; мінімізація ймовірності настання небажаних подій; унеможливлення несанкціонованого доступу; профілактика апаратури;
- якщо небажана подія сталася, система має бути побудована так, щоб мінімізувати шкоду, якої ця подія завдасть;
- створення процедур архівації та поновлення інформації у випадку її втрати.

Як же на практиці відбувається надання та обмеження прав доступу? Найпростіше описати цей механізм використанням таблиць чинності. Таблиця чинності відображає певну категорію об'єктів операційної системи прав доступу до ресурсів мережі: створення, використання, управління ресурсом тощо. Об'єктами можуть бути:

- окремі користувачі чи групи користувачів;
- ступінь таємності;
- прикладні програми;
- час доби;
- робоча станція;
- довільна комбінація цих об'єктів (контейнер).

Такий підхід дає змогу гнучко формулювати складні обмеження доступу (наприклад, доступ до каталогу з розважальними програмами тільки на час обідньої перерви або з певних робочих станцій). Чинні права доступу для користувача, сформовані як комбінація обмежень з таблиць чинності, названо ефективними правами доступу цього користувача.

У деяких системах (наприклад, банківських чи податкових) потрібна ідентифікація не користувача, а фізичної особи. Розрізняють кілька способів такої ідентифікації:

- за персональними фізичними ознаками (біометрія). Знімають відбиток пальця, а потім ідентифікують чинність особи. Інший спосіб: система пропонує вголос повторити певну кількість випадково вибраних слів та аналізує особливості голосу. Такі системи досить надійні, однак значно дорожчі за традиційні;
- за предметом, який особа-користувач носить з собою. Таким предметом може бути спеціальний значок, магнітна картка з кодом. Цей спосіб є дешевим, проте ненадійним, предмет можна підробити, вкрасти тощо;
- за тим, що особа повинна знати або пам'ятати. Треба пам'ятати пароль або правильно відповісти на низку питань. Цей метод найдешевший і найпоширеніший, але ненадійний (пароль можна підібрати, відповіді вгадати).

Запропоновані методичні вказівки до виконання лабораторних робіт з розділу захист інформації в комп'ютерних мережах стосуються першого рівня (рис. 2.1) схеми захисту, а саме: вбудованих засобів захисту.

Перша лабораторна робота присвячена програмному та апаратному забезпеченню, що його використовують для побудови гетерогенних (з різними операційними системами) комп'ютерних мереж. Для її виконання потрібно ознайомитися з сучасним пасивним та активним мережевим обладнанням і засвоїти практичні навики реалізації прямого, віддаленого та множинного з'єднання комп'ютерів у мережі, а також безпечного розподілу їхніх ресурсів.

Інформаційний захист мережі від зовнішніх втручань (intrusions) здійснюється з використанням брандмауерів та серверів–посередників (proxy–серверів). Питанням конфігурації брандмауерів в ОС UNIX присвячена наступна лабораторна робота.

Вивченню вбудованих засобів захисту трьох поширених операційних систем, що мають розвинені засоби підтримки мереж, а саме: Novel NetWare, Windows NT та UNIX, відведені три лабораторні роботи.

Остання лабораторна робота стосується деяких питань захисту однієї з найпопулярніших послуг Інтернету – електронної кореспонденції (E–mail).

2.1. Технології з'єднань комп'ютерів

Фізичне підключення двох ПК. Більшість ПК має один або декілька послідовних портів. Їх можна використовувати для підключення будь-якого пристрою з інтерфейсом RS–232–C і для зв'язку або управління. В цьому розділі ми розглянемо, як підключити інтерфейс RS–232–C для забезпечення зв'язку типу ПК – ПК, термінал – ПК і модем – ПК.

Почнемо з розгляду базової моделі RS–232–C, показаної на рис. 2.2. Ця модель ілюструє, як можуть з'єднуватися один з одним два ПК і/або термінали

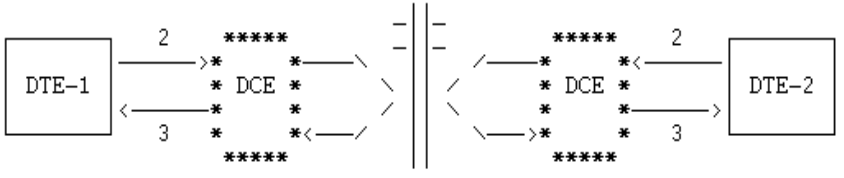


Рис. 2.2. Стандартна модель інтерфейсу RS–232–C

через модеми телефонними лініями або прямим зв'язком. Хоча дальше обговорення ми ведемо переважно в термінах телефонних з'єднань, ті ж базові принципи стосуються і прямого зв'язку, за винятком того, що комунікаційні пристрої (DCE, Data Communication Equipment) в цьому випадку не потрібні.

На кожному кінці знаходяться термінальні пристрої, т. зв. DTE (Data Terminating Equipment). В ролі DTE може виступати термінал, наприклад, VT–100, або центральний процесор мікро-, міні або великої ЕОМ.

У кожному термінальному пристрої DTE має бути використаний комунікаційний пристрій DCE (Data Communication Equipent), який зазвичай називають модемом, для модуляції і демодуляції

сигналів, які проходять по телефонних лініях. Кожний DTE використовує вивід 2 для передавання даних і вивід 3 для отримання даних. Оскільки те, що передано з виводу 2 на кожній машині, приймається на виводі 3 іншої машини, виникає перехрещення телефонних ліній між пристроями DCE.

Під'єднання й оброблення сигналу між DTE і DCE повністю відповідають стандарту RS–232–C. Апаратний протокол дає можливість DTE використовувати DCE для надсилання і приймання даних від іншого DTE.

Кабель, що зв'язує фізично DTE і DCE, називається "прямим" кабелем. Завдяки йому пристрій DTE посилає команди (або сигнали з виводів) на DCE, а пристрій DCE відправляє команди назад на DTE. Підключення DCE однієї машини до DCE іншої машини відбувається через звичайні телефонні лінії.

Пристрої DCE необхідні з тієї причини, що пристрої DTE є цифровими, а телефонні лінії – аналоговими. Єдиний спосіб передати цифрову інформацію аналоговими лініями – закодувати цифрову інформацію в аналоговий сигнал, послати цей сигнал по телефонних лініях, а потім декодувати аналоговий сигнал у цифрову інформацію.

Підключення без комунікаційних пристроїв. Якщо машини розміщені досить близько (в межах 15 метрів), то не потрібен модем, є можливість використовувати кабель "нуль-модема".

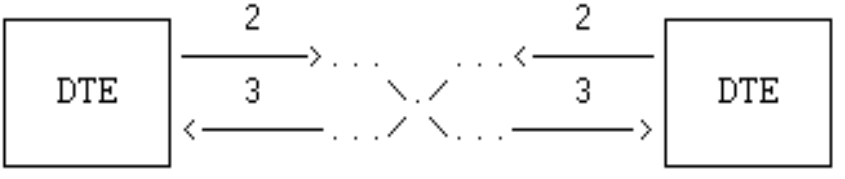


Рис. 2.3. Конфігурація з'єднання нуль–модемом

Кабель нуль-модема імітує такий же протокол, що і DCE, але не потребує наявності модема для комунікацій. Основна задача підключення нуль-модема – забезпечити перехрещення між передаючими і приймаючими сигналами. На рис. 2.3 показана загальна схема підключення без пристроїв DCE.

Для того, щоб виконати підключення, яке імітує DCE, потрібні деякі маніпуляції з сигналами. Ці маніпуляції також стандартизовані в кабелі нуль-модема. За схемою цього кабелю, зображеного на рис. 2.4, розглянемо, як він імітує сигнали DCE.

Лінії 1 і 7 використовують для шасі і сигнальної землі. Лінії 2 і 3 перетинаються так, що коли одна сторона говорить, інша слухала. Обидві сторони можуть говорити одночасно (режим Full Duplex), якщо використовувати різні набори дротів.

Для імітації управляючих сигналів лінії 4, 5 і 8 приєднують так, щоб кожного разу, коли пристрій DTE–1 активізує лінію “Request To Send” (“запит на передавання”), тобто передає по ній сигнал, він одержував сигнал “Clear To Send” (“готовий до передавання”), який свідчить про те, що відповідь інша сторона готова прийняти. Потім, посилаючи сигнал по лінії “Data Carrier Detect” (“виявлення потоку даних”), пристрій DTE–1 повідомляє іншу сторону, що надходять дані. Таке методичне “апаратне рукостискання” гарантує, що ніякі дані не будуть відправлені, поки інша сторона не буде готова їх прийняти.

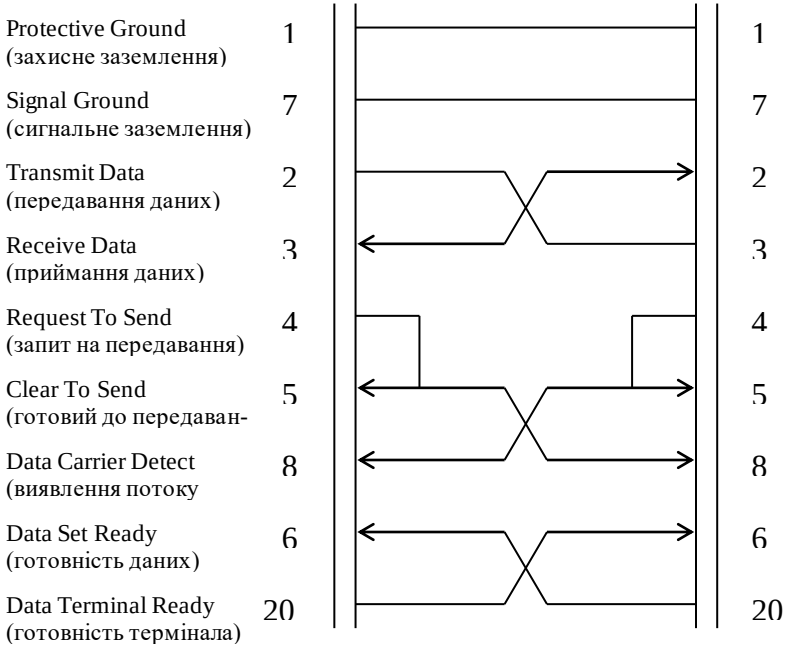


Рис. 2.4. Кабель нуль-модема RS–232–C

Лінії 6 і 20 приєднують таким чином, щоб забезпечити решту управляючих сигналів нуль-модема. Поки DTE активний (“Data Terminal Ready” – “готовність терміналу”, лінія 20), інша сторона вважає, що має справу з активним модемом (“Data Set Ready” –

“готовність даних”, лінія 6). При такому способі з’єднання ліній 6 і 20 кожного разу, коли висмикнути кабель з ПК або перемкнути його на інший канал сполучної коробки, інша сторона втрачає сигнал активності і відключається (або генерує сигнал HUP – Hangs UP, повісити трубку). Щоб зробити такий кабель, який не спричиняє відключення при вийманні штепселя (тобто NOHUP), слід приєднати вихід “Data Terminal Ready” до входу “Data Set Ready” на тому ж пристрої DTE. Це примушує систему повідомляти самій собі, що модем завжди готовий.

Зауважимо, що хоча схема підключення нуль-модема є рекомендованою, але відомі й інші способи. У кожному конкретному випадку для нуль-модемів враховують певне оточення або функцію, наприклад, наявність безобривного (nohup) варіанта підключення. Розглянемо способи комунікацій і типи найчастіше використовуваних підключень.

Дистанційне підключення. Альтернативою прямому підключенню є дистанційне підключення через модемну лінію, показане на рис. 2.5. Установка термінала або конфігурація ПЕОМ виглядають приблизно так само, як і у попередньому випадку, за винятком швидкості обміну, на якій працює термінал. Для більшості модемів вона має бути не менше 1 200 бод. Термінал (коли він встановлений на 1 200 бод) “спілкується” безпосередньо з модемом. Водночас задіяні модемні команди “набрати телефонний номер” (dial), “повісити трубку” (hang) і т.д. ПЕОМ, що запускає комунікаційне програмне забезпечення, звичайно має команду набору номера, яка генерує команду для модема. З’єднання між терміналом/ПЕОМ і модемом має бути виконано у вигляді прямого кабелю. Модем має також телефонний кабель, що йде в телефонну систему.

Підключення по виділеній лінії. Одна з технологій для одночасної голосової телефонії, інтерактивного відео і передавання даних з великою швидкістю – FTTN (Fiber all the way To The Home) – це високошвидкісна цифрова абонентська лінія, або VDSL (Very high rate Digital Subscriber Line). VDSL передає дані з великою швидкістю по витій парі мідних телефонних ліній, не приєднаних до апаратури АТС (виділена лінія), з рядом швидкостей, залежних від фактичної довжини лінії. Максимальна швидкість у 55 Мб/с досягається для ліній довжиною до 300 метрів та 13 Мб/с – до 1 500 метрів (рис. 2.6).

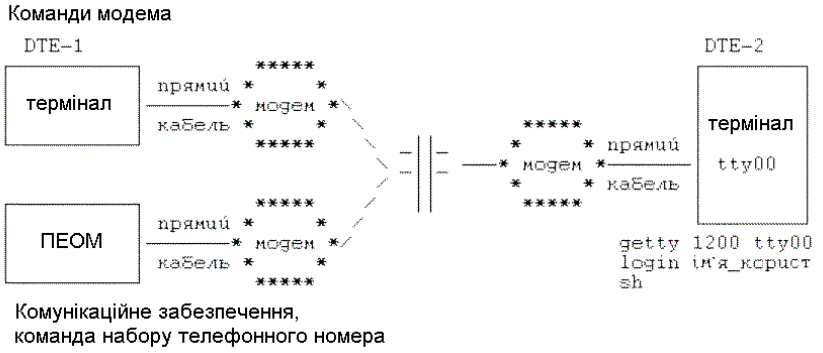


Рис. 2.5. Дистанційне підключення терміналів і ПЕОМ (DTE–1) до термінала ПК (DTE–2)

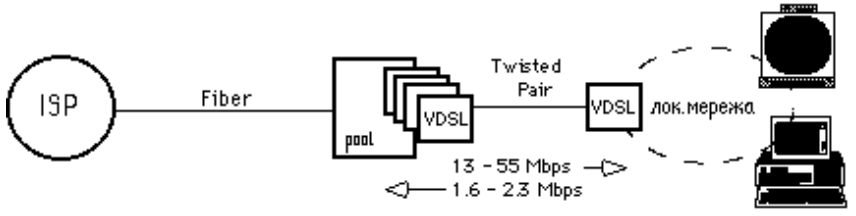


Рис. 2.6. Дистанційне підключення за допомогою технології VDSL

VDSL знаходиться все ще в стадії вивчення; не досить відомі особливості впливу телефонної лінії, радіоемісія, придатність для мультиплексного з'єднання та інформаційні вимоги для створення набору стандартних властивостей.

Локальні мережі множинного доступу. Безумовно, найпопулярнішим стандартом у мережі з магістральним організуванням передавального середовища (множинного доступу) з тих, що використовуються на сьогодні є стандарт Ethernet (IEEE 802.3). Мережі Ethernet працюють зі швидкістю 10 Мбіт/с або 100 Мбіт/с (новий стандарт – Fast Ethernet). Ethernet пропонує краще співвідношення продуктивність / вартість, високу гнучкість при налаштуванні і нарощуванні потужностей, а також відносну простоту в експлуатації.

У Ethernet використовують метод передавання даних, відомий як CSMA/CD (Carrier Sense Multiple Access with Collision Detection – метод доступу з прослуховуванням інформації і виявленням зіткнень). Перед відправленням даних мережею вузол спочатку "прослуховує", чи не надходить в цей момент інформація якого-небудь

іншого вузла. Якщо ж по мережі передається якась інформація, вузол, який намагається відправити дані, чекає якийсь час і потім знову повторює спробу.

Є декілька типів Ethernet, що їх використовують сьогодні:

- 10Base5 (Thicknet – товстий Ethernet)
- 10Base2 (Thinnet – тонкий Ethernet)
- 10BaseT (UTP – вита пара)
- 100BaseTX, 100BaseT4 (Fast Ethernet)
- 100BaseFX (оптоволокно).

Дозволено змішувати різні стандарти Ethernet. Наприклад, якщо концентратори, які використовують як точки центрального з'єднання для комп'ютерів у мережі UTP Ethernet також містять порт BNC, це дає змогу використовувати сегмент кабелю тонкого Ethernet (thinnet) для з'єднання різних концентраторів.

Основні правила, встановлені між двома вузлами мережі Ethernet:

- може бути сполучено до п'яти мережевих сегментів підряд;
- може бути до чотирьох повторювачів / концентраторів;
- може бути до трьох заповнених сегментів (в описаному випадку тонкий Ethernet).

Наявні в лабораторії типи мереж Ethernet:

10Base2 (Thinnet), або тонкий Ethernet, – це дуже відомий тип Ethernet (особливо, для малих мереж). У тонкому Ethernet використано топологію шини, що складається з коаксіального кабелю RG58A/U з навантаженням 50 Ом на кожному кінці (термінатором).

Комп'ютери підключають до сегмента кабелю тонкого Ethernet за допомогою Т-подібних BNC-конекторів, які вставлено безпосередньо в плату мережевого адаптера Ethernet.

До тонкого Ethernet застосовують такі правила:

- максимальна довжина кабельного сегмента (відстань між двома обмежувачами-термінаторами з навантаженням по 50 Ом) не більше 185 м;
- кожний сегмент мережевого кабелю має навантаження в 50 Ом на обох кінцях;
- максимальне число вузлів на сегмент не більше 30;
- довжина відрізка кабелю між мережевими адаптерами не менше 2 м;

- максимальне число вузлів у мережі не більше 1 024;
- максимальна відстань між двома вузлами не більше 1 425 м.

10BaseT/UTP (Unshielded Twisted Pair – неекранована вита пара), або просто вита пара, призначена для нових мереж. UTP використовує топологію зірки, де кожний вузол підключають до концентратора (Hub), або комутатора (Switch). Комутатор є центральною точкою з'єднання; можна об'єднати декілька розподільників. Кабель, використовуваний для UTP, складається з двох неекранованих витих пар і часто його називають кабелем категорії 3; він підтримує швидкість до 10 Мбіт/с (кабель категорії 5 також може бути використаний і він з відповідним устаткуванням може підтримувати швидкість до 100 Мбіт/с).

До витої пари застосовують такі правила:

- довжина кабельного сегмента між вузлом і розподільником не більше 100 м;
- у з'єднанні RJ–45 використано напряму сполучені контакти 1, 2, 3 і 6, причому контакти 1 і 2 – передаючі, а контакти 3 і 6 – приймаючі;
- до центрального комутатора може бути підключено до 12 інших комутаторів;
- у мережі витої пари може бути не більше 1 024 робочих станцій (без використання мостів).

100BaseTX, або 100BaseT, чи швидкий Ethernet (Fast Ethernet), за топологією подібний 10BaseT, з тією лише різницею, що він працює зі швидкістю 100 Мбіт/с замість 10 Мбіт/с. 100BaseT, як і 10BaseT, використовує дві неекрановані виті пари, але, щоб підтримувати швидкість в 100 Мбіт/с для нього необхідний кабель категорії 5 і строге дотримання стандартів обтискання. Для роботи зі швидкістю 100 Мбіт/с мережевий адаптер, як і концентратор, має підтримувати 100BaseTX. 100BaseTX також підтримує більш повільний стандарт (10 Мбіт/с), у результаті можна використовувати 100 BaseTX – адаптери в мережі 10BaseT (100BaseTX – адаптери працюватимуть зі швидкістю 10 Мбіт/с замість 100Мбіт/с).

Лабораторна робота № 2.1. Програмне та апаратне забезпечення з'єднання ПК

Мета роботи: ознайомитися з пасивним та активним мережевим обладнанням і засвоїти практичні навики реалізації прямого, віддаленого та множинного з'єднання комп'ютерів для розподілу їхніх ресурсів.

Прилади та матеріали:

- кабель для прямого з'єднання двох ПК і тестер;
- фрагменти тонкого коаксіального кабелю з BNC-трійниками, BNC-конекторами та термінаторами, фрагменти кабелю "вита пара" з UTP-конекторами RJ-45 і мережний концентратор (HUB) та мережевий тестер;
- телефонний кабель з конекторами RJ-12 і модеми для комутованої та виділеної ліній.

Хід виконання роботи.

1. З'єднати два ПК прямим кабельним включенням, для цього:
   - перевірити за допомогою тестера правильність розпайки кабелю для прямого з'єднання двох ПК через їхні зовнішні порти – послідовний (**COM**) чи паралельний (**LPT**);
   - з'єднати через зовнішні порти два вимкнені ПК та увімкнути їх;
   - в оболонці NC вибрати **F9 → Link → потрібний порт**, режим **Master** для першого ПК та **Slave** для другого; одночасно на обох ПК натиснути ***<Enter>;***
   - заміряти швидкодію з'єднання, передаючи довільні файли об'ємом не менше 100 КБ, порівняти отримані результати зі швидкістю передання даних у порті ПК.
2. З'єднання множинного доступу за допомогою тонкого коаксіального кабелю та кабелю "вита пара".

2.1. З'єднати групу ПК за допомогою тонкого коаксіального кабелю, для цього:

- перевірити за допомогою мережевого тестера як функціональність кожного сегмента коаксіалу зокрема, так і мережі загалом;
- з'єднати за допомогою коаксіальних кабелів BNC-коне-

ктори мережевих адаптерів групи вимкнених ПК та увімкнути їх;

- перевірити правильність налаштування параметрів отриманої мережі: **Start → Settings → Control Panel → Network →** закладка **Configuration: TCP/IP → Properties,** та закладка **Identification**: **Computer name** та **Workgroup**;
- заміряти швидкодію з'єднання, передаючи довільні файли об'ємом не менше 10 Мб, порівняти отримані результати з максимальною швидкістю передання даних у 2 Мб/сек для такого типу мереж.

2.2. З'єднати групу ПК за допомогою кабелю "вита пара" та мережевого концентратора, для цього:

- перевірити за допомогою мережевого тестера функціональність кожного фрагмента "витої пари" і мережі загалом;
- з'єднати за допомогою "витої пари" UTP-конектори мережевих адаптерів групи вимкнених ПК з концентратором та увімкнути їх;
- перевірити правильність налаштування параметрів отриманої мережі як в п. 2.1;
- заміряти швидкодію з'єднання, передаючи тестовий файл об'ємом не менше 100 МБ, порівняти отримані результати з максимальною швидкістю передання даних у 10/100 Мб/сек для такого типу мереж;
- при наявності режиму Full Duplex у мережевих адаптерів – повторити вимірювання за попереднім завданням в цьому режимі (**Start → Settings → Control Panel → Network → Properties → Additional → Full Duplex Mode: AutoDetect / Enable / Disable**).

3. З'єднати два ПК за протоколом PPP (Point-to-Point Protocol – протокол "точка–точка").

3.1. Приєднатися до віддаленого ПК за допомогою хомутова ного з'єднання, для цього:

- перевірити за допомогою мережевого тестера справність телефонного кабелю;
- підключити при вимкненому ПК модем до відповідного COM-порту за допомогою стандартного шлейфа, підключити телефонний кабель до роз'єма LINE та увімкнути живлення модема;
- увімкнути ПК, та перевірити справність підключення мо-

дема, для цього на панелі керування вибрати пристрій **Modem**: на вкладці **General** вибрати потрібний модем та переглянути його властивості (General: порт COM1 чи COM2, швидкість з'єднання 38 400 кб/сек; Connection: Data bits – 8, Parity – None, Stop bits – 1, та **Advanced** – Use flow control: Hardware (RTS/CTS); на вкладці **Diagnostics** вибрати потрібний порт та виконати операцію "опитування" модема (More info). Отримавши перелік характеристик та доступних команд модема, констатуємо його правильне функціонування;

- підключитися до Інтернет-провайдера (ISP): **Start → Program → Accessories → Communications → Dial–Up Networking,** вибрати вказане викладачем з'єднання, що потребує аутентифікації: User name, Password та Phone number;
- після встановлення з'єднання, заміряти його швидкодію за допомогою отримання за протоколом FTP довільних файлів об'ємом не менше 10 КБ; порівняти отримані результати зі швидкістю з'єднання та швидкістю передання даних у порті ПК.

3.2. Приєднатися до віддаленого ПК за допомогою VDSL-з'єднання по виділеній лінії, для цього:

- встановити FTP-сеанс з сервером провайдера, IP-адреса якого задана;
- заміряти швидкодію з'єднання, отримавши довільні файли об'ємом не менше 500 КБ, порівняти отримані результати зі швидкістю передання даних VDSL-з'єднання.

2.2. Інформаційний захист мережі з використанням брандмауерів та серверів-посередників

Захист інформації у мережі від зовнішніх втручань здійснюють, використовуючи брандмауери та сервери-посередники (рис. 2.7).

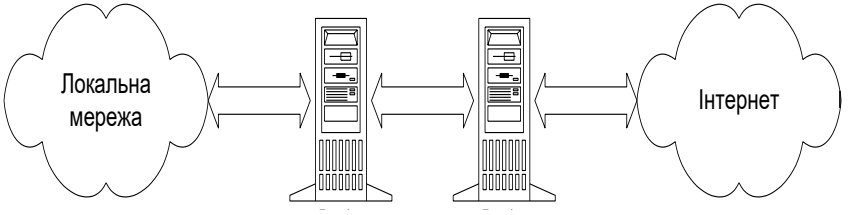


Рис. 2.7. Брандмауер та сервер-посередник

Первинне значення терміна брандмауер (firewall) – це стіна у будівлі, зроблена з вогнетривких та незаймистих матеріалів, яка має перешкодити поширенню пожежі. У комп'ютерній мережі **брандмауер** – це комп'ютер з програмною системою, який ставлять на межі внутрішньої мережі і який перепускає тільки авторизовані певним чином пакети.

Найчастіше брандмауери захищають внутрішню корпоративну мережу від несанкціонованого доступу із зовнішньої мережі. Однак їх можна використовувати для фільтрування вихідної інформації, обмеження доступу користувачів внутрішньої мережі назовні.

Брандмауери застосовують різні алгоритми фільтрування, вони мають різні ступені захисту та вартість. З метою класифікації брандмауерів їхню роботу описують з використанням семи рівнів еталонної моделі взаємодії відкритих систем (OSI).

Розрізняють:

- брандмауери з фільтруванням пакетів (Packet Filtering Firewall), які працюють на канальному та мережевому рівнях);
- шлюзи рівня сеансу (Circuit Level Gateway); працюють на рівні розпізнання сеансу;
- шлюзи рівня застосувань (Application Level Gateway); фільтрують інформацію згідно з програмними застосуваннями);
- брандмауери експертного рівня (Stateful Inspection Firewall); виконують функції брандмауерів усіх нижніх рівнів.

Вважають, чим вищий рівень роботи брандмауера, тим більший рівень захисту, який він забезпечує, і тим більша його вартість.

Брандмауери з функцією фільтрування пакетів працюють разом з апаратним або програмним маршрутизатором. Вони аналізують IP-заголовки пакетів і на підставі інформації у них та своєї таблиці

правил приймають рішення про проходження пакета чи його відкидання.

Брандмауери порівняно дешеві, вони можуть дещо затримувати передавання повідомлень. Часто функції фільтрування пакетів інтегрують у маршрутизатори. Водночас рівень захисту у таких брандмауерів незначний – кваліфікований зловмисник може підмінити адресну частину IP-пакета.

В ідеальному випадку брандмауер має бути прозорим (непомітним) для клієнтів мережі. Це означає, що він не спричиняє суттєвої затримки в передаванні інформації, не потребує від клієнтів спеціальної реєстрації на брандмауері, відокремленої від реєстрації користувача в мережевій ОС. На практиці вимога прозорості брандмауера тою чи іншою мірою порушується.

Інколи функції брандмауера в складних системах розподілені між брандмауерами та серверами-посередниками (proxy-серверами). У чому ж різниця між цими серверами? Брандмауер традиційно захищає мережу від зовнішніх втручань. Він фільтрує кадри канального рівня, розпізнає сеанс, який відкриває зовнішній користувач. Сервер-посередник контролює та обмежує вихід внутрішнього користувача назовні, а також часто є його представником. Функції сервера-посередника такі:

- приховати адреси внутрішніх станцій, подаючи всю мережу назовні як один комп'ютер з адресою сервера;
- зберігати популярні web-сторінки, файли так, щоб користувачі не були змушені звертатися до зовнішньої мережі при повторному запиті. Популярну інформацію сервер оновлює автоматично з визначеною періодичністю.

Конфігурація брандмауера в ОС UNIX. У UNIX легко встановити заснований на правилах фільтрування IP-пакетів мережевий захист. Можна захистити тільки один ПК або всю мережу.

Типи мережевого захисту мають бути "клієнтом" ("client"), щоб забезпечити єдину автономну машину, або "простий" ("simple") для входу, що охороняє внутрішню мережу.

Важливе зауваження: мережевий захист UNIX розробляють максимально безпечним за замовчуванням. Отож, якщо не додають ніяких правил, то заборонені будуть всі пакети. Може виявитися, що неможливо дістатися до машини користувача через мережу, тому доводиться реєструватися з консолі ПК. Мережевий захист також запобігає новим зв'язкам із зовнішньою частиною

мережі за винятком декількох протоколів, як наприклад, електронна пошта), що унеможливлює такі звичні мережні протоколи, як FTP, telnet тощо.

Може виявитися, що користувачеві не сподобається консервативний набір правил за замовчуванням. Якщо це так, легко зробити індивідуальний. Перша річ, яку можна зробити, це – дозволити зв'язки через **ssh** (**ssh** – це безпечна заміна **telnet** / **rlogin**, її можна знайти за адресою http://www.openssh.org). Там, де в наборі правил говориться "Дозволити отримувати електронну пошту", потрібно додати подібне правило для **ssh** за допомогою заміни номера порту 25 на 22. Або можна зробити повністю новий набір правил. Тут наведено два фрагменти наборів правил для типового клієнта ("client") і для мережі ("simple"):

Набір правил firewall для окремого ПК:

```
# Встановити IP адресу сервера
    ip="194.44.198.193"
    setup_loopback
# Дозволити весь вихідний потік із сервера
    $fwcmd add allow all from $ip to any out
# Заборонити вихідний потік з будь-яких інших адрес
    $fwcmd add deny log all from any to any out
# Дозволити пакети для яких вже встановлено TCP з'єднання
    $fwcmd add allow tcp from any to any established
# Дозволити фрагментовані IP-пакети
    $fwcmd add allow all from any to any frag
# Дозволити пакети, які ініціюють з'єднання ftp, ssh, email, tcp–dns, http
    $fwcmd add allow tcp from any to $ip 21 setup
    $fwcmd add allow tcp from any to $ip 22 setup
    $fwcmd add allow tcp from any to $ip 25 setup
    $fwcmd add allow tcp from any to $ip 53 setup
    $fwcmd add allow tcp from any to $ip 80 setup
```

Набір правил Firewall для мережі:

```
# Опис зовнішнього інтерфейсу
    oif="fxp0"
    onet="194.44.198.192"
    omask="255.255.255.224"
    oip="194.44.178.193"
# Опис внутрішнього інтерфейсу
```

iif=”fxp1”
inet=”192.168.2.19”
imask=”255.255.255.0”
iip=”192.168.2.119”
setup_loopback

Трансляція мережевих адрес (natd) розміщена після правил перевірки # адрес з тим, щоб пакети зі станцій внутрішньої мережі (192.168.x.x) # транслювалися natd після того, як вони будуть відкинуті правилами # заборони (deny) перед цим.

case $natd_enable in
[Yy][Ee][Ss])
if [–n “$natd_interface”]; then
$fwcmd add divert natd all from any to any via $natd_interface
fi ;;
esac

Дозволити всі пакети у внутрішній мережі
$fwcmd add allow all from any to any via $iif
Дозволити всі пакети назовні
$fwcmd add allow all from $onet:$omask to any out via $oif
Заборонити всі пакети назовні з інших підмереж
$fwcmd add deny log all from any to any out via $oif
Дозволити пакети для яких вже встановлено TCP з’єднання
$fwcmd add allow tcp from any to any established
Дозволити фрагментовані IP-пакети
$fwcmd add allow all from any to any frag
Все інше заборонити і протоколювати
$fwcmd add deny log all from any to any

Лабораторна робота № 2.2. Методика захисту мережі за допомогою брандмауера

Мета роботи: реалізувати на практиці методику захисту мережі за допомогою брандмауера.

Хід виконання роботи.

1. За набором правил брандмауера лабораторії, налаштованого на сервері доступу до ресурсів Інтернету, встановити

чинність доступу робочих станцій до ресурсів внутрішньої мережі та до ресурсів Інтернету:

```
# Загальні правила брандмауера
pipe 171 config bw 8000 queue 100
pipe 172 config bw 8000 queue 100
add 00100 allow ip from any to any via lo0
add 00200 deny ip from any to 127.0.0.0/8
# Дозволи для SSH-протоколу
add 00400 allow tcp from any to 192.168.2.119 22 in recv any
add 00410 allow tcp from 192.168.2.119 22 to any out xmit any
# Внутрішня мережа
# вхідні
add 10040 deny udp from 192.168.1.0/24 137,138 to not
 192.168.1.0/16 137,138
add 10503 allow tcp from any to 192.168.2.119 25,110,143
add 10505 deny ip from 192.168.1.128/25 to any
add 10511 pipe 171 ip from 192.168.1.0/25 to any
add 10900 allow ip from any to any
# вихідні
add 15503 allow tcp from 192.168.2.119 25,110,143 to any
add 15505 deny ip from any to 192.168.1.128/25
add 15511 pipe 172 ip from any to 192.168.1.0/25
add 15900 allow ip from any to any
# INTERNET
# вхідні
add 40505 allow udp from any 53 to 192.168.2.119 1053
add 40506 allow udp from any to 192.168.2.119 53
add 40507 allow tcp from any to 192.168.2.119 53
add 40508 allow tcp from 194.44.198.32/27 to 192.168.2.119 25
add 40510 divert 8668 ip from any to 192.168.2.119
add 40900 allow ip from any to 192.168.2.119
# вихідні
add 45505 allow udp from 192.168.2.119 1053 to any 53
add 45506 allow udp from 192.168.2.119 53 to any
add 45507 allow tcp from 192.168.2.119 53 to any
add 45508 allow tcp from 192.168.2.119 25 to 194.44.198.32/27
add 45520 divert 8668 ip from any to any
add 45900 allow ip from 192.168.2.119 to any
```

Заборонити все інше
add 65500 deny log ip from any to any

2. Динамічно задати тимчасові правила обмеження ширини каналу (pipe) та повної заборони на вхідні/вихідні пакети для вказаних викладачем станцій та сегментів внутрішньої мережі за допомогою процедури **ipfw**. Заміряти реальну швидкодію каналу за допомогою ftp-з'єднання з вказаних станцій.
3. Відновити початковий набір правил брандмауера.

2.3. Захист ресурсів у мережевій ОС Novel NetWare

Мережа NetWare – це група ПК (файл-серверів та робочих станцій) і принтерів, які з'єднані разом так, що їх користувачі можуть використовувати спільні ресурси.

Файл-сервер – це ПК, на якому встановлена операційна система NetWare, що керує мережею. Файл-сервер координує роботу всіх робочих станцій і регулює, хто з користувачів може мати доступ до потрібних ресурсів, хто може змінювати дані.

Можливість працювати в мережі отримують замовники, попередньо зареєстровані як користувачі мережі.

Є чотири рівні доступу до ресурсів мережі:

- звичайні користувачі мережі;
- оператори файл-серверів;
- менеджери підгруп та менеджери обліку;
- адміністратори мережі.

Вся інформація мережі NetWare зберігається на жорсткому диску, який знаходиться на файл-сервері. Тим не менше, не всі користувачі можуть мати доступ до повної інформації (наприклад, до файлів обліку). Також користувачі не завжди можуть одночасно мати доступ до одних і тих же даних, бо інакше вони впливатимуть на роботу один одного.

Щоб запобігти таким проблемам, NetWare передбачає потужну систему безпеки, яка захищає користувачів від пошкодження даних в мережі й унеможливлює несанкціонований доступ до заборонених файлів.

Система безпеки NetWare складається з таких компонентів:

- система реєстрації (керує обліковими записами, які включають імена користувачів, їхні паролі та набір прав і обмежень користувача в мережі);
- систему привілеїв, які надають користувачам дозвіл працювати з ресурсами;
- атрибути, призначені каталогам і файлам.

Система NetWare дає можливість забезпечувати високий ступінь захисту інформації, збереженої на мережевих томах, а також контроль за тим,

- хто може звертатися до мережевих каталогів;
- до яких каталогів і файлів можуть звертатися користувачі;
- що користувачі можуть робити з каталогами і файлами;
- хто може виконувати задачі на консолі файл-сервера.

Захист в ОС NetWare має три рівні:

- захист входу користувача в систему;
- захист за допомогою схеми прав власності;
- захист за допомогою схеми атрибутів.

Захист входу в систему керує доступом до ресурсів мережі: тут визначається, які користувачі можуть працювати на файл-сервері, коли вони можуть працювати, на яких робочих станціях і які ресурси можуть використовувати.

Мережевий адміністратор встановлює захист входу в систему, використовуючи три інструментальні засоби:

- usernames (імена користувачів);
- passwords (паролі);
- restrictions (обмеження).

Тільки мережеві адміністратори і менеджери робочих груп можуть створювати нові імена користувачів. Усім новоствореним користувачам призначені паролі і членство в групі EVERYONE.

Використовують три типи обмежень входу в систему:

- з яких робочих станцій може входити в систему користувач;
- в який робочий час користувачі можуть увійти в систему;
- якщо перевищені квоти робочого простору чи ін., обліковий запис користувача блокується системою аж до втручання адміністратора мережі.

Захист за допомогою схеми прав власності визначає, до яких каталогів, підкаталогів і файлів користувач має доступ і як саме він може ними розпоряджатися.

Захист правами визначено довірчими правами та маскою успадкованих прав, які містять однакові вісім атрибутів:

- контролю (Supervisory, S);
- читання (Read, R);
- запису (Write, W);
- створення (Create, C);
- вилучення (Erase, E);
- зміни (Modify, M);
- перегляд файлу (File scan, F);
- контроль доступу (Access control, A).

Сервісні програми NetWare відображають початкові символи цих прав у дужках: [S R W C E M F A].

Щоб переглянути ефективні права для каталогу чи файлу, використовують команди RIGHTS або WHOAMI.

Захист за допомогою схеми атрибутів полягає у присвоєнні спеціальних властивостей індивідуальним каталогам або файлам, які перекривають довірчі права і можуть запобігати діям, які б дозволяли ефективні права.

Атрибути можуть запобігати від вилучення, копіювання, модифікації чи перегляду файлу або каталогу.

Атрибути також використовують для контролю за спільним використанням ресурсів (shared), маркуванням модифікованих файлів для того, щоб утиліти резервного копіювання могли вибирати тільки змінені файли, а також для запобігання перекрученням файлів (corruption).

ОС NetWare використовує такі атрибути каталогів:

- заборона вилучення (Delete Inhibit, D);
- прихований (Hidden, H);
- очищення (Purge, P);
- заборона перейменування (Rename Inhibit, R);
- системний (System, Sy), а також такі атрибути файлів:
- підлягає архіву (Archive Needed, A);
- заборона копіювання (Copy Inhibit, C);
- заборона видалення (Delete Inhibit, D);
- тільки для виконання (Execute Only, X);
- прихований (Hidden, H);
- індексований (Indexed, I);
- очищення (Purge, P);
- аудит читання (Read Audit, Ra);

- тільки для читання (Read Only, Ro);
- читання/запис (Read Write, Rw);
- заборона перейменування (Rename Inhibit, R);
- спільний (Shareable, S);
- системний (System, Sy);
- переміщуваний (Transactional, T);
- аудит запису (Write Audit, Wa).

Зауваження:

A. Якщо користувачі мають право модифікації каталогу чи файлу, вони можуть змінювати атрибути і виконувати будь-яку задачу, дозволену їхніми ефективними правами.
B. Атрибути каталогів і файлів потрібно використовувати для посилення захисту там, де багато користувачів мають доступ до файлів. Приклад: утиліти ОС NetWare так захищено атрибутами, що навіть СУПЕРВІЗОР не може видаляти їх без того, щоб не зняти спочатку відповідні прапорці.
C. Усі файли ОС NetWare у системних каталогах SYS:SYSTEM, SYS:PUBLIC і SYS:LOGIN мають атрибути Ro, S, D, і R.
D. Файли бази даних користувачів мають атрибути Sy, H, і T.
E. Для зміни чи перегляду атрибутів використовують утиліти FILER, FLAG, or FLAGDIR.

Система простежування транзакцій (TTS). Система простежування транзакцій (переміщень даних) ОС NetWare (Transaction Tracking System, TTS) захищає прикладні програми від перекручування, виконуючи зворотне трасування (backing out) незавершених транзакцій, які виникають при відмові мережевих компонентів.

При зворотному трасуванні, дані й індексна інформація в базі даних повертаються до того стану, у якому вони були, перш, ніж почалася транзакція.

TTS – невід'ємна частина ОС NetWare v3.x; навіть без бази даних для багатьох користувачів на сервері; вона реалізована на рівні операційної системи файл-сервера. Перевагою такого підходу є те, що навіть прикладні програми, спеціально не розроблені для оперативного повернення, отримують такі можливості.

TTS захищає дані при невдачі, роблячи копію первісних даних перш, ніж записати поверх нові дані. Якщо невдача відбувається протягом транзакції, TTS відновлює первісні дані. TTS може за-

хищати проти цих типів невдач будь-які прикладні програми, що допускають запити з блокуванням записів і зберігають інформацію в записах на жорсткому диску. Файли оброблення текстів, що не організовані в дискретні записи, не захищені TTS.

Перелічимо типи потенційних проблем захисту:

A. Користувачі, що були зроблені еквівалентом супервізора.
B. Користувачі, що мають небезпечні паролі або не мають ніяких.
C. Користувачі, що мають довірчі права в кореневому каталозі будь-якого то́му.
D. Користувачі, що мають права на SYS:SYSTEM.

Лабораторна робота № 2.3. Реєстрація, розподіл та захист ресурсів у ОС Novel NetWare 3.11

Мета роботи: навчитися реєструвати користувачів ОС Novel NetWare, використовуючи весь комплекс захисних засобів системи.

Приклад реєстрації. Для реєстрації нового користувача на файл-сервері, використайте утиліту **SYSCON**, яка знаходиться в каталозі

<ім'я файл-сервера>\SYS:PUBLIC\SYSCON <ENTER>

- виберіть пункт "User Information" з головного меню;
- за допомогою <INSERT> уведіть ім'я нового користувача <USER>, водночас у каталозі *<ім'я файл-сервера>/SYS:STUDENT/<USER>* буде створено робочу директорію з атрибутами дозволу [**SRWCEMFA**];
- після цього користувачу надають додаткові привілеї та обмеження:

Account Balance	Початкові обмеження
Account Restrictions	Обмеження для конкретного користувача
Change Password	За побажанням користувача
Full name	Повне ім'я користувача
Groups Belonged To	До якої групи належить користувач
Intruder Lockout Status	Стан заблокування при порушеннях
Login Script	Виконання стартових процесів при вході
Managers	Хто керує обліковим записом

Other Information	Ідентифікатор користувача, повне ім'я та ін.
Security Equivalences	Рівень доступу до ресурсів
Station Restrictions	Доступ до робочих станцій
Time Restrictions	Обмеження часу використання ресурсів
Trustee Directory Assignments	Доступ до каталогів з атрибутами [R F]
Trustee File Assignments	Доступ до файлів з атрибутами [R F]
Volume/Disk Restrictions	Обмеження на об'єм дискового простору

Для програм, які потребують при завантаженні виконання стартових пакетів, вказуємо їм шлях у файлі **login** у головному з каталогів MAIL\UserID\login.

Хід виконання роботи. Зареєструвати нового користувача F–21, який має потребу в таких навчальних програмах: Turbo Pascal 7.0, PCAD, NUMERI), використовуючи утиліту SYSCON, яка знаходиться у каталозі

TOEP\SYS:PUBLIC\SYSCON

(TOEP – <ім'я файл-сервера>). Водночас у каталозі

TOEP/SYS:STUDENT/

буде створено робочу директорію F–21 з атрибутами дозволу [**SRWCEMFA**], які потрібно скоректувати (S, A – заборонити).

Надати користувачу F–21 додаткові привілеї та обмеження:

Account Balance	Не змінюємо
AccountRestrictions	Не змінюємо
Change Password	За побажанням користувача
Full name	Група F–21
Groups Belonged To	Додаємо групу TP7 користувачів Pascal
Intruder Lockout Status	Не змінюємо
Login Script	Не змінюємо
Managers	Не змінюємо
Other Information	Отримуємо інформацію про користувача (User ID)
Security Equivalences	Не змінюємо
Station Restrictions	Не змінюємо
Time Restrictions	Надаємо обмеження у часі
Trustee Directory Assignments	*SYS:APPLICAT/NUMERI* з атрибутами [R F]
Trustee File Assignments	Не змінюємо
Volume/Disk Restrictions	3000 (об'єм до 3 Мб)

Для нормального функціонування програми PCAD потрібно задати такі шляхи у файлі **login** в головному каталозі MAIL\UserID\login:

map s16:=toep\sys:applicat\pcad\exe
map s16:=toep\sys:applicat\pcad\drv
map s16:=toep\sys:applicat\pcad\prt
map s16:=toep\sys:applicat\pcad\sym

Всі програми користувач F–21 запускає з робочої директорії *SYS:STUDENT/F–21* (тільки в ній він має право створювати, змінювати, вилучати файли).

2.4. Захист інформації в операційній системі Windows NT

Безпека інформаційної системи – це низка організаційних і технічних заходів, спрямованих на уникнення проблем, пов'язаних як з надійністю технічного забезпечення, так і цілеспрямованих шкідливих дій. У процедурах підтримки безпеки комп'ютерної системи, мають бути передбачені всі можливі наслідки цих дій.

Система безпеки Windows NT складається з таких компонентів:

- система реєстрації (керує обліковими записами, які включають імена користувачів, їхні паролі та повноваження користувача в мережі);
- набір атрибутів, призначених каталогам і файлам;
- розподіл ресурсів обчислювальної системи та мережі.

Система реєстрації. Основна мета системи безпеки Windows NT – контроль доступу. Для цього в системі підтримується інформація безпеки (security information), пов'язана як з суб'єктами доступу (користувачі, групи), так і з об'єктами (робочі станції, файли, принтери).

Система безпеки контролює доступ за запитом користувача або програмою, запущеною від його імені, як до об'єктів, які можна спостерігати через інтерфейс користувача (файли, принтери), так і до тих, які є невидимі (процеси, іменовані канали тощо).

Система безпеки ідентифікує і перевіряє істинність користувача, а потім дає змогу виконувати тільки ті дії з об'єктами, які надані йому власниками об'єктів.

В операційній системі Windows NT можлива єдина система для

ідентифікації, перевірки істинності, контролю доступу і запису інформації про події, пов'язані з безпекою системи.

Основні компоненти цієї системи безпеки показано на рисунку

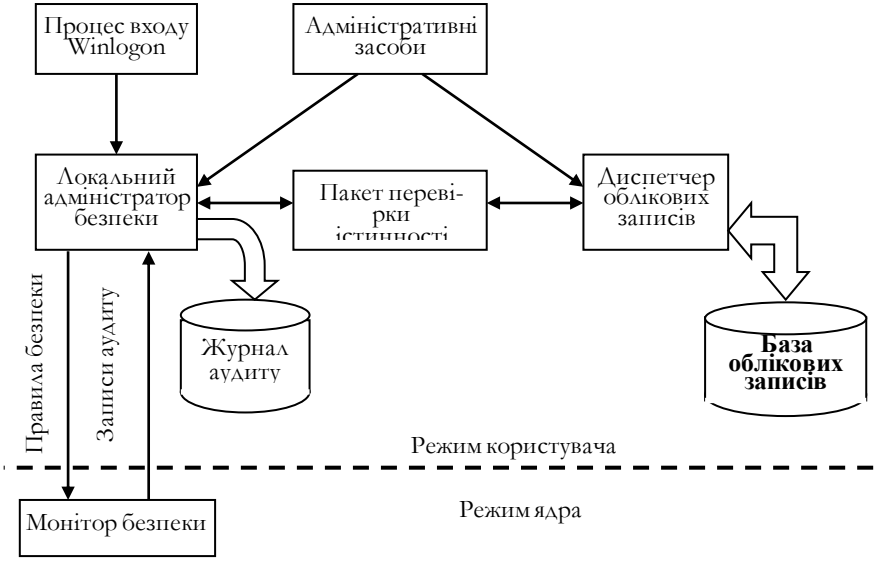


Рис. 2.8. Основні компоненти системи безпеки Windows NT

Центральна частина системи безпеки Windows NT – локальний адміністратор безпеки (Local Security Authority, LSA) перевіряє, чи є в користувача необхідні права для входу в систему. Цей компонент створює маркери доступу, керує локальними правилами безпеки (Local Security Policy), забезпечує служби інтерактивної перевірки істинності. LSA також контролює правила аудиту і записує в журнал аудиту повідомлення, отримані від монітора безпеки.

Основну роботу з контролю за доступом у Windows NT виконує монітор безпеки (Security Reference Monitor, SRM), який перевіряє права користувача для доступу до об'єкта (ресурсу). Він працює в режимі ядра. Компоненти ядра і процеси користувача звертаються до монітора безпеки для вияснення чинності прав користувача в процесі отримання доступу до об'єкта. SRM зберігає в собі ввесь код, який відповідає за підтвердження доступу, і це єдина копія коду для будь-якої системи Windows NT, завдяки чому всі перевірки виконуються однаково для всіх об'єктів у системі.

Диспетчер облікових записів забезпечує взаємодію інших компонентів системи безпеки – програм і служб Windows NT з базою

даних облікових записів (Security Account Database, SAM). Одна з основних функцій SAM – підтримка механізмів ідентифікації (identification) і перевірки істинності (authentication) користувачів при інтерактивному вході в систему або при доступі до неї по мережі. Тільки через диспетчер облікових записів всі інші компоненти системи безпеки Windows NT (у т. ч. і локальний адміністратор безпеки, LSA) можуть отримати доступ до інформації, яка зберігається в базі даних SAM.

Інтерактивний вхід (logon) в систему і перевірка істинності (authentication) складається з декількох етапів: при старті операційної системи спочатку запускається підсистема Win32, що автоматично ініціює процес WINLOGON, який запускає Локальний адміністратор безпеки LSASS. Лише потім Winlogon виводить діалогове вікно Press **Ctrl+Alt+Del** to logon

Перед виконанням будь-яких дій користувач ОС Windows NT має ввійти в систему, для чого слід увести ім'я користувача (username), яке потрібне для ідентифікації в системі та пароль (password), який дає змогу перевірити його істинність.

Інформація, введена користувачем в діалоговому вікні Logon Information, порівнюється з тією, яка є в базі облікових записів, розміщеній на комп'ютері входу (коли користувач входить за локальним обліковим записом), або контролера домену (коли вхід здійснюється за обліковим записом домену).

Розподіл ресурсів. Після одноразової перевірки істинності користувача для нього є доступними всі ресурси, пов'язані з обліковим записом. Ресурси – це файли і принтери серверів Windows NT, які є в домені, а також ресурси Microsoft Backoffice і сумісних з ним програм.

У Windows NT режим підтримки багатьох користувачів реалізований на основі повноважень доступу до будь-яких об'єктів: як до реальних (файли, пристрої, каталоги), так і до віртуальних (процеси, потоки). Операція доступу до об'єкта контролюється монітором безпеки **(**Security Reference Monitor, SRM**)**, який і перевіряє відповідність "пропуску" і "турнікету". Користувач отримує "пропуск" – маркер SAT (Security Access Token) – після входу в систему на підставі даних з облікового запису. Об'єкту, при його створенні, призначається "турнікет" – дескриптор SD (Security Descriptor). NTFS підтримує SD, а FAT/FAT32 – ні, тому NTFS забезпечує захист на рівні файлів і каталогів, а FAT/FAT32 – ні. Як

SAT, так і SD можуть змінюватися адміністратором системи (користувачем зі спеціальними правами). В підсумку користувач бачить тільки ті об'єкти, на які в нього є право доступу (порівняйте з UNIX і Novell NetWare, де користувачу відводять визначений каталог, у межах якого йому і слід працювати). Отже, у різних користувачів будуть різні робочі середовища на тому самому комп'ютері.

Власником будь-якого об'єкта стає його автор. Власником операційної системи стає суб'єкт, що встановив її на комп'ютері. Він дістає права адміністратора, а користувач стає власником усіх створених ним файлів. Адміністратор може "взяти" у власність будь-який об'єкт, але не може "віддати" його будь-кому примусово.

Атрибути файлів та каталогів. Файлова система NTFS розроблена для швидкого виконання стандартних файлових операцій типу читання, запису і пошуку, а також для ефективного відновлення файлової системи на великих жорстких дисках. Вона включає засоби підтримки безпеки, необхідні як для файлових серверів, так і робочих станцій. NTFS підтримує керування доступом до даних і повноважень користувача, що є важливим для цілісності системи та корпоративних даних. Тоді як каталогам, розділюваним для спільного використання (shared) за допомогою системних засобів Windows NT, призначають специфічні дозволи, файлам і каталогам NTFS можуть бути призначені дозволи поза тим, розділювані вони чи ні.

Вся інформація на томі NTFS є файлом чи частиною файлу. Кожен розміщений на томі NTFS-сектор належить деякому файлу. Кожен файл на томі NTFS репрезентований записом у спеціальному файлі – головній файловій таблиці (Master File table, MFA). NTFS резервує перші 16 записів таблиці для спеціальної інформації. Перший запис цієї таблиці описує безпосередньо головну файлову таблицю; за нею – дзеркальний запис (mirror record) MFT. Якщо перший запис MFT зруйнований, то NTFS читає другий запис для відшукання дзеркального файлу MFT. Місця розміщення сегментів даних MFT і дзеркального файлу MFT записані в секторі початкового завантаження. Дублікат сектора початкового завантаження знаходиться в логічному центрі диска.

Третій запис MFT – файл реєстрації (Log File) – використовують для відновлення файлів. Сімнадцятий і наступний записи го-

ловної файлової таблиці використовують під файли і каталоги, які також розглядають як файли.

NTFS також забезпечує численні розширені (extended) атрибути і дає можливість майбутнім програмам визначати ці атрибути.

Мережеві засоби захисту. Для забезпечення захисту мереж на базі Windows NT необхідно чітко розуміти процеси, які відбуваються при перевірці повноважень користувачів і в якому вигляді реєстраційна інформація передається по мережі. Наприклад, стандартний мережевий сервіс telnet пересилає ім'я користувача і пароль у відкритому вигляді (планарно). Високий ступінь захисту досягається шляхом заміни стандартних відкритих сервісів на такі, що шифрують параметри користувача (машини – клієнта), щоб навіть перехоплення пакетів не давало змоги розкрити ці дані (наприклад, SSH).

Доступ до ресурсів мережі за протоколом SMB, який використовує програмний інтерфейс NETBIOS, в операційній системі Windows NT забезпечує сервер SMB. Клієнтом SMB називають програмний компонент, який звертається по мережі до ресурсів сервера. SMB забезпечує сервер засобами для перевірки істинності клієнта, який намагається отримати доступ до ресурсів мережі. В цьому протоколі визначені два режими роботи системи контролю: перевірка на рівні ресурсу (Share level) і перевірка на рівні користувача (User level).

При перевірці на рівні ресурсу з кожним мережевим ресурсом пов'язують один або декілька паролів доступу. Для різних ресурсів одного і того ж сервера паролі можуть бути різними. Щоб отримати доступ до ресурсу, клієнт повинен увести пароль, який зв'язаний з цим ресурсом. Отже, для доступу до декількох мережевих ресурсів одного і того ж сервера користувач вимушений декілька разів вказувати різні паролі.

Перевірка на рівні ресурсів – захист простий, але ненадійний, оскільки не закладена можливість отримання інформації про те, хто персонально здійснює доступ, тому операційна система Windows NT не підтримує доступ на рівні ресурсу.

Протокол SMB, який забезпечує захист у момент відкриття сеансу, згодом усі дані передає по мережі планарно. Якщо потрібно забезпечити конфіденційність інформації, потрібно застосовувати програмні й апаратні засоби шифрування транспортного каналу, наприклад, протокол PPTP.

Для того, щоб зменшити залежність операційної системи Windows NT від NetBIOS, розробники Microsoft у версії 5.0 реалізували використання протоколу Common Internet File System (CIFS), а не SMB.

Лабораторна робота № 2.4. Методи інформаційної безпеки в ОС Windows NT

Мета роботи: навчитися коректно реєструвати користувачів у мережі WINDOWS NT та вміти сканувати ресурси мережі і добиватись адекватного захисту від сканування.

Програмне забезпечення, яке буде використано в роботі:

- адміністративні засоби управління ресурсами домену WINDOWS NT 4.0;
- програма перехоплення та аналізу IP-пакетів у мережі Ethernet (WinSniffer);
- програми розшифрування паролів (xIntruder);
- програма пошуку доступних мережевих ресурсів (xShares);
- програма VPN-клієнт захищеного мережевого з'єднання PGPnet.

Хід виконання роботи. ***Реєстрація користувачів домену.*** Реєстрацію користувачів у мережі WINDOWS NT здійснюють наступним чином:

1) через Start-меню заходять послідовно:
   Start → Programs → Administrative tools (common) → User manager for domains;
2) для введення нового користувача у вікні user обирають:
   New user;
3) у вікні задають:

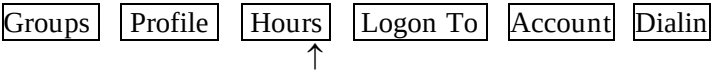
User name – ім'я користувача: наприклад, fzp–88,
Full name – повне ім'я користувача: група fzp–88,
Description – опис: domain users,
Password – пароль: asd88,
Confirm password – підтвердити пароль: asd88;

4) встановлюють відповідні прапорці:

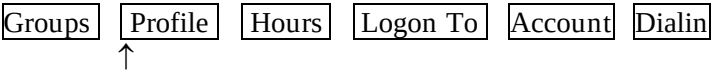
□ User must change Password at Next Logon,

☒ User Cannot Change Password,
☒ Password Never Expires,
□ Account Disabled;

5) розгортають закладку Profile і задають ім'я script-файлу (Logon Script Name), який виконується при реєстрації користувача в домені, наприклад, fzp–88.bat:



6) розгортають закладку Hours і задають час доступу користувача до ресурсів:



7) виходять з процедури New user, натиснувши OK і закривають User manager for domains;
8) створюють за допомогою Notepad у папці C:\SERVNT\system32\Repl\import\Scripts, script-файл fzp–88.bat у вигляді:

net use w: \\sphinx\fzp–88$
net use l: \\sphinx\bp$
net time \\sphinx /set /yes

тут: *w* – домашній каталог користувача fzp–88;
l – спільний робочий ресурс (каталог з необхідним програмним забезпеченням bp$);

третя стрічка засвідчує на обов'язкову часову синхронізацію подій на станції з сервером часу (тут це контролер домену \\sphinx).

9) на диску Net–disk(E):\users\ створюють каталог Fzp–88. У контекстному меню для цього каталогу (клік правою клавішею мишки на значку каталогу) вибираємо опцію Sharing, активізуємо ● Share as: і у вікні Share Name набираємо ім'я Fzp–88$.

10) перевірити реєстрацію користувача Fzp–88 на робочій станції і всі доступні йому ресурси.

Для вилучення облікового запису користувача зі списку користувачів домену необхідно виконати таке:

1) Start → Programs → Administrative tools → User manager for domains;

2) вибрати у списку користувача і натиснути клавішу Del, або в закладці User вибрати команду Delete.

Завдання. Зареєструвати в домені вказані у таблиці групи користувачів і надати їм доступ до необхідних ресурсів; перевірити реєстрацію користувачів і всі доступні ресурси на робочій станції; після звіту викладачу – вилучити ці облікові записи з домену.

Користувач	Група	Час занять	Самостійна робота	Під'єднання ресурсів
1	Fzr–12	Пн–1 пара, Ср–4 пара	з Пн по Пт з 19^{00} по 21^{00}	Bp$; Fzr–12
2	Fzf–17	Вт–2,3 пара, Пт–0 пара		Bp$; Fzf–17
3	викладач	цілодобово		Bp$; Fzr–12; Fzf–17

Приклад сканування мережі:

1. Увімкнути на робочій станції Lab0 засоби розподілу ресурсів (каталогів та принтерів) у мережі Microsoft Networks:
   - Start–>Settings–>Control Panel–>Network
   - Add–>Service–>File and printer sharing for Microsoft Networks
   - у каталозі C:\Temp контекстного меню вибрати Sharing–>Shared As–>Full–>Password–>OK.
2. На робочій станції Lab1, що знаходиться в тій же мережі, виконати програму xShares, просканувати мережу на доступні ресурси, отримати пароль доступу до ресурсу \\Lab0\C:\Temp (утиліта xIntruder) і переглянути його вміст.
3. На іншій робочій станції (Lab2) з цієї ж мережі, виконати програму WinSniffer, отримати IP-пакети з мережі та проаналізувати їхній зміст (адреси, протоколи, імена та паролі користувачів мережі, що намагаються в цей час приєднатися до ресурсу \\Lab0\C:\Temp.
4. Виконати пп.2 і 3 при застосуванні захищеного з'єднання між станціями Lab0 та Lab1 за допомогою PGPnet.

2.5. Методи інформаційної безпеки в ОС UNIX

Адміністративне управління в системі UNIX відокремлено від загальнопризначеного для користувача доступу. Привілейований користувач в UNIX може виконувати такі важливі задачі, як управління процесами і підключення пристроїв.

На процеси і файли в ОС UNIX розповсюджується єдина система приналежності об'єктів. Право контролю над файлом або процесом належить власнику. Права власника можуть відмінятися тільки привілейованим користувачем.

Власник файлу – це завжди одна людина або група. Інформація про групи зберігається у файлі */etc/group*. Для зміни прав доступу до файлу послуговуються командою *chmod*. У кожного UNIX-файлу є власник і група. Власник файлу має тільки один привілей, який іншим користувачам системи недоступний: він може змінювати права доступу до файлу. Зокрема, власник може встановити права доступу так, що ніхто, окрім нього, не зможе звертатися до цього файлу. Власник файлу визначає, які операції можуть виконувати над файлом члени групи. У такій схемі можливе колективне використання файлів.

Файлу можна призначити іншого власника за допомогою команди *chown* і іншу групу, використовуючи команду *chgrp*.

UNIX відстежує не символьні імена власників і груп, а їхні ідентифікатори. Ідентифікатори користувачів (скорочено UID) і відповідні їм імена користувачів зберігаються у файлі */etc/passwd*, а ідентифікатори груп (GID) і імена, що відповідають їм, – у файлі */etc/group*.

Символьні імена, відповідні UID і GID, визначають виключно для зручності користувачів системи. Щоб команда типу *ls* могла вивести інформацію про приналежність файлу в легкому для читання вигляді, вона має знайти кожне ім'я у відповідному файлі.

Ядро призначає кожному процесу чотири ідентифікатори: реальний і ефективний UID, реальний і ефективний GID. Реальні ID використовують для обліку використовування системних ресурсів, а ефективні – для визначення прав доступу. Зазвичай реальні й ефективні ID збігаються. Власник процесу може посилати в процес сигнали, а також знижувати пріоритет процесу.

У принципі процес не може змінити жодного з елементів своєї приналежності (власника і групу), але є особливий випадок, коли зміна ефективних ідентифікаторів власника і групи можлива. Процес, під час якого починається виконання іншого програмного файлу, здійснює один з системних викликів сімейства *exec*. Коли таке трапляється, ефективний UID і ефективний GID процесу можуть бути встановлені рівними UID і GID файлу, що містить образ нової програми, якщо у цього файлу встановлені біти зміни іден-

тифікатора користувача й ідентифікатора групи. Системний виклик *exec* – це механізм, за допомогою якого такі програми, як */bin/paswd*, тимчасово одержують пільги привілейованого користувача (програмі *passwd* вони потрібні для того, щоб модифікувати */etc/passwd*).

Системним адміністраторам доводиться відміняти дію захисних механізмів UNIX у самих різних ситуаціях. Для забезпечення такої можливості система виділяє серед усіх ідентифікаторів користувачів один особливий, нульовий, який належить привілейованому користувачу. UNIX-системи визначають для цього UID користувача з іменем “root”.

ОС UNIX дає змогу привілейованому користувачу виконувати над файлом або процесом будь-яку операцію. Крім того, деякі системні виклики (звернення до ядра) може виконувати тільки привілейований користувач. Такі виклики доступні всім користувачам, але мають спеціальні опції для користувача root. Ось приклади операцій, які може виконати тільки привілейований користувач:

- монтування і демонтаж файлових систем;
- зміна командою *chroot* кореневого каталогу процесу;
- створення файлів пристроїв;
- установка системного годинника;
- зміна приналежності файлів (у BSD-системах);
- збільшення лімітів використовування ресурсів і призначення пріоритетів процесів;
- задання host-імені системи;
- налаштування мережних інтерфейсів;
- зупинку системи.

Прикладом можливостей привілейованого користувача може служити здатність процесу, що належить йому, змінювати на свій розсуд параметри приналежності. Один з таких випадків – програма *login*; процес, який запрошує Вас при вході в систему ввести свій пароль. Він спочатку виконується як кореневий. Якщо введені пароль і ім’я користувача правильні, то *login* замінює свої UID і GID відповідними ідентифікаторами користувача і запускає інтерпретатор команд *shell*. Після того, як кореневий процес, змінивши свою приналежність, стане звичайним призначеним для користувача процесом, відновити свій попередній привілейований стан він не зможе.

Права доступу до файлів. Кожному файлу відповідає набір, що складається з дев'яти бітів коду прав доступу для користувача, який визначає, які користувачі мають право читати файл, записувати в нього дані або виконувати його. Разом з іншими трьома бітами, якими задають коди прав доступу для виконуваних файлів, цей набір утворює код прав доступу до файлу. Дванадцять бітів коду прав доступу зберігаються разом з чотирма бітами інформації про тип файлу в 16-бітовому слові.

Чотири біти типу файлу встановлюють при його створенні і вони зміні не підлягають. Дванадцять бітів коду прав доступу можуть змінюватися власником файлу або привілейованим користувачем за допомогою команди *chmod* (change mode – змінити режим). Перегляд значень цих бітів здійснюють за допомогою команди *ls*.

Біти зміни ідентифікатора користувача та ідентифікатора групи. Біти з вісімковими значеннями 4 000 і 2 000 – це біти зміни ідентифікатора користувача й ідентифікатора групи. Вони дають змогу програмам "діставати" доступ до файлів і процесів, які інакше будуть недоступні користувачу, що виконує ці програми. Хоча ці біти є для всіх файлів, в більшості версій UNIX використовують лише ті, які встановлені для виконуваних файлів.

Sticky-біт. Біт з вісімковим значенням 1 000 називається sticky. Якщо sticky-біт встановлюють для каталогу, то деякі версії UNIX забезпечують можливість видаляти і перейменовувати файли тільки у випадку, якщо користувач є власником каталогу, власником файлу або привілейованим користувачем. Мати лише дозвіл на запис в каталозі недостатній. Такий захід направлений на те, щоб зробити каталоги типу */tmp* дещо більш закритими.

Біти коду прав доступу для користувача. Дев'ять бітів коду прав доступу для користувача призначено для того, щоб визначити, хто і які операції може виконувати над файлом. В ОС UNIX не можна встановлювати біти прав доступу окремо для кожного користувача. Наявні окремі набори бітів для власника файлу, групи й інших користувачів. Кожний набір складається з трьох бітів: біт читання, біт запису і біт виконання (для каталогу останній названо "бітом пошуку").

Три старші біти (з вісімковими значеннями 400, 200 і 100) служать для управління доступом для власника файлу. Другі три біти (40, 20 і 10) задають доступ для групи. Останні три біти (4, 2 і 1)

визначають доступ усіх інших користувачів. Старший біт кожної трійки – біт читання, середній – біт запису, молодший – біт виконання. Кожний користувач потрапляє тільки в одну з категорій, відповідних одному з трьох наборів бітів прав доступу. Використовують ті права доступу, які найбільш строгі в кожному класі. Для звичайного файлу біт читання дає можливість відкривати і читати файл. Біт запису – змінювати вміст файлу. Можливістю видалення і перейменування файлу управляють біти дозволу, встановлені для його батьківського каталогу.

Установкою біта виконання задається дозвіл виконувати файл. Відомі два типи виконуваних файлів: двійкові файли, які виконуються безпосередньо центральним процесором, і сценарії, які підлягають інтерпретації *shell* або іншою програмою. Установкою біта виконання для каталогу (в цьому контексті часто званого бітом пошуку) дається дозвіл входити в каталог, але при цьому не можна одержати список його вмісту. Установка комбінації бітів читання і виконання дає змогу одержати список вмісту каталогу. Комбінація бітів запису і виконання дає можливість створювати, видаляти і перейменовувати файли в каталозі. Наприклад, командою *chmod 711 myprog* власнику надаються всі права, а всім іншим користувачам – тільки право виконання.

Індексні дескриптори. Ядро зберігає інформацію про кожний файл у структурі, яка називається індексним дескриптором. При створенні файлової системи формуються таблиці індексних дескрипторів. Їхній розмір і розміщення на диску ніколи не змінюються. Кожний індексний дескриптор містить близько сорока окремих порцій інформації, але переважно ці дані використовуються тільки ядром. Системного адміністратора цікавитимуть кількість посилань, власник, група, права доступу, розмір, час останньої зміни і тип файлу. Всю цю інформацію можна одержати за допомогою команди *ls*, яка має різні аргументи. В BSD-системах команда *ls –lg* видає список, що містить код прав доступу, розмір, час останньої зміни, ідентифікатор користувача, ідентифікатор групи, кількість посилань і тип файлу.

Розглянемо рядок, одержаний за допомогою команди *ls –lg /bin/sh*

–rwxr–xr–x 1 root bin 85924 Sep 27 1994 /bin/sh

Перше поле – це ім'я файлу і режим доступу до нього. Оскільки перший символ – дефіс, то це звичайний файл. Різні типи файлів розрізняють за односимвольними кодами.

Кодування типів файлів у списку команди ls

Звичайний файл	**–**	**редактори, *ср, rm***	***rm***
Каталог	*D*	*mkdir*	*Rmdir, rm –r*
Байт–орієнтованний файл пристрою	*C*	*mknod*	*Rm*
Блок–орієнтованний файл пристрою	*B*	*mknod*	*rm*
Доменне гніздо UNIX	*S*	*socket (2)*	*rm*
Іменований канал	*P*	*mknod*	*rm*
Символічне посилання	*1*	*In –s*	*rm*

Наступні дев'ять символів у цьому полі – це три набори бітів коду прав доступу. Ці біти мають тільки двійкові значення, але в списку виводу за командою – це букви *r, w* і *x* (відповідно читання, запис і виконання). В цьому випадку власник має всі права доступу до файлу, а решта користувачів – право тільки на читання і виконання.

Якби був встановлений біт зміни ідентифікатора користувача, то замість букви *x*, що позначає право власника на виконання, стояла б буква *s*. Якби був встановлений біт зміни ідентифікатора групи, то замість букви *x* для групи теж стояла б буква *s*. Останній символ коду прав доступу (право виконувати для інших користувачів) показано як *t,* якщо sticky-біт файлу встановлений. Якщо біт зміни ідентифікатора користувача або sticky-біт встановлений, а відповідний біт виконання – ні, ці біти позначено як *S* і *T*.

Наступне поле списку – лічильник посилань на файл. В цьому разі тут стоїть одиниця, яка свідчить про те, що */bin/sh* – єдине ім'я, під яким відомий файл. Кожного разу при створенні жорсткого посилання на файл цей лічильник збільшується на одиницю.

Кожний каталог має мінімум два посилання: одне з батьківського каталогу і посилання зі спеціального файлу "**.**" (dot) всередині самого каталогу. Символічні посилання в лічильнику не враховуються.

Наступні два поля – власник і група файлу. Власник файлу – root; файл належить групі bin. Насправді в ядрі зберігаються не текстові дані, а ID користувача і групи. Якщо символьні версії імен визначити неможливо, ці поля містять числа.

Ще одне поле – розмір файлу в байтах. Цей файл має розмір 85 924 байти. Потім слідує дата останньої зміни: 20 грудня 1993 року. Останнє поле списку містить ім'я файлу: */bin/sh*.

Для файлу пристрою команда *ls* видає дещо іншу інформацію. Нижче подано рядок списку, який виводиться за командою *ls –lg /dev/ttya:*

crw–rw–rw– 1 root daemon 12, 0 Dec 20 1993 /dev/ttya

Зазвичай поля ті ж самі, але замість розміру в байтах показані старший і молодший номери пристрою: */dev/ttya*, – цей перший пристрій, керований драйвером пристрою 12 (в цій системі це драйвер термінала). Час зміни, число посилань і розмір файлу система відстежує автоматично. Біти коду прав змінюються тільки безпосередньо користувачем.

Команду *chown* використовують для зміни власника файлу, а команду *chgrp* – для зміни його групи. В деяких системах *chown* може змінювати власника і групу файлу одночасно.

Синтаксис команд *chown* і *chgrp* збігається з синтаксисом команди *chmod* за винятком того, що першим аргументом є ім'я нового власника або нової групи файлу. Для того, щоб застосувати *chgrp*, користувач має бути власником файлу і входити до групи, яку збирається призначити файлу, або бути привілейованим користувачем.

У більшості версій команд *chown* і *chgrp* передбачений прапорець *–R*, який змінює власника або групу каталогу і всіх його підкаталогів і файлів. Наприклад, послідовність:

 # chmod 755 ~matt
 # chown –R matt ~matt
 # chgrp –R staff ~matt

можна використовувати для задання початкового каталогу нового користувача після копіювання стандартних файлів запуску (~matt – переважно позначає зрозуміле для *shell* скорочення від "початковий каталог користувача matt").

Методи захисту в ОС UNIX. В моделі UNIX-системи є декілька вад, які неможливо подолати:

- UNIX зорієнтована передусім на зручність у використовуванні, що зовсім не припускає природність і простоту її захисту. Цю систему розробляли дослідники для дослідників, і концепція UNIX полягає в забезпеченні зручного маніпулю-

вання даними в мереженому, розрахованому на багато користувачів, середовищі;

- захист у UNIX, по суті справи, припускає всього два варіанти статусу користувача: користувач, що не володіє привілеями, або привілейований користувач. Такі засоби UNIX, як виконання програм зі встановленим бітом зміни ідентифікатора користувача, призначені для забезпечення привілейованого доступу до всіх обчислювальних ресурсів системи. Разом з тим через незначні огріхи в захисті може бути поставлено під загрозу нормальне функціонування системи як такої;
- більшість адміністративних функцій реалізована ззовні ядра, тому до них можна без особливого клопоту дістати доступ з метою перегляду і внесення змін;
- програми, які виконуються зі зміненим ідентифікатором користувача, особливо ті, для яких встановлений ідентифікатор привілейованого користувача, є джерелом проблем безпеки системи.

Система Kerberos. Дістати несанкціонований доступ до комп'ютера, що працює в мережі, іноді дуже легко. Такі тривіальні прорахунки, як передання паролів по мережі у вигляді звичайного тексту, зводять нанівець будь-який захист. Система Kerberos, розроблена в Масачусетському технологічному інституті, зорієнтована на захист у мережах.

При використовуванні системи Kerberos забезпечується більш ефективний захист даних у мережах, ніж при повній відсутності системи захисту як такої. На жаль, вона рясніє "дірами", починаючи з вікон, які залишаються аутентифікованими під час відсутності користувача, і закінчуючи паролями, які записують на сервері аутентифікації в незашифрованому вигляді.

Фільтрування пакетів. Крім захисту окремих машин, можна вжити заходи безпеки на мережевому рівні. Основний інструмент системи захисту мережі – фільтрування пакетів.

Фільтруючи пакети, обмежують трафік через Internet-шлюз (або через шлюз, який сполучає локальні підмережі в межах організації). Вказавши, які адреси пунктів призначення, номери портів і типи протоколів є допустимими, шлюз просто відкидає всі інші пакети, які не відповідають заданому критерію. Фільтрування виконують спеціалізовані апаратні маршрутизатори (наприклад, ті що їх випускають фірми CISCO, Allied Telesyn та ін.). Можливе

також програмно реалізоване фільтрування; все залежить від машини, яка виконує функції шлюзу і її конфігурації.

Фільтрування пакетів не має бути основним засобом захисту – кожну машину необхідно захищати індивідуально, користуючись такими програмами, як, наприклад, *COPS, crack, tcpd* чи *tripwire*.

Списки розсилки з питань захисту. Наявна низка телеконференцій Usenet і списків розсилки Internet, в яких є оперативна інформація про проблеми захисту.

Джерела інформації з питань захисту

Ім'я	Предмет	Як отримати
Unix–security	Загальні питання захисту	*S securify@cpd.com*
Security–misc	Загальні питання захисту	*T comp.security.misc*
Virus–list	Віруси	*T comp.virus*
Sgi–bugs	Помилки в IRIX	*T comp.sys.sgi.bugs*
Hpux–list	Загальні питання по HP–UX	*T comp.sys.hp.hpux*
Solaris–list	ОС Solaris 2.X	*T comp.unix.solaris*
Sun–managers	Адміністрація Sun	*S sun–managers–request@eecs.nwu.edu*
ACM risks	Технічні проблеми	*T comp.risks*
Cert–tools	Нові засоби захисту	*S cert–tools–request@cert.org*
Cert–advisory	Рекомендації CERT	*S cert–advtsory–request@cert.org* *T comp.security.announce*

Примітка:

S – список розсилки (вказана адреса для контакту)

T – телеконференція Usenet

Лабораторна робота № 2.5. Методи інформаційної безпеки в ОС UNIX

Мета роботи: навчитися реєструвати користувачів в ОС UNIX, надавати права доступу до об'єктів ОС UNIX та сканувати мережу і керувати процесами в системі вбудованими в ОС засобами.

Програмне забезпечення, яке буде використано у роботі:

утиліти *mount, mkdir, cp, chown, chmod, ping, trafshow, ps, kill* (формат команд та їхніх ключів можна довідатися за допомогою програми *man <ім'я команди>*).

Хід виконання роботи. Зареєструвати користувача у ОС FreeBSD 4.x / 5.x можна, наприклад, за допомогою perl-сценарію *adduser*. У поданому зразку опущено коментуючі стрічки, запити виділено курсивом, варіанти відповідей у списку розділені пропусками, пропоновані по замовчуванню відповіді (якщо такі можливі) взято у квадратні дужки, набір на клавіатурі виділено курсивом та жирністю, коментарі – після двох символів slash "//", знак "↵" – це клавіша ***Enter***.

#adduser <Enter>
Enter your default shell: bash csh date no sh tcsh [sh]: ↵
Enter your default HOME partition: [/home]: ↵
Copy dotfiles from: /usr/share/skel no [/usr/share/skel]: ↵
Send message from file: /etc/adduser.message no [/etc/adduser.message]: ↵
Create "/etc/adduser.message"? (y/n) [y]: ↵
Use password (y/n) [y]: ↵
Write your configuration to /etc/adduser.conf? (y/n) [y]: ***n*** *↵*
Enter username [a–z0–9_–]: test ↵
Enter full name []: for learning task ↵
Enter shell bash csh date no sh tcsh [sh]: ↵
Enter home directory (full path) [/home/test]: ↵
Uid [1000]: ↵ // щоразу автоматично збільшується на 1
Enter login class: default []:↵
Login group test [test]: guest ↵
Login group is "guest". Invite test into other groups: guest no [no]: ↵
Enter password []: testlab ↵ // відображається зірочками
Enter password again []: testlab ↵ // теж саме – для контролю
// далі подають зведені реєстраційні дані
Send message to "test" and: no root second_mail_address [no]: ↵
Add anything to default message (y/n) [n]: ↵
Send message (y/n) [y]: ↵
Add another user? (y/n) [n]: ***n*** *↵*

Завдання 1: завести реєстраційні записи для користувачів ABC_Fep–51 (група guest) та Ivaniv (група staff – персонал). Зареєструватись на консолях 2 та 3 (перемикання на консоль ***N*** – за допомогою $\boldsymbol{Alt+F_{N+1}}$) за створеними записами.

Завдання 2: змонтувати ГМД, даний викладачем, у підкаталог */mnt/floppy*, переписати вказані файли в новостворений підкаталог *data* в домашньому каталозі користувача Ivaniv та надати необхідні для роботи з ними права власності та доступу: повні права – для самого користувача, читання та виконання – для групи, тільки читання – для всіх інших. Перевірити можливість читання та модифікації файлу *zavd.lab5* з консолі користувача Ivaniv. В домашньому каталозі користувача ABC_Fep–51 створити символічне посилання на файл */home/ivaniv/data/zavd.lab5* та перевірити можливість його читання та модифікації з консолі ABC_Fep–51.

Завдання 3: зареєструватися з віддаленої консолі (SSH) з обліковим записом ABC_Fep–51 та виконати програму *ping* до віддаленої машини; з консолі root зупинити цей процес за допомогою команди *kil-9 PID*, визначивши перед цим номер процесу PID за допомогою команди *ps –auxw | grep ping*.

З віддаленої машини отримати за допомогою SFTP файл розміром не менше 10 МБ, в цей же час з консолі root №1 сканувати мережу за допомогою програми *trafshow*, а з консолі root №2, застосовуючи правила firewall (програма *ipfw*), фільтрувати ftp–трафік за портом, протоколом та IP–адресою віддаленої машини. Результати реєструвати на консолі root №1.

Виконавши завдання, вилучити облікові записи користувачів ABC_Fep–51 та Ivaniv за допомогою perl-сценарію *rmuser*.

2.6. Захист електронної пошти

Електронна пошта, чи пошта e–mail, – один з найпопулярніших видів використання Інтернету. За допомогою електронної пошти в Інтернеті можливо відіслати лист мільйонам людей по всій планеті і одночасно листи отримати.

Електронна пошта стає усе більш важливою умовою ведення повсякденної та ділової діяльності.

Основні групи загроз, що походять від електронного листування, це:

- троянські коні;
- віруси;
- програми зловмисного характеру, що містяться в прикріплених до листів файлах;

- поштові віруси – черв'яки (Melissa, Back Door, Sobig та ін.);
- спамові листи.

Для безпечного листування потрібно встановити антивірусну програму, що має у своєму складі резидентний модуль, який постійно зберігається в пам'яті комп'ютера і який відловлює всі підозрілі рухи поштового клієнта. Вибір тут достатньо великий, але рекомендують Антивірус Касперського (AVP) або Данилова (DrWeb) з регулярним поновленням антивірусних баз. Програми надійні і забезпечують захист від усіх видів комп'ютерних вірусів і троянських коней.

Можуть бути небезпечними електронні листи, які не містять ніяких вкладень, зате уражені т. зв. скрипт-вірусами (поштовими вірусами – черв'яками). Серед найвідоміших, потрібно зокрема, згадати KakWorm, Stages і ILOVEYOU (LoveLetter). Вони написані на Visual Basic for Applications (VBA), використовують Windows Scripting Host (машину для запуску скрипт-програм) і вкрай небезпечні. Проти них часто безсилі традиційні антивірусні засоби, які не в змозі знайти вірус, якщо він не звертається до жорсткого диска, а оперує виключно в оперативній пам'яті комп'ютера.

Евристичний аналізатор AVP Script Checker, спеціально призначений для боротьби зі скрипт-вірусами. Перед виконанням скриптів Checker проводить евристичний аналіз коду і його перевірку за допомогою AVP Монітора. При виявленні вірусу або підозрілого коду на екран буде виведено відповідне попередження і скрипт не буде виконаний.

Вільнопоширювану програму MailCleaner, також призначену для боротьби зі скрипт-вірусами, можна отримати за адресою: *ftp://www.mailcleaner.com/MCSetup.exe*.

Дуже оперативно програми, призначені для боротьби з конкретними видами вірусів, з'являються на сайті *http://www.computerra.ru/scallwin/www.download.com*, в розділі Downloads : PC : Utilities : Antivirus.

Для боротьби зі спамовими листами розроблено протокол безпечної електронної пошти (SSL). Більшість клієнтів електронної пошти можна сконфігурувати для безпечних операцій з електронною поштою, використовуючи SSL. На вкладці Advanced в MS Outlook Express, наприклад, є опція: "This server requires a secure connection (SSL)". Поштовий клієнт автоматично встановить нові порти для такого з'єднання. Іноді слід задати ці порти вручну. До-

зволені такі порти SSL для наявних поштових послуг: SMTP–SSL (465), POP3–SSL (995) та IMAP–SSL (993).

Сервер електронної пошти використовує непідписане посвідчення SSL для безпечного кодування операцій пересилання електронної пошти. Зазвичай видається попередження про "непідписане посвідчення" при пересилці і отриманні електронної пошти, але процес залишається безпечним і шифрованим. Те ж справедливо і для клієнта webmail, який доступний з HTTPS.

Цифрове посвідчення SSL – це електронний файл, який унікально ідентифікує індивідуумів і сервери. Цифрові посвідчення дають змогу клієнту (мережевий навігатор) засвідчити сервер до установки сеансу SSL. Звичайно, цифрові посвідчення підписує незалежна і довірена третя сторона, щоб гарантувати їхню переконливість. Сторона, що підписала документ, називається уповноваженою (CA) стороною, як наприклад VeriSign.

При повсюдному використанні протоколу SSL стане можливим заборонити передавання та прийом непідписаної кореспонденції, що дасть можливість уникнути небажаного спамового засилля.

А тим часом в боротьбі зі спамом є ефективні спеціально призначені для цього програми:

- Telos версії 2.0 сканує вміст поштових ящиків щодо виявлення заголовків спамових листів (які листи віднести до спаму, визначає сам користувач) і видаляє їх. Програма може працювати в автоматичному режимі, скануючи поштові ящики через певні проміжки часу. Telos можна налаштувати і для знищення листів, що приходять з певних адрес: *http://members.xoom.com/bsoft/ telos200.zip* ;
- SpammerSlammer, який працює фільтром між поштовою програмою користувача і POP3-сервером, відсікає небажані листи (критерії небажаності визначаються самим користувачем): *http://sb.nowtools.com/spammerslammer.exe* ;
- Якщо троянському коневі все-таки вдалося якимось чином "пробратися" у комп'ютер, то систему захистить програма Jammer чи Ad–Aware. Вони відстежують спроби запису в реєстр і встановлення з'єднання між серверною і клієнтською частинами трояна: *http://www.agnitum.com/download/jammer.exe* або *http://www.ad–aware.com*.

Лабораторна робота № 2.6. Антивірусний захист електронної пошти

Мета роботи: реалізувати на практиці методику ефективної та безпечної електронної кореспонденції.

Хід виконання роботи.

1. Підготувати типовий демонстраційний псевдовірусний файл ***test.com***, розроблений EICAR (European Institute for Computer Anti–Virus Research), який дає змогу протестувати працездатність антивірусних програм, які знаходять віруси за їхніми сигнатурами (читати інструкцію ***test.txt***) та долучити його в двох електронних листах на власну адресу. Отримати один з цих листів без антивірусного ПЗ і переконатися в безперешкодності запуску долучення з поштового клієнта OutLook Express.

2. Встановити демонстраційну версію антивірусної програми DrWeb v.4.32 з підтримкою поштового клієнта (Spider mail) (читати інструкцію з встановлення програми ***DRWwin.ru***).

3. Отримати другий з підготовлених в п.1 "інфікованих" листів. Долучення TEST.COM визначається більшістю антивірусних програм як вірус. Разом з тим Dr.Web називає цей вірус таким чином: "**EICAR Test File (Not a Virus!)**". Приблизно так його називають й інші антивірусні програми.

4. Перевірити ефективність антивірусного ПЗ при долученні архівних копій ***test.com*** та вмонтованих фрагментів ***test.com*** в документи інших аплікацій (аудіо-, відеофайли, графічні та офісні документи).

5. Отримати за web–адресою http://home.netscape.com/eng/ssl3/ модуль підтримки POP3–SSL та встановити його відповідно до вказівок (***draft302.txt***). Обмінятися листами згідно з протоколом SSL на будь–якому поштовому сервері, що його підтримує (н-д, hotmail.com).

Контрольні запитання до розділу 2

1. Що таке безпека даних у комп'ютерних мережах?
2. Способи ідентифікації за персональними фізичними ознаками.
3. Способи з'єднань комп'ютерів у мережу.
4. Програмне та апаратне забезпечення з'єднання комп'ютерів у мережі.

5. Захист мережі з використанням брандмауерів і серверів- посередників.
6. Захист ресурсів у мережевій ОС Novel NetWare.
7. Захист інформації в ОС Windows NT.
8. Адміністративні засоби управління ресурсами домену Windows NT 4.0.
9. Особливості роботи з пакетами Win Snifter та x Intruder.
10. Інформаційна безпека в ОС UNIX.
11. Робота адміністратора в UNIX мережі.
11. Система Kerberos.
12. Робота з ОС Free BSD 3x, BSD 4x.
13. Захист електронної пошти.

Розділ 3

ФІЗИКО-ТЕХНІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ ТА ТЕЛЕОХОРОНИ

3.1. Загальні питання захисту інформації в автоматизованих системах оброблення даних (АСОД)

Комп'ютеризація всіх сфер діяльності людини, процеси інформатизації, впровадження нових засобів зв'язку з застосуванням мікропроцесорів і мікропроцесорних комплектів для швидкісного передавання і приймання інформації набуває глобального характеру. Інформація стає важливим компонентом соціального прогресу, високоцінним товаром, невід'ємною частиною валового національного продукту країни. Вперше в історії цивілізації зусилля, яке витрачає суспільство на одержання і оброблення знань, перевершили витрати на отримання сировини, енергії, матеріалів і предметів матеріального вжитку. На думку спеціалістів, на початку третього тисячоліття близько половини працівників будуть знаходитися у сфері виробництва інформації. Тому проблема отримання, передання й оброблення інформації набуває особливого значення, оскільки рівень розвитку суспільства значною мірою пов'язаний як з передаванням інформації, так і з технологією зберігання та захисту від несанкціонованого доступу до неї. Заходи з захисту інформації спрямовані на запобігання витоку або порушення її цілісності.

Можна досить наближено звести ці таємниці до двох великих груп: державні таємниці та конфіденційні таємниці – це державна інформація і конфіденційна інформація (комерційна, службова, професійна, персональна – особиста, банківська).

Отже, є внутрішні і зовнішні загрози нашій молодій державі в інформаційній сфері. Перші пов'язані з тим, що розмежовується єдиний інформаційний простір. Другі – з тим, що простежується цілеспрямоване втручання іноземних держав у інформаційний простір України. Особливо це явище посилилося з появою лока-

льних і глобальних комп'ютерних мереж, електронної пошти, широкого обміну інформацією і програмними продуктами у світі через ІНТЕРНЕТ. Зросла можливість несанкціонованого доступу до інформаційних систем держави, тому сьогодні актуальним стає завдання захисту інформації, захисту інформаційних систем та захисту самої людини, тобто гостро стає проблема т. зв. інформаційної безпеки. І українська держава, починаючи з 1995 р., робить перші кроки в цьому напрямку, реалізувавши за допомогою низки стандартів норми законів України "Про інформацію", "Про державну таємницю", "Про захист інформації в автоматизованих системах" і т. п.

У розроблених стандартах України з технічного захисту інформації (ТЗІ) наведені основні положення, терміни і визначення та порядок проведення робіт за ТЗІ. Так, наприклад, ДСТУ 3396.0 – 96 встановлює, що об'єктом технічного захисту є інформація, що становить державну або іншу, передбачену законодавством України, таємницю: конфіденційна інформація, що є державною власністю чи передана державі у володіння, користування, розпорядження, тобто це інформація з обмеженим доступом (ІзОД).

Носіями ІзОД можуть бути фізичні поля, сигнали, хімічні речовини, що утворюються в процесі інформаційної діяльності, виробництва й експлуатації продукції різного призначення. Середовищем поширення носіїв ІзОД можуть бути лінії зв'язку, сигналізації, керування, енергетичні мережі, прикінцеве й проміжне обладнання, інженерні комунікації і споруди, відгороджувальні будівельні конструкції, а також світлопроникні елементи будинків і споруд (отвори), повітряне, водне та ін. середовища, ґрунт, рослинність тощо.

Загальний підхід до захисту інформації має відбуватися такими трьома напрямками:

а) введення міжнародних обмежень на припинення інформаційної війни і завезення інформаційної зброї задля припинення дій "хакерів";
б) вироблення уніфікованих законів про відповідальність усіх країн, у т. ч. і тих держав, звідки надходить інформація;
в) пріоритет вітчизняних засобів захисту інформації.

При реалізації основних прав і свобод людини захист самої людини від зовнішньої шкідливої інформації є визначним для держа-

ви, тому що наслідки цього інформаційного впливу можуть носити негативний характер.

Уже теоретично доведено, а практикою багатократно підтверджено, що психіка і мислення людини схильні до зовнішніх інформаційних впливів, і якщо організовано впливати на людину, то можна запрограмувати її поведінку до самої зміни її віри і світогляду.

Отже, актуальною є проблема не тільки захисту інформації, але й захист від інформації.

Проблема захисту інформації від стороннього доступу і необмежених впливів на неї виникла давно, але зараз, як бачимо, ця проблема різко загострилась, тим більше, що сучасне суспільство входить у постіндустріальний період свого розвитку, який має бути названий інформаційним.

Інформація – це результат відображення й оброблення у людській свідомості розмаїття світу, це знання про оточуючі людину предмети, явища природи, діяльність інших людей і т. п. Оскільки у людському суспільстві завжди є люди, які бажають незаконним шляхом отримати цінну інформацію, то зрозуміло, що у її володаря виникає необхідність її захисту.

Дехто з багатьох науковців розробив свій поділ інформації за рівнем важливості:

1. Життєво важлива, незамінна інформація, наявність якої необхідна для функціонування організму;
2. Важлива інформація – інформація, яка може бути замінена або поновлена, але процес її поновлення досить складний і пов'язаний з великими затратами;
3. Корисна інформація – інформація, яку складно поновити, але організація може ефективно функціонувати і без неї;
4. Несуттєва інформація – інформація, якої більше організація не потребує.

Категорії важливості, як і цінність інформації, змінюються з часом і залежать від ставлення до неї різних споживачів та потенційних злодіїв.

Відповідно до цього поділу інформації, яка обробляється в автоматизованих системах оброблення даних (АСОД), її можна за категоріями важливості і секретності зобразити як піраміду, що складається з декількох шарів по вертикалі. Вершиною піраміди є найбільш важлива інформація, а фундаментом –

несекретна інформація, пов'язана з обробленням більш важливої інформації.

Інформацію оцінюють щодо достовірності і корисності. Частину інформації знищують, а іншу готують до зберігання (систематизують, перетворюють у зручну для зберігання форму, сортують за масивами зберігання). Зі сховища вибирають тільки необхідну інформацію, яку обробляють і використовують.

3.2. Потенційні загрози безпеці інформації в АСОД

Неконтрольоване поширення інформації, яке призводить до її несанкціонованого одержання, називають витоком інформації. Витік, можливість блокування або порушення цілісності інформації (спотворення, руйнування або знищення) і є загрозою для інформації.

Аналіз численних випадків впливів на інформацію та несанкціонованого доступу до неї свідчать, що всі загрози можуть бути розділені на випадкові та навмисні.

Навмисні загрози, з огляду на їхнє систематичне застосування, можуть бути приведені до виконання через випадкові, шляхом довготривалої масованої атаки несанкціонованими запитами або вірусами.

Наслідки, до яких призводить реалізація загроз: руйнування (втрата) інформації, модифікація (заміна інформації на хибну) та ознайомлення з нею сторонніх осіб. Вартість цих подій може бути різною: від невинних непорозумінь до сотень тисяч і більше доларів. Запобігання наслідкам в АСОД і є основною метою утворення системи безпеки інформації.

Для побудови засобів захисту інформації (ЗЗІ) необхідно визначити природу загроз, форми та шляхи їхнього можливого виявлення і здійснення в АСОД.

Випадкові загрози. Дослідження досвіду проектування, виготовлення, випробувань і експлуатації автоматизованих систем засвідчують те, що на інформацію в процесі введення, зберігання, оброблення, виведення і передавання впливають різні випадкові загрози. Однією з таких загроз є організування ненавмисного каналу витоку інформації, коли носії інформації та середовище її поширення формуються самочинно. В результаті таких

впливів на апаратному рівні відбуваються фізичні зміни рівнів сигналів у цифрових кодах, що несуть інформацію.

Водночас спостерігають в одному, двох, трьох і т.д. розрядах зміни 1 на 0 чи 0 на 1, чи перше і друге разом, але в різних розрядах, унаслідок чого змінюється код. Якщо засоби функціонального контролю, що їх використовують з цією метою, здатні виявити зміни (наприклад, контроль за модулем 2 легко виявляє однократну помилку), вибраковується код, а пристрій, блок, модуль чи мікросхема, що задіяні в обробленні, оголошуються несправними. Якщо функціонального контролю немає чи він не може виявити несправність на етапі оброблення, процес продовжується хибним шляхом, тобто відбувається модифікація інформації. В процесі дальшого оброблення (залежно від змісту і призначення хибної команди) можливі або пересилання інформації за хибною адресою, або стирання чи запис іншої інформації адресату, або стирання чи запис іншої інформації в ОЗП чи ПЗП, тобто виникають небажані події: руйнування і витік інформації.

На програмному рівні в результаті випадкових впливів може відбутися зміна алгоритму обробленя інформації на непередбачений, характер якого теж може бути різним: в кращому випадку – зупинення обчислювального процесу, а в гіршому – його модифікація. Якщо засоби функціонального контролю зміну алгоритму не виявлять, наслідки модифікації алгоритму чи даних можуть бути невиявленими, пройти непоміченими, що може призвести до руйнування інформації, а при зміні адреси пристрою – до витоку інформації. У разі програмних помилок можуть підключатися програми введення-виведення і передавання їх на заборонені пристрої.

Причинами випадкових впливів при експлуатації автоматизованої системи можуть бути:

- відмови і збої апаратури;
- завади в лініях зв'язку від впливів зовнішніх чинників;
- помилки людини як складової системи;
- схемні і системотехнічні помилки проектантів;
- структурні, алгоритмічні і програмні помилки;
- аварійні ситуації та інші впливи.

Частота відмов і збої апаратури збільшуються при виборі і проектуванні системи, яка є слабкою щодо надійності функціонування апаратури. Завади в лініях зв'язку залежать від прави-

льності вибору розміщення технічних засобів АСОД відносно один одного і щодо апарата і агрегатів сусідніх систем.

Під час розроблення складних автоматизованих систем збільшується число схемних, схемотехнічних, структурних, алгоритмічних і програмних помилок. На їхню кількість у процесі проектування великий вплив має багато інших чинників: кваліфікація проектантів, умови роботи, наявність досвіду і ін.

На етапах виготовлення і випробувань на якість апаратури, що входить у АСОД, впливають повнота і якість документації, за якою її виготовляють, технологічна дисципліна тощо.

До помилок людини, як ланки системи, відносять помилки людини як джерела інформації, людини-оператора, неправильні дії обслуговуючого персоналу і помилки людини як ланки, що приймає рішення.

Помилки людини бувають логічні (неправильно прийняті рішення), сенсорні (неправильне сприйняття оператором інформації) й оперативні, чи моторні (неправильна реалізація рішення). Інтенсивність помилок людини може коливатися в широких межах: від (1–2)% до (15–40)% і вище від загального числа операцій, що виконуються при вирішенні задачі.

До загроз випадкового характеру відносять аварійні ситуації, які можуть виникнути на об'єкті розміщення автоматизованої системи. До аварійних ситуацій належать:

- відмова функціонування АСОД, наприклад, вихід з ладу електроживлення й освітлення;
- стихійні лиха: пожежа, повінь, землетрус, урагани, удари блискавки, обвали і т. п.;
- відмова систем життєзабезпечення на об'єкті експлуатації АСОД.

Імовірність цих подій пов'язана передусім з правильним вибором розміщення АСОД, включаючи географічне положення, й організуванням протипожежних заходів.

Навмисні загрози. Утворення штучного каналу витоку інформації є навмисною цілеспрямованою загрозою, яка пов'язана з діями людини. Причинами цих дій можуть бути: невдоволення своєю життєвою ситуацією, чисто матеріальний інтерес чи проста розвага з самоствердженням, як у хакерів і т.п. Зауважимо одразу, що вивчення мотивів поведінки порушника є завданням певних структур. Наше завдання – запобігання, виявлення і блокування можливих негативних дій в

АСОД. Потенційні загрози з цього боку розглядатимемо тільки в технічному аспекті.

Для того, щоб поставити завдання більш конкретно, проаналізуємо об'єкт захисту інформації щодо введення-виведення, зберігання й оброблення інформації і можливостей порушника з доступу до інформації при браку засобів захисту в цій автоматизованій системі.

Об'єктом захисту виберемо обчислювальну систему, що може бути елементом обчислювальної мережі. Для обчислювальної системи в цьому випадку характерні такі штатні (законні) канали доступу до інформації:

- термінали користувачів;
- термінал адміністратора системи;
- термінал оператора функціонального контролю;
- засоби відображення інформації;
- засоби документування інформації;
- засоби завантаження програмного забезпечення в обчислювальний комплекс;
- носії інформації (ОЗП, ПЗП, паперові носії);
- зовнішні канали зв'язку.

Маючи на увазі, що без захисту порушник може використати як штатні, так і інші фізичні можливі канали доступу, назвемо ймовірні канали несанкціонованого доступу (ЙКНСД) в обчислювальній системі, через які з'являється доступ до апаратури, програмного забезпечення і здійснення крадіжки, руйнування, модифікації інформації й ознайомлення з нею:

а) усі описані штатні засоби при їхньому використанні законними користувачами не за призначенням і за межами своїх повноважень;
б) усі описані штатні засоби при їхньому використанні сторонніми особами;
в) технологічні пульти управління;
г) внутрішній монтаж апаратури;
ґ) лінії зв'язку між апаратними засобами обчислювальної системи;
д) побічне електромагнітне випромінювання інформації з апаратури системи;
е) побічні спотворення інформації по колу електроживлення і заземлення апаратури;
є) побічні спотворення інформації на допоміжних і сторонніх комунікаціях;

ж) відходи оброблення інформації у вигляді паперових і магнітних носіїв, викинутих у смітникову корзину.

Очевидно, що без законного користувача, контролю і розмежування доступу до терміналів, кваліфікований порушник дуже легко скористається його функціональними можливостями для несанкціонованого доступу до інформації шляхом уведення відповідних запитів і команд. При наявності вільного доступу в приміщення можна візуально спостерігати інформацію на засобах відображення і документування, а на останніх вкрасти паперові носії, зняти зайву копію, а також викрасти інші носії з інформацією. Особливо небезпечним є безконтрольне завантаження програмного забезпечення в ЕОМ, в якому можуть бути змінені дані, алгоритми чи введена програма "троянський кінь" (програма, що виконує додаткові незаконні функції: записує інформацію на сторонній носій, передає її каналами зв'язку іншому абоненту обчислювальної мережі, вносить у систему комп'ютерний вірус і т.п.). При відсутності розмежування і контролю доступу до технологічної і оперативної інформації можливий доступ до оперативної інформації з боку термінала функціонального контролю. Небезпечною є ситуація, коли порушником є користувач обчислювальної системи, який за своїми функціональними обов'язками має законний доступ до однієї частини інформації, а звертається до іншої – за межами своїх повноважень.

З боку законного користувача є багато способів, щоб порушити роботу обчислювальної системи, зловживати нею, добувати, модифікувати чи знищувати інформацію. Для цієї мети можуть бути використані привілейовані команди введення-виведення, безконтрольні запити і звертання до адрес пам'яті ОЗП, ПЗП і т.п. При неоднозначній ідентифікації ресурсів порушник може подавити системну бібліотеку своєю бібліотекою, а модуль, що завантажується з його бібліотеки, може бути введений у супервізорному режимі. Вільний доступ дає змогу йому звертатися до чужих файлів і банків даних і змінювати їх випадково чи цілеспрямовано.

При технічному обслуговуванні (профілактиці чи ремонті) апаратури можуть бути виявлені залишки інформації. Стирання інформації звичайними методами не завжди ефективне. Її залишки можуть бути легко прочитані. При транспортуванні носія по території, що не охороняється, є небезпека його перехоплення

та дальше ознайомлення сторонніх осіб з секретною інформацією.

Немає сенсу створювати системи контролю і розмежування доступу до інформації на програмному рівні, якщо не контролюється доступ до пульта управління ЕОМ, до внутрішнього монтажу апаратури та кабельних з'єднувачів.

Порушник може стати законним користувачем системи в режимі розділення часу, визначивши порядок роботи законного користувача або працюючи вслід за ним по одних і тих самих лініях зв'язку. Він може також використати метод проб і помилок, реалізувавши "дірки" в операційній системі, прочитавши паролі. Без знання паролів він може "селективно" підключитися в лінію зв'язку між терміналом і процесором; без переривання роботи законного користувача може продовжити її від його імені, відмінивши сигнали відключення законного користувача.

Процеси оброблення, передавання і зберігання інформації апаратними засобами автоматизованої системи забезпечуються спрацюванням логічних елементів, побудованих на базі напівпровідникових приладів, які часто реалізовані у вигляді інтегральних схем.

Спрацювання логічних елементів зумовлено високочастотною зміною рівнів напруг і струмів, що приводить до виникнення в ефірі, колах живлення і заземлення, а також у паралельно розміщених колах і індуктивностях сторонньої апаратури, електромагнітних полів і наводок, які несуть у амплітуді, фазі і частоті своїх коливань ознаки оброблюваної інформації. Використання порушником різноманітних приймачів може спричинити витік інформації. Зі зменшенням відстані між приймачем порушника й апаратними засобами ймовірність приймання сигналів такого характеру збільшується.

Безпосереднє підключення порушником приймальної апаратури і спеціальних сенсорів до кіл електроживлення, заземлення, до каналів зв'язку також дає змогу здійснювати несанкціоноване ознайомлення з інформацією, а несанкціоноване підключення до зв'язку передавальної апаратури може призвести і до її модифікації.

Особливо потрібно остерігатися загроз, які впливають на канали і лінії зв'язку обчислювальної мережі.

Припустимо, що порушник може знаходиться в певній точці мережі, через яку має проходити вся інформація, що його цікавить. Наприклад, у міжмережевих умовах порушник може прийняти вигляд шлюзу в деякій проміжній мережі, яка забезпечує єдиний шлях з'єднання між двома процесорами, що є кінцями з'єднання, яке цікавить порушника. В цьому випадку, незважаючи на те, що мережа-джерело (А) і мережа адресата (Г) захищені, порушник може діяти на з'єднання, оскільки воно проходить через шлюз, що з'єднує мережі Б і В. Вважають, що порушник може займати позицію, яка дає змогу здійснювати пасивне й активне перехоплення.

У разі пасивного перехоплення порушник тільки і слідкує за повідомленнями, розкриваючи їхній зміст. Порушник може також слідкувати за заголовками повідомлень, навіть якщо дані не зрозумілі йому, з метою визначення місця розміщення й ідентифікаторів процесів, що беруть участь у передаванні даних. Порушник може визначити довжини повідомлень, частоту їхнього передавання для визначення характеру даних, які передають, тобто проаналізувати потік повідомлень.

Порушник може також займатись активним перехопленням, виконуючи різні дії над повідомленнями, що їх передають з'єднанню. Ці повідомлення можуть бути вибірково змінені, знищені, затримані, перевпорядковані, задубльовані і введені в з'єднання пізніше. Порушник може створювати фальшиві повідомлення і вводити їх у з'єднання. Подібні дії можна визначити як зміну потоку і змісту повідомлень.

Крім того, порушник може скидати всі повідомлення чи затримувати їх. Подібні дії можна класифікувати як переривання передавання повідомлень.

Спроби використовувати запис попередніх послідовностей повідомлень за ініціюванням з'єднань класифікують як ініціювання хибного з'єднання.

За останній час у різних країнах проведений великий обсяг дослідницьких робіт з метою виявлення потенційних каналів несанкціонованого доступу до інформації в обчислювальних мережах. Разом з тим розглядали не тільки можливості порушника, що отримав законний доступ до обладнання мережі, але й впливи, зумовлені помилками програмного забезпечення чи властивостями протоколів мережі, що їх використовують. Вивчення

каналів несанкціонованого доступу продовжується до сих пір, тому на початку 80-х років минулого століття були сформульовані п'ять основних категорій загроз безпеці даних в обчислювальних мережах:

1) розкриття змісту повідомлень;
2) аналіз трафіку, що дає можливість визначити належність відправника й одержувача даних до однієї з груп користувачів мережі, пов'язаних спільною задачею;
3) зміна потоку повідомлень, що може призвести до порушення режиму роботи якого-небудь об'єкта, що управляється з віддаленої ЕОМ;
4) неправомірна відмова в наданні послуг;
5) несанкціоноване встановлення зв'язку.

Такий підхід не суперечить визначенню терміна "безпека інформації" і поділу потенційних загроз на витік, модифікацію і втрату інформації. Насправді загрози 1 і 2 можна віднести до витоку інформації, загрози 3 і 5 – до її модифікації, а загрозу 4 – до порушення процесу обміну інформацією, тобто до її втрати для одержувача.

В обчислювальних мережах порушник може використовувати такі стратегії:

1) отримати несанкціонований доступ до секретної інформації;
2) видати себе за іншого користувача, щоб зняти з себе відповідальність або ж використати його повноваження з метою формування неправдивої інформації, використання фальшивого посвідчення особи, санкціонування удаваних обмінів інформацією або ж її підтвердження;
3) відмовитися від факту формування інформації, що була передана;
4) стверджувати, що інформація отримана від певного користувача, хоча насправді вона сформована самим порушником;
5) стверджувати, що користувачу в певний момент була надіслана інформація, яку насправді не надсилали (чи надсилали в інший час);
6) відмовитися від факту отримання інформації, яка насправді була отримана, чи стверджувати про інший час її отримання:

7) незаконно розширити свої повноваження щодо доступу до інформації та її оброблення;
8) незаконно змінити повноваження інших користувачів (розширити чи обмежити, вивести чи ввести других осіб);
9) приховати факт наявності певної інформації в іншій інформації (приховане передання однієї у змісті іншої);
10) підключитися до лінії зв'язку між другими користувачами як активного ретранслятора;
11) вивчити, хто, коли і до якої інформації має доступ (навіть, якщо сама інформація залишається недоступною);
12) заявити про сумнівність протоколу забезпечення інформацією через розкриття певної інформації, яка згідно з умовами протоколу має залишатися секретною;
13) модифікувати програмне забезпечення шляхом вилучення чи додавання нових функцій;
14) цілеспрямовано змінити протокол обміну інформацією з метою його порушення чи підриву довіри до нього;
15) завадити обміну повідомленнями між другими користувачами шляхом введення завад з метою порушення автентифікації повідомлень.

Аналіз описаних можливих стратегій порушника в обчислювальній системі свідчить про те, наскільки важливо знати, кого вважати порушником. Як порушника розглядають не тільки сторонню особу, але й законного користувача. Напевне, ці завдання слід розглядати окремо. З цих позицій наведені вище п'ять видів загроз характерні для поведінки стороннього порушника: 1, 10, 11, 15.

Аналіз загроз свідчить про те, що завдання захисту від них можна умовно розділити на завдання двох рівнів: користувачів і елементів мережі, з якими працюють користувачі мережі. До рівня елементів мережі можна віднести загрози під номерами 2, 7, 8, 13 і 14. Рівень взаємовідносин користувачів називають рівнем довіри одного користувача до іншого. Для забезпечення гарантій цієї довіри, очевидно, потрібні спеціальні засоби і критерії оцінення їхньої ефективності.

3.3. Обмеження, розмежування і контроль доступу до апаратури

Сучасні методи захисту інформації включають до свого складу такі поняття, як обмеження, розмежування та контроль доступу до інформації, тобто до об'єкта захисту.

Обмеження доступу полягає, як ми вже зазначали, в утворенні певної фізичної замкненої перепони навколо об'єкта захисту з організуванням контрольованого доступу осіб, які пов'язані з об'єктом захисту своїми функціональними обов'язками.

Обмеження доступу до комплексів засобів автоматизації (КЗА) оброблення інформації полягає:

- у виділенні спеціальної території для розміщення КЗА;
- у побудові по периметру зони спеціальних огороджень з охоронною сигналізацією;
- у побудові спеціальних будівель або інших споруджень;
- у виділенні спеціальних приміщень у будинку;
- у створенні контрольно-пропускного режиму на території, в будинках та приміщеннях.

Завданням засобів обмеження доступу є виключення випадкового і навмисного доступу сторонніх осіб на територію розміщення КЗА і безпосередньо до апаратури. З цією метою утворюється захисний контур, який замикається двома видами перешкод (перепон): фізичною і контрольно-пропускною. Такі перепони часто називають системою охоронної сигналізації і системою контролю доступу.

Традиційні засоби контролю доступу у зону захисту – це виготовлення і надання допущеним особам спеціальних перепусток з розміщеною на ній фотографією особистості власника та відомостей про нього. Такі перепустки можуть зберігатися у власника або безпосередньо у пропускній кабіні охорони. В останньому випадку допущена особа називає прізвище і свій номер, або набирає його на спеціальній панелі кабіни при проходженні через турнікет. Перепустка-посвідчення випадає з касети і потрапляє до рук працівника охорони, котрий візуально звіряє особу власника з відображенням його на фотографії, назване прізвище з прізвищем на перепустці. Ефективність захисту та-

кої системи краща (вища) від першої. Разом з тим виключається: втрата перепустки; її перехоплення і підробка.

Окрім того, ще є резерв у підвищенні ефективності захисту за допомогою збільшення кількості параметрів, що перевіряються. Але основне навантаження лягає на людину, а вона, як відомо, може помилятися.

У зарубіжній літературі є повідомлення про застосування біометричних методів автентифікації людини, коли використовують ідентифікаторами відбитки пальців, долоні, голос, особистий підпис і т.п. (сканер долоні фірми Northern Computers, Inc (Великобританія), типу ID3D має час перевірки 2°с, а габарити його становлять 16,4×21×18,5 см).

На побутовому рівні це настільки звичний для людського мозку процес, що відбувається миттєво на рівні підсвідомості. Однак попри легкість та природність такої процедури, спроба її реалізації технічними засобами наштовхується на істотні труднощі.

Перша робота з біометрики була опублікована в 1864 році доктором Нейманом Гроу, який запропонував ідентифікувати особу за відбитком пальців, а уже в 1905 році у Лондонському суді підсудний був засуджений до смертної кари на основі ідентифікації відбитків пальців. З тих часів біометрика зробила великий крок вперед – від відбитків пальців до бази даних ДНК. Сьогодні біометрика займається двома питаннями: отримання даних та їхня верифікація (ідентифікація особи; порівняння щойно одержаних даних з даними, що отримані раніше і які зберігаються в пам'яті).

Значущість біометрики як складової сучасних інформаційних технологій важко переоцінити. Сьогодні проводять інтенсивні роботи з запровадження засобів біометрики не тільки у таких областях, як захист інформації й об'єктів, але і в кримінальній медицині, при юридичному підтвердженні права власності чи користуванні, контролю та обліковуванні використання різних ресурсів, службах соціального забезпечення, еміграційних службах тощо.

Незалежно від методу реалізації, засоби біометрики складаються з таких структурних компонентів:

- механізму автоматичного сканування інформативного параметра (характеристики особи);
- блоків оброблення одержаного сигналу (фільтрація, стиснення, формування і запам'ятовування образу);
- пристрою для зіставлення поточного образу з даними, що зберігаються в пам'яті;

- інтерфейсного вузла, що забезпечує взаємодію біометричного пристрою з системою, в якій цей пристрій може виступати як складова.

Використанню біометричних пристроїв передує етап навчання, на якому створюють еталонні математичні образи осіб, що ідентифікуються вперше (реєстрація абонентів). Надалі у процесі функціонування системи формування робочого образу, який використовують для зіставлення з еталонним, здійснюється багатократно, тобто щоразу при спробі особи ввійти у систему.

Найважливішою класифікаційною ознакою біометричних засобів є фізіологічний параметр чи процес, або ж їхня комбінація, що лежить в основі створення математичного образу особи. Придатними можуть вважатися лише такі характеристики, що надають двом найважливішим вимогам унікальності та стійкості. Під унікальністю слід розуміти таку властивість фізіологічної характеристики людини, яка дає змогу гарантовано виділяти кожну особу через маси інших. Стійкість можна трактувати як незмінність у часі вибраного фізіологічного параметра, його відтворюваність. Між унікальністю та стійкістю наявний суперечливий зв'язок: унікальність можна посилювати ускладненням образу, але лише до межі, при якій ще забезпечується відтворюваність образу особи як в часі, так і на фоні інших перешкоджаючих факторів.

Можна виділити три типи біометричних систем, які реалізують фізіологічні, поведінкові і змішані методи розпізнавання. Фізіологічні методи спираються на статичні характеристики людини, що є відносно стабільними, якщо звичайно особа не травмована. Найпоширенішими серед цієї групи є методи розпізнавання, як відзначено попередньо, за відбитками пальців, за формою долоні, за райдужною оболонкою ока, за сітківкою ока, за зображенням обличчя. Поведінкові методи полягають в оціненні певних дій користувача. Серед поведінкових виділяють методи розпізнавання за підписом, за голосом і за манерою роботи на клавіатурі. Також є системи, в яких поєднано фізіологічні і поведінкові методи. Найбільш характерними комбінаціями є методи розпізнавання за відбитками пальців і голосом, за відбитками пальців і зображенням обличчя, за зображенням обличчя і голосом. Сьогодні системи, робота яких базується на використанні поведінкових характеристик, не здатні забезпечити такий

рівень захисту, який властивий системам, що працюють з фізіологічними характеристиками. Насамперед це пов'язано зі значною залежністю поведінкових характеристик від факторів, що впливають на людину (здоров'я, настрій або ж емоційний стан).

Для біометричних пристроїв, використовуваних у системах захисту інформації, визначальними є такі характеристики, як надійність, пропускна здатність, ергономічність, толерантність і обсяг математичного шаблону. Вони формуються в процесі досліджень системи і на їхній основі оцінюють якість системи загалом.

Надійність систем розмежування доступу прийнято оцінювати за такими показниками, як рівень неправильного дозволу на допуск (РНДД) і рівень неправильної відмови у допуску (РНВД). РНДД – це виражене у відсотках число хибних допусків системою неавторизованих осіб за певний період функціонування системи. РНВД – це виражене у відсотках число помилкових відмов системи у доступі авторизованим особам за певний період функціонування системи. Між цими показниками наявний взаємообернений зв'язок: підвищуючи чутливість системи, збільшують значення РНВД, водночас зменшуючи РНДД. Очевидно, для кожної біометричної системи необхідно віднайти певний оптимум, за якого величина сумарних помилок системи буде мінімальною.

Пропускна здатність є дуже важливою характеристикою засобів біометрики і нерідко саме цей показник стає вирішальним при виборі того чи іншого пристрою. Обсяг математичного шаблону також дуже важливий показник. Адже між обсягом пам'яті, що його займає кодова інтерпретація образу, та пропускною здатністю системи є пряма залежність.

Потрібно додати, що вартість біометричних пристроїв також вважають одним із головних показників у картині загального оціненння якості. Щодо ергономічності і толерантності, то кожен біометричний пристрій має відповідати мінімальним вимогам зручності у користуванні, універсальності, естетичності і гігієни. Крім того, сам процес розпізнавання не має спричиняти у користувачів дискомфорт, страх та інші неприємні відчуття.

Організовуючи захист особливо важливих об'єктів з використанням біометричних систем контролю доступу, не можна не враховувати зростаючу освіченість та технічну оснащеність зло-

вмисників, спроможних виготовити і використовувати для "обману" систем імітацію описаних персональних характеристик суб'єктів, що володіють правом доступу. З цієї причини біометричні системи ідентифікації доповнюють і дублюють різними апаратними засобами, що у підсумку дає можливість підвищувати їхню надійність.

Деякі системи та пристрої, що реалізують біометричні технології, вже сертифіковані міжнародною асоціацією з комп'ютерної безпеки.

3.4. Системи охоронної сигналізації (СОС)

Гарантувати ефективність роботи систем охоронної сигналізації (СОС) можливо лише в тому випадку, якщо забезпечити надійність всіх їхніх елементів та їхнє узгоджене функціонування. Тут має значення все: тип сенсора, спосіб повідомлення і контролю, перешкодостійкість, а також реакція на сигнал тривоги.

Місцева звукова або світлова сигналізації можуть бути недостатніми, тому місцеві засоби охорони доцільно підключати до спеціалізованих засобів централізованого управління, коли при одержанні сигналу тривоги направляється на місце спеціалізована група охорони (захист квартир, офісів, магазинів, малих підприємств).

Слідкувати за станом сенсорів, як ми вже зазначали, може автоматична система, розміщена в центрі управління, або співробітник охорони, який знаходиться на об'єкті і при появі світлового або звукового сигналу приймає відповідне рішення.

В першому випадку місцеві охоронні засоби – пристрої вмикаються до центральної системи через телефонні лінії зв'язку, а спеціалізований цифровий пристрій здійснює періодичне опитування стану сенсорів, автоматично набираючи номер прийомовідповідача, який знаходиться на об'єкті, що охороняється. При надходженні до центру сигналу тривоги автоматична система вмикає сигнал повідомлення.

Сенсори сигналів встановлюють на різного роду огорожах, у середині приміщень, безпосередньо на вікнах і стелях, сейфах і т.п.

Розробляючи комплексну систему охорони конкретного об'єкта, треба враховувати його специфіку: внутрішній план

будівлі, планування вікон, вхідних дверей; розміщення найбільш важливих технічних засобів. Бо всі ці фактори впливають на вибір типу сенсорів, їхнє розміщення і визначають низку інших особливостей системи.

За принципом дії системи тривожної сигналізації можна класифікувати таким чином:

- традиційні (звичайні), які базуються на використанні кіл сигналізації та індикації у комплексі з різними контактами (сенсорами);
- ультразвукові;
- з давачами руху;
- переривання променя;
- телевізійні;
- радіолокаційні;
- мікрохвильові;
- інші.

З метою контролю доступу до внутрішнього монтажу, лінії зв'язку та технологічних органів управління використовують апаратуру контролю розкриття апаратури. Це означає, що внутрішній монтаж апаратури і технологічні органи та пункти управління закриті кришками, дверцятами або кожухами, на яких встановлені сенсори. Сенсори спрацьовують при розкритті апаратури і видають електричні сигнали, які по колу збору надходять на централізований пристрій контролю. Установка такої системи має сенс при найбільш повному перекритті всіх технологічних підходів до апаратури, вбираючи і засоби завантаження програмного забезпечення, пульт управління ЕОМ і зовнішні кабельні з'єднання технічних засобів, які входять до складу обчислювальної системи.

В ідеальному випадку для систем з підвищеними вимогами ефективності захисту інформації доцільно закривати кришками під механічний замок з сенсором або ставити під контроль вмикання також штатних засобів входу в систему – терміналів користувачів.

Контроль розкриття апаратури необхідний не тільки в інтересах захисту інформації від несанкціонованого доступу (НСД), але й для додержання технологічної дисципліни з метою забезпечення нормального функціонування обчислювальної системи, тому що дуже часто при експлуатації паралельно до вирішення

основних задач відбувається ремонт або профілактика апаратури, і може статися таке, що випадково забули підключити кабель або з пульта ЕОМ програму оброблення інформації.

Отже, з позицій захисту інформації від несанкціонованого доступу, контроль розкриття апаратури захищає від дій:

- зміни і руйнування принципової схеми обчислювальної системи й апаратури;
- підключення стороннього пристрою;
- завантаження сторонніх програм та "вірусів" у систему;
- зміну алгоритму роботи ОС шляхом використання технологічних пультів та органів управління;
- завантаження сторонніх програм і внесення програмних "вірусів" у систему;
- використання терміналів сторонніми особами і т. п.

Основним завданням системи контролю розкриття апаратури є перекриття на період експлуатації всіх позаштатних і технологічних підходів до апаратури. Якщо останні знадобляться в процесі експлуатації системи, то апаратуру, яку виводять на ремонт або профілактику, перед початком робіт вимикають від робочого контуру обміну інформацією, яка підлягає захисту, і вводять у робочий контур під наглядом і контролем осіб, які відповідальні за безпеку інформації.

Доступ до штатних входів у систему – терміналом контролюється за допомогою контролю за видачею механічних ключів користувачам, а доступ до інформації – за допомогою системи розпізнавання і розмежування доступу, в якій передбачено застосування кодованих паролів, за допомогою відповідних функціональних задач програмного забезпечення та спеціального термінала служб інформації підприємства (фірми).

Термінал і пристрій контролю розкриття апаратури є у складі робочого місця служби безпеки інформації, адже саме з цього місця відбувається централізований контроль за доступом до апаратури й інформації, а також управління її захистом на АСОД.

3.5. Сучасні системи контролю доступу

Системи контролю доступу (СКД) є найдавнішою складовою системи безпеки.

Електронні системи контролю доступу почали широко використовувати у системах безпеки з 80-х років минулого сторіччя у зв'язку з розвитком мікропроцесорної техніки.

Масове впровадження цих систем в Україні почалося з 1993–1997 років. За останні десять років сучасні системи контролю доступу (ССКД) набули в Україні широкого застосування.

За можливістю об'єднання контролерів поділено на дві основні групи: а) автономні контролери; б) мережеві контролери.

Автономні контролери зазвичай працюють з одним виконавчим пристроєм, у них не передбачено можливості об'єднання з іншими аналогічними контролерами. Простим прикладом таких систем є замки з вмонтованими кодонабірними клавіатурами і зчитувачами пластикових карт. Ці пристрої об'єднані з кодонабірною клавіатурою і зчитувачем карт, а деякі моделі дають можливість додатково приєднувати принтер для реєстрації подій. Для професійних систем безпеки автономні контролери рідко застосовують.

Мережеві контролери дають змогу об'єднати в єдину систему від двох до декількох сотень контролерів. Їх поділено за ємністю на малі (до 16 пристроїв ідентифікації), середні (від 16 до 32 пристроїв ідентифікації) і великі (більше 32 пристроїв ідентифікації).

До одного мережевого контролера, залежно від його моделі, можна підключити два і більше пристроїв ідентифікації і виконавчих пристроїв. Здебільшого в мережевих контролерах передбачено використання в системі персонального комп'ютера, за допомогою якого слідкують за роботою системи, управляють нею і вносять необхідні зміни в її бази даних.

У випадку найпростіших систем база даних може зберігатися на персональному комп'ютері, але стійкість роботи таких систем щодо зовнішніх впливів досить мала (якщо виходить з ладу комп'ютер, вся система припиняє свою роботу). Більшість контролерів може працювати як в діалоговому, так і в буферному (автономному) режимах, що значно підвищує стійкість усієї системи контролю доступу. Додатково ці пристрої можуть контролювати шлейфи охоронно-пожежної сигналізації і додаткові релейні

виходи для управління системами теленагляду, оповіщення і пожежогасіння.

Можливості програмного забезпечення для мережевих контролерів дуже великі: є змога відтворювати місця спрацювання пристрою ідентифікації, керувати додатковими системами (наприклад, телевізійними), вести облік робочого часу співробітників, визначати їхнє можливе місцезнаходження, тестувати систему і т. ін. Окрім цього, є можливість підтримувати комп'ютерні мережі з різними робочими станціями, правами доступу і передавання інформації по телефонній мережі зв'язку.

3.6. Архітектура побудови систем контролю доступу

За архітектурою побудови всі системи контролю доступу на базі мережевих контролерів можна поділити на три групи:

- системи з зосередженою логікою;
- системи з розподіленою логікою;
- комп'ютерні системи.

Системи з зосередженою логікою. Головною ознакою системи з зосередженою логікою є те, що кожний її елемент є повністю функціонально завершеним модулем, об'єднаним у мережу разом з іншими елементами.

Кожний контролер такої системи вміщує в собі практично всю максимально можливу конфігурацію, незалежно від того, чи потрібні в якомусь конкретному випадку і місці ці функції, чи ні. Внаслідок цього такі системи достатньо прості у проектуванні і встановленні, досить стійкі до несприятливих зовнішніх впливів, але їхня собівартість вища, ніж інших.

Системи з розподіленою логікою. Особливістю таких систем є фізичне розділення окремих частин контролера СКД у вигляді окремих модулів.

Системи зазвичай мають т. зв. інтелектуальні пристрої ідентифікації, в яких інтегрована частина схем контролера. Варіанти побудови таких систем можуть по-різному розподіляти різні функції контролера. Системи дуже гнучкі у побудові необхідної на об'єкті конфігурації і виграють у вартості при побудові великих систем (більше 10 пристроїв ідентифікації). Прикладом може бути система фірми Apollo (США).

Комп'ютерні системи. В комп'ютерних системах база даних та буфер обліку наявні лише всередині керуючої програми, і в тому випадку, коли програма або комп'ютер дасть збій, вся система стає непрацездатною. Тому для вирішення завдань безпеки такі системи практично не використовують, незважаючи на їхню низьку вартість і велику кількість фірм, які їх випускають. Це системи суто офісного типу.

Отже, класифікація систем контролю доступу є достатньо умовною. Визначення розмірів системи за числом пристроїв ідентифікації, а не за числом контрольованих дверей, більш показне, оскільки на кожні двері може припадати один або два пристрої ідентифікації, залежно від застосованої технології проходження. При застосуванні технології проходження "вхід за пристроєм ідентифікації/ вихід вільний" вартість системи нижча, але ускладнюється облік робочого часу, бо губиться інформація про те, хто саме вийшов. Технологія проходження "вхід і вихід за пристроєм ідентифікації" дає змогу повніше реалізувати можливості системи, але вартість її вища.

Лабораторна робота № 3.1. Біометрія як засіб ідентифікації особи в охоронних системах

Мета роботи: порівняння отриманих відбитків пальців з даними бази даних відбитків санкціонованих осіб та встановлення їхньої ідентичності.

Прилади та матеріали:

- комп'ютерна система з інстальованим пакетом програм оброблення графічних зображень Paint;
- Сканер Bear@Paw 2400 CU Plus;
- Лазерний принтер;
- Приладдя для зняття відбитків пальців.

Хід виконання роботи.

1. Отримати відбитки пальців ідентифікованої особи та сканувати їхнє зображення.
2. За допомогою пакета Paint порівняти отримане зображення з зображеннями відбитків у базі даних відбитків допущених осіб.
3. Роздрукувати отримане зображення на прозорому папері.
4. Встановити біометричну ідентичність порівнюваних відбитків.

3.7. Засоби захисту інформації АСОД та їхня класифікація

Сьогодні зроблений дуже великий за номенклатурою перелік різноманітних засобів захисту інформації, за допомогою яких може бути забезпечено певний рівень безпеки інформації в АСОД.

З-поміж способів захисту інформації зазначимо такі, як: перепони, управління, маскування, регламентація, примушування, спонукання.

Розглянемо їх детальніше:

- перепона полягає у створенні на шляху виникнення або розповсюдження дестабілізуючого фактора певного бар'єра, який не дає змоги цьому фактору набувати загрозливих розмірів. Типовими прикладами перепон є блокування, що не дає можливості технічному пристрою або програмі вийти за небезпечні межі; утворення фізичних перепон на шляху зловмисника і т. д.;
- управління – це визначення на кожному кроці функціонування АСОД таких керуючих впливів на елементи системи, наслідком яких буде рішення (або сприяння рішенню) однієї або декількох задач ЗІ;
- маскування (інформація, що її захищають) передбачає таке перетворення, внаслідок якого інформація стає недоступною для зловмисника або доступ до неї суттєво ускладнений;
- регламентація, як спосіб ЗІ полягає в розробленні і реалізації в процесі функціонування АСОД комплексу заходів, які утворюють такі умови оброблення інформації, при яких суттєво ускладнюється проявлення і вплив дестабілізуючих факторів;
- примушування – це також спосіб захисту, при якому користувачі і персонал АСОД вимушені дотримуватися правил і умов оброблення під загрозою матеріальної, адміністративної або карної відповідальності;
- спонукання є способом ЗІ, при якому користувачі та персонал АСОД внутрішніми (матеріальними, моральними, етичними, психологічними та ін.) методами змушені до дотримуватися всіх правил оброблення інформації.

Розглянуті способи забезпечення захисту інформації реалізуються в АСОД шляхом застосування різних засобів, як формальних, так і неформальних. До формальних відносять такі засоби, які виконують свої функції за ЗІ формально, переважно без участі людини; до

неформальних – засоби, в основі яких знаходиться діяльність людей.

Формальні засоби поділяють на технічні (фізичні) й апаратні, та програмні; неформальні – це організаційні, законодавчі і морально-етичні.

До фізичних засобів відносять механічні, електричні, електромеханічні, електронні, електронно-механічні і т.п. пристрої і системи, які функціонують автономно, створюючи різного роду перешкоди на шляху дестабілізуючих факторів.

До апаратних засобів відносять електронні, електронно-механічні і т.п. пристрої, які схемно вмонтовують в апаратуру системи оброблення даних або об'єднують з нею спеціально для вирішення задачі ЗІ.

До програмних засобів відносять спеціальні пакети програм або окремі програми, які включають (входять) до складу програмного забезпечення АСОД з метою вирішення задач ЗІ.

До організаційних засобів відносять комплекс організаційно-технічних заходів, який спеціально передбачений в технології функціонування АСОД з метою вирішення задач ЗІ.

До законодавчих засобів відносять нормативно-правові акти за допомогою яких регламентують права й обов'язки, а також встановлюють відповідальність усіх осіб і підрозділів, які мають відношення до функціонування системи, за порушення правил оброблення даних, наслідком яких може стати порушення її захищеності.

До морально-етичних заходів відносять моральні норми, або правила, які склалися у суспільстві або колективі.

Якщо законодавчі засоби сформовано шляхом видання відповідних юридичних актів, що є прерогативою відповідних органів, то морально-етичні норми формуються в процесі життєдіяльності суспільства.

Технічні засоби захисту. Діяльність, спрямована на запобігання витоку інформації різними каналами, її блокування чи порушення цілісності – це технічний захист інформації. Останній виконують технічними засобами захисту.

Технічними засобами захисту називають такі засоби, в яких функція захисту інформації є основною і реалізується певними пристроями (комплексом, системою), яких на сьогодні вироблено значну кількість.

Згідно з Державним стандартом України (ДСТУ 3396.2-97) технічному захисту підлягає інформація, відомості про суб'єкти, об'єкти, явища та процеси. Інформація може бути з обмеженим доступом, коли право доступу до неї встановлюється правовими нормами чи правилами.

Інформація може бути таємною, тобто інформація з обмеженим доступом (ІзОД), яка містить відомості, що становлять державну чи іншу передбачену законом таємницю.

Технічно захищають і конфіденційну інформацію – інформацію з обмеженим доступом, якою володіють, користуються чи розпоряджаються окремі фізичні чи юридичні особи або держава, а права доступу до неї встановлюються ними.

Технічний захист інформації здійснюють поетапно. Визначають і аналізують загрози, розробляють систему захисту інформації (СЗІ), реалізують плани захисту інформації і контролюють функціонування та керування СЗІ.

До переваг технічних засобів захисту інформації (ТЗЗІ) відносять: достатньо широке коло вирішуваних задач і достатньо високу надійність; можливість створення розвинених комплексних систем захисту; гнучке реагування на спроби несанкціонованих дій; традиційність використовуваних методів здійснення захисних функцій.

Недоліками ТЗЗІ вважають: високу вартість багатьох засобів і необхідність регулярного проведення регламентних робіт і контролю: можливість подачі хибної тривожної сигналізації.

Класифікацію технічних засобів захисту проводять за трьома критеріями: на підставі сполучення з основними засобами АСОД; за виконуваними функціями захисту; за ступенем складності пристрою.

Сполучення з основними засобами АСОД**: автономні** – це засоби, які виконують свої захисні функції незалежно від функціонування засобів АСОД, тобто повністю автоматично; **сполучені** – це засоби, які виконані у вигляді самостійних пристроїв, але здійснюють захисні функції у сполученні (разом) з основними засобами; **вбудовані** – це засоби, які конструктивно включені до складу апаратури технічних засобів АСОД.

Виконувана функція захисту: зовнішній захист – захист від впливів дестабілізуючих факторів, які проявляються за межами основних засобів АСОД; пізнавання – спеціальна група засобів, яку використовують для розпізнавання людей за різними індивідуальними характеристиками; внутрішній захист – за-

хист від впливів дестабілізуючих факторів, які проявляються безпосередньо у засобах оброблення інформації.

Ступінь складності пристрою: прості пристрої – нескладні пристрої, які виконують окремі процедури захисту; складні – комбіновані агрегати, що складаються з певної кількості простих пристроїв і які здатні здійснювати складні процедури. Системи – це завершені технічні комплекси, які спроможні виконати певну комбіновану процедуру захисту, що має самостійне значення.

Технічні засоби охоронної сигналізації. Технічні засоби охоронної сигналізації (ТЗОС) призначені для виявлення загроз і повідомлення співробітників охорони або персоналу об'єкта про виникнення і наростання загрози. Охоронна сигналізація (ОС) за своєю будовою і застосовуваною апаратурою має багато спільного з пожежною сигналізацією, тому їх дуже часто об'єднують в одну систему охоронно-пожежної сигналізації (ОПС).

Важливим елементом ОПС є сенсори, характеристики яких визначають основні параметри всієї системи.

За своїм функціональним призначенням їх поділяють на такі типи:

1) об'ємні, що дають змогу контролювати простір приміщення;
2) лінійні, або поверхневі, для контролю периметра територій і будівель;
3) локальні, або точкові, для контролю окремих предметів.

Сенсори можна встановлювати як відкрито, так і приховано. Приховано встановлені сенсори монтують у ґрунті або під покриттям доріг, у стінах приміщень, різноманітних будівельних конструкціях і т. п.

Найбільш розповсюджені такі типи сенсорів:

1) вимикачі і розмикачі, які діють за принципом механічного або магнітного управління розмиканням електричного кола при появі порушника;
2) інфраакустичні, встановлені на металевих огорожах, і які вловлюють низькочастотні звукові коливання;
3) електричного поля, що складаються з випромінювача і декількох приймачів. Як випромінювач, так і приймачі виготовляють з електричних кабелів, натягнутих між стовпами. При появі порушника між випромінювачем і приймачем змінюється електричне поле, зміну якого і фіксує сенсор.
4) інфрачервоні, які діють за тим же принципом, що і сенсори

електричного поля, але випромінювачами слугують інфрачервоні світлодіоди або невеликі лазерні установки;

5) мікрохвильові, які складаються з надвисокочастотних передавача і приймача. При спробі проходу між передавачем і приймачем змінюється електромагнітне поле, що і реєструється приймачем;
6) тиску, що реагують на механічні навантаження на середовище, в якому вони закладені;
7) магнітні, які виготовляють у вигляді металевої сітки і які реагують на металеві предмети, що є у порушника;
8) ультразвукові, які реагують на ультразвукові хвилі, які виникають при діях порушника на елементи конструкції об'єкта, що охороняється;
9) ємнісні, що реагують на зміну електричної ємності між підлогою приміщення і решітчастою внутрішньою огорожею.

Засоби повідомлення і зв'язку – це сирени, дзвоники і лампи, які подають постійні сигнали про те, що сенсор зафіксував появу загрози.

Каналами зв'язку в системі охоронної сигналізації можуть бути прокладені дротові лінії, телефонні лінії об'єкта, телефонні лінії та радіозв'язок. Найбільш розповсюджені канали зв'язку – це багатожильні кабелі, що їх для підвищення надійності і безпечної роботи сигналізації вміщують у металеві або пластмасові труби, або в рукави.

Енергопостачання системи охоронної сигналізації обов'язково має бути зарезервовано, тоді у випадку його несправності функціонування сигналізації не припиниться за рахунок автоматичного підключення резервного (аварійного) енергоджерела.

Лабораторна робота № 3.2. Електронні системи захисту автомобілів

Мета роботи: практичне встановлення і робота автомобільних захисних систем.

Прилади та матеріали:

- захисна система "Півень".
- система тривожної сигналізації Mongoose EMS 1.7R;
- система захисту A.P.S 2500;

Хід виконання роботи.

1. Захисна система “Півень”.
   1.1. Ознайомлення з інструкцією з експлуатації та технічними даними.
   1.2. Під’єднання, встановлення передавача.
   1.3. Перевірка роботи системи.
   1.4. Визначення максимальної дальності впевненого приймання сигналу передавача.
2. Системи захисту “Mongoose EMS 1.7R”.
   2.1. Ознайомлення з технічною документацією охоронної системи Mongoose EMS 1.7R.
   2.2. Технологія динамічного кодування, функція антисканування, функція пам’яті станів, функція обходу несправної зони.
   2.3. Робота пульта дистанційного керування з функцією пейджера.
   2.4. Управління основними режимами охорони.
   2.5. Рекомендації з встановлення охоронної системи Mongoose EMS 1.7R.
3. Автомобільний захист A.P.S. 2500.
   3.1. Технічні функції та параметри охоронної системи A.P.S. 2500.
   3.2. Аварійне від’єднання системи. Режим “Valet”.
   3.3. Електричне під’єднання системи.

3.8. Інфрачервоні пасивні сенсори охоронної сигналізації

На теплове випромінювання людини, яка рухається, реагують інфрачервоні пасивні сенсори (ІЧПС), які також називають оптико-електронними і відносять до класу детекторів руху. Принцип дії цих сенсорів оснований на реєстрації зміни в часі різниці між інтенсивністю ІЧ-випромінювання від людини і фонового теплового випромінювання.

На сьогодні ІЧПС найбільш поширені. Вони становлять невід’ємну частину, невід’ємний елемент, охоронної системи практично кожного об’єкта.

Для того, щоб порушник був виявлений ІЧПС, необхідно дотримуватися таких умов:

1) порушник повинен перетнути у поперечному напрямку промінь зони чутливості сенсора;
2) рух порушника має відбуватися у певному інтервалі швидкостей;
3) чутливість сенсора має бути достатньою для реєстрації різниці температур поверхні тіла порушника (з урахуванням впливу його одягу) і фону (стін, підлоги).

Інфрачервоні пасивні сенсори складаються з трьох основних елементів:

а) оптичної системи, що формує діафрагму спрямованості сенсора і визначає форму і вигляд просторової зони чутливості;
б) піроприймача, який реєструє теплове випромінювання людини;
в) блока оброблення сигналів піроприймача, який виділяє сигнали, зумовлені людиною, що рухається, на фоні завад природного і штучного походження.

Розглянемо складові ІЧПС.

Оптична система. Сучасні інфрачервоні пасивні детектори (ІЧПД) характеризуються великим розмаїттям можливих форм діаграм спрямованості. Зона чутливості ІЧПС – це набір променів різної конфігурації, які розходяться від сенсора за радіальними напрямками в одній або декількох площинах. Оскільки в ІЧ-детекторах використовують здвоєні піроприймачі, то кожен промінь у горизонтальній площині розщеплюється на два.

Зона чутливості детектора може мати вигляд:

а) одного або декількох, зосереджених у малому куті, вузьких променів;
б) декількох вузьких променів у вертикальній площині (променевий бар'єр);
в) одного широкого променя у вертикальній площині (суцільна завіса) або багатовіяльної завіси;
г) декількох вузьких променів у горизонтальній або нахиленій площині (поверхнева одноярусна зона);
ґ) декількох вузьких променів у декількох нахилених площинах (об'ємна багатоярусна зона).

Водночас можливі зміни у широкому діапазоні довжин зони чутливості (від 1 до 50 м), кута огляду (від 3° до 180°, а для сенсорів, які розміщені на стелі, – 360°), кута нахилу кожного променя (від 0° до 90°), кількості променів (від одного до декількох десятків). Різноманітність і складність конфігурацій форм зон чутливості залежать передусім від таких факторів:

а) намагання розробників забезпечити універсальність при обладнанні різних за конфігурацією приміщень – невеликі кімнати, довгі коридори, формування зони чутливості спеціальної форми, наприклад, зони нечутливості (алеї) для домашніх тварин поблизу підлоги і т. п.;

б) необхідності забезпечити рівномірну чутливість ІЧ-детектора за об'ємом, який охороняють.

При побудові оптичних систем ІЧ-сенсорів можуть бути використані:

а) лінзи Френеля – сегментовані лінзи, що становлять собою пластикову пластину з відштампованими на ній декількома призматичними лінзами-сегментами;

б) дзеркальну оптику – у сенсорі встановлюють декілька дзеркал спеціальної форми, які фокусують теплове випромінювання на пріоприймач.

в) комбіновану оптику, що використовує і дзеркала, і лінзи Френеля.

У більшості ІЧПС використовують лінзи Френеля, до переваг яких відносять:

1) простоту конструкції детектора на їхній основі;
2) низьку вартість;
3) можливість використання одного сенсора у різних випадках при використанні змінних лінз.

Принцип роботи лінз Френеля ґрунтується на розділенні оптичної лінзи на маленькі секції, які концентрично збирають ІЧ-випромінювання на сенсор. Площа області формується спеціальною формою оптичних секцій і кривизною всіх оптичних лінз. Використання сучасних технологій виготовлення лінз дає змогу забезпечити практично постійну чутливість детектора за всіма променями шляхом підбору і оптимізації параметрів кожної лінзи-сегмента: площі сегмента, кута нахилу і відстані до пріоприймача, прозорості, відбивальної здатності, ступеня дефокусування.

Останнім часом освоєна технологія виготовлення лінз Френеля зі складною точною геометрією, що дає нове (30% збільшення зібраної енергії порівняно зі стандартними лінзами) зростання рівня корисного сигналу від людини на великих відстанях. Матеріал, з якого виготовляють сучасні лінзи, забезпечує захист піроприймача від білого світла. До незадовільної роботи ІЧ-сенсора можуть призвести такі ефекти, як теплові потоки, що є наслідком нагрівання електричних компонентів сенсора, можливі перевідбиття інфрачервоного випромінювання від внутрішніх частин детектора. Для усунення цих дефектів в ІЧ-сенсорах останнього покоління застосовують спеціальну геометричну камеру між лінзою і піроприймачем (герметична оптика), наприклад, у нових ІЧ-сенсорах фірм PYRONIX і C&K. На думку спеціалістів, сучасні високоточні лінзи Френеля за своїми оптичними характеристиками практично не поступаються дзеркальній оптиці.

В дзеркальній оптичній системі інфрачервоне випромінювання збирається в фокусі дзеркала і концентрично передається на піроелектричний сенсор. Сегменти дзеркала використовують для формування визначених зон спостереження. Дзеркальну оптику як сучасний елемент оптичної системи, застосовують достатньо рідко. ІЧ-сенсори з дзеркальною оптикою виготовляють, наприклад, фірми SENTROL і ARITECH. Перевагами дзеркальної оптики є: можливість більш точного формування променя, і, як наслідок, збільшення чутливості, що дає можливість виявляти порушника на великих відстанях. Використання декількох дзеркал спеціальної форми, в т. ч. багатосегментних, сприяє забезпеченню практично постійної чутливості по відстані, до того ж, ця чутливість на великих відстанях на 60% вища, ніж для простих лінз Френеля. За допомогою дзеркальної оптики простіше забезпечується захист ближньої зони, яка розміщена безпосередньо під місцем встановлення сенсора (т. зв. антисаботажна зона). За аналогією зі змінними лінзами Френеля ІЧ-сенсори з дзеркальною оптикою комплектують зі змінними дзеркальними масками, які знімаються, і застосування яких дає змогу вибрати необхідну зону чутливості та забезпечити можливість адаптації сенсора до різних конфігурацій захищуваного приміщення.

У сучасних високоякісних ІЧ-детекторах використовують комбінацію лінз Френеля і дзеркальної оптики. Разом з тим лінзи Френеля використовують для формування зони чутливості на середніх відста-

нях, а дзеркальну оптику – для формування антисаботажної зони і для забезпечення дуже великої відстані виявлення порушника.

Елементи захисту інфрачервоних сенсорів. В ІЧ-сенсорах застосовано т. зв. схеми антимаскінгу. Суть проблеми полягає в тім, що звичайні ІЧ-сенсори можуть бути виведені порушником з ладу шляхом попереднього (коли система не поставлена на охорону) заклеювання або зафарбовування вхідного вікна сенсора. Для боротьби з цим способом виведення з ладу ІЧ-сенсорів застосовують схеми антимаскінгу. Метод оснований на застосуванні спеціального каналу ІЧ-випромінювання, який спрацьовує при появі маски або перепони, що відбиває випромінювання на невеликій відстані від сенсора (від 3 до 30 см).

Встановлення та використання інфрачервоних пасивних сенсорів. Вибираючи типи і кількість сенсорів для забезпечення охорони конкретного об'єкта, треба враховувати можливі шляхи і способи проникнення порушника, необхідний рівень надійності виявлення, витрати на придбання, монтаж і експлуатацію сенсорів, особливості об'єкта, тактико-технічні характеристики сенсорів.

Універсальність – характерна особливість ІЧПС. Використання цих приладів дає можливість запобігати проникненню до різноманітних приміщень, конструкцій і предметів: вікон, вітрин, прилавків, дверей, стін, перекрить, перегородок, сейфів і окремих предметів, коридорів. Водночас у низці випадків не потрібна велика кількість сенсорів для захисту кожної конструкції – може так статися, що для цього достатньо одного або декількох сенсорів з необхідною конфігурацією зони чутливості. Розглянемо деякі елементи (особливості) ІЧ-сенсорів. Загальний принцип використання ІЧПС – промені зони чутливості мають бути перпендикулярні можливому напрямку руху порушника. Місце встановлення сенсора треба вибирати так, щоб мінімізувати мертві зони, спричинені наявністю у приміщенні, що охороняється, крупних предметів, які перекривають промені (наприклад, меблі, кімнатні рослини і т. д.). Якщо у приміщенні двері відкриваються в середину, треба враховувати можливе маскування порушника за відкритими дверима. При неможливості усунути мертві зони треба використовувати декілька сенсорів, а, блокуючи окремі предмети, сенсор або сенсори встановлювати так,

щоб промені зони чутливості блокували всі можливі підходи до предметів захисту.

Дотримуються і заданого у документації діапазону допустимих максимальної і мінімальної висоти фіксування положення сенсора. Особливо це стосується діаграм спрямованості з нахиленими променями: якщо висота фіксування перевищуватиме максимально допустиму, то це призведе до зменшення сигналу далекої зони і зростання мертвої зони перед сенсором, якщо ж висота фіксування буде менша за мінімально допустиму, то це зумовить зменшення відстані виявлення з одночасним зменшенням мертвої зони перед сенсором.

До хибних спрацювань ІЧПС можуть призвести завади теплового, світлового, електромагнітного характеру. Незважаючи на це, сучасні ІЧПС мають високий ступінь захисту від описаних впливів, хоча доцільно дотримуватися таких рекомендацій:

1. Для захисту від потоків повітря і пилу не рекомендується розміщувати сенсор у безпосередній близькості повітряних потоків (вентиляція, відкрите вікно);
2. Треба уникати прямого потрапляння на сенсор сонячних променів і яскравого світла; обираючи місце установки, необхідно враховувати можливість засвітлення протягом невеликого часу рано-вранці або при заході сонця, або засвітлення фарами транспорту, який проїжджає ззовні;
3. Вмикаючи охоронну систему, доцільно відключити можливі джерела потужних електромагнітних завад, а саме: джерела світла не на основі ламп розжарювання: люмінесцентні, неонові, ртутні, натрієві;
4. Для зменшення впливу вібрацій доцільно встановлювати сенсори на капітальних або носійних конструкціях;
5. Не рекомендують направляти сенсор на джерело тепла (пічка, радіатор) і предмети, які коливаються (штори, рослини), а також у бік, де знаходяться домашні тварини.

Лабораторна робота № 3.3. Вивчення роботи систем з ІЧ-сенсором руху та протипожежними оповіщувачами

Мета роботи: практичне встановлення та особливості роботи захисних систем.

Прилади та матеріали:

- ІЧ-сенсори руху TLC-15;
- пожежні повідомлювачі;
- блок затримування "Оріон-2.1.А";
- сирена;
- джерело живлення.

Хід виконання роботи.

1. Під'єднання пасивного ІЧ-сенсора в схему захисту.
   1.1. Під'єднати компоненти згідно зі схемою.
   1.2. Перевірити функціонування схем (після натискання кнопки "вмк" блоку затримання має спрацювати сирена при русі людини в приміщенні).
   1.3. Дослідити діаграму направленості роботи сенсора та розрахувати оптимальну кількість сенсорів у приміщенні.
   1.4. Вивчити реакцію системи на вимкнення напруги в освітлювальній мережі.
   1.5. Дослідити вплив випадкових факторів на фальшиві спрацювання системи та динаміку її роботи.
2. Створення макета ІЧ-сенсора та протипожежних повідомлювачів.
   2.1. Під'єднати сенсори TLC15 та п'єзоелектронну сирену.
   2.2. Дослідити факти та максимальні віддалі спрацювання макета при русі людей та при виникненні тютюнового задимлення в приміщенні.
3. Випробовування систем захисту в лабораторних умовах.

3.9. Комбіновані сенсори охоронної сигналізації

Комбіновані сенсори (КС), які названо сенсорами подвійної технології, з'явилися недавно і на цей час мають широке застосування. Перевагою таких сенсорів є суттєве зниження частоти хибних спрацювань, а сигнал тривоги видається тільки у тому випадку, якщо одночасно або протягом невеликого інтервалу часу спрацьовують обидва детектори, в яких використано різні фізичні принципи виявлення порушень.

Таким чином, у комбінованих сенсорах ОС використано комбінацію мікрохвильового активного і ІЧП принципів виявлення або комбінацію ультразвукового і ІЧП детектора. Наявні й окремі зразки, в яких використовують три різні фізичні принципи виявлення, але такі сенсори не завоювали популярності.

Мікрохвильовий метод виявлення. Принцип дії мікрохвильового (МХ) активного методу (АМ) – МХАМ – виявлення побудовано на випромінюванні в навколишній простір електромагнітного поля НВЧ-діапазону і реєстрації його зміни, зумовленої відбиттям від порушника, який рухається у зоні чутливості сенсора. Мікрохвильові активні сенсори (МХАС), які реалізують цей метод, відносять до класу детекторів руху. Вони складаються з таких елементів:

- НВЧ-генератора;
- антенної системи, що утворює електромагнітне поле в навколишньому просторі; приймає відбиті сигнали; формує діаграму спрямованості сенсора і визначає форму просторової зони чутливості;
- НВЧ-приймача, який реєструє зміну характеристик прийнятого сигналу;
- блока, який виділяє сигнали, спричинені рухом людини на фоні завад.

Генератор мікрохвильового сенсора призначений для формування НВЧ-сигналу зазвичай у трисантиметровому діапазоні довжин хвиль 10÷11 ГГц. Останнім часом розробники почали освоювати і більш короткі діапазони 24÷25°ГГц. На початку у МХАС використовували генератори на діодах Гана, а зараз перейшли на транзисторні генератори. Сучасні НВЧ-генератори дають змогу формувати стабільний сигнал з необхідними характеристиками при малих габаритах і малому споживанні.

Антенною системою в МХАС слугує одна суміщена приймально-передавальна антена. У більшості сучасних сенсорів застосовують мікросмужкові антени, які мають менші габарити, вагу і вартість порівняно з рупорними антенами, які і сьогодні використовують виробники сенсорів, оскільки вони забезпечують більш високу точність формування діаграми спрямованості.

Якщо порівнювати конфігурації зон чутливості ІЧПС і МХАС, то останні не відрізняються такою різноманітністю. Конфігурація зони чутливості МХАС – це об'ємне тіло, яке нагадує за формою еліпсоїд.

Антенна система має випромінювати (і приймати) тільки у передній напівпростір без заднього і бокового випромінювання (з метою мінімізації хибних спрацювань). Для такої ідеальної антенної системи зона чутливості становить собою об'ємне тіло каплеподібної форми, що характеризується кутами огляду Θ (у горизонтальній і вертикальній площинах) і шириною D (висотою). Саме ці параметри наводять у документації для МХАС (іноді доповнюють величинами контрольованих сенсором площі й об'єму приміщення).

Розміри зони чутливості для МХАС: R_{max}= 10÷15 м; D=5÷10м; Θ=60°÷100°.

Зона чутливості, що формується антенною системою, відрізняється від ідеальної через появу заднього і бокового випромінювань. Разом з тим вона набуває двопелюсткову форму R_1, R_2. Відношення R_1/R_2 може становити 0,03÷0,1.

Все це стосується вільного простору. А при розміщенні сенсора у приміщенні форма зони чутливості суттєво спотворюється. За рахунок відбиття від огороджуючих конструкцій (коефіцієнт відбиття по полю від цегляних і залізобетонних стін становить 0,03÷0,6) електромагнітне поле заповнює з більшим чи меншим ступенем рівномірності практично все приміщення, якщо розміри цього приміщення не перевищують розміри зони чутливосгі. З іншого боку, тонкі перегородки з легких матеріалів, дерев'яні двері, скло, штори не є суттєвою перешкодою для електромагнітного поля, тому зона чутливості може розповсюджуватися і за межі приміщення, яке охороняють, що може призвести до хибних спрацювань, наприклад, коли люди проходять по коридору, або переміщенні транспорту поблизу вікон першого поверху. Крім того, крупногабаритні предмети (шафи, сейфи і т. д.), які знаходяться у приміщенні, утворюють "тіні" (зони нечутливості). Все це має бути враховано при виборі місця установки і кількості сенсорів, що їх використовують.

Переміщення порушника приводить до появи в часі відбитого від нього сигналу, який змінюється. Тут треба розрізняти два ефекти: зміну просторової картини стійких хвиль і частотний зсув хвилі (ефект Доплера), відбитої від людини, яка рухається.

МХАС, які основані на реєстрації першого ефекту. Називають амплітудно-модуляційними, другого – доплерівськими, хоча обидва вони нерозривно пов'язані, мають загальну природу й одночасне проявлення, тому практично нероздільні. Але все ж

таки відмінності простежуються у структурі побудови і характеристиках НВЧ-приймача МХАС.

Більшу застосованість одержали доплерівські МХАС, які мають високу чутливість. Доплерівський зсув частоти Δf виникає при русі порушника по променю (або упоперек променя), частота відбитого сигналу зростає при русі до сенсора і зменшується при русі від сенсора. Абсолютна величина Δf пропорційна частоті збуджуючого сигналу f та складовій швидкості руху за променем (чи упоперек променя).

Для боротьби з цими завадами сучасні МХАС комплектують режекторними фільтрами гармонік мережі (в т. ч. адаптивними). Іншими джерелами завад, які спричиняють хибні спрацювання доплерівських МХАС, є відбиття від об'єктів, що вібрують, коливаються і рухаються.

Джерелами хибних спрацювань можуть бути:

- установочна арматура увімкнених ламп денного світла;
- увімкнене електрообладнання, яке створює вібрацію;
- потоки дощової води на віконному склі;
- рух води у пластикових трубах;
- дрібні тварини і птахи.

Декілька років тому, до появи ІЧПС, МХАС користувалися великим попитом. На сьогодні окреме застосування МХАС у СОС дещо знизилось, але зате ширше почали застосовувати комбіновані сенсори.

Всі сенсори призначені для встановлення в приміщеннях, мають суцільну об'ємну зону чутливості і можливість регулювання дальності виявлення. Рекомендована висота їхнього встановлення лежить у межах 2÷2,5 м. Допускається експлуатація декількох сенсорів в одному приміщенні.

Краще встановлювати комбіновані сенсори, вони суттєво зменшують імовірність хибних тривог. Якщо б хибне спрацювання кожного детектора, який входить до комбінованого сенсора, було зумовлено абсолютно різними фізичними явищами (тобто, ці події були б незалежними), то ймовірність хибної тривоги $P_{хтр}$ дорівнювала б добутку ймовірностей хибних тривог для кожного з детекторів: $P_{хтр} \sim P_1 P_2$, і якщо $P_1 = P_2 = 10^{-5}$, то ми потенційно отримали б зниження частоти хибних спрацювань в 100 000 разів. У реальних умовах виграш не такий великий, але у сучасних комбінованих ІЧПС-МХАС середній час наробітку на

хибну тривогу становить 3000–5000 годин, що суттєво перевищує аналогічний показник інших типів.

Перевагами сенсорів подвійної технології є високий імунітет щодо можливих помилок інсталятора та змін навколишнього середовища після встановлення і налаштування КС.

Переваги комбінованих сенсорів добре простежуються у вузьких коридорах і різних проходах. Для ГЧПС рухи порушника відбуваються без попереднього перетину декількох променів, це призводить до відмови багатократного підрахунку імпульсів, і як наслідок – до підвищення частоти хибних спрацювань. Застосування КС вирішує цю проблему.

Встановлення та використання комбінованих сенсорів. Основні рекомендації для встановлення КС збігаються з рекомендаціями зі встановлення ІЧП-сенсорів. Зупинимося на особливостях, які входять до складу сенсорів подвійної технології.

До хибних спрацювань сенсорів можуть призвести різні завади та зміна навколишнього середовища. Незважаючи на те, що КС мають високий ступінь захисту, треба притримуватися такого:

1. Під час постановки на охорону доцільно відключати джерела потужних електромагнітних завад і вібрацій (люмінесцентні джерела світла), а для чергового освітлення – використовувати лампи розжарювання;
2. Для зменшення впливу електромережевих завад прокладання ліній живлення та шлейфів сенсорів необхідно проводити за можливістю перпендикулярно до силових мереж, а при паралельному прокладанні – на відстані не менше 80 см;
3. Для зменшення впливу вібрацій доцільно встановлювати сенсори на капітальних стінах або підтримкових конструкціях;
4. Не радять встановлювати сенсори на струмопровідних конструкціях (металеві болти, сира цегляна кладка і т. д.), оскільки між сенсором і джерелом живлення виникає подвійний контур заземлення, що може призвести до хибного спрацювання;
5. Поблизу сенсора не має бути габаритних металевих конструкцій і об’єктів, оскільки в цьому випадку через перевідбиття НВЧ-сигналів може виникнути непередбачене спотворення зони чутливості;

6. При малій товщині стін і перегородок прорізів, вікон, дверей треба встановлювати екрани – металеві сітки або металізовані матеріали, які можна застосувати від хибних спрацювань, спричинених рухом води у пластикових трубах і дощових потоків по шибках.

3.10. Фотоелектричні сенсори та системи охорони периметра

Фотоелектричні (ФЕС) сенсори випромінюють відбитий сигнал до інфрачервоного випромінювання довжина хвилі якого один мікрометр. Їх використовують у складі систем захисту внутрішнього і зовнішнього периметра, для прольотів, дверей, ліфтів, прорізів, коридорів і т. д. Вони відрізняються високою стійкістю і надійністю в роботі.

Фотоелектричні сенсори складаються з двох частин – передавача і приймача. Вони розміщені повздовж лінії охорони. Між ними проходить система модульованих інфрачервоних променів.

Сенсори цього типу спрацьовують при спробі порушника перетнути систему променів.

Найбільш удосконалені моделі фотоелектричних сенсорів працюють автономно. Для цього їх комплектують сонячними елементами, які заряджають акумуляторні батареї живлення сенсорів.

Для охорони периметрів, при зовнішньому встановленні (на вулиці), найбільш розповсюджені ІЧ-сенсори фотоелектричного типу фірми ОРТЕХ серії АХ, які застосовують для охорони відкритої або закритої території з периметром від десяти до тисячі метрів.

Системи охорони периметра встановлюють на огорожах і якщо навіть таких немає. Використовують для охорони постійних об'єктів, території будівництва і т. д. Основу системи охорони периметра становлять фотоелектричні сенсори.

Фотоелектричні сенсори АХ-70Т, АХ-ІЗОТ надійно працюють, незважаючи на зміну погодних умов. За ясної погоди інтенсивність променів автоматично зменшується. При розсіюванні до 99% енергії променів дощем або снігом, які потрапляють на сенсори, ті продовжують надійно працювати, автоматично адаптувавшись до зовнішніх умов.

Система сенсорів може утворювати як замкнений, так і розімкнений контур. Сенсори можна розміщувати на довільній висоті й утворювати бар'єри довільної конфігурації.

Допустимий час переривання променя може бути відрегульований відповідно до особливостей ділянки встановлення.

При захисті стін або огорожі сенсори регулюють таким чином, щоб вони не реагували на птахів, комах, дрібних тварин і т. д.

Сенсори АХ-1ЗОТ розрізняють порушення периметра за часом переривання променя. Спрацьовування сенсора відбувається тільки при перериванні двох променів одночасно.

Сенсори АХ-200SOL – бездротові фотоелектричні бар'єрні сенсори з сонячними батареями й автономним живленням.

Перший сенсор бар'єра двопровідною лінією підключають до пульта-концентратора. Інші сенсори працюють дистанційно, підживлюючись автоматично від сонячної батареї. Чотирьох годин достатньо, при помірній освітленості, для повного зароджування акумуляторів сенсора. Якщо ж розряджається батарея, сигнал про це надходить на пульт-концентратор. Зверху, на сонячних батареях, розміщені пружинні штирі для запобігання пошкодження птахами. Сенсори цієї моделі укомплектовані покращеною системою випромінювання, яка дає змогу одній людині упоратися з її встановленням і юстуванням. Вони призначені для встановлення там, де встановлення провідних сенсорів ускладнено або неможливо.

Останнім часом системи охорони периметра широко застосовують на об'єктах, які потребують тимчасової охорони, наприклад, при сезонних роботах, на будівництві та у сільському господарстві, для забезпечення збереженості культур, які дозрівають, та техніки.

Іноді системи охорони з фотоелектричними сенсорами називають оптико-електронними охоронними повідомлювачами Серед таких повідомлювачів надають перевагу повідомлювачам російських фірм "СПЭК-5" та "Вектор-СПЭК", які також призначені для охорони. Вони мають достатній запас за потужністю, завдяки чому працюють в умовах поганої видимості (великих оптичних втрат, тобто при дощі, снігу, тумані і т.д.). Повідомлювачі виконані на сучасній елементній базі, їх не складно встановлювати і налаштувати, вони дають змогу утворювати багатопроменеві бар'єри будь-якої густини в ІЧ-діапазоні.

Пристрої мають дистанційний контроль функціонування, а для точного встановлення оптичних осей приймача і випромінювача передбачено режим "контроль" або режим "переривання" у "СПЭК-5".

Один повідомлювач перекриває дільницю території одним ІЧ-променем. Умова працездатності повідомлювана – наявність прямої видимості між випромінювачем і приймачем.

Для блокування периметра, одна сторона якого становить 150 м, однопроменевим ІЧ-бар'єром необхідно встановити чотири випромінювачі і чотири приймачі. Для охорони більшої ділянки необхідно послідовно встановити певну кількість повідомлювачів, кожен з яких буде перекривати ділянку до 350 м.

Наявності стороннього об'єкта в області потоку ІЧ-енергії недостатньо для формування сигналу тривоги. Необхідною умовою ввімкнення тривожної сигналізації приладу є перекриття оптичної осі (умовної прямої між оптичними осями випромінювача і приймача), коли тінь від об'єкта потрапляє на вікно приймача повідомлювача.

Для реєстрації несанкціонованого переміщення в зоні, що охороняється, можна використовувати один або декілька ІЧ-променів як у вертикальній (по висоті), так і у горизонтальній площинах, які перекривають необхідну площу або периметр території, підходи до приміщення, воріт і т. д.

Для побудови охоронного ІЧ-бар'єра зазвичай використовують декілька варіантів, у кожному з яких передбачено застосування одного або декількох повідомлювачів, до складу кожного, як ми вже зазначали, входить випромінювач і приймач.

При утворенні однопроменевого ІЧ-бар'єра використовують один повідомлювач.

При утворенні двопроменевого ІЧ-бар'єра використовують два повідомлювачі.

Для того, щоб організувати багатопроменевий ІЧ-бар'єр (більше двох ІЧ-променів), необхідно мати два повідомлювачі та два додаткові приймачі, а з кожного боку бар'єра встановлюють по одному випромінювачу.

Випромінювачі встановлюють з одного боку бар'єра, а приймачі – з іншого.

Живлення декількох повідомлювачів можна здійснювати як по одній лінії, так і окремо. Можливе живлення випромінювача і приймача одного повідомлювача від різних джерел.

Лабораторна робота № 3.4. Охорона периметра з допомогою оптоелектронної (лазерної) системи

Мета роботи: показати ефективність охорони периметра будівлі з допомогою оптоелектронної (лазерної) системи захисту.

Прилади та матеріали:

- лазер;
- фотодіод ФД-7;
- електронна схема увімкнення сигналу (сирени) або передачі інформації про проникнення через периметр по стільниковій мережі.

Хід виконання роботи.

1. Зібрати оптоелектронну схему захисту периметра.
2. Імітувати несанкціонований перетин периметра та зареєструвати факт перетину периметра і передати інформацію SMSкою.
3. Застосувати дзеркала для формування захищеного периметра.

3.11. Детектори вібрацій, розбиття скла та ультразвукові детектори

Детектор вібрацій з п'єзосенсором. Мікрофоном детектора вібрацій слугує п'єзоелектрична пластина від зумера. Вона має чіткий пік частотної характеристики (залежно від типу зумера) в області частот 1 500÷3 000 Гц. Така характеристика пластини дає можливість з достовірністю виявити імпульсні сигнали на фоні шумів. Притиснута або приклеєна до скла пластина миттєво реагує на шуми, які виникають при розрізанні скла алмазом і не реагує на шуми, які утворюються, наприклад, транспортом, який проїжджає поряд.

Ефективність роботи пристрою залежить від способу встановлення самого сенсора. Якщо необхідно захистити велике вікно, то краще сенсор розмістити безпосередньо на склі й експериментальним шляхом вибрати таке його положення, при якому чутливість пристрою максимальна.

Детектори розбиття скла. Завдання виявлення розбитого скла може бути вирішено за допомогою різних фізичних принципів. До основних можна віднести:

1. Реєстрацію механічних руйнувань елементів повідомлювача. В цьому випадку використовують електромагнітні сенсори з фольги або провідники зі спеціального армованого скла. Механічне руйнування цілісності провідника при руйнуванні скла фіксується схемою оброблення.
2. Використання інерційних властивостей. У цьому випадку повідомлювач має два елементи: один міцно закріплений на поверхні скла, а другий – рухомий. При механічних коливаннях скла контакт між цими елементами порушується, що і фіксується схемою оброблення.
3. Використання п'єзоефекту: повідомлювачі можуть бути як пасивними, так і активними. В пасивному варіанті п'єзосенсор розміщують на поверхні скла. Він перетворює механічні коливання скла в електричний сигнал, який обробляється відповідною схемою. Такі сенсори мають низьку завадостійкість і не дають змоги контролювати їхню працездатність. Кращі характеристики мають активні повідомлювачі, які складаються з передавача і приймача акустичних коливань. Оскільки частота коливань, випромінюваних передавачем, відома, є змога відділити приймачем саме її, що різко підвищує завадостійкість.
4. Реєстрація акустичних коливань, які виникають при руйнуванні скла. Цей принцип реалізовано у більшості сучасних детекторів розбиття скла. Якщо у третьому варіанті майже на кожному склі встановлювали повідомлювач, то тут встановлюють один детектор, який реагує на звук розбитого скла.

Більш сучасні моделі детекторів аналізують спектр звукових сигналів у приміщенні. Якщо цей спектр вміщує складову, яка збігається зі спектром розбиття скла, то детектор спрацьовує. Наявні двопорогові детектори розбиття скла реєструють звук удару по склу і звук скла, що розбивається. Тобто детектор реєструє два сигнали з інтервалом між ними не більше 150 мс.

До особливостей цих детекторів треба віднести таке:

- високу чутливість і достовірність реєстрації;
- цифрове оброблення сигналів;

- режим тестування;
- простий контроль працездатності;
- стійкість до хибних спрацювань;
- простоту при встановленні і підключенні;
- стійкість до дії радіозавад.

Але вони мають один недолік – реагують як на звуки всередині приміщення, так і на акустичні коливання від скла, що призводить до хибних спрацювань охоронної системи. Тому застосовують акустичний повідомлювач FG1025Z, який реєструє акустичні коливання, що надходять тільки з боку скла, що охороняється. Такий детектор використовує нову запатентовану технологію оброблення акустичних сигналів – за часом надходження її з контрольованої зони. Ця нова технологія – Time-oґ-Arrival – заснована на використанні двох незалежних мікрофонів, які реєструють акустичні коливання, що надходять з зони охоронної області простору. Акустичні коливання приймають два мікрофони, направлені в протилежні боки під кутом 180°, і обробляються залежно від того, який з мікрофонів раніше прийняв акустичний сигнал. Сигнал, прийнятий мікрофоном, спрямованим у бік простору, що охороняється, ідентифікується схемою оброблення – чи дійсно він виник унаслідок руйнування скла, причому сигнал, прийнятий другим мікрофоном, ігнорується.

Отже, навколишній простір можна умовно розділити на контрольовану і виключену зони.

Ультразвукові детектори. Ультразвукові сенсори (УС) застосовують для охорони закритих приміщень. Вони мають високу чутливість, але і високий рівень хибних спрацювань. Налаштовуючи їх, зважають на зміну навколишнього середовища (вологість, перепад температур і т. д.), тому їх застосовують обмежено і використовують головно для охорони не дуже цінних об'єктів.

Принцип дії УС засновано на інтерференції ультразвукових коливань (20÷60 кГц). До складу УС входять випромінювач і приймач. При закритих вікнах і дверях простір, контрольований УС, обмежений, тому в місці, в якому знаходиться приймач, формується стійка інтерференційна картина. При появі порушника у приміщенні стійкість інтерференційної картини порушується і приймач формує сигнал тривоги.

Сенсор можна встановлювати як на стіні, так і на стелі. Залежно від місця встановлення вони мають різний вигляд. Такі детектори широко використовують у музеях, виставкових залах, коли треба

контролювати експонати, оргтехніку, прилавки, розміщені в ізольованих закритих великих приміщеннях.

3.12. Пожежні повідомлювачі

Сучасне суспільство велику увагу приділяє системам пожежної безпеки об'єктів, які призначені для захисту життя людей і матеріальних цінностей від пожежі. Небезпека для життя, пов'язана з виникненням пожежі, і збитки, спричинені вогнем, в десятки разів перевищують ті, що можуть бути зумовлені крадіжками, пограбуванням і т. д. Створено велику кількість автоматичних систем пожежної сигналізації для швидкого і надійного попередження пожежі, за допомогою розпізнавання явищ, які супроводжують пожежу, таких як виділення теплоти, диму, невидимих продуктів спалювання (згоряння), інфрачервоного випромінювання і т. д. У разі виявлення пожежі центральна станція (ЦС) передбачає приписи дій з управління системами автоматики приміщення (будови), а саме: відключення системи вентилювання, включення систем димовидалення та систем оповіщення – світлових і звукових оповіщувачів, запуск системи пожежогасіння, зупинки ліфтів, розблокування дверей і т. п. Це дає можливість людям, які знаходились у приміщенні, а також пожежній частині або локальному посту пожежної охорони об'єкта застосувати певні дії і засоби для ліквідації пожежі на стадії її загоряння (на стадії зародження) і мінімізувати збитки, які можуть статися внаслідок пожежі.

Призначення системи пожежної сигналізації (ПС) визначає її загальну структуру – наявність трьох складових системи, які виконують різні функції:

- виявлення пожежі здійснюється автоматичними пожежними оповіщувачами з різними принципами виявлення і різними методами оброблення й обміну інформацією:
- оброблення інформації, яка надходить від оповіщувачів, і надання інформації оператору виконуються центральною станцією і пультом управління;
- виконання приписів з повідомлення персоналу і пожежної частини для усунення вогнища, виконується ЦС, з метою швидкого і точного реагування підрозділів пожежної частини та локальних постів пожежної охорони.

Всі три ланки тісно взаємопов'язані між собою й ефективність роботи системи пожежної сигналізації залежить від надійної і стабільної роботи кожної з її складових, але основну роль при утворенні професійних систем пожежної безпеки об'єктів відіграють пожежні оповіщувачі. Саме вони мають забезпечити швидке і надійне виявлення вогнища (пожежі).

Сучасні пожежні повідомлювачі використовують низку основних принципів виявлення пожежі, що ґрунтуються на розпізнаванні різних характерних ддя неї ознак (утворення диму, виділення тепла, інфрачервоного випромінювання і т.п.).

Відомі декілька типів пожежних повідомлювачів, серед яких можна виділити іонізаційні та оптичні димові повідомлювачі, теплові та комбіновані повідомлювачі, світлові повідомлювачі, термокабелі і системи раннього виявлення диму за пробами повітря. Дим є найбільш характерною ознакою пожежі, оскільки практично всі пожежі супроводжуються утворенням великої кількості невловимих димових частинок. Найбільш численною і розповсюдженою групою пожежних повідомлювачів є димові, в яких реалізовані різні принципи виявлення димових частинок, залежно від їхнього розміру, кольору і т. д., тому розглянемо димові повідомлювачі.

В іонізаційних димових повідомлювачах (ІДП) використано властивість іонів повітря притягуватися димовими частинками. Зважаючи на це, в електричному полі вимірювальної камери повідомлювача повітря іонізується за допомогою слабкого радіоактивного джерела. Іонізовані, додатно і від'ємно заряджені молекули газу рухаються під дією електричного поля до протилежно заряджених електродів. Водночас у вимірювальній камері виникає електричний струм, величина якого залежить від кількості і швидкості іонів. У процесі рекомбінації заряду додатних і від'ємних іонів (під час їхнього руху в камері) кількість іонів, які відповідають за перенесення заряду, зменшується. Разом з тим струм вимірювальної камери стабілізується на певному кінцевому значенні, який відповідає черговому режиму роботи повідомлювача.

Коли димові частинки потрапляють у простір між електродами відкритої вимірювальної камери повідомлювача, то вони починають перешкоджати вільному руху іонів. Деяка кількість іонів стикається з більш важкими димовими частинками і затримується на їхній поверхні: збільшується рівень рекомбінації заряду, а висока інерційність димових частинок фактично перешкоджає потраплянню

заряду на електроди, спричиняючи зменшення струму вимірювальної камери, що є критерієм для прийняття рішення про надходження сигналу повідомлювача. Таким чином, іонізаційні димові повідомлювачі підходять для раннього виявлення пожеж, які супроводжуються утворенням димових частинок будь-якого розміру і кольору.

Термомаксимальний повідомлювач. У теплових повідомлювачах для виявлення пожежі використано ефект виділення тепла в процесі горіння. Також може бути використаний максимальний або диференційний принцип виявлення, або їхнє поєднання.

Застосовуючи цей принцип, виявляють максимальне значення температури, при якій повідомлювач видає на ЦС сигнал тривоги.

Теплові пожежні повідомлювачі, побудовані на максимальному принципові виявлення, постійно вимірюють абсолютне значення зовнішньої температури за допомогою чутливого елемента, яким може бути термістор, або керамічна плівка, біметалева пластинка, або елемент, побудований на принципі розширення рідини. Якщо температура в контрольованому приміщенні перевищує задане порогове значення, то сигнал з чутливого елемента фіксується й оцінюється блоком оброблення сигналу для прийняття рішення про видання тривожного сигналу. Теплові повідомлювачі, що працюють за принципом максимального вимірювання тепла, підходять для виявлення пожеж з відкритим полум'ям, які супроводжуються різким збільшенням температури.

Термодиференційний повідомлювач. За допомогою цього принципу виявляють значення швидкості зростання температури (°С/хв), при якому повідомлювач видає на ЦС сигнал тривоги. Як чутливий елемент найчастіше використовують термістори, або елементи, які виготовлені за принципом розширення рідини.

Тепловий пожежний повідомлювач вимірює абсолютну і відносну зміну зовнішньої температури за допомогою двох окремих чутливих елементів, наприклад, термісторів, які включені у мостову схему.

Теплові пожежні повідомлювачі, що працюють за принципом диференційного вимірювання тепла, підходять для виявлення всіх типів пожеж з відкритим полум'ям, оскільки вони достатньо точно оцінюють різке зростання температури, незалежно від її початкового значення.

Комбіновані пожежні повідомлювачі. Для контролю захищуваного приміщення у комбінованому пожежному повідомлювачі засто-

совано як димовий, так і тепловий принципи виявлення пожежі. Вимірюють оптичну густину диму за розсіюванням світла. У чутливій системі для вимірювання температури навколишнього середовища може бути використаний принцип максимального або диференційного вимірювання тепла.

Сигнали, вироблювані тепловим і димовим чутливими елементами, слугують критерієм для прийняття рішення про видачу тривожного сигналу повідомлювачем. Комбіновані пожежні повідомлювачі використовують як універсальні пожежні повідомлювачі для виявлення різних типів пожеж.

Світловий пожежний повідомлювач. Для виявлення пожежі у світловому повідомлювачі використано властивість продуктів горіння випромінювати інфрачервону енергію, яку приймають і перетворюють в електричний сигнал піроелектричні сенсори-повідомлювачі. Двоканальний світловий повідомлювач контролює зону виявлення за допомогою двох піроелектричних сенсорів, які мають чутливість у двох різних діапазонах довжин хвиль.

3.13. Виконавчі пристрої охоронних систем

Виконавчі пристрої під'єднують до центрального пульта керування за допомогою дротяного або бездротяного зв'язку. В системах охоронної сигналізації можуть бути використані такі виконавчі пристрої:

- потужна сирена;
- миготливе світло;
- графічні панелі з планом приміщень;
- система підсвічування;
- принтер для реєстрації часу, місця і характеру порушення і т.д.

Сирени – це пристрої звукового сповіщення про сигнал тривоги. Сирени бувають однотональними, багатотональними, з автономним живленням, з голосовим супроводженням, з шокуючим ефектом.

Найбільш суттєвим фактором, що безпосередньо діє на злочинця, є звук сирени і миготливе світло.

Лабораторна робота № 3.5. Система захисту, основана на передаванні інформації через стільникові лінії зв'язку

Мета роботи: створити реально діючу систему захисту приміщення (автомобіля) з застосуванням стільникового каналу зв'язку.

Прилади та матеріали:
- мобільний телефон марки "Motorola";
- джерело живлення 3,6 V;
- датчики відкриття дверей або ІЧ-датчики руху.

Хід виконання роботи.
1. Перепрограмувати мобільний телефон на номер охорони (господаря).
2. Підключити мобільний телефон у коло з джерелом живлення та охоронним датчиком.
3. Випробувати дію охоронної системи й описати параметри її ефективності.

3.14. Охоронні системи телеспостереження

Системи теленагляду призначені для забезпечення безпеки об'єкта, який охороняють. Вони дають змогу одному або декільком охоронцям одночасно стежити за одним або багатьма об'єктами, які перебувають іноді на значній відстані один від одного і від місця спостереження.

Найпростіша система теленагляду складається з телевізійної камери і монітора. Камера може бути підключена безпосередньо до телевізора або до монітора і розміщуватися як у середині будинку, так і ззовні.

Кількість камер, які одночасно працюють, має бути обмеженою, оскільки при збільшенні кількості моніторів оператору важко стежити за всіма змінами на них. Тому у багатокамерних системах використовують додаткові пристрої – детектори руху, що аналізують зміни зображення, наприклад, переміщення будь-якого предмета в полі зору камери, сигналізуючи оператору про це.

Для одночасного одержання декількох зображень на екрані одного монітора (до 16) використовують квадратори (“дільники екрана”). Квадратори перетворюють сигнали від декількох відеокамер у зображення на одному моніторі. Разом з тим зображення від будь-якої камери оператор може миттєво розгорнути на ввесь екран.

Для послідовного виведення на екран зображень від декількох камер у системах теленагляду використовують мультиплексори (комутатори), які у режимі перегляду послідовно підключають камери до монітора, а при оперативній роботі оператор має можливість вивести на екран будь-яке зображення або вимкнути будь-яку камеру. Для підвищення ефективності роботи оператора використовують матричні комутатори, які дають можливість створити гнучку і нарощувану систему безпеки, до якої можуть входити не тільки компоненти телевізійних систем, але й систем сигналізації і контролю доступу.

Відеозображення може бути записано на спеціалізовані відеомагнітофони, завдяки чому з’являється змога робити запис через декілька кадрів (стартстопний режим), причому час запису збільшується (більше 960 годин).

Комп’ютерні системи теленагляду мають низку особливостей, що у різноманітних ситуаціях може відігравати як позитивну, так і негативну роль. Перерозподіл функцій між програмними засобами призводить до того, що комп’ютерні системи не завжди можуть забезпечити швидке переключення режимів. Окрім того, підвищуються вимоги до оператора – вміння працювати з комп’ютером і графічним інтерфейсом.

Якість зображення залежить насамперед від телевізійної камери. Сьогодні в системах теленагляду використовують численні відеокамери, які відрізняються:

- характером зображення (чорно-біле або кольорове);
- чіткістю зображення;
- світлочутливістю (мінімальною робочою освітленістю об’єкта знімання);
- можливістю цифрового оброблення відеосигналу;
- допустимими кліматичними умовами роботи;
- напругою живлення.

Для забезпечення якісної роботи в умовах змінної яскравості зображення і різноманітних рівнів фонових засліплень сучасні телекамери оснащують підсистемами компенсації цих впливів.

Для збільшення сектора огляду телекамери встановлюють на поворотні пристрої з горизонтальним або з горизонтально-вертикальним скануванням. Перевертаючи телекамеру, треба враховувати можливі реагування систем компенсації зовнішніх впливів (засліплення, вплив імпульсних джерел штучного освітлення тощо).

Другим важливим елементом систем теленагляду є відеомонітор, який має забезпечувати високу довготривалу стабільність, бути надійним і не потребувати регулярного калібрування.

Технологія виробництва відеомоніторів за останні роки зазнала істотних змін, що яскраво засвідчують деякі розробки закордонних фірм.

Елементи і вузли систем теленагляду. В конструкції відеокамери можна виділити такі основні функціональні системи: перетворювач "світло-сигнал"; синхронізації; автоматичного регулювання підсилення; електронний затворний механізм; установлення балансу чорного та гама-корегування; знімання при низьких рівнях освітленості; об'єктив з автоматичною діафрагмою.

Найважливішим елементом конструкції відеокамери є перетворювач "світло-сигнал", який забезпечує кодування зображення, в електричні сигнали. У сучасних відеокамерах переважно застосовують ПЗЗ, які забезпечують високу надійність роботи. Кількість рядків матриці може коливатися від 380 до 900.

У третьому поколінні ПЗЗ (Нурег HAD) використано низку нових електронних прийомів, які значно поліпшили якісні показники сформованого зображення. У матриці Нурег HAD застосовано оригінальний і простий метод, який полягає у використанні мініатюрної прецизійної збірної фокусуючої лінзи точно на кожний світлочутливий елемент. Це дає змогу сконцентрувати світловий потік без зайвого його розсіювання і як результат – досягти різкого (приблизно вдвічі) зростання чутливості матриці.

Поліпшені показники дають змогу працювати камерам не тільки в умовах недостатньої освітленості, але й у процесі використання джерел інфрачервоного випромінювання.

Відзначимо, що вертикальне замазування при роботі на ПЗЗ з порядковим перенесенням заряду типу Нурег HAD має такий са-

мий незначний рівень, як і в матрицях з порядково-кадровим перенесенням зарядів.

Об'єктиви, якими комплектують відеокамери, відрізняються розміром фокусної відстані, світлосилою та характером утворюваного оптичного зображення.

Короткофокусний об'єктив має велику глибину різкості; довгофокусний об'єктив – обмежену глибину різкості.

Об'єктиви камер вибирають відповідно до їхнього призначення. Для максимального огляду вибирають ширококутові об'єктиви з фокусною відстанню 3,5 мм. Водночас кут огляду камери становитиме близько 90°.

Для спостереження периметра об'єкта використовують довгофокусні об'єктиви з фокусною відстанню 12 мм і кутом зору 30°.

Для забезпечення ефекту збільшення зображення використовують об'єктиви з трансфокатором, спеціальні телекамери з електронним трансфокатором або цифрову апаратуру (відеопроцесори).

У приміщенні варто використовувати камери з автоматичною діафрагмою для автоматичної компенсації зміни освітленості в різний час доби. Залежно від плану приміщення вибирають об'єктив з необхідним кутом огляду. Якщо необхідно сховати камеру, використовують мініатюрні камери з Pin-hole об'єктивами. У таких об'єктивів діаметр вихідної зіниці становить від 0,8 до 2÷4 мм. Таку камеру можна встановлювати, наприклад, за шпалерами, невеличкий отвір під об'єктив якої не привертає уваги.

Відеокамери мають додаткові можливості і сервісні пристрої.

Монітори є другим вузлом систем теленагляду.

Для систем теленагляду використовують головно монітори з діагоналлю 9", 12", 14" і 15" і розбиттям 500...800 пл.

Горизонтальне розділення для моніторів може становити:

- для чорно-білих – 750, 800, 900 і 1000 пл;
- для кольорових – 240, 300, 320 і 450 пл.

У системах теленагляду найширше застосовують чорно-білі монітори з розміром екрана 9" і 12". При використанні квадраторів і відеопроцесора доцільніше використовувати монітори з розміром 12" і 17".

Відеомонітор має забезпечувати параметри, які визначають його якість зображення, а саме: чіткість, фокусування, відтворення кольору, зведення та ін.

Відеомонітори можуть бути обладнані звуковим каналом для передавання аудіоінформації.

Додаткові пристрої систем теленагляду. До них відносять спеціалізовані відеомагнітофони, відеокомпресори, мультиплексори, детектори руху, матричні комутатори, поворотні і захисні пристрої, відеопринтери.

Одним з найважливіших параметрів відеомагнітофона є його роздільна здатність при записі зображення та надійність роботи. Висока роздільна здатність запису дає змогу фіксувати дрібні деталі, а надійність важлива тому, що відеомагнітофон призначений для безупинної роботи протягом декількох років.

Спеціалізовані відеомагнітофони можуть виконувати такі функції: записувати та відтворювати чорно-біле або кольорове зображення; виводити на екран час і дату; записувати за таймером або за зовнішнім сигналом; програмувати таймер на щоденне встановлення початку і закінчення запису, а також установлення режиму запису на тиждень; спеціальні режими відтворення (покадрове відтворення, пауза, швидкісний пошук вперед і назад); стоп-кадр; видавання сигналів синхронізації на зовнішні пристрої; програмування режимів роботи при спрацьовуванні сигналізації; реєстрація часу аварійного від'єднання живлення; збереження інформації в енергонезалежній пам'яті.

У багатокамерних системах теленагляду відеомагнітофони використовують разом з відеокомпресорами і мультиплексорами.

Відеокомпресор (квадратор) дає змогу на екрані монітора одночасно спостерігати в режимі реального часу зображення від декількох відеокамер і записувати його на відеомагнітофон, а наявність входу тривоги (ALARM-вхід) – підключити до відеокомпресора систему сигналізації, яка при спрацьовуванні автоматично підключить необхідну камеру для спостереження за об'єктом тривоги.

За допомогою відеокомпресора виводять на екран зображення від однієї до восьми відеокамер (більше – рідко). Він простий в управлінні і надає можливість спостерігати на екрані одного монітора зображення в комбінаціях, обраних оператором, які можуть бути довільними.

Мультиплексор дає змогу послідовно виводити на монітор і записувати на один відеомагнітофон інформацію від декількох камер. Водночас запис здійснюється без втрати якості зображення,

оскільки досягається послідовний запис кадрів на відеокасету з відеокамер. До мультиплексорів можна під'єднати систему сигналізації за ALARM-входом, що дає можливість автоматично увімкнути ту камеру, де відбулося порушення.

Детектори руху обробляють відеозображення від телекамер і, якщо необхідно, можуть вмикати відеомагнітофон для запису зображення або подавати сигнал тривоги.

При значній кількості камер ефективність роботи оператора може бути підвищена через застосування матричних комутаторів. За наявності детектора руху комутатор самостійно відстежує ситуацію і у разі тривоги виводить зображення від камер на монітори.

Матричний комутатор дає можливість звільнити стіл оператора від великої кількості пультів керування. Одним комутатором можливо керувати 128 поворотними пристроями, трансфокаторами і камерами. Донедавна матричні комутатори були єдиним прийнятним рішенням для великих об'єктів і споруд.

Повертальні пристрої відеокамер призначені для розширення кутів огляду. Камера, встановлена на поворотному пристрої, переміщується в горизонтальному і вертикальному напрямках. Поворотні пристрої для зовнішнього встановлення камер можуть працювати в складних погодних умовах. Для керування повертальними пристроями використовують спеціальну клавіатуру і телеметричні пристрої.

Відеопринтери (разом зі спеціальними відеомагнітофонами) також застосовують у системах охорони об'єктів для реєстрації відеозображень. На них роздруковують: фотографії клієнтів; фотографії небажаних відвідувачів; кадри надзвичайних ситуацій; кадри з будь-якої записаної відеокасети.

Традиційні системи теленагляду, зокрема системи з прихованими камерами, можуть бути застосовані для широкого спектра об'єктів: від квартир, офісів і дач до складських приміщень, банків, магазинів, автомобільних стоянок тощо. На "простих" об'єктах встановлюють системи телевізійного спостереження, які містять не більше чотирьох телекамер, монітор і прості засоби оброблення відеосигналу. Такі системи дають змогу чітко розрізняти дрібні предмети, номери автомашин, а комутатор дає можливість спостерігати на екрані монітора зображення в автоматичному режимі, послідовно від кожної камери, з певною періодичністю, обраною оператором.

Комп'ютерні системи застосовують для комплексного керування системами теленагляду, які здійснюють охорону і контроль доступу у приміщення як невеликих, так і великих офісів, банків тощо.

Програмні засоби призначені для керування системами теленагляду, сигналізації за системами контролю доступу. Саме програмні методи керування пристроями теленагляду дають можливість управляти комутаторами, відеомагнітофонами, мультиплексорами, трансфокаторами камер, моніторами і т.п.

Для створення систем відеоспостереження з великою кількістю камер використали комплекс великої кількості матричних комутаторів, у яких збирали відеосигнали, передавали різноманітним споживачам за допомогою коаксіального кабелю, витої пари, оптичного волокна і т.д.

На сьогодні технологія LAN (локальна мережа) є найбільш поширеною і побудована з використанням Ethernet, Fast Ethernet, FDDI, ATM і т.д. Локальні мережі більшості підприємств використовують схожу топологію побудови. Окремі LAN-сегменти можуть бути підключені за допомогою маршрутизаторів цифровими лініями типу T1, E1, ISDN і т.д., які знімають обмеження за розмірами і відстанями для локальних мереж.

Використовуючи алгоритм компресії, максимально знижують час передавання високоякісного кадру з високим рівнем частоти його відновлення.

У помешканні, де підключення до LAN недоступне, можливе використання вільного телефонного каналу телефонної мережі. Разом з тим центральна станція також має бути обладнана комунікаційним каналом, в якому використовують телефонну мережу. Очевидно, що зв'язок по телефонних лініях за допомогою модемів потрібно використовувати тільки тоді, коли немає можливості під'єднання до LAN.

Лабораторна робота № 3.6. Захисні системи відеоспостереження

Мета роботи: практичне встановлення захисних відеосистем та дослідження особливостей їхньої роботи.

Прилади та матеріали:

- відеокамера Trust 300;
- комп'ютер з USB-портами;
- керуюча комп'ютерна програма;
- омофон.

Хід виконання роботи.

1. Застосувати Web-камеру для відеоспостережень;
   1.1. Під'єднати камеру до USB-порту комп'ютера.
   1.2. Інсталювати керуючу програму на комп'ютері та перевірити роботу камери в різних режимах.
   1.3. Сфокусувати камеру на вхідні двері приміщення №1.
   1.4. За допомогою комп'ютерного мережевого зв'язку організувати спостереження та відеозапис вхідних дверей приміщення №1 з віддаленого приміщення №2.
2. Робота домофона.
   2.1. Принцип роботи та будова домофона.
3. Створення системи відеоспостереження на основі кількох відеокамер та плати квадратора.

3.15. Побічні електромагнітні випромінювання (ПЕМВ)

Найбільшу небезпеку з погляду витоку інформації становлять побічні (паразитні, ненавмисні) випромінювання технічних засобів, що беруть участь у процесі передавання, оброблення і зберігання секретної інформації.

Під витоком інформації каналами ПЕМВ розуміють можливість доступу до інформації в ІС, здійснюваного шляхом перехоплення і відповідного оброблення побічних (паразитних, ненавмисних) випромінювань технічних засобів передавання інформації, що їх використовують у системі для збирання, оброблення, зберігання й обміну інформацією.

Канал просочування інформації включає технічні засоби передавання, оброблення або зберігання секретної інформації, середовище розповсюдження паразитних електромагнітних або інших випромінювань і засіб перехоплення і первинного оброблення побічних (паразитних) випромінювань.

Контрольована територія включає простір навколо технічних засобів, у межах якого виключається неконтрольоване перебування сторонніх осіб, транспортних засобів і інших сторонніх об'єктів, що не мають постійного або разового допуску.

До технічних засобів, які можуть бути джерелом просочування інформації каналами ПЕМІН, відносять:

- засоби і системи телефонного, телеграфного (телетайпного), директорського, гучномовного, диспетчерського, внутрішнього, службового, технічного зв'язку;
- засоби і системи звукопідсилення, звукозаписи і звуковідтворення;
- пристрої, створюючі дискретні канали зв'язку: абонентна апаратура з засобами відображення і сигналізації, апаратура підвищення достовірності передавання, каналоутворююча і т.п.;
- апаратуру перетворення, оброблення, передавання і приймання відеоканалів, що містять інформацію факсиміле;
- засоби і системи спеціальної охоронної сигналізації (на розкриття дверей, вікон і проникнення в приміщення сторонніх осіб), пожежної сигналізації (з датчиком, реагуючими на дим, світло, тепло, звук);
- систему сигналізації дзвінка (виклик секретаря, вхідна сигналізація);
- контрольно-вимірювальну апаратуру;
- засоби і системи кондиціонування (датчики температури, вологості, кондиціонери);
- засоби і системи дротової радіотрансляційної мережі і приймання програм радіомовлення і телебачення (абонентні гучномовці системи радіомовлення й оповіщення, радіоприймачі і телевізори);
- засоби і системи часофікації (електронний годинник, вторинний електрогодинник);
- засоби і системи електроосвітлення і побутового електроустаткування (світильники, люстри, настільні і стаціонарні вентилятори, електронагрівальні прилади, холодильники, паперорізальні машини, дротова мережа електроосвітлення);
- електронну й електричну оргтехніку.

Усі ці технічні засоби можуть бути зосередженими випадковими антенами (апаратура і її блоки) і розподіленими випадковими антенами (кабельні лінії і дроти).

Вказаними елементами можуть бути:

- технічні засоби і прилади;
- кабельні мережі і розведення, що сполучають пристрої і устаткування;
- комутаційні пристрої (комутатори, кроси, бокси і т.п.);
- елементи заземлення й електроживлення.

Основними параметрами можливого просочування інформації каналами ПЕМІН є:

- напруженість електричного поля інформативного (небезпечного) сигналу;
- величина звукового тиску;
- величина напруги інформативного (небезпечного) сигналу;
- величина напруги наведеного інформативного (небезпечного) сигналу;
- величина напруги шумів (перешкод);
- величина струму інформативного (небезпечного) сигналу;
- величина чутливості до дії магнітних полів для точкового джерела;
- величина чутливості апаратури до дії електричних полів (власна місткість апаратури);
- величина чутливості до дії акустичних полів;
- відношення “інформативний сигнал/шум”;
- відношення напруги небезпечного сигналу до напруги шумів (перешкод) у діапазоні частот інформативного сигналу.

До засобів технічного захисту відносять:

- фільтри-обмежувачі і спеціальні абонентні пристрої захисту для блокування просочування мовної інформації через дводротові лінії телефонного зв’язку, системи директорського і диспетчерського зв’язку;
- пристрої захисту абонентних однопрограмних гучномовців для блокування просочування мовної інформації через радіотрансляційні лінії;
- фільтри мережні для блокування просочування мовної інформації каналами електроживлення змінного (постійного) струму;

- фільтри захисту лінійні (високочастотні) для встановлення в лініях апаратів телеграфного зв'язку;
- генератори лінійного зашумлення;
- екрановані камери спеціальної розробки.

Найбільш ефективно гальванічну й електромагнітну розв'язку кабелів електроживлення ТС ЕВТ від промислової мережі забезпечує їхня роздільна система типу "електродвигун-генератор". Електроживлення можливо також здійснювати через завадостійкі фільтри.

Інформація, відображена на екрані дисплея, може бути відновлена за допомогою ТВ-приймача. Він обробляє лише невелику частину шириною близько 8 Мгц на частотах в діапазонах метрових і дециметрових хвиль. Сьогодні наявна система захисту інформаційних об'єктів від витоку інформації, що включає проведення організаційних, організаційно-технічних, технічних заходів і заходів, пов'язаних з контролем за виконанням захисту.

Контрольні запитання до розділу 3

1. Види інформації та актуальність захисту інформації й інформаційних об'єктів.
2. Потенційні загрози безпеці інформації в інформаційних системах.
3. Обмеження, розмежування і контроль доступу до інформаційних об'єктів.
4. Види систем охоронної сигналізації.
5. Сучасні системи контролю доступу на захищену територію.
6. Види засобів захисту інформації та їхня класифікація.
7. Технічні засоби захисту інформаційних об'єктів.
8. Засоби охоронної сигналізації.
9. Охоронне телебачення.
10. Інфрачервоні сенсори охорон ної сигналізації. Фізичні основи функціонування.
11. Комбіновані сенсори охоронної сигналізації.
12. Фотоелектричні сенсори та системи охорони периметра.
13. Детектори вібрацій, розбиття скла, ультразвукові детектори, протипожежні детектори.
14. Охоронні системи телеспостереження.

ДОДАТКИ

4.1. Комп'ютерна стеганографія – технологія інформаційної безпеки XXI століття

Завдання надійного захисту інформації від несанкціонованого доступу є однією з найдавніших і не вирішених до тепер проблем. Методи (факти) приховання секретних повідомлень відомі з давніх часів, і така людська діяльність отримала назву стеганографія. Це слово походить від грецьких слів "steganos" (секрет, таємниця) і "graphy" (запис) і, отже, означає буквально "тайнопис", і хоч методи стеганографії з'явилися, можливо, раніше, ніж з'явилася сама писемність (спочатку використовували умовні знаки і позначення) [1].

Згодом для захисту інформації почали використовувати більш ефективні методи кодування і криптографії. Як відомо, мета криптографії полягає в блокуванні несанкціонованого доступу до інформації шифруванням вмісту секретних повідомлень. Стеганографія має інше завдання, її мета – приховати сам факт наявності секретного повідомлення, разом з тим обидва способи можуть бути об'єднані і використані для підвищення ефективності захисту інформації (наприклад, для передавання криптографічних ключів) [1].

Комп'ютерні технології надали новий імпульс розвитку і вдосконаленню стеганографії, з'явився новий напрямок захисту інформації – комп'ютерна стеганографія (КС). Сучасний прогрес в області глобальних комп'ютерних мереж і засобів мультимедії привів до розроблення нових методів, призначених для убезпечення передавання даних каналами телекомунікацій Ці методи, враховуючи природні неточності засобів цифрування і надмірність аналогового відео- або аудіосигналу, дають змогу приховувати повідомлення в комп'ютерних файлах (контейнерах), причому на відміну від криптографії ці методи приховують сам факт передавання інформації.

Основні принципи комп'ютерної стеганографії й області її використання. В сучасній комп'ютерній стеганографії є два типи файлів: файл-повідомлення, який призначений для приховування, і файл-контейнер, який може бути використаний для приховування в ньому повідомлення. Контейнери бувають двох типів: контей-

нер-оригінал (або “порожній” контейнер) – це контейнер, який не містить прихованої інформації, і контейнер-результат (або “заповнений” контейнер) – це контейнер, який містить приховану інформацію. Під ключем розуміють секретний елемент, який визначає порядок внесення повідомлення в контейнер. Основними положеннями сучасної комп’ютерної стеганографії є такі:

- методи приховування мають забезпечити автентичність і цілісність файлу;
- передбачено, що супротивнику повністю відомі можливі стеганографічні методи;
- безпечність методів ґрунтується на збереженні стеганографічних перетворень основних властивостей файлу, що його відкрито передають, внісши в нього секретне повідомлення і деяку невідому супротивнику інформацію – ключ;
- якщо факт приховання повідомлення став відомим супротивнику через спільника, вилучення самого секретного повідомлення є складною вичислювальною задачею.

Внаслідок зростання ролі глобальних комп’ютерних мереж, все більш важливим є значення стеганографії. Аналіз інформаційних джерел комп’ютерної мережі Інтернет дає можливість зробити висновок, що сьогодні стеганографічні системи активно використовують для вирішення таких основних завдань.

Захист конфіденційної інформації від несанкціонованого доступу. Використання КС вважають найбільш ефективним при вирішенні проблем захисту конфіденційної інформації. Так, наприклад, тільки одна секунда оцифрованого звуку з частотою дискретизації 44 100 Гц і рівень відрахунку 8 бітів у стереорежимі дає змогу приховати за рахунок заміни найменш значущих молодших розрядів на приховане повідомлення близько 10 кбайт інформації.

Водночас зміна значень відліків становить менше відсотка. Таку зміну фактично не виявляють при прослуховуванні файлу більшість людей [1].

Подолання систем моніторингу та управління мережевими ресурсами. Стеганографічні методи, спрямовані на протидію системам моніторингу та управління мережевими ресурсами (промислове шпигунство), дають можливість протистояти спробам контролю над інформаційним простором під час проходження інформації через сервери управління локальних і глобальних вичислювальних мереж.

Камуфлювання програмного забезпечення (ПЗ) – ще одне важливе завдання стеганографії. Коли використання ПЗ незареєстрованими користувачами є небажаним, воно може бути закамуфльовано під стандартні універсальні програмні продукти (наприклад, текстові редактори) або приватно у файлах мультимедіа (наприклад, у звуковому супроводі комп'ютерних ігор).

Захист авторських прав від піратства. На комп'ютерні графічні зображення наносять спеціальну позначку, що залишається невидимою для очей, але розпізнається спеціальним ПЗ. Таке програмне забезпечення вже використовують у комп'ютерних версіях деяких журналів. Цей напрямок стеганографії призначений не тільки для оброблення зображень, але і для файлів з аудіо- та відеоінформацією, і має забезпечити захист інтелектуальної власності. Методи комп'ютерної стеганографії розвиваються за двома основними напрямками:

- засновані на використанні спеціальних властивостей комп'ютерних форматів;
- засновані на надмірності аудіо- та візуальної інформації.

Перший напрямок ґрунтується на використанні спеціальних властивостей комп'ютерних форматів репрезентації даних, а не на надмірності самих даних. Спеціальні властивості форматів вибирають з урахуванням захисту схованого повідомлення від безпосереднього прослуховування, перегляду або прочитання. Аналізуючи, можна зробити висновок, що основним напрямком комп'ютерної стеганографії є використання надлишку аудіо- та візуальної інформації. Цифрові фотографії, цифрова музика, цифрове відео передано матрицями чисел, що кодує інтенсивність у дискретні моменти в просторі або часі. Цифрова фотографія – це матриця чисел, що передає інтенсивність світла в певний момент часу. Цифровий звук – це матриця чисел, побудована на інтенсивності звукового сигналу в послідовні моменти часу. Всі ці числа неточні, оскільки неточні пристрої оцифрування аналогових сигналів, тобто є шуми квантування. Молодші розряди цифрових відліків містять мало корисної інформації про поточні параметри звуку та візуального образу. Їхнє заповнення відчутно не впливає на якість сприйняття, що і дає можливість для приховування додаткової інформації. Графічні кольорові файли зі схемою змішування RGB кодують кожну точку рисунка трьома байтами. Кожна така точка складається з адитивних складових: червоного, зеленого,

синього. Зміна кожного з трьох найменш значущих бітів веде до зміни менше відсотка інтенсивності цієї точки, що дає змогу приховувати у стандартній графічній картинці об'ємом 800 кбайтів близько 100 кбайтів інформації, що непомітно при перегляді зображення.

Аналіз тенденцій розвитку КС свідчить, що найближчими роками інтерес до розвитку методів стеганографії посилюватиметься. Передумови до цього вже сформувалися. Зокрема, загальновідомо, що актуальність проблеми інформаційної безпеки постійно зростає і стимулює пошук нових методів захисту інформації. Крім того, бурхливий розвиток інформаційних технологій забезпечує можливість реалізації цих нових методів захисту інформації. І, звичайно, сильним каталізатором процесу є лавиноподібний розвиток комп'ютерної мережі загального користування Інтернет, у т.ч. такі невирішені протиріччя Інтернету, як захист авторського права, захист прав на особисту таємницю, організування електронної торгівлі, протизаконна діяльність хакерів, терористів і т. д. Досить характерною тенденцією, пов'язаною з захистом інформації, є впровадження криптологічних методів. Однак на цьому шляху ще багато невирішених проблем, що стосуються руйнівного впливу на криптосередовище таких складових інформаційної зброї, як комп'ютерні віруси, логічні бомби, автономні реплікативні програми і т.д. Поєднання методів комп'ютерної стеганографії та криптографії стало б хорошим виходом з цієї ситуації, адже вдалося б усунути слабкі сторони відомих методів захисту інформації та розробити більш ефективні нетрадиційні методи забезпечення інформаційної безпеки.

Останніми роками з'явилися програмні комплекси, що забезпечують приховування інформації в цифрових аудіо- і відеофайлах за допомогою методів стеганографії. Однією з найбільш актуальних і складних проблем комп'ютерної стеганографії є виявлення факту такого приховування. Без апріорної інформації виявлення приватного повідомлення можливе на основі виявлення порушень природних залежностей, властивих натуральному файлу-контейнеру [1, 2].

Одним з найбільш перспективних підходів до аналізу стеганографічного приховування є підхід, суть якого полягає у введенні в файл прихованої інформації як втручання у статистичні закономірності, порушення природності фізичного процесу: процес прихо-

вування описують недетермінованим чином, а ймовірнісним, тобто прогнозованою з деякою ймовірністю зміною природних зв'язків.

Місцями для впровадження прихованої інформації зазвичай є молодші розряди, які прийнято називати найменш значимими бітами (НЗБ). Статистичні дослідження звукових файлів дали змогу виявити низку перспективних для аналізу статистик: Хі-квадрат, Спірмена, Кендалла і коефіцієнт кореляції [1, 2].

Звуковий контейнер можна описати як два об'єкти: перший – це НЗБ, другий – старші біти (всі біти звукових відліків, за винятком найменш значущих). Кожен з цих об'єктів має свою ознаку. НЗБ набувають значеннь 0 або 1; старші біти (двійкове передавання числа) мають значення (0, 1,. ... $2^{к-1}$-1), де к – число рівнів квантування. Необхідно з'ясувати, чи ці ознаки пов'язані між собою або ж їх необхідно вважати незалежними (у ймовірнісному сенсі).

За допомогою функції Хі-квадрат, використовуваної в критерії незалежності двох випадкових величин, вказують, що для вихідного контейнера НЗБ та інші розряди статистично залежні. Показником є той факт, що впровадження прихованого повідомлення порушує природу цифрового аудіоконтейнера, що виражається у зменшенні значень статистики Хі-квадрат, тобто у випадку часткового заповнення НЗБ інші розряди продовжують залишатися залежними, але все ж ступінь залежності порівняно з вихідною зменшується. При повному заміщенні НЗБ стають незалежними від інших розрядів. Ці результати свідчать, що зміна значення статистики Хі-квадрат є демаскуючою ознакою і дає можливість виявляти стеганографічне приховування інформації.

За допомогою статистики Хі-квадрата та коефіцієнта кореляції було проведено стеганографічний аналіз програм Steganos (Version 1.0a) і S-Tools (Steganography tools for Windows 4,0), які приховують інформацію в найменш значущі біти звукових відліків. Значення, наближені до нуля, мають дуже слабку залежність або її зовсім немає, що можливо тільки після впровадження додаткової інформації. Тому за зміною значень статистики Хі-квадрат та коефіцієнта кореляції визначають факт приховування інформації в звукових файлах.

Лабораторна робота № 4.1. Система захисту, що ґрунтується на шифруванні інформації у зображенні і звуці

Мета роботи. Практична робота з пакетом S-tools.

Хід виконання роботи.

1. Стеганографія звукових файлів.
2. Робота з графічними файлами.

З поширенням інформаційних технологій все ширшого використання набуває обмін інформацією. Досить часто важливою вимогою під час передавання інформації є питання безпеки та конфіденційності. А це, своєю чергою, спонукає до розвитку технологій шифрування інформації. Цікавим способом шифрування інформації є "стеганографія". Ключовий принцип стеганографії полягає у розміщенні інформації, яку необхідно зашифрувати, у цифровому потоці, такому як зображення чи звук. Більшість комп'ютерної інформації має бути передана зі стовідсотковою точністю, для коректного функціонування, але зображення та звуку це не стосується. Потрібну інформацію можна "заховати" у цифровому потоці, вносячи непомітні для ока (чи вуха) зміни у зображення чи звук.

Як інформацію приховують у звуці? Звукова інформація у WAV-файлах зберігається за допомогою 8- або 16-бітних чисел, які подають на ЦА-конвертор звукової карти. Основний принцип, відповідно до якого інформацію шифрують у звуці, полягає у тому, що бітове повідомлення, яке потрібно зашифрувати та передати, розповсюджується рівномірно по звуковому файлові так, що змінюються найменш важливі, в плані сприйняття вухом, частини звукової інформації.

Найпростіший спосіб – це заміна молодшого біта кожного байта звукового файлу відповідним бітом повідомлення, яке необхідно зашифрувати та передати. Наприклад, звуковий файл містить десь у собі таку послідовність байтів: 132 134 137 141 121 101 74 38. В двійковому описові це виглядає так:
10000100 10000110 10001001 10001101 01111001 01100101 01001010 00100110. Припустимо, що нам потрібно "сховати" двійкове число 11010101 (213) у цій послідовності. Все, що нам потрібно зробити, це замінити молодший біт у кожному байті звукового файлу відповідним бітом того байта, який нам потрібно приховати,

тобто послідовність байтів зміниться на: 133 135 136 141 120 101 74 39. Що у двійковому поданні виглядає так:
10000101 10000111 10001000 10001101 01111000 01100101 01001010 00100111. Отже, значення байтів звукового файлу змінилися, максимум, на одиничку. Людське вухо не відчує таких змін, а ми маємо можливість восьму частину звукового файлу використати для нашого повідомлення.

Як інформація "ховається" у зображенні? Усі комп'ютерні зображення сформовані як масиви точок, які називають пікселями. Кожен піксель має свій власний колір, репрезентований трьома числами – червоним, зеленим та синім (т. зв. RGB-подання). У BMP-графічному форматі ці значення можуть бути у діапазоні від 0 до 255. Колір (0,0,0) – чорний; (255,255,255) – білий. Основний принцип, згідно з яким інформація зашифрована у зображенні, полягає у тому, що бітове повідомлення, котре потрібно зашифрувати та передати, розповсюджується рівномірно по графічному файлу так, що змінюються найменш важливі, в плані сприйняття оком, частини графічної інформації.

Найпростіший спосіб шифрування – це заміна молодшого біта кольорових рівнів зображення відповідним бітом повідомлення, яке необхідно зашифрувати та передати. Для 24-bit зображення це досить просто тому, що у них колір визначається трійкою байтів, і все, що нам потрібно зробити, – це розповсюдити біти нашого повідомлення.

Як працювати з пакетом S-Tools? Щоб користуватися пакетом S-Tools, необхідно також запустити або Windows Explorer, або File Manager (що більше до вподоби). Розміщують його вікно на десктопі (робочому столі) так, щоб одночасно бачити вікно запущеного пакета S-Tools.

Далі необхідно перемістити файл (версія 4,00 пакета підтримує такі формати: графічні BMP, GIF та звукові WAV), у якому розміщуватимуть приховану інформацію у вікно пакета S-Tools.

Виділяють файли, які будуть приховувати та переміщати їх на об'єкт (файл зображення чи звуку). З'явиться пропозиція ввести двічі Passphrase (фразу-пароль), яку необхідно запам'ятати, щоб мати можливість "відшукати" інформацію. Для відтворення прихованої інформації з графічного чи звукового файлу необхідно помістити цей файл у вікно пакета S-Tools та, натиснувши праву клавішу мишки, вибрати пункт Reveal (виявити).

Робота зі звуковими файлами. Для відкриття звукового файлу використовують програму Windows Explorer (Провідник) для того, щоб знайти звуковий файл, в якому розміщатимуть інформацію та перемістять його на порожнє місце вікна пакета S-Tools.

S-Tools працює лише зі звуковим форматом WAV. Всі маніпуляції з цим файлом здійснюють, натиснувши праву клавішу мишки на зображенні файлу.

Для того, щоб приховати потрібний файл з інформацією, потрібно перемістити його у вікно звукового файлу. Після чого є можливість увести пароль та метод шифрування (IDEA, DES, Triple DES чи MDC). Після процесу приховування з'являється нове вікно звукового файлу, в якому заховано секретний файл. Далі цей файл можна записати.

Щоб отримати приховану інформацію зі звукового файлу, необхідно помістити файл-носій у вікно пакета S-Tools та натиснути на вікні файлу правою клавішею мишки. Вибравши пункт Reveal та ввівши пароль, отримують прихований файл.

Робота з графічними файлами. Процес роботи з графічними файлами аналогічний роботі зі звуком. З'являється можливість конвертувати файл-носій у 24-bit кольорове подання або у зменшену за кількістю кольорів палітру.

Список літератури

1. *Барсуков В.С., Романцов А.П.* Компьютерная стеганография вчера, сегодня, завтра // – М.: Специальная техника, 1998. – С. 16–19.
2. *Романцов А.П.* Статистический метод выявления стеганографического скрытия информации в звуковых: файлах // Матер. Междунар. форума информатиз. МФИ–2000 (Междунар. конгресс "Коммуникационные технологии: и сети."). – Москва, ноябрь, 2000. – М.: Информсвязьиздат, 2000. – С. 703–204.
3. *Романцов А.П., Петраков А.В., Кондратьев А.Н.* Стеганографическая защита видеокадра // Матер. Международ. форума информатиз. МФИ–2002 (Междунар. конгресс "Коммуникационные технологии и сети") – Москва, ноябрь, 2002, – М.: Информсвязьиздат, 2002. – С. 160.

СПИСОК ЛІТЕРАТУРИ

1. *Андрианов В.Н., Бородин В.А., Соколов А.В.* “Шпионские штучки” и устройства для защиты объектов и информации / Под ред. С.А. Золотарева Справочное пособие. – СПб.: Лань, 1996. – 272 с.
2. *Андрианов В.Н., Соколов А.В.* “Шпионские штучки 2” или как сберечь свои секреты. -– СПб.: Полигон. 1997. – 272 с.
3. *Андрианов В.Н., Соколов А.В.* Охранные устройства для дома и офиса / Под ред. С.А. Колесниченко, И.В. Шишигина – СПб.: Лань, 1997. – 304 с.
4. *Анин Б.* Защита компьютерной информации. – СПб.: БХВ-Петербург, 2000. – С.384.
5. *Армстронг Дж.* Секреты UNIX. – Киев: Диалектика, 1996. – С.576.
6. *Баричев С.С., Гончаров В.В., Серов Р.Е.* Основы современной криптографии. – М.: Мир, 1997. – 176 с.
7. *Варфоломеев А.А., Жуков А.Е., Мельников А.Б. и др.* Блочные криптосистемы. Основные свойства и методы анализа устойчивости. – М.: МИФИ, 1998. – 200 с.
8. *Вербіцький О.В.* Вступ до криптології. – Л.: ВНТЛ, 1998. – 248 с.
9. *Виноградов Ю.А.* Электронная охрана. (Элементы и узлы охранных систем). – М.: Символ-Р, 1996. – 95 с.
10. *Герасименко В.А., Малюк А.А.* Основы защиты информации. – М.: МГИФИ, 1997. – 538 с.
11. *Голубєв В.О., Юрченко О.М.* Злочини в сфері комп’ютерної інформації: способи скоєння та засоби захисту. / За ред. О.П. Снігерьова та М.С. Вертузаєва. – З.: Павел, 1998. – 157 с.
12. *Грушо А.А., Тимонина Е.Е.* Теоретические основы защиты информации. – М.: Яхтсмен, 1996. – 31 с.
13. *Домашов А.В., Попов В.О., Правиков Д.И., и др.* Программирование алгоритмов защиты информации. – М.: Нолидж, 2000. – 288 с.
14. *Ємець В., Мельник А., Попович Р.* Сучасна криптографія основні поняття. – Л.: БАК, 2003. – 144 с.

15. *Зегжда Д.П., Ивашко А.М.* Как построить информационную защищенную систему/ Под ред. П.Д. Зегжды – СПб.: Мир и семья-95, 1997. – 312 с.
16. *Казаков С.И.* Основы сетевых технологий. – М.: Академич. экспресс, 1998. – С.456.
17. *Коркішко Т., Мельник А., Мельник В.* Алгоритми та процесори симетричного блокового шифрування. – Л.: БАК, 2003. – 168 с.
18. *Мельников В.В.* Защита информации в компьютерных системах. – М.: Финансы и статистика; Электронинформ, 1997. – 368 с.
19. *Молдовян А.А., Молдовян Н.А., Рад Б.Я.* Криптография. – СПб.: Лань, 2000. – 224 с.
20. Охранные системы. Сер.: Информационное издание. Вып. 4. – М.: Наука и техника, 1996. – 130 с.
21. *Петерсен Ричард.* Энциклопедия LINUX. – СПб.: Питер, 2002. – С.1008.
22. *Петраков А.В., Дорошенко П.С., Савлуков Н.В.* Охрана и защита современного предприятия. – М.: Энергоатомиздат, 1999. – 568 с.
23. *Петров А.А.* Компьютерная безопасность. Криптографические методы защиты. – М.: ДМК, 2000. – С.448.
24. *Ростовцев А.Г., Матвеев В.А.* Защита информации в комп'ютерных системах. Элементы криптографии / Под ред. П.Д. Зегжды. – СПб.: ГТУ, 1993. – 365 с.
25. *Сидоров И.Н.* Устройства охраны и сигнализации для квартир, дач и автомобилей. Справочник домашнего мастера. – СПб.: Лениздат, 1996. – 315 с.
26. *Спесивцев А.В.* Защита информации в персональных ЭВМ. – М.: Мир, 1992. – 278 с.
27. *Спортак М., Паппас Ф., Реззинг Э.* Высокопроизводительные сети. Энциклопедия пользователя. – Киев: Диасофт, 1998. – С 432.
28. *Хорев А.А.* Способы и средства защиты информации. – М.: МОРФ, 2000. – 316 с.
29. *D. Brent Chapman, Elizabeth D. Zwicky,* Building Internet Firewalls. O'Reilly & Associates, 1995. – P 546.

Список питань з курсу “Системи і методи захисту інформації”

1. Квантова криптографія.
2. Захист інформації в стільникових мережах.
3. Аналіз можливих загроз в інформаційних системах.
4. Система Райвеста, Шаміра, Адлемана.
5. Класичні шифри. Комп’ютерна реалізація алгоритмів.
6. Бінарний метод піднесення до степеня за модулем числа *n*.
7. Система Діффі-Гелмана.
8. Робота з камерами відеоспостережень. Пакети Netmeeting та Videoinspector.
9. Стеганографія. Пакет S-tools.
10. Кількаразове шифрування. Суперпозиція шифрів.
11. Криптографічні схеми сучасності.
12. Типи сенсорів, які застосовують для захисту інформаційних об’єктів.
13. Методи частотного аналізу та прямого перебору.
14. Системи ADFGVX.
15. Технічні засоби охоронної сигналізації.
16. Подання тексту у цифровій формі. Шифр одноразового блокнота.
17. Біомедичні індентифікаційні системи.
18. Елементи теорії чисел. Функція Ойлера.
19. Безпека інформації операційних систем.
20. Детектори вібрацій, розбиття скла та ультразвуку.
21. Алгоритм Евкліда в теорії чисел.
22. Симетричні криптосистеми та системи з відкритим ключем.
23. Комбіновані сенсори охоронної сигналізації.
24. Системи PGP.
25. Системи електронного підпису.
26. Безпека інформації в комп’ютерних мережах.
27. Фотоелектричні сенсори та системи охорони периметра.
28. Принципи сучасної криптології.
29. Елементи і пристрої фізичної та електронної охорони об’єктів.
30. Захист інформації в автоматизованих системах оброблення даних.
31. Елементи теорії чисел. Конгруенції та їхні властивості.

32. Інформаційний захист ПК.
33. Принципи побудови, структури і завдання служби захисту інформації.
34. Знаходження обернених елементів у кільці зведених лишків. Елементи теорії чисел.
35. Законодавчі і правові аспекти захисту інформації в Україні.
36. Захист інформації в Interneti.
37. Хеш-функції. Вимоги до хеш-функцій. Схема цифрового підпису при застосуванні H(M) для алгоритму RSA.
38. Піднесення великого числа до великого степеня та взяття залишку за модулем третього великого числа.
39. Відкритий розподіл криптографічних ключів. Алгоритм Діффі-Гелмана.
40. Криптосистема Ель-Гамаля.
41. Проблеми генерування випадкових послідовностей та генерування псевдовипадкових чисел операційними системами і мовами програмування. Добування великих простих чисел.
42. Особливості стандарту AES.
43. Потокові шифри, алгоритм потокового шифру RC4. Потоковий шифр на основі генератора BBS. Переваги і недоліки потокових шифрів.
44. Афінні шифри
45. Стеганографія.
46. Що таке криптографія та криптоаналіз?
47. Типи криптографічних систем.
48. Означити криптостійкість та електронний підпис.
49. Описати типову схему криптосистем.
50. Навести приклади класичних криптосистем.
51. Шифр Віженера та програмна реалізація алгоритму на прикладі шифрування за методом Цезаря.
52. Порівняти блочну та асиметричну криптографії.
53. Описати алгоритм DES.
54. Математичні основи асиметричних криптосистем. Важкооборотні функції.
55. Основні означення дискретного аналізу та алгоритм Евкліда.
56. Алгоритм RSA.
57. Електронний підпис на основі асиметричного алгоритму.
58. Описати роботу з пакетом PGP.
59. Прикладні застосування криптографічних методів.

60. Що таке безпека даних у комп'ютерних мережах?
61. Способи ідентифікації за персональними фізичними ознаками.
62. Способи з'єднань комп'ютерів у мережі.
63. Програмне та апаратне забезпечення з'єднання комп'ютерів у мережі.
64. Захист мережі з використанням брандмауерів і серверів-посередників.
65. Захист ресурсів у мережевій ОС Novel NetWare.
66. Захист інформації в ОС Windows NT.
67. Адміністративні засоби управління ресурсами домену Windows NT 4,0.
68. Особливості роботи з пакетами Win Snifter та x Intruder.
69. Інформаційна безпека в ОС UNIX.
70. Робота адміністратора в UNIX мережі.
71. Система Kerberos.
72. Робота з ОС Free BSD 3x, BSD 4x.
73. Захист електронної пошти.
74. Види інформацій і актуальність захисту інформацій та інформаційних об'єктів.
75. Потенційні загрози безпеці інформації в інформаційних системах.
76. Обмеження, розмежування і контроль доступу до інформаційних об'єктів.
77. Види систем охоронної сигналізації.
78. Сучасні системи контролю доступу на захищену територію.
79. Види засобів захисту інформації та їхня класифікація.
80. Технічні засоби захисту інформаційних об'єктів.
81. Засоби охоронної сигналізації.
82. Охоронне телебачення.
83. Інфрачервоні сенсори охоронної сигналізації. Фізичні основи функціонування.
84. Комбіновані сенсори охоронної сигналізації.
85. Фотоелектричні сенсори та системи охорони периметра.
86. Детектори вібрацій, розбиття скла, ультразвукові детектори, протипожежні детектори.
87. Охоронні системи телеспостереження.
88. Інтерфейс CRYPTO API Windows XP.
89. Сенсорні пристрої.

90. Голосова ідентифікація.
91. Захист салону автомобіля від зчитування інформації.
92. Автомобільні сигналізації та їхні характеристики.
93. Ідентифікація ДНК особи.
94. Біометрія. Відбитки пальців. Розпізнання.
95. Шифрувальна система на основі шифру гамування.
96. Вчені, які зробили великий внесок у криптографію.
97. Елементи теорії криптографічних систем.
98. Класичні криптосистеми.
99. Програмна реалізація алгоритму шифрування за методом Цезаря.
100. Сучасні блочна та асиметрична криптографії. Стандарт шифрування даних ГОСТ 28147–89.
101. Блочні криптосистеми типу DES, IDEA,BLOWFISH.
102. Криптопакет KRYPTON.
103. Асиметричні криптосистеми.
104. Прикладні застосування криптографічних методів.
105. Комплексне застосування криптографічних перетворень, кодування і стискування інформації.
106. Технології з'єднань комп'ютерів.
107. Програмне та апаратне забезпечення з'єднання ПК.
108. Інформаційний захист мережі з використанням брандмауерів та серверів-посередників.
109. Реєстрація, розподіл та захист ресурсів у ОС Novel NetWare 3,11.
110. Захист інформації в операційній системі Windows N.
111. Методи інформаційної безпеки в ОС.
112. Антивірусний захист електронної пошти.
113. Загальні питання захисту інформації в автоматизованих системах оброблення даних (АСОД).
114. Потенційні загрози безпеці інформації в АСОД.
115. Обмеження, розмежування і контроль доступу до апаратури.
116. Системи охоронної сигналізації (СОС).
117. Сучасні системи контролю доступу на територію, що її охороняють.
118. Архітектура побудови систем контролю доступу.
119. Біометрія як засіб ідентифікації особи в охоронних системах.
120. Засоби захисту інформації АСОД та їхня класифікація.
121. Електронні системи захисту автомобілів.

122. Інфрачервоні пасивні сенсори охоронної сигналізації.
123. Комбіновані сенсори охоронної сигналізації.
124. Фотоелектричні сенсори та системи охорони периметра.
125. Охорона периметра з допомогою оптоелектронної (лазерної) системи.
126. Детектори вібрацій, розбиття скла та ультразвукові детектори.
127. Пожежні повідомлювачі.
128. Виконавчі пристрої охоронних систем.
129. Система захисту, основана на передаванні інформації через стільникові лінії зв'язку.
130. Охоронні системи телеспостереження.
131. Побічні електромагнітні випромінювання (ПЕМВ).
132. Комп'ютерна стеганографія – технологія інформаційної безпеки XXI століття.

Тести з курсу “Системи і методи захисту інформації”

Алгоритм шифрування в системі RSA

1) $C=M^e \bmod n$
2) C=M +R
3) C=M-R
4) $C=M^2 \bmod n$

Автори системи RSA

1) Адлеман
2) Райвест
3) Шамір
4) Всі

Типи файл-контейнерів у стеганографії

1) Аудіо
2) Відео
3) Фото
4) Текстові

Назвати однотипні алгоритми шифрування

1) DES, ГОСТ, BLOWFISH
2) RSA, Diffi-Helman, Віженера
3) Матричний обходу, ADFGVX, заміна
4) Електронні кодові книжки, гомофонний шифр

Шифр-системи ADFGVX – це

1) Шифр підставляння
2) Переставляння
3) Суперпозиція 1 і 2
4) Проста заміна

Алгоритм дешифрування $M=C^d \bmod n$ названо

1) Diffi-Helman
2) DES
3) RSA
4) AES

При застосуванні програми VideoInspector здійснюється

1) Увімкнення та вимкнення відеозапису за таймером
2) Увімкнення та вимкнення відеозапису за сенсором руху
3) Постійне ввімкнення програми
4) Одночасно 1,2,3

Робота з пакетом PGP потребує

1) Обрання одного ключа
2) Генерування двох ключів
3) Генерування ключа
4) Вибору двох ключів

Вказати в переліку класичні криптосистеми: DES, Віженера, GVX, RSA, AES

1) DES
2) Віженера
3) GVX
4) RSA, AES

Види криптостійкості шифрів

1) Абсолютна
2) Стійкість в обчислювальному сенсі
3) Одночасно 1 і 2
4) Немає правильної відповіді

Інфрачервоні сенсори – це

1) Сенсори розбиття світла
2) Сенсори руху
3) Радіочастотні детектори
4) Одночасно 1 і 2

Симетричні криптосистеми – це

1) RSA
2) DES
3) AES
4) 1 і 2

Файл-контейнери в стеганографії

1) Аудіо
2) Відео
3) Текстові
4) 1 і 2

Зашифрувати алгоритмом Цезаря послідовності 15,17,01,30,14

1) 13, 15, 31, 28, 12
2) 17, 19, 03, 32, 16
3) 16, 18, 02, 15
4) 19, 21, 07, 16, 05

Вибрати правильний запис алгоритму *DESX*

1) $C = DESX_{KK_1K_2} = K_2 + DES_K(K_1 + M)$
2) $C = DESX_{KK_1K_2} = K_2 \oplus DES_K(K_1 \oplus M)$
3) $C = DESX_{KK_1K_2} = K_2 - DES_K(K_1 - M)$
4) $C = DESX_{KK_1K_2} = K \oplus DES_{K_1}(K_2 \oplus M)$

Відшукати правильний запис алгоритму $3DES_{KK_1K_2}$

1) $C = DESX_{K_2}\left(DESX_{K_1}^{-1}\left(DES_{K_3}(M)\right)\right)$
2) $C = 3DESX_{K_1K_2K_3}(M) = DES_{K_3}\left(DES_{K_2}^{-1}\left(DES_{K_1}(M)\right)\right)$
3) $C = DESX_{K_1}\left(DESX_{K_1}^{-1}\left(DES_{K_3}(M)\right)\right)$
4) $C = DESX_{K_2}\left(DESX_{K_3}^{-1}\left(DES_{K_1}(M)\right)\right)$

Записати алгоритм шифрування Рабіна

1) $C = M^1_{\bmod n}$
2) $C = M^2_{\bmod n}$
3) $C = M^{-2}_{\bmod n}$
4) $C = M^{-1}_{\bmod n}$

Тип систем охоронних сигналізацій за принципом дії

1) Контактні, ультразвукові, реєстратори руху
2) Переривання променя, телевізійні, радіолокаційні, мікрохвильові
3) Сенсори задимленості
4) Сенсори груп 1 і 2

Довжина блоку в шифрі DES

1) 64 бітів
2) 56 бітів
3) 128 бітів
4) 256 бітів

Квантова криптографія як одиниця інформації

1) Біт
2) Байт
3) Кубіт
4) Кілобайт

Частотний аналіз – це метод дослідження криптосистем

1) Криптографічний
2) Криптоаналітичний
3) 1 і 2
4) Ні 1, ні 2

Знайти значення функцій Ойлера $\varphi(n)$ від чисел 1, 2, 3, 4, 5, 6, 7, 8, 9, 10

1) 11224264610
2) 11214264610
3) 11224254610
4) 11214254610

Записати наслідок алгоритму Евкліда для взаємно простих чисел a і b і цілих u і v

1) $ua + vb = 0$
2) $ua + vb = 1$
3) $ua - vb = 0$
4) $ua - vb = 1$

Знайти всі n, для яких $\varphi(n) \leq 5$

1) 1, 2, 3, 4, 5, 6, 8, 10, 12
2) 1, 2, 3, 4, 5, 7, 8, 10, 12
3) 1, 2, 3, 4, 5, 7, 9, 10, 12
4) 1, 2, 3, 4, 5, 7, 9, 11, 12

Найпоширеніші за частотою символи в українській та англійській мовах (по два символи)

1) о, н; e, t
2) о, а; e, i
3) а, т; i, a
4) н, о; t, e

Записати математичні вирази алгоритмів шифрування афінного шифру

1) $E(x) = (ax + S)\text{mod}n$
2) $D(x') = (a'x' + S')\text{mod}n$
3) $E(x) = (ax^2 + S)\text{mod}n$
4) $D(x') = (a'x' - S')\text{mod}n$

Скільки можливих ключів є для алгоритму *DES*?

1) 10^{64}
2) 10^{56}
3) 2^{64}
4) 2^{56}

Записати вираз для знаходження оберненого до e елемента d через функцію Ойлера $\varphi(x)$

1) $ed \equiv 1(\text{mod})\ \varphi(x))$
2) $ed \equiv 0(\text{mod})\ \varphi(x))$
3) $de \equiv 1(\text{mod})\ \varphi(x))$
4) $de \equiv 1(\text{mod})\ \varphi(x))$

Найбільш вживані біграми в українській мові (2 прикл.)

1) ст, на
2) на, ст
3) ст, ан
4) на, ти

Записати перетворення, що назване цифровим підписом

1) $S = M^d \text{mod}n$
2) $S = M^e \text{mod}n$
3) $S = M^{ed} \text{mod}n$
4) $S = M^{de} \text{mod}n$

Записати вираз для цифрового підпису при застосуванні хеш-функцій h(M)

1) $S=[h(M)]^e \text{ mod}n$
2) $S=[h(M)]^d \text{ mod}n$
3) $S=[h(M)]^{ed} \text{ mod}n$
4) $S=[h(M)]^{de} \text{ mod}n$

У схемі організування охоронного телебачення передбачено

1) Наявність пов’язаних між собою кількох камер
2) Виведення зображень з камер на монітор у приміщенні охорони
3) Наявність охоронного освітлення
4) Одночасну наявність 1, 2, 3

Комбіновані сенсори охоронної сигналізації включають

1) Активний мікрохвильовий та пасивний інфрачервоний принципи виявлення
2) Мікрохвильовий принцип
3) Пасивний інфрачервоний принцип
4) Ультразвуковий та ін.

Пожежні повідомлювачі

1) Іонізаційні димові
2) Термомаксимальні
3) Термодиференційні
4) Можливі 1, 2, 3

Шифр одноразового блокнота

1) Блочного типу
2) У цифровому поданні інформації
3) Ні 1, ні 2
4) Блочного типу з цифровим поданням інформації

Вибрати вірно алгоритми криптування шифру одноразового блокнота

1) $C=M+K$
2) $C=M \oplus K$
3) $C=M-K$
4) $C=M \theta K$

Вибрати алгоритм дешифрування системи одноразового блокнота

1) $M=C+K$
2) $M=C \oplus K$
3) $M=C-K$
4) $M=C \theta K$

Записати алгоритм Евкліда

1) $HCD(ab)=HCD(b,\ a \bmod b)$
2) $HCD(ab)=HCD(b,\ a)$
3) $HCD(ab)=HCD(b \bmod a,\ a \bmod b)$
4) $HCD(ab)=HCD(a \bmod b,\ b \bmod a)$

Конгруенція двох величин X та Y означає

1) $X \equiv Y$
2) $X \bmod n = Y \bmod n$
3) $Y=X+hn$
4) $Y=X$

Те, що два числа a і b взаємно прості, означає

1) $a \bmod b=0$
2) $HCD(a,b)=0$
3) $HCD(a,b)=1$
4) $HCD(a,b)=a$

Ефективний захист від вірусів можна забезпечити

1. Профілактикою, застосувавши антивірусні програми з оновленими базами
2. Стиранням електронних листів від невідомих осіб
3. Використанням надійних поштових програм
4. Використавши 1, 2, 3

Типи сучасних криптосистем

1) Симетрична
2) Асиметрична
3) Комбінована

Вказати розмір блоку та розмір ключа SDES

1) 10, 8
2) 8, 10
3) 8, 8
4) 10, 10

Вказати розмір блоку та розмір ключа ГОСТ

1) 64, 128
2) 64, 256
3) 128, 128
4) 128, 256

Розв’язати приклади (4+5)mod7=, (3x5)mod7=

1) 1, 2
2) 2, 1
3) 1, 1
4) 2, 2

Знайти HCD(150, 19)

1) 0
2) 1
3) 19
4) 150

Зашифрувати символ В укр. алфавіту за алгоритмом RSA з ключем (e,n)=(13,77)

1) 40
2) 30
3) 20
4) 10

Охоронні системи телеспостережень складаються з

1) Відеомагнітофона
2) Відеокомутатора
3) Мультиплексора
4) 1+2+3

Метод частотного аналізу придатний для

1) Шифру простої заміни
2) Шифру зсуву
3) Шифру перестановки
4) Для всіх шифросистем

Як застосувати метод частотного аналізу для криптоаналізу шифру Віженера?

1) Традиційним способом
2) Не застосовують
3) Розбивши криптотекст на підпослідовності
4) Одночасно 1 і 3

Зашифрувати алгоритмом Цезаря символи англ. алфавіту *abcd*

1) *bcde*
2) *cdef*
3) *defg*
4) *efqh*

Що належить до біометричних даних?

1) Частота пульсу
2) Відбитки пальців
3) Динаміка роботи з клавіатурою комп'ютера
4) Всі відповіді правильні

Як забезпечити анонімність свого комп'ютера для web-вузла?

1) Неможливо
2) За допомогою проксісервера
3) Видаленням з web-вузла інформації
4) За допомогою спеціальної програми

Інфрачервоний датчик руху є

1) Активним
2) Пасивним
3) Комбінованим
4) Жодна попередня відповідь неправильна

Який алгоритм захисту застосовують у системі Skype?

1) DES
2) 3DES
3) AES
4) Всі алгоритми

ПРЕДМЕТНИЙ ПОКАЖЧИК

Навчальне видання

МОНАСТИРСЬКИЙ ЛЮБОМИР СТЕПАНОВИЧ

СИСТЕМИ І МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

Навчальний посібник

Редактор *Л. Макітринська*
Коректор *І. Пірожик*
Технічний редактор *С. Сеник*
Комп'ютерне верстання *Г. Сметана*

Формат 60×90/16. Умовн. друк. арк. 10.6. Тираж 100 прим. Зам. .

Видавець та виготовлювач:
Львівський національний університет імені Івана Франка.
вул. Університетська,1, м. Львів 79000

Свідоцтво
про внесення суб'єкта видавничої справи до Державного реєстру
видавців, виготівників і розповсюджувачів видавничої продукції.
Серія ДК №3059 від 13.12.2007 р.