МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

Методичні рекомендації щодо написання курсових проєктів для студентів спеціальності 125 "Кібербезпека" першого (бакалаврського) рівня

Укладачі: Євсеєв С. П.
Король О. Г.
Гаврилова А. А.
Коц Г. П.

Відповідальний за випуск Євсеєв С. П.

Харків
ХНЕУ ім. С. Кузнеця
2020

УДК 004.056.5(07.034)
М 54

Укладачі: С. П. Євсеєв
О. Г. Король
А. А. Гаврилова
Г. П. Коц

Затверджено на засіданні кафедри кібербезпеки та інформаційних технологій.
Протокол № 2 від 13.09.2019 р.

Самостійне електронне текстове мережеве видання

М 54 **Методичні** рекомендації щодо написання курсових проєктів для студентів зі спеціальності 125 "Кібербезпека" першого (бакалаврського) рівня / уклад. С. П. Євсеєв, О. Г. Король, А. А. Гаврилова, Г. П. Коц. – Харків : ХНЕУ ім. С. Кузнеця, 2020. – 85 с.

Надано структуру та рекомендації щодо виконання курсових проєктів із технічного захисту інформації, інформаційних систем та інтернет-технологій студентами факультету економічної інформатики на базі матеріалу з вивчення навчальних дисциплін "Основи технічного захисту інформації" й "Інформаційних систем та інтернет-технологій", а також сучасних національних і міждержавних стандартів.

Рекомендовано для студентів 2-го року навчання (термін навчання 1 рік 10 місяців) та II курсу першого (бакалаврського) рівня вищої освіти спеціальності 125 "Кібербезпека".

УДК 004.056.5(07.034)
М 54

Вступ

Проблема захисту комп'ютерних мереж від несанкціонованого доступу набула в останнє десятиліття особливої гостроти. Бурхливе зростання комунікаційних і обчислювальних технологій дозволяє будувати мережі розподіленої архітектури, що об'єднують велику кількість сегментів, розміщених на значній відстані один від одного. Це викликає збільшення кількості вузлів мереж і різних ліній зв'язку між ними, що, своєчергово, підвищує ризик несанкціонованого підключення до мережі й доступу до конфіденційної інформації користувачів комп'ютерних систем і мереж (КСіМ).

Захищати цінні відомості й організовувати роботу контролюючої структури може кожна фізична або юридична особа, залежно від характеру і рівня захисту інформації, відповідно до законів України. Розроблення інженерно-технічної системи й заходів здійснюють після вивчення питання та визначення необхідних заходів щодо збереження інформації. Для цього цінні дані має бути захищено від усіх можливих каналів витоку, несанкціонованого доступу і необережних (ненавмисних) дій персоналу організації. Дані можуть не просто вкрасти, а спотворити шляхом дописування недостовірних відомостей, скопіювати та виставити від свого імені і, що ще гірше, заблокувати доступ до неї. Систему дій і заходів має бути спрямовано на захист не тільки відомостей, а й носія інформації, а також на весь інформаційний процес роботи із секретними даними.

Мету виконання курсових проєктів за означеними навчальними дисциплінами пов'язано, передусім, із необхідністю поєднати теоретичні знання з вирішенням практичних ситуацій у сфері кіберзахисту мережі Інтернет.

Перелік завдань подаснояк розділи кожного виду проєкту.

Об'єкт дослідження за проєктами – це інформаційні системи, інтернет-технології та підсистема технічного захисту інформації.

Предметом дослідження є комплексна система захисту інформації об'єкта, пов'язана з діяльністю об'єкта, його форми власності, внутрішніх процесів, розмірів і т. ін.

Вихідними даними для курсового проєктування слугує деякий варіант завдання, що відображає характеристики досліджуваного об'єкта. Оформлення роботи робити згідно з [2].

Розділ 1
Курсовий проєкт із технічного захисту інформації

Структура змісту

№ п/п	Назва розділів та підрозділів	Орієнтовна кількість сторінок
ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ		1
ВСТУП		2
1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ЗА ТЕМОЮ <НАЗВА ТЕМИ>		10
1.1.	Коротка характеристика об'єкта захисту <назва об'єкта захисту> та аналіз захищеності його інформації від несанкціонованого втручання	
1.2.	Інформація підприємства, що підлягає захисту	
1.3.	Розроблення схеми інформаційних потоків на підприємстві	
2. АНАЛІЗ ІСНУЮЧОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В <НАЗВА ОБ'ЄКТУ ЗАХИСТУ>		15
2.1.	Побудова моделі загроз	
2.2.	Побудова моделі порушника	
2.3.	Опис системи захисту інформації в <назва об'єкта захисту>	
2.4.	Інженерно-технічні, апаратні та програмні засоби захисту інформації в <назва об'єкта захисту>	
3. ПРОВЕДЕННЯ РОЗРАХУНКІВ, НЕОБХІДНИХ ДЛЯ ПЕРЕДАВАННЯ / ОТРИМАННЯ ІНФОРМАЦІЇ ЗАСОБАМИ ТЕЛЕКОМУНІКАЦІЙ		15
3.1.	Використання шифру Цезаря	
3.2.	Алгоритм шифрування ДСТУ 28147-89	
3.3.	Алгоритм шифрування RSA	
3.4.	Функція гешування	
3.5.	Електронний цифровий підпис	
ВИСНОВКИ		1
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ		2
ДОДАТКИ		

1. Аналіз предметної області за темою <назва теми>

Метою розділу 1 є здійснення детального аналізу сфери діяльності об’єкта захисту (підприємства/організації/закладу) та виникнення можливих проблем із захисту інформації у процесі використання сучасних інтернет-технологій під час ведення бізнесу.

1.1. Коротка характеристика об'єкта захисту <назва об'єкта захисту> та аналіз захищеності його інформації від несанкціонованого втручання

Необхідно коротко описати напрями діяльності об'єкта захисту (підприємства, організації, закладу); визначити проблеми із захистом інформації, що мають/можуть мати місце у процесі використання сучасних технологій обробки даних; які заходи із захисту інформації може бути застосовано та підрозділ, якому делеговано ці функції; розробити схему інформаційних уразливостей організаційної структури управління підприємством.

1.2. Інформація <назва об'єкта захисту>, що підлягає захисту

Необхідно перелічити за підрозділами об’єкта назви документів на паперових та електронних носіях, що підлягають захисту (табл. 1.1).

Таблиця 1.1

Перелік документів, що підлягають захисту

№ п/п	Підрозділи	Назви документів	Типи документів (паперовий, електронний)	Категорія таємності

1.3. Розроблення схеми інформаційних потоків у <назва предметної області>

Необхідно зробити аналіз структури та захисту інформаційних потоків із врахуванням таких положень.

1.3.1 Аналіз структурно-функціональних задач відокремлених підрозділів і систем

Загальний аналіз структурно-функціональних задач відокремлених підрозділів і систем із погляду захисту інформаційних потоків за кожною задачею, наведено в табл. 1.2.

Таблиця 1.2

Структура та захист інформаційних потоків <об'єкта інформаційного захисту>

Назви підрозділів	Склад інформаційних потоків	Ступінь захищеності

1.3.2 Аналіз криптографічних методів захисту і шифрування

Необхідно зробити порівняльний аналіз криптографічних методів захисту та шифрування інформації з наведенням критеріїв, за якими проводять дослідження. Результати навести в табл. 1.3.

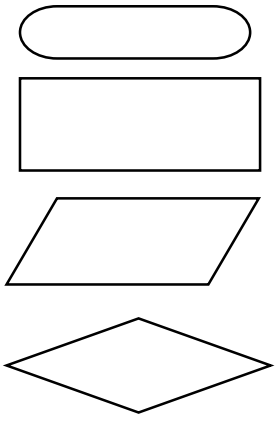
Таблиця 1.3

Результати аналізу сучасних криптографічних методів захисту і шифрування інформації

Критерії	<Назва методу захисту інформації>	<Назва методу шифрування інформації>

1.3.3 Побудова алгоритмічної схеми системи захисту інформації в окремих потоках даних

Під час побудови схеми необхідно використовувати логіку здійснення аналізу за допомогою таких символів:



– початок та закінчення процесу;

– обчислювальна дія або послідовність дій;

– уведення-виведення в загальному вигляді;

– перевірка умови.

Під час здійснення аналізу необхідно отримати свій варіант у викладача та виконати роботу за відповідною темою (табл. 1.4).

Таблиця 1.4

Перелік завдань розділу за варіантами

№ варі-анта	Назви тем
1	Захист банківських ресурсів в автоматизованій банківській системі (АБС)
2	Захист інформації в корпоративних мережах
3	Захист інформації у віртуальних приватних мережах
4	Забезпечення захисту передавання даних за допомогою інтернет-протоколів
5	Захист фінансової інформації в системі Казначейства
6	Захист інформації від несанкціонованого доступу
7	Захист інформації в інформаційно-телекомунікаційних системах
8	Захист інформації в автоматизованих системах
9	Захист інформації в комп'ютерних системах та мережах
10	Захист інформації в аналітичних системах
11	Захист інформації в системах електронного урядування
12	Захист інформації в системах електронного документообігу
13	Захист інформації в системах мобільного зв’язку
14	Захист інформації в системах електронної пошти
15	Системи захисту «розумного будинку»
16	Захист інформації в локальних мережах
17	Захист інформації в системах комунального сервісу

2. Аналіз наявної системи захисту інформації в <назва об'єкту захисту>

Метою розділу 2 є здійснення детального аналізу загроз інформаційній безпеці об'єкта захисту та розроблення моделей загроз і порушника з описом системи захисту інформації, інженерно-технічних, апаратних та програмних засобів.

2.1. Побудова моделі загроз

Перелік загроз інформаційній безпеці необхідно розглянути за цільовою ознакою класифікації та описом складових інформаційних потоків, критичних до модифікування. Для системи визначити перелік класів загроз (якості моделі) за: 1) природою виникнення; 2) ступенем навмисності; 3) безпосереднім джерелом загроз; 4) станом джерела загроз; 5) мірою залежності від активності інформаційної системи (ІС); 6) мірою впливу на ІС; 7) етапами доступу користувачів або програм до ресурсів ІС; 8) способом доступу до ресурсів ІС; 9) поточним місцем розміщення інформації, що зберігають і обробляють в ІС. Розглядаючи питання захисту ІС, доцільно використовувати чотирирівневу градацію доступу до ін-

формації, що зберігають, обробляють та залишають в ІС: 1) рівень носіїв інформації; 2) рівень засобів взаємодії з носіями; 3) рівень подання інформації; 4) рівень змісту інформації.

2.2. Побудова моделі порушника

З урахуванням технології обробки інформації та побудови моделі загроз інформації необхідно розробляти модель порушника, яка має бути адекватною реальному порушнику для певної ІС.

Модель порушника має визначати: 1) можливу мету порушника та її градацію за ступенем небезпеки для ІС; 2) категорії осіб, із яких може бути порушник; 3) можлива кваліфікація порушника; 4) можливий характер його дій.

2.3. Опис системи захисту інформації в <назва об'єкта захисту>

2.3.1 Аналіз теоретичних визначень сутності та структури систем захисту інформації у відповідних системах

Для цього необхідно зробити аналіз теоретичних визначень сутності та структури систем захисту інформації у відповідних системах:

законодавчого поля функціонування систем захисту інформації у відповідних системах в Україні;

наявних теоретико-практичних розробок зі створення системи захисту інформації у відповідних системах;

методики комплексного оцінювання профілів захищеності інформації у відповідних системах.

2.4. Інженерно-технічні, апаратні та програмні засоби захисту інформації в <назва об'єкта захисту>

2.4.1 Описати склад фізичних об'єктів, механічних, електричних та електронних пристроїв, елементів конструкцій будівель, засобів пожежогасіння та інших засобів, що забезпечують на об'єкті захисту:

захист території та приміщень від проникнення порушників;

захист апаратних засобів і носіїв інформації від розкрадання;

запобігання можливості віддаленого (із-за меж території, що охороняють) відеоспостереження (підслуховування) за роботою персоналу і функціонуванням технічних засобів;

запобігання можливості перехоплення побічних електромагнітних випромінювань і наведень (ПЕМВН), викликаних працюючими технічними засобами і лініями передавання даних;

організацію доступу у приміщення співробітників;

контроль над режимом роботи персоналу;

контроль над переміщенням співробітників у різних виробничих зонах;

протипожежний захист приміщень;

мінімізацію матеріальних збитків від утрат інформації, що виникли в результаті стихійних лих і техногенних аварій.

2.4.2 Опис апаратних пристроїв, а саме:

пристроїв для введення інформації, що ідентифікує користувача (магнітних і пластикових карт, відбитків пальців і т. ін.);

пристроїв для шифрування інформації;

пристроїв для перешкоджання несанкціонованому вмиканню робочих станцій і серверів (електронні замки та блокатори).

2.4.3. Програмні засоби захисту інформації

Основні програмні засобі захисту інформації такі:

програми ідентифікації й автентифікації користувачів корпоративної мережі;

програми розмежування доступу користувачів до ресурсів корпоративної мережі;

програми шифрування інформації;

програми захисту інформаційних ресурсів (системного і прикладного програмного забезпечення, баз даних, комп'ютерних засобів навчання і т.ін.) від несанкціонованої зміни, використання та копіювання.

Допоміжні програмні засоби захисту інформації такі:

програми знищення залишкової інформації (у блоках оперативної пам'яті, тимчасових файлах і т.ін.);

програми аудиту (ведення реєстраційних журналів) подій, пов'язаних із безпекою корпоративної мережі, для забезпечення можливості відновлення і доведення факту існування цих подій;

програми імітації роботи з порушником (відволікання його на отримання нібито конфіденційної інформації);

програми тестового контролю за захищеністю корпоративної мережі та ін.

3. Виконання розрахунків, необхідних для передавання / отримання інформації засобами телекомунікацій

Метою розділу 3 є виконання розрахунків за п'ятьма завданнями, пов'язаними із шифруванням, гешуванням та формуванням електронного цифрового підпису (ЕЦП).

Завдання 1. Шифр Цезаря

Використовуючи шифр Цезаря, зашифруйте свої дані: прізвище, ім'я, по батькові.

Завдання 2. Алгоритм шифрування ДСТУ 28147-89

Виконайте перший цикл алгоритму шифрування ДСТУ 28147 89 в режимі простої заміни. Для отримання 64 бітів вихідного тексту використовуйте 8 перших букв зі своїх даних: прізвища, імені, по батькові. Для отримання ключа (256 бітів) використовують текст, що складається із 32 букв. Перший підключ містить перші 4 букви.

Завдання 3. Алгоритм шифрування RSA

Згенеруйте відкритий і закритий ключі в алгоритмі шифрування RSA, вибравши прості числа p і q із першої сотні. Зашифруйте повідомлення, що складається з ваших даних: прізвища, імені, по батькові.

Завдання 4. Функція гешування.

Знайти геш-образ свого прізвища, використовуючи геш-функцію $H_i = (H_{i-1} + M_i)^2 \bmod n$, де $n = p \cdot q$, p, q узяти з завдання 3.

Завдання 5. Електронна цифрова підпис.

Використовуючи геш-образ свого прізвища, обчисліть електронний цифровий підпис за схемою RSA.

Приклади виконання завдань

Завдання 1. Шифр Цезаря. Використовуючи шифр Цезаря, зашифруйте свої дані: прізвище, ім'я, по батькові.

Початковий текст:

«КОЗИНА ГАЛИНА ЛЕОНИДОВНА»

Використовують алфавіт, що містить 33 літери та пробіл, що стоїть після букви Я:

АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ*пробіл*

Ключем у шифрі Цезаря є число 3. Кожну букву в початковому тексті зсувають за алфавітом на 3 позиції. Таким чином, знаходять:

Початковий текст	КОЗИНА		ГАЛИНА		ЛЕОНИДОВНА
Зашифрований текст	НСКЛРГ	В	ЁГОЛРГ	В	ОЗСРЛЖСЕРГ

Завдання 2. Алгоритм шифрування ДСТУ 28147-89. Виконайте перший цикл алгоритму шифрування ДСТУ 28147-89 в режимі простої заміни. Для отримання 64 бітів вихідного тексту використовуйте 8 перших букв зі своїх даних: прізвища, імені, по батькові. Для отримання ключа (256 бітів) використовують текст, що складається із 32 букв. Перший підключ містить перші 4 букви.

Вихідні дані для зашифрування: КОЗИНА Г

Для ключа візьміть послідовність, що складається із 32 букв:

АЛИНа пошла в лес собирать грибы

Для першого підключа *X* використовують перші 4 букви ключа: АЛИН.

Переведіть вихідний текст і перше з'єднання у двійкову послідовність (додаток А):

початковий текст

К	11001010
О	11001110
З	11000111
И	11001000
Н	11001101
А	11000000
пробіл	00100000
Г	11000011

перший підключ X0

А	11000000
Л	11001011
И	11001000
Н	11001101

Таким чином, перші 64 біти визначають вхідну послідовність

L0: 11001010 11001110 11000111 11001000

R0: 11001101 11000000 00100000 11000011

наступні 32 біти визначають перший підключ
X0: 11000000 11001011 11001000 11001101

I. Знайдіть значення функції перетворення *f(R0,X0)* (додаток Б):
1) обчислення суми *R0* та *X0* за *mod* 2^{32}

R0: 1100 1101 1100 0000 0010 0000 1100 0011
X0: 1100 0000 1100 1011 1100 1000 1100 1101

1000 1110 1000 1011 1110 1001 1001 0000

2) перетворення у блоці підстановки
Результат підсумовування *R0+X0* за *mod* 2^{32}
1000 1110 1000 1011 1110 1001 1001 0000
перетворіть у блоці підстановки (додаток В). Для кожного 4-бітного блоку обчисліть його адресу в таблиці підстановки. Номер блоку відповідає номеру стовпчика, десяткове значення блоку відповідає номеру рядка в таблиці. Таким чином, 5-й блок (1011) замінюють заповненням 11-го рядка і п'ятого стовпчика в таблиці підстановки (1110):

номери блоків
8 7 6 5 4 3 2 1
1000 1110 1000 1011 1110 1001 1001 0000
відповідні номери рядків у таблиці підстановки
8 14 8 11 14 9 9 0
заповнення
9 2 3 14 5 15 3 4
результат
1001 0010 0011 1110 0101 1111 0011 0100

3) циклічний зсув результату п. 2 на 11 бітів уліво
1111 0010 1111 1001 1010 0100 1001 0001
Таким чином, знайшли значення функції *f (R0,X0)*:
1111 0010 1111 1001 1010 0100 1001 0001

II. Обчисліть *R1= f(R0,X0)* $\oplus$ *L0*.
Результат перетворення функції f(R0,X0) додайте з L0 за mod2:
L0: 1100 1010 1100 1110 1100 0111 1100 1000
f(R0,X0): 1111 0010 1111 1001 1010 0100 1001 0001

R1: 0011 1000 0011 0111 0110 0011 0101 1001

Завдання 3. Алгоритм шифрування RSA. Згенеруйте відкритий і закритий ключі в алгоритмі шифрування RSA, вибравши прості числа *p* і

q із першої сотні. Зашифруйте повідомлення, що складається з ваших даних: прізвища, імені, по батькові.

I. Генерація ключів (додаток Г).

Виберіть два простих числа ***p* = 13 та *q* = 19** (додаток Д).

Тоді модуль $n = p \cdot q = 13 \cdot 19 = 247$ і функція Ейлера $\varphi(n) = (p - 1) \cdot (q - 1) = 12 \cdot 18 = 216$.

Закритий ключ *d* виберіть з умов $d < \varphi(n)$ і *d* взаємно прості з $\varphi(n)$, тобто *d* і $\varphi(n)$ не мають загальних дільників.

Нехай $d = 25$.

Відкритий ключ *e* обираємо з умов $e < \varphi(n)$ і $de = 1 (\mathrm{mod}\ \varphi(n))$:

$$e < 216,\ 25e = 1 (\mathrm{mod}\ 216).$$

Остання умова означає, що число $25e - 1$ має ділитися на 216 без остачі.

Таким чином, для визначення *e* треба підібрати таке число *k*, що $25e - 1 = 216k$.

За $k = 14$ отримуємо $25e = 3024 + 1$ чи $e = 121$.

У нашому прикладі (121, 247) – відкритий ключ, (25, 247) – секретний ключ.

II. Шифрування.

Наведіть повідомлення, що шифруються «КГЛ» як послідовність цілих чисел. Нехай буква «К» відповідає числу 12, буква «Г» – числу 4 та буква «Л» – числу 13.

Зашифруйте повідомлення, використовуючи відкритий ключ (121, 247):

$C_1 = (12^{121}) \bmod 247 = 12$

$C_2 = (4^{121}) \bmod 247 = 199$

$C_3 = (13^{121}) \bmod 247 = 91$

Таким чином, вихідному повідомленню (12, 4, 13) відповідає криптограма (12, 199, 91).

IV. Розшифрування.

Розшифруйте повідомлення (12, 199, 91), користуючись секретним ключем (25, 247):

$M_1 = (12^{25}) \bmod 247 = 12$

$M_2 = (199^{25}) \bmod 247 = 4$

$M_3 = (91^{25}) \bmod 247 = 13$

У результаті розшифрування було знайдено початкове повідомлення (12, 4, 13), тобто «КГЛ».

Примітка.

1. Числа *a* та *b* можна порівняти за *mod n*, якщо їхня різниця ділиться на *n*:

$$a = b(\text{mod } n) \Leftrightarrow a - b \text{ ділиться на } n.$$

Наприклад, $6 \equiv 2(\text{mod } 4)$, $15 \equiv 3(\text{mod } 6)$, $45 \equiv 1(\text{mod } 22)$.

2. Обчислення можна виконати, використовуючи правила модульної алгебри:

$$a = b(\text{mod} n) \Rightarrow a^k = b^k(\text{mod} n).$$

Для розглянутого прикладу знаходять

$$a = b(\text{mod} n) \Rightarrow ac = bc(\text{mod} n)$$

$$12^3 = 1728 \equiv 246 \text{ mod } 247 = -1 \text{ mod } 247$$

$$12^{120} = \left(12^3\right)^{40} = (-1)^{40} \text{ mod } 247 = 1 \text{ mod } 247$$

$$12^{121} = 12 \text{ mod } 247 = 12$$

$$4^4 = 256 \text{ mod } 247 = 9 \text{ mod } 247$$

$$4^{12} = \left(4^4\right)^3 \text{ mod } 247 = 9^3 \text{ mod } 247 = 729 \text{ mod } 247 = 235 \text{ mod } 247$$

$$4^{60} = \left(4^{12}\right)^5 = 235^5 = 716703146875 = 144 \text{ mod } 247$$

$$4^{120} = \left(4^{60}\right)^2 = 144^2 = 20736 \equiv 235 \text{ mod } 247$$

$$4^{121} = 4 \cdot 4^{120} = 235 \cdot 4 = 940 \equiv 199 \text{ mod } 247 \text{ і т.ін.}$$

Завдання 4. Функція гешування. Знайти геш-образ свого прізвища, використовуючи геш-функцію $H_i = \left(H_{i-1} + M_i\right)^2 \text{mod} n$, де $n = p \cdot q$, p, q узяти із завдання 3.

Повідомлення, що гешують «КОЗИНА». Візьміть два простих числа $p = 13$, $q = 19$ (додаток Е). Визначимо $n = p \cdot q = 13 \cdot 19 = 247$. Вектор ініціалізації H_0 виберіть таким, що дорівнює 8 (вибирайте випадковим чином). Слово «КОЗИНА» можна уявити послідовністю чисел (12, 16, 9, 10, 15, 1) за номерами букв в алфавіті. Таким чином, n = 247, $H_0 = 8$, $M_1 = 12$, $M_2 = 16$, $M_3 = 9$, $M_4 = 10$, $M_5 = 15$, $M_6 = 1$.

Використовуючи формулу $H_i = \left(H_{i-1} + M_i\right)^2 \text{mod} n$, знаходять геш-образ повідомлення «КОЗИНА»:

$H_1 = (H_0 + M_1)^2 \text{ mod } n = (8 + 12)^2 \text{ mod } 247 = 400 \text{ mod } 247 = 153,$

$H_2 = (H_1 + M_2)^2 \text{ mod } n = (153 + 16)^2 \text{ mod } 247 = 28\,561 \text{ mod } 247 = 156,$

$H_3 = (H_2 + M_3)^2 \bmod n = (156 + 9)^2 \bmod 247 = 27\,225 \bmod 247 = 55,$

$H_4 = (H_3 + M_4)^2 \bmod n = (55 + 10)^2 \bmod 247 = 4\,225 \bmod 247 = 26,$

$H_5 = (H_4 + M_5)^2 \bmod n = (26 + 15)^2 \bmod 247 = 1\,681 \bmod 247 = 199,$

$H_6 = (H_5 + M_6)^2 \bmod n = (199 + 1)^2 \bmod 247 = 40\,000 \bmod 247 = 233.$

У підсумку отримуємо геш-образ повідомлення «КОЗИНА», що дорівнює 233.

Завдання 5. Електронний цифровий підпис. Використовуючи геш-образ свого прізвища, обчисліть електронний цифровий підпис за схемою RSA.

Нехай геш-образ прізвища дорівнює 233, а закритий ключ алгоритму RSA – (25, 247). Тоді електронний цифровий підпис повідомлення, що складається із прізвища, обчислюються за правилом (додаток Ж) $s = 233^{25} \bmod 247 = 168$.

Для перевірки ЕЦП, використовуючи відкритий ключ (121, 247), знаходять $H = 168^{121} \bmod 247 = 233$.

Оскільки геш-образ повідомлення збігається зі знайденим значенням H, то підпис визнають справжнім.

Розділ 2
Курсовий проєкт з інформаційних систем та інтернет-технологій

Структура змісту

№ п/п	Назви розділів та підрозділів	Орієнтовна кількість сторінок
ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ		1
ВСТУП		2
1. Побудова моделей порушника й атак на комп'ютерні мережі та системи		20
1.1. Аналіз умов функціонування та сучасних загроз інформації в комп'ютерних мережах і системах		
1.2. Побудова класифікацій криптографічних засобів		
1.3. Побудова моделі порушника безпеки у КміС		
1.4. Побудова моделі реалізації загроз безпеки у КміС		
1.5. Побудова математичної моделі пасивних атак у КміС		
1.6. Побудова моделі активних атак у КміС із блокуванням передавання інформації		
1.7. Побудова моделі активних атак у КміС з внесенням перешкод		
1.8. Побудова моделі активних атак "маскарад" у КміС		
1.9. Побудова та аналіз моделі оцінювання ризику реалізації загроз безпеки комунікаційних систем		
1.10. Оцінювання ризику реалізації загроз у комунікаційних системах		
1.11. Приклад розрахунків ризику інформаційної безпеки у ВПБС		
2. Основні принципи захисту інформації під час підключення до Інтернет		15
2.1. Firewall (Брандмауер)		
2.2. NAT		
2.3. Демілітаризована зона		
2.4. Другий firewall		
2.5. Proxy-сервер		
2.6. Другий mail-сервер		
2.7. Антивірусний захист поштової системи		
2.8. Log-сервер		
3. Виконання завдання		10
3.1. Графічне завдання		
3.2. Розрахункове завдання		
ВИСНОВКИ		2
СПИСОК ЛІТЕРАТУРИ		2
ДОДАТКИ		

1. Побудова моделей порушника й атак на комп'ютерні мережі та системи

1.1. Аналіз умов функціонування та сучасних загроз інформації в комп'ютерних мережах та системах

Аналіз умов функціонування локальних і глобальних обчислювальних систем показав, що головною вимогою, яку висувають до них, є забезпечення користувачам потенційної можливості доступу до розподілюваних ресурсів усіх комп'ютерів, об'єднаних у мережу.

До основних вимог функціонування глобальних обчислювальних систем (ГОС) належать: продуктивність, надійність, сумісність, керованість, захищеність, розширюваність і масштабованість. Основні вимоги та їхні складові наведено на рис. 1.1.

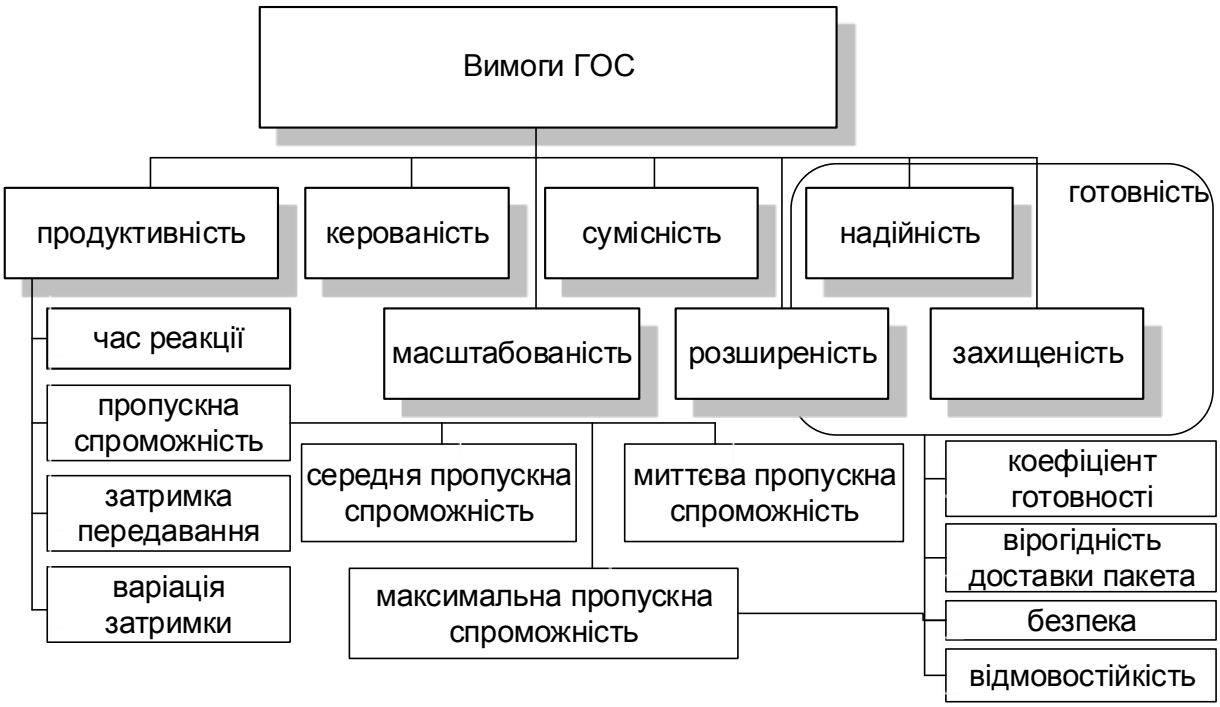


Рис. 1.1. **Вимоги, які висувають до обчислювальних мереж та систем**

Нині для оцінювання функціонування локальних обчислювальних систем (ЛОС) і ГОС уведене поняття «якість обслуговування» (Quality of Service, Qps) комп'ютерної мережі, що містить тільки дві найважливіші характеристики – продуктивність і надійність.

Зроблений аналіз показника якості обслуговування мережі визначає два підходи до його забезпечення.

Перший підхід полягає в гарантованому забезпеченні користувачеві дотримання деякої числової величини показника якості обслуговування (забезпечення встановленого показника середньої пропускної спроможності, показника часу затримки передавання та ін.). Так, наприклад, технології Frame Relay і ATM дозволяють будувати мережі, що гарантують якість обслуговування за продуктивністю (показники середньої пропускної спроможності, часу реакції, часу затримки та ін.).

Другий підхід полягає у пріоритетному обслуговуванні користувачів відповідно до встановленої ієрархії мережі. Таким чином, якість обслуговування залежить від ступеня привілейованості користувача або групи користувачів, до якої він належить. Для уповноважених користувачів ГОС якість обслуговування не гарантовано, а гарантовано тільки рівень їхніх привілеїв. Таке обслуговування називаються обслуговуванням best effort – із найбільшим старанням. Зроблений аналіз функціонування локальних мереж показує, що за таким принципом працюють ЛОС, побудовані на комутаторах із пріоритетом кадрів.

Для забезпечення необхідного показника якості обслуговування ГОС необхідно забезпечити продуктивність і надійність. Під **продуктивністю** розуміють властивість, що забезпечує можливість розпаралелювання робіт між декількома комп'ютерами мережі.

Основними характеристиками продуктивності є час реакції, пропускна спроможність, затримка передавання та її варіація.

Час реакції є інтегральною характеристикою продуктивності мережі, що визначаються як інтервал часу між виникненням запиту користувача до якої-небудь мережевої служби й отриманням відповіді на цей запит.

Зроблений аналіз цього показника свідчить, що його значення залежить тільки від типу служби, до якої звертається користувач, статусу користувача в мережі, типу сервера, а також від поточного стану елементів ГОС – завантаженості сегментів, комутаторів і маршрутизаторів, через які проходить запит, завантаженості сервера та ін.

Час реакції мережі розподіляють на час підготовки запитів на клієнтському комп'ютері, час передавання запитів між клієнтом і сервером через комунікаційне устаткування, час опрацювання запитів на сервері, час передачі відповідей від сервера клієнту та час обробки отримуваних від сервера відповідей на клієнтському комп'ютері.

Для визначення обсягу переданих даних за одиницю часу використовують пропускну спроможність та її похідні (миттєва, максимальна і середня пропускні здатності).

Водночас середню пропускну здатність визначають як співвідношення загального обсягу переданих даних до часу їхнього передавання за тривалий проміжок часу (доба, місяць, рік), миттєву пропускну здатність визначають за дуже маленький проміжок часу (від 0,1 до 10^{-3} с) і максимальну пропускну здатність визначають як найбільшу миттєву пропускну здатність, зафіксовану протягом періоду спостереження.

Аналіз функціонування ГОС показує, що для проєктування, настроювання й оптимізації використовують такі показники, як середня й максимальна пропускні здатності. Для визначення якості мережі загалом, не диференціюючи його за окремими сегментами або обладнаннями, використовують загальну пропускну здатність мережі, яку визначають як середню кількість інформації, передану між усіма вузлами мережі за одиницю часу. Для визначення якості мережі так само використовують кількісний показник максимальної затримки передавання її та варіації.

Затримку передавання визначають як час знаходження пакета в будь-якому мережному обладнанні або частині мережі. Цей параметр продуктивності за змістом близький до реакції мережі, але відрізняється тим, що завжди характеризує тільки мережні етапи обробки даних, без затримок обробки комп'ютерами ЛОС.

Зроблений аналіз створення розподілених систем і експлуатації ЛОС і ГОС показує, що для забезпечення їхної надійності застосовують характеристики складних систем: готовність або коефіцієнт готовності, що означає проміжок часу, протягом якого систему може бути використано; вірогідність даних, тобто захист їх від викривлень; погодженість (несуперечність) та їхню ідентичність.

Для опису передавання пакетів між кінцевими вузлами використовують імовірнісні характеристики каналу зв'язку: імовірність доставляння пакета вузлу призначення без викривлень, імовірність утрати пакета (за кожною із причин – переповнення буфера маршрутизатора, через розбіжність контрольної суми, відсутність працездатного шляху до вузла призначення і т. ін.), імовірність викривлення окремого біта переданих даних.

До показника загальної надійності входить безпека – це здатність системи захистити дані від несанкціонованого доступу, і відмовостійкість – здатність системи сховати від користувача її окремі елементи.

Під час проєктування і модернізації ЛОС ураховують додаткові вимоги до обчислювальних мереж:

Розширюваність (extensibility) – це можливість порівняно легкого додавання окремих елементів мережі (користувачів, комп'ютерів, додатків, служб), нарощування довжини сегментів мережі та заміни наявної апаратури могутнішою.

Масштабованість (scalability) – це можливість мережі нарощувати кількість вузлів і довжину зв'язків у дуже широких межах, водночас зберігати показник продуктивності мережі.

Прозорість (transparency) – це можливість роботи з вилученими ресурсами з використанням тих же команд і процедур, що й для роботи з локальними ресурсами.

Комп'ютерні мережі споконвічно призначено для спільного доступу користувача до ресурсів комп'ютерів: файлів, принтерів і т. ін.

Зроблений аналіз працездатності ЛОС (ГОС) показує, що особливу складність становлять сполучення в одній мережі традиційного комп'ютерного та мультимедійного трафіка. Для обліку складеного трафіка використовують такі додаткові параметри мережі:

Керованість – це можливість централізовано контролювати стан основних елементів мережі, виявляти та вирішувати проблеми, що виникають під час роботи мережі, виконувати аналіз продуктивності та планувати розвиток мережі.

Планування – це можливість прогнозування змін вимог користувачів до мережі, застосування нових додатків і мережних технологій.

*Сумісність або інтегрован*ість – це можливість додавання в ЛОС (ГОС) найрізноманітнішого програмного й апаратного забезпечення (різні операційні системи, що підтримують різні стеки комунікаційних протоколів, апаратні засоби й додатки від різних виробників).

Таким чином, аналіз основних вимог, які висувають до ЛОС і ГОС, показує, що для виконання головного завдання забезпечення користувачам потенційної можливості доступу до розподілюваних ресурсів усіх комп'ютерів, об'єднаних у мережу, необхідно виконати вимоги двох основних характеристик показника якості обслуговування – продуктивності та надійності.

Для оцінювання надійності мережі використовують основні характеристики складних систем: коефіцієнт готовності – проміжок часу, протягом якого система може бути використана; безпека – здатність системи захис-

тити дані від несанкціонованого доступу і відмовостійкість – здатність системи працювати в умовах відмови деяких її елементів.

Проблема захисту комп'ютерних мереж від несанкціонованого доступу набула особливої гостроти.

Розвиток комунікаційних технологій дозволяє будувати мережі розподіленої архітектури, що поєднують велику кількість сегментів, розташованих на значній відстані один від одного. Усе це викликає збільшення кількості вузлів мереж і різних ліній зв'язку між ними, що, своєю чергою, підвищує ризик несанкціонованого підключення до мережі й доступу до важливої інформації.

Збільшення обсягів оброблюваних і переданих даних у комп'ютерних системах і мережах, насамперед, у банківських системах, системах управління великими фінансовими та промисловими організаціями, підприємствами енергетичного сектору, транспорту нових підходів до побудови протоколів і механізмів забезпечення безпеки інформаційних систем.

Природня вимога до безпеки та вірогідності оброблюваної й переданої інформації в таких системах постає дуже гостро, оскільки відмова системи або вихід за встановлені обмеження зазначених властивостей може призвести до значних фінансових і матеріальних утрат, збитку екології, життя та здоров'я людей.

Аналіз показує, що за останній час загальний обсяг опрацьованої й переданої інформації в комп'ютерних системах і мережах збільшився в декілька разів (на два – три порядки кожні п'ять – десять років) і загальні тенденції свідчать, що така динаміка збереглася.

Сучасні криптографічні засоби захисту інформації мають забезпечувати своєчасне оброблення величезних обсягів даних (десятки – сотні Мбіт/с) і задовольняти твердим вимогам до вірогідності та безпеки інформації.

Крім того, сучасний розвиток інформаційних технологій, високий рівень комп'ютеризації й інформатизації сучасного суспільства обумовили виникнення нових загроз безпеці інформації.

1.2. Побудова класифікацій криптографічних засобів

У процесі розробленняпідходів до аналізу криптографічної захищеності інформаційної системи необхідно враховувати, яких загроз зазнає система з боку противників. Розроблені класифікації дозволяють визначити залежність атак, яких може зазнати криптосистема, від галузі її використання.

Класифікація криптографічних засобів

Існує кілька способів, відповідно до яких можуть класифікуватися криптографічні системи. Розроблена класифікація дозволяє визначити схильність криптосистеми до різних атак з боку противника, ідентифікуючи її відповідно до особливостей її реалізації. Пропонується розрізнити криптографічні засоби за критеріями, які наведені на рис. 1.2.

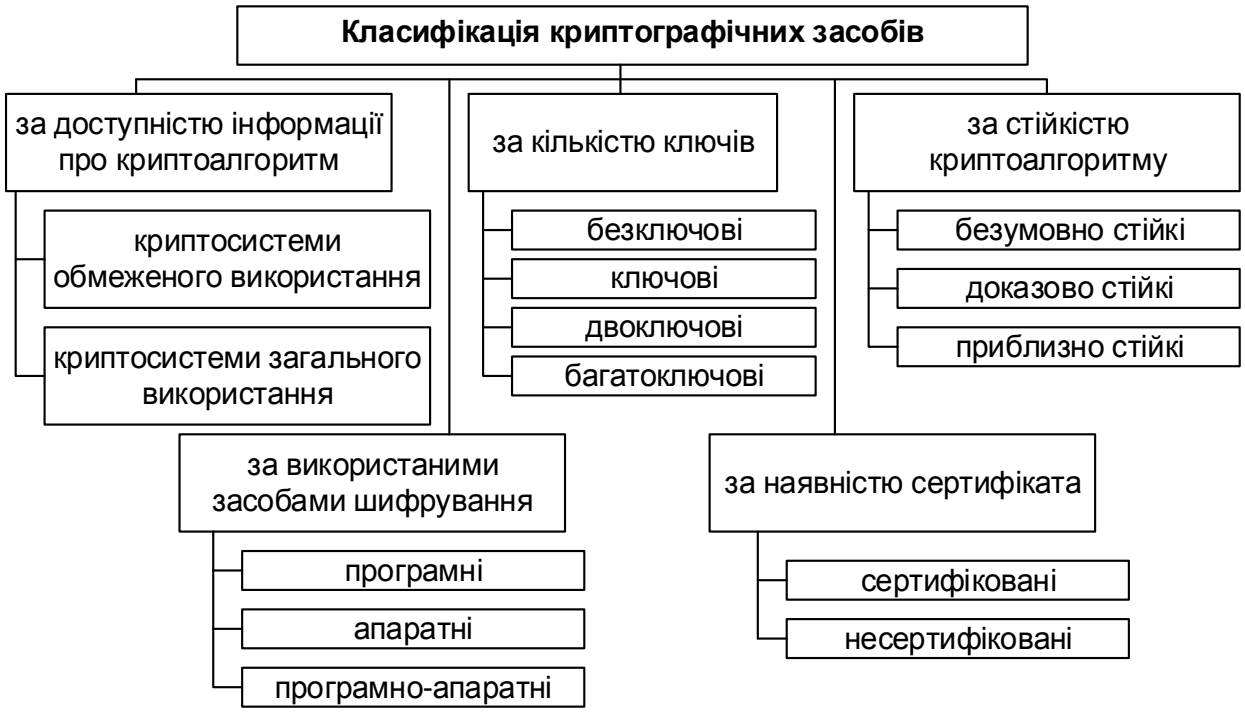


Рис. 1 2. **Класифікація криптографічних засобів**

Класифікація за доступністю інформації про криптоалгоритм

Запропоновано таку класифікацію криптосистем:

криптосистеми обмеженого використання;

криптосистеми загального використання.

Криптографічну систему називають **криптосистемою обмеженого використання**, якщо її стійкість ґрунтується на збереженні в секреті самого характеру алгоритмів шифрування й розшифрування. Найпростішим прикладом такої системи можна вважати шифр Цезаря, у якому

перетворення інформації зведено до простої заміни кожного символу відкритого тексту третім, наступним за ним, символом алфавіту.

Стійкість **криптосистеми загального використання** ґрунтується не на секретності алгоритмів шифрування і розшифрування, а на секретності деякого значення, яке називають її ключем. Такий ключ мають виробляти конкретні користувачі таким чином, щоб навіть розроблювач криптосистеми не міг розкрити її, не маючи доступу до ключа. Зберігаючи інформацію про алгоритм у секреті, можна забезпечити деяку додаткову безпеку. Дослідження надійності таких систем завжди мають проводити із припущеннями, що потенційному противнику відома вся інформація про криптосистему, за винятком використовуваного ключа.

Класифікація за кількістю ключів

За класифікаційною схемою криптосистеми підрозділяють на три типи:

безключові, які не використовують ключі у процесі криптографічних перетворень;

одноключові**,** що використовують у своїх обчисленнях тільки секретний ключ;

двоключові, у яких на різних етапах обчислень застосовують два види ключів: закриті (особисті) та відкриті.

Ця класифікація є неповною, тому що в ній відсутні **багатоключові** криптосистеми. До цього типу можна зарахувати **схеми розподілу секрету**, або *(m, n)*-**граничні схеми**. У такій системі секретний ключ розподіляють на n частин (де n – кількість учасників схеми розподілу секрету) так, що за кожними m частинами можна відновити зашифровану інформацію ($m \le n$). Отримані “частки” ключа розподіляють між усіма учасниками, після чого будь-які m учасників можуть спільно реконструювати зашифровану інформацію. В окремому випадку, якщо $n = m$, для відновлення секрету необхідна присутність усіх учасників.

Класифікація за стійкістю криптоалгоритма

Здатність криптосистеми протистояти атакам криптоаналітика називають *стійкістю*. Кількісно стійкість вимірюють як складність найкращого алгоритму, що приводить криптоаналитика до успіху із прийнятною ймовірністю. Універсальний метод прямого перебору множини всіх можливих ключів дозволяє отримати оцінку зверху для стійкості алгоритму шифрування. Відносний очікуваний *безпечний час* визначають як напівдобуток кількості відкритих ключів і часу, необхідного криптоанали-

тику для того, щоб випробовувати кожний ключ. Залежно від мети й можливостей криптоаналитика, змінюється і стійкість. Розрізняють стійкість ключа (складність розкриття ключа найкращим відомим алгоритмом), стійкість безключового читання, імітостійкість (складність нав'язування неправильної інформації найкращим відомим алгоритмом) і ймовірність нав'язування неправильної інформації. Аналогічно можна розрізняти стійкість власне криптоалгоритму, стійкість протоколу, стійкість алгоритму генерації й поширення ключів.

Залежно від складності зламу, алгоритми забезпечують різні ступені захисту. За основу беруть принципову можливість отримання з перехоплення деякої інформації про відкритий текст або використаний ключ**.** Є безумовно стійкі (або теоретично стійкі)**,** доказово стійкі та приблизно стійкі криптоалгоритми.

Теоретично стійкі системи створюють шифртексти, що містять недостатню кількість інформації для однозначного визначення відповідних їм текстів (або ключів). У найкращому разі відкритий текст може бути локалізований у досить великій підмножині множини всіх відкритих текстів, і його можна лише "угадати" з мізерно малою ймовірністю. Ніякий метод криптоаналізу, включаючи повний перебір ключів, не дозволяє не тільки визначити ключ або відкритий текст, але навіть отримати деяку інформацію про них. Алгоритм безумовно стійкий, якщо відновлення відкритого тексту неможливе за будь-якого обсягу шифртексту, отриманого криптоаналітиком. Безпеку безумовно стійких криптоалгоритмів засновано на доведених теоремах про неможливість розкриття ключа.

Стійкість **доказово стійких** криптоалгоритмів визначено складністю розв'язання добре відомого математичного завдання, яке намагалися розв'язати багато математиків і яке є загальновизнано складним. Як приклад можна навести системи DH (Діффі – Хелмана) і RSA (Рівеста – Шаміра – Адельмана), засновані на складностях дискретного логарифмування й розкладання цілого числа на множники, відповідно. Підвищення стійкості в криптоалгоритмах досягають збільшенням розміру математичного завдання або її заміною, що, пекреважно, тягне ланцюг змін в апаратурі, яку використовують для шифрування.

Приблизно стійкі криптоалгоритми засновано на складності розв'язання приватного математичного завдання, яке не зведено до добре відомих завдань і яку намагалися розв'язати один або кілька чо-

ловік. Прикладами можуть бути блокові шифри. Приблизно стійкі криптоалгоритми характеризуються порівняно малою вивченістю математичних завдань, на яких грунтується їхня стійкість. Однак такі шифри мають велику гнучкість, що дозволяє в разі виявлення слабких місць не відмовлятися від алгоритмів, а їх дороблятим.

Класифікація за використовуваними засобами

Розгляньте цю класифікацію в застосуванні до генераторів псевдовипадкових чисел. Для генерації ключової інформації, призначеної для використання в межах симетричної криптосистеми, використовують такі методи (у порядку зростання якості):

програмна генерація, що припускає обчислення чергового псевдовипадкового числа як функції поточного часу, послідовності символів, уведених користувачем, особливостей його клавіатурного почерку та. ін.;

програмна генерація, заснована на моделюванні якісного псевдовипадкового генератора з рівномірним законом розподілу;

апаратна генерація з використанням якісного псевдовипадкового генератора;

апаратна генерація з використанням генераторів випадкових послідовностей, побудованих на основі фізичних генераторів шуму та якісних псевдовипадкових генераторів.

Кращий спосіб генерації множини випадкових бітів – витяг їх із природно випадкових подій реального світу. Часто такий метод потребує наявності спеціальної апаратури, але можна реалізувати його й на комп'ютерах. Як випадкові величини можна також розглядати інтервали між натисканнями клавіш клавіатури. Головний недолік подібних систем – можливі закономірності в послідовності, яку генерують. Використовувані фізичні процеси можуть бути випадкові, однак використання вимірювальних інструментів може призвести до появи проблем: зсуву, відхилення або кореляції між бітами. Обійти ці недоліки можна, використовуючи не один, а кілька випадкових джерел.

Класифікація за наявністю сертифіката

Відповідно до чинного на території України законодавства, якщо організація використовує **несертифіковані** в Україні криптографічні алгоритми шифрування й електронний цифровий підпис даних, вона не може вести обмін документами з державними установами. Забезпечити юридичну значущість електронних документів під час обміну ними між користувачами дозволить використання **сертифікованих** криптоалгоритмів.

Класифікація криптоаналітичних атак

Наведена на рис. 1.3 класифікація дозволяє розрізняти криптоаналітичні атаки та їхні наслідки одночасно за декількома параметрами.

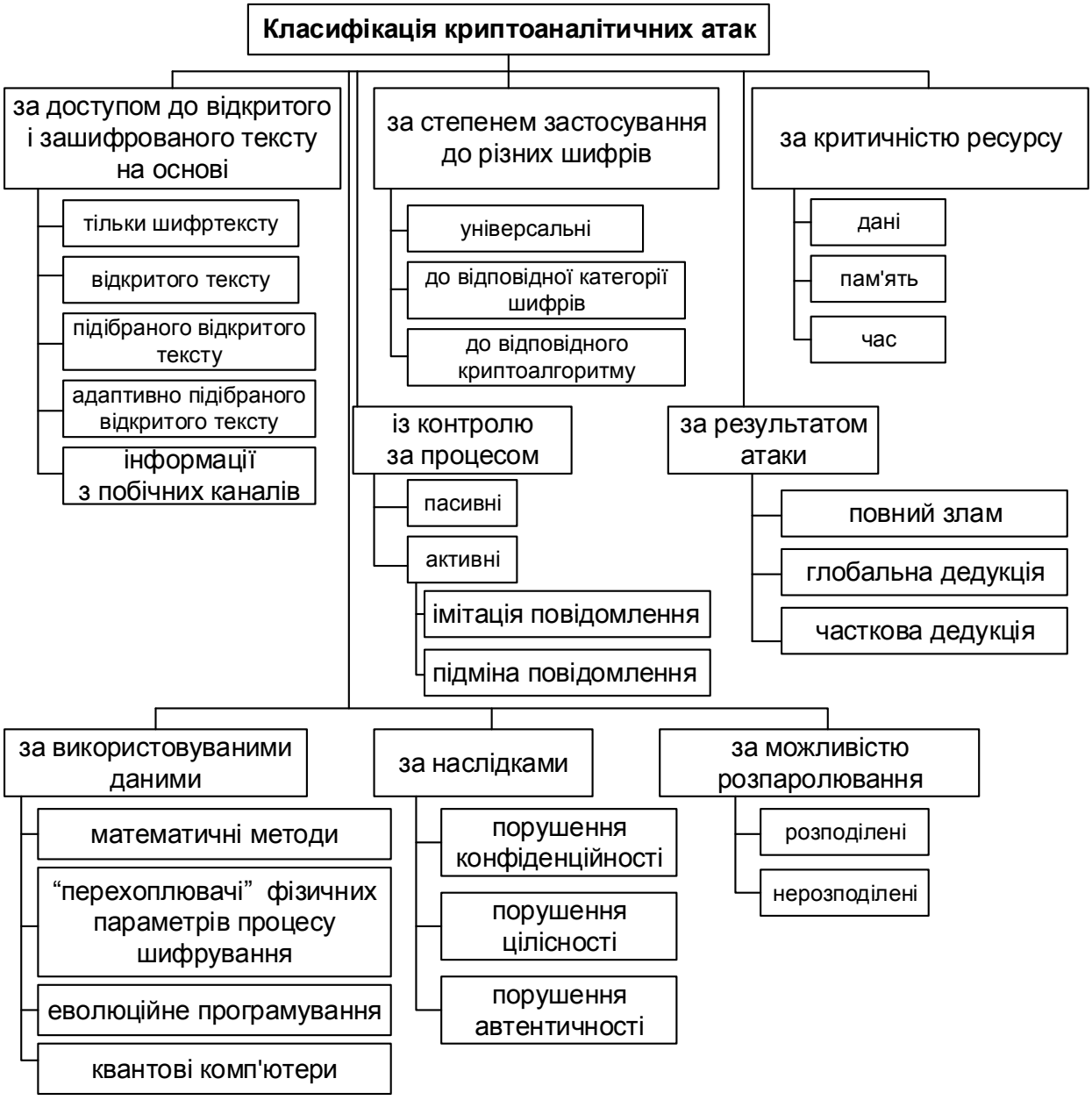


Рис. 1.3. **Класифікація криптографічних атак**

Класифікація з доступу до відкритого й зашифрованого тексту

Перш ніж класифікувати атаки слід увести ряд позначень: відкритий текст будемо позначати буквою M, шифртекст – C (як M може бути будь-яка послідовність бітів: текстовий файл і т. ін.). Нехай для шифрування і розшифрування використовують ключі k і $k^{/}$, відповідно, (у симетричній криптографії $k = k^{/}$); позначають функцію шифрування E_k, розшифрування – D_k.

Тоді виконують співвідношення $E_k(M) = C$, $D_k(C) = M$. Донедавна за критерієм доступу до відкритого і шифрованого тексту виділяли чотири основні типи криптоаналітичних атак. Однак останнім часом одним із найактуальних напрямів криптоаналізу стало здійснення атак, що використовують особливості реалізації та робочого середовища.

Атаки стороннiми або побічними каналами – це вид криптографічних атак, що використовують інформацію, отриману зі сторонніх або побічних каналів. У кожному разі передбачено, згідно з фундаментальним допущенням Кірхгофа, що криптоаналітик знає використовуваний алгоритм шифрування.

Атака на основі тільки шифртексту. Криптоаналітик розташовує шифртекстами c_1, ..., c_m, отриманими з невідомих відкритих текстів m_1, ...,m_m різних повідомлень. Потрібно знайти хоча б один з m_i i = i, ..., m (або відповідний ключ k_i), виходячи з достатнього числа m криптограм, або переконатися у своїй спроможності зробити це. В окремих випадках можливий збіг ключів або відкритих текстів.

Атака на основі відкритого тексту. Криптоаналітик має у своєму розпорядженні пари (m_1, c_1), ..., (m_m, c_m) відкритих і відповідних їм зашифрованих текстів. Потрібно визначити ключ k_i для хоча б однієї з пар. В окремому випадку, коли $k_1 = ... = k_m = k$, потрібно визначити ключ *k* або, переконавшись у своїй неспроможності зробити це, визначити відкритий текст m_{m+1} ще однієї криптограми c_{m+1}, шифрованої на тому ж ключі.

Атака на основі підібраного відкритого тексту відрізняється від попередньої лише тим, що криптоаналітик має можливість вибору відкритих текстів m_1, ..., m_m. Мета атаки така сама, що й попередньої. Подібна атака можлива, наприклад, у разі, коли криптоаналітик має доступ до шифратора передавальної сторони.

Атака на основі адаптивно підібраного відкритого тексту. Це окремий випадок описаної раніше атаки з використанням підібраного відкритого тексту. Криптоаналітик може не тільки вибирати використовуваний текст, що шифрується, але також уточнювати свій наступний вибір на основі добутих раніше результатів шифрування.

Атака на основі інформації з побічних каналів. Криптоаналітик має інформацію, яка може бути отримана з обладнання шифрування й не є до того ж ні відкритим текстом, ні шифртекстом.

Атаки з побічних каналів, своєю чергою, класифікують за такими типами:

за контролем над обчислювальним процесом: *пасивні* й *активні*;

за способом доступу до модуля**:** *агресивні* (invasive), *напівагресивні* (semi-invasive) і *неагресивні* (non-invasive);

за методом, застосованим у процесі аналізу: *прості* – simple side channel attack (SSCA) і *різницеві* – differential side channel attack (DSCA);

за видом використовуваного побічного каналу:

атаки за часом виконання (Timing Attacks);

атаки за енергоспоживанням (Power Analysis Attacks);

атаки за помилками обчислень (Fault Attacks);

атаки за електромагнітними випромінюваннями (Electromagnetic Analysis);

атаки за помилками у каналі зв'язку (Error Message Attacks);

атаки за кеш-пам'яттю (Cache-based Attacks);

акустичні атаки (Acoustic Attacks);

атаки за світловім випромінюванням (Visible Light Attacks).

Атаки з використанням відомого або підібраного відкритого тексту зустрічаються частіше, ніж можна подумати. Необхідною вимогою до криптоалгоритму є здатність протистояти таким атакам. Це означає, що розсекречення деякої інформації, що передають каналами зв'язку в шифрованому вигляді, не має приводити до розсекречення іншої інформації, шифрованої на цьому самому ключі. Крім того, зазначена вимога враховує особливості експлуатації апаратури й допускає деякі вільності з боку оператора або осіб, що мають доступ до формування засекреченої інформації. Атаки на основі підібраних текстів уважають найнебезпечнішими.

Класифікація з контролю над процесом шифрування

До класу **пасивних** атак належать дії противника, який "пасивно вивчає" шифровані повідомлення, може їх перехопити й піддати криптоаналізу із метою одержання інформації про відкритий текст або ключ. Однак сучасні технічні засоби дозволяють потенційному противнику "активно" втручатися у процес передавання повідомлення. Звичайно розрізняють два типи **активних** атак, які мають назви **імітації** й **підміни повідомлення**. **Атака імітації** полягає в тому, що противник "вставляє" у канал зв'язку сфабриковане ним "шифроване повідомлення", яке насправді не передавали від законного одержувача до одержувача. Водночас противник розраховує на те, що одержувач сприйме це повідомлення як справжнє (автентичне). **Атака підміни** полягає в тому, що про-

тивник, спостерігаючи передане каналом зв'язку справжнє повідомлення від відправника, "вилучає" його й заміняє підробленим. Різні шифри можуть бути більш-менш уразливими до активних атак. Здатність самого шифру (без використання додаткових засобів) протистояти активним атакам звичайно називають **імітостійкістю шифру**. Кількісною мірою імітостійкості шифру є ймовірності успіху імітації й підміни, відповідно. Ці ймовірності визначають шанси противника на успіх у разі нав'язування одержувачу неправильного повідомлення.

Класифікація за результатом атаки

Криптоаналіз ставить своїм завданням у різних умовах отримувати додаткові відомості про ключ шифрування, щоб значно зменшити діапазон імовірних ключів. Результати криптоаналізу можна варіювати за ступенями практичної застосовності. Шифр уважають зламаним, якщо в системі виявлено слабке місце, яке може бути використано для більш ефективного зламу, ніж метод повного перебору ключів (brute-force approach). Допустіть, що для дешифрування тексту методом повного перебору потрібно перебрати 2^{128} можливих ключів; тоді винахід способу, що потребує для дешифрування 2^{110} операцій із підбору ключа, будуть вважати зламом. Такі способи можуть потребувати нереалістично великих обсягів підібраного відкритого тексту або пам'яті ЕОМ. Під *зламом* розуміють лише підтвердження наявності вразливості криптоалгоритму, що свідчить про те, що властивості надійності шифру не відповідають заявленим характеристикам. Переважно, криптоаналіз починається зі спроб зламу спрощеної модифікації алгоритму, після чого результати поширюють на повноцінну версію. Криптограф Ларс Кнудсен [93] пропонує таку класифікацію успішних наслідків криптоаналізу блокових шифрів залежно від обсягу і якості секретної інформації, яку вдалося отримати:

повний злам – криптоаналітик отримує секретний ключ;

глобальна дедукц*ія* – криптоаналітик розробляє функціональний еквівалент досліджуваного алгоритму, що дозволяє шифрувати й розшифровувати інформацію без знання ключа;

часткова дедукція – криптоаналітику вдається розшифрувати або шифрувати деякі повідомлення;

інформаційна дедукція – криптоаналітик отримує деяку інформацію про відкритий текст або ключ.

Класифікація за обсягом необхідних ресурсів

Атаки можна також класифікувати за обсягом ресурсів, необхідних для їхнього здійснення:

пам'ять – обсяг пам'яті, необхідний для реалізації атаки;

час – кількість елементарних операцій, які необхідно виконати;

дані – необхідний обсяг відкритих і відповідних їм зашифрованих текстів.

У деяких випадках ці параметри є взаємозалежними: наприклад, за рахунок збільшення пам'яті можна скоротити час атаки.

Класифікація за степенем застосовності до різних шифрів

Якщо метою криптоаналітика є розкриття більшої кількості шифрів (незалежно від того, чи прагне він цим завдати шкоди суспільству, попередити його про можливу небезпеку або просто набути популярності), то для нього найкращою стратегією є розроблення **універсальних методів аналізу**. Але це завдання є також і найбільш складним. Та обставина, що будь-яке завдання пошуку способу розкриття деякої конкретної криптосистеми можна переформулювати як привабливе математичне завдання, під час розв'язання якого вдається використовувати багато методів тієї самої теорії складності, теорії чисел і алгебри, привело до появи методів криптоаналізу, застосованих до різних класів шифрів. Нарешті, є атаки, що використовують деяку вразливість у процесі проєктування або реалізації конкретного шифру. Ці атаки не може бути в загальному випадку перенесено на цілий клас шифрів, однак можуть ефективно застосовуватися для зламу відповідного криптоалгоритму.

Класифікація за використовуваними засобами

Та обставина, що будь-яке завдання пошуку способу розкриття деякої конкретної криптосистеми можна переформулювати як привабливе математичне завдання, під час розв'язанні якого вдається використовувати багато **методів теорії складності, теорії чисел** і **алгебри**, привело до розкриття багатьох криптосистем. Майже всі здійснені на практиці вдалі атаки на криптосистеми використовують слабкості в реалізації й розміщенні механізмів криптоалгоритму. Такі атаки засновано на кореляції між значеннями **фізичних параметрів, вимірюваних у різні моменти під час обчислень** (споживання енергії, час обчислень, електромагнітне випромінювання тощо), і внутрішнім станом обчислювального обладнання, стосуються секретного ключа. На практиці атаки побічними каналами на багато порядків більш ефективні, ніж традиційні атаки, засновані тільки на математичному аналізі. До того ж ата-

ки побічними каналами використовують особливості реалізації (тому їх іноді також називають атаками на реалізацію – implementation attacks) для витягання секретних параметрів, задіяних в обчисленнях. Такий підхід менш узагальнений, оскільки прив'язаний до конкретної реалізації, але найчастіше могутніший, ніж класичний криптоаналіз. Нині методи, засновані на використанні нових інформаційних технологій (еволюційного програмування і квантових комп'ютерів), у криптоаналізі не привели до серйозних проривів у зламі шифрів і становлять скоріше академічний інтерес, ніж практичний.

Криптосистему можна розглядати як "чорний ящик", тобто обладнання або програму, про внутрішню структуру якої нічого не відомо, але, подаючи сигнали команди або дані на вхід, можна отримати реакцію на виході. Завдання криптоаналізу – ідентифікація цієї системи, тобто визначення її структури на основі сигналів, що надходять на її вхід і отримають на виході. Одним з інструментів розв'язання цього завдання можуть бути нейронні мережі. Генетичні алгоритми успішно застосовують у криптоаналізі переставних і підставних шифрів.

Класифікація за наслідками атаки

Можливі наслідки реалізації атаки розгляньте з погляду порушення властивостей інформації – конфіденційності, цілісності й автентичності (доступності). Можна виділити три стратегії дій, які може почати порушник у разі успішної реалізації атаки:

перехоплення інформації, переданої каналами зв'язку;

модифікація інформації, переданої каналами зв'язку (підміна, неправильні повідомлення, блокування передавання тощо);

робота від чужого імені (обхід засобів автентичності учасників інформаційної взаємодії каналами зв'язку).

Класифікація за можливістю распаралелювання

Распаралелюванню піддаються не всі алгоритми криптоаналізу, однак воно дозволяє значно прискорити знаходження ключа. Таким чином, під час оцінювання ефективності методу криптоаналізу необхідно враховувати не тільки його часову і ємнісну складність, але й можливість распаралелювання на багатопроцесорній системі. Так, алгоритм Полларда має складність $O\left(\sqrt{n}\right)$, однак *не піддається розпаралелюванню*. Водночас метод повного перебору, який на однопроцесорній машині

уступає за ефективністю методу Полларда, становить простий приклад методу криптоаналізу, що *допускає розпаралелювання*.

Відомо два напрями в організації паралельного обчислення ключа. По-перше, побудова **конвеєра**. Нехай алгоритм співвідношення $E_k(M) = C$ подано у вигляді детермінованого ланцюжка найпростіших дій (операцій): O_1, O_2, …, O_N. Візьміть N процесорів A_1, A_2, …, A_N**,** задайте їхній порядок і доведіть, що *i*-й процесор виконує три однакові за часом операції:

1) приймання даних від (i – 1)-го процесора;

2) виконання операції O_i;

3) передавання даних наступному (i + 1)-му процесору.

Тоді конвеєр із N послідовно з'єднаних процесорів, що паралельно й синхронно працюють зі швидкістю $\frac{v}{3}$, де v – швидкість виконання однієї операції процесором.

Другий напрямк розпаралелювання полягає в тому, що множину K розподіляють на неперетинні підмножини K_1, K_2 …, K_Q. Система з *Q* машин перебирає ключі так, що *i*-а машина здійснює перебір ключів із множини $K_i, i = \overline{1,Q}$. Система припиняє роботу, якщо одна з машин знайшла ключ. Найбільшою складністю у викладеному підході є організація розподілу ключової множини. Однак якщо організувати пошук ключа таким чином, що під час кожного чергового випробування кожний із N процесорів стартує з випадкової точки, то час випробування збільшиться, але схема значно спроститься. Середня кількість кроків випробування N процесорами (машинами) ключів із множини K у цьому разі становить $\frac{|K|}{N}$. Реалізація такого паралелізму припускає різні розв'язання. Найбільш очевидне розв'язання – створення комп'ютерного вірусу для поширення програми-зломника у глобальній мережі. Вірус має використовувати періоди простою комп'ютера (за даними досліджень, комп'ютер простоює 70 – 90 % часу) для здійснення перебору за множиною ключів. Рано або пізно один із заражених комп'ютерів виявить шуканий ключ (необхідно передбачити механізм сповіщення противника); зі зростанням продуктивності комп'ютерів і швидкості поширення вірусів погроза успішного результату такої атаки зростає.

Класифікація зломників криптосистем

Під час оцінювання стійкості криптосистеми необхідно брати до уваги можливості потенційного противника, який може здійснити атаки на систему. Інакше кажучи, необхідно попередньо відтворити збірний образ (модель) порушника. Така модель має вказувати:

категорії осіб, серед яких може виявитися порушник;

припущення про кваліфікацію порушника і його технічну оснащеність;

можливі цілі порушника й очікуваний характер його дій.

За основу для розроблення класифікаційної схеми було взято модель порушника, класифікація дозволяє під час побудови моделі зломника криптосистеми враховувати різні параметри й, тим самим, установити залежність можливих сценаріїв атак від характеристик противника, із боку яких систему піддають нападам. На рис. 1.4 наведено класифікацію противника.

Рис. 1.4. **Класифікація порушника криптосистем**

Класифікація за технічною оснащеністю

На сьогодні великій компанії з більшими обчислювальними мережами під силу методом перебору розкрити ключ довжиною 64 – 80 бітів. Підтвердженням цьому є розкриття RC5-64 (блокового шифру компанії RSA, що використовує 64-бітний ключ, що стартував 1997 р. на сайті www.distributed.net (проєкт “розподіленого зламу”), у якому на добровільній основі взяли участь понад 300 тисяч користувачів глобальної мережі, був успішно завершений за п’ять років (1 757 днів) – за цей час було пе-

ребрано 85 % усієї множини ключів. Крім того, для розв'язання завдань криптоаналізу можна використовувати суперкомп'ютери.

Класифікація за кінцевою метою

В основі дій хакерів звичайно лежить корислива мотивація, рідше – бажання прославитися, завдати моральної шкоди законному власнику шифрованої інформації або інші причини. Мета криптоаналітика полягає у створенні нових і підвищенні ефективності наявних методів аналізу стійкості криптографічних засобів. Кожний новий метод криптоаналізу приводить до перегляду безпеки шифрів, до яких він застосовний.

Класифікація за доступом до засобів, що шифрують

Порушником може бути не тільки стороння особа, але й законний користувач системи, а також особа із-поміж обслугового персоналу. Якщо роль зломників виконують ненадійні співробітники компанії, то можливостей для здійснення атак виникає набагато більше, ніж у будь-яких інших зломників.

Класифікація за рівнем підготовки

Кваліфікацію зломника визначено наявністю релевантних знань, умінь і навичок. Можна виділити чотири основні сфери, освоєння яких може бути корисним порушнику для здійснення атаки на криптосистему:

взаємодія з комп'ютером на рівні користувача – для здійснення атак із використанням доступних інструментальних засобів;

математичний апарат – для створення нових методів криптоаналізу й підвищення ефективності наявних методів;

програмування – для розроблення інструментальних засобів, що реалізують алгоритми криптоаналізу; створення вірусів для розпаралелювання пошуків ключа й т. ін.;

електротехніка й фізика – для реалізації криптоатак побічними каналами з використанням інформації, яку можна витягти з обладнання, що шифрує. Наприклад, зломник може відстежувати енергію, споживану смарт-картою, коли вона виконує такі операції із закритим ключем, як розшифрування або генерація підпису. Противник може також вимірювати час, витрачуваний на виконання криптографічної операції або аналізувати поведінку криптографічного обладнання під час виникнення певних помилок;

соціальна інженерія – потужна зброя зломника, що дозволяє обійти захист найстійкіших криптосистем, скориставшись довірливістю користувачів.

Градація противників за їхньою кваліфікацією може бути різною. Наприклад, виділено три класи противників:

висококваліфікований зловмисник-професіонал;

кваліфікований зловмисник-непрофесіонал;

некваліфікований зловмисник-непрофесіонал.

Класифікація за первинною інформацією про засіб шифрування

Порушнику може бути відома інформація (зокрема секретна) про принципи функціонування криптосистеми. Так, однією із причин ненадійності криптосистем є використання слабких ключів. **Слабкий ключ** – це ключ, що не забезпечує достатнього рівня захисту, або той що використовує в шифруванні закономірності, які може бути зламано. Це означає що, якщо для генерації ключів використовують криптографічний слабкий алгоритм, то, незалежно від шифру, який використовують, уся система буде нестійкої. *Генератори випадкових чисел* – це те місце, у якому часто ламають криптографічні системи. Знаючи принцип витягування випадкових чисел, противник може значно скоротити область перебору можливих ключів системи.

Особливої уваги заслуговує технологія ***"***клептографія***"***. Розробловач може випадково або навмисно вмонтувати у криптосистему лазівки, що дозволяють отримувати доступ до зашифрованої інформації без знання секретного ключа. Через "чорний хід" інформована людина може легко подолати захист. Якщо механізм дії шифру тримають у секреті, імовірність наявності подібної "лазівки" підвищується.

Класифікація за можливістю кооперації

Останнім часом, у зв'язку з розвитком мереж (зокрема, інтернету), стало можливим ефективно використовувати метод "грубої сили" (перебору) шляхом розпаралелювання операцій. Нерідко професійні хакери поєднуються у злочинні угруповання, що прагнуть до наживи та виконуючи розкрадають конфіденційну інформацію із замовлень конкурентних фірм і навіть іноземних спецслужб. Альтернативний варіант – створення вірусу, непомітно для користувача, що встановлює на підключений до мережі комп'ютер програму, здатну здійснювати дешифрування повідомлення шляхом перебору ключів. Після запуску програму підключено до сервера, отримує від нього набір ключів для перебору й після закінчення роботи повертає результат. Програма може працювати у фоновому режимі як скринсейвер або активуватися ночами. Такий підхід застосовують не тільки для зламу шифрів, але й для підбору двох текстів, що мають однакове значення геш-функції, обчисленої зазначеним алгоритмом.

Рис. 1.5. **Загрози інформації у критичних інформаційних системах і технологіях**

На рис. 1.5 наведено приклад класифікації загроз інформації в загальному вигляді.

Таким чином, оцінювання ефективності криптографічних засобів захисту інформації становить складне науково-технічне завдання.

Під час вибору криптосистеми необхідно робити аналіз погроз безпеки в конкретній комп'ютерній системі, що передбачає оцінювання стійкості до досить різноманітних типів криптоаналітичних нападів.

Модель погроз можна розглядати як композицію моделі противника, моделі атак і моделі криптосистеми. Ці моделі може бути побудовано на основі наведених класифікацій.

1.3. Побудова моделі порушника безпеки у КміС

Спроба отримати несанкціонований доступ до комп'ютерних мереж, із метою ознайомитися з ними, залишити записку, виконати, знищити, змінити або викрасти програму або іншу інформацію кваліфікують як *комп'ютерне піратство.* Як соціальне явище подібні дії простежують останні 10 років, але водночас відбувається тенденція до їхнього стрімкого зростання по мірі збільшення кількості побутових комп'ютерів.

Зростання кількості комп'ютерних порушень очікують у тих країнах, де вони широко рекламують у фільмах і книгах, а діти у процесі ігор рано починають знайомитися з комп'ютерами. Разом із тим зростає кількість серйозних навмисних злочинів.

Однак комп'ютерні злочинці не цікавляться, наскільки добре здійснюють загалом контроль у комп'ютерній системі; вони шукають єдину лазівку, яка приведе їх до бажаної мети. Для отримання інформації вони виявляють винахідливість, використовуючи психологічні фактори, детальне планування та активні дії. Необхідно відокремити два поняття: "хакер" (hacker) і "кракер" (cracker). Основна відмінність полягає у постановці мети зламу комп'ютерних систем: перші ставлять дослідницькі завдання з оцінки та знаходження вразливостей, із метою подального підвищення надійності комп'ютерної системи. Кракери ж втручаються в систему із метою руйнування, крадіжки, псування, модифікації інформації, і роблять правопорушення з корисливими намірами швидкого збагачення.

Для запобігання можливим погрозам необхідно не тільки забезпечити захист операційних систем, програмного забезпечення і контроль за доступом, але й виявити категорії порушників і ті методи, які вони використовують.

Залежно від мотивів, цілей і методів дії порушників безпеки інформації можна розподілити на чотири категорії:

шукачі пригод;

ідейні хакери;

хакери-професіонали;

ненадійні (неблагополучні) співробітники.

Шукач пригод, переважно, це студент, у якого рідко є продуманий план атаки. Він вибирає мету випадковим чином і звичайно відступає, стикаючись із труднощами. Знайшовши діру в системі безпеки, він намагається зібрати закриту інформацію, але практично ніколи не намагається її таємно змінити. Своїми перемогами такий шукач пригод ділиться тільки зі своїми близькими друзями-колегами.

Ідейний хакер – це той самий шукач пригод, але більш митецький. Він уже вибирає собі конкретні цілі (хости та ресурси) на підставі своїх переконань. Його улюбленим видом атаки є зміна інформаційного наповнення web-сервера або, у більш рідких випадках, блокування роботи ресурсу, що атакують. Порівняно з шукачем пригод, ідейний хакер розповідає про успішні атаки набагато більш широкій аудиторії, звичайно розміщаючи інформацію на хакерському web-вузлі або в конференціях Usenet.

Хакер-професіонал має чіткий план дій і націлюється на конкретні ресурси. Його атаки добре продумані та звичайно їх здійснюють у кілька етапів. Спочатку він збирає попередню інформацію (тип операційної системі (ОС), сервіси що надають, і заходи захисту що застосовують). Потім він становить план атаки з урахуванням зібраних даних і підбирає (або навіть розробляє) відповідні інструменти. Провівши атаку, він отримує закриту інформацію, і нарешті, знищує всі сліди своїх дій. Такого професіонала, що атакує, звичайно добре фінансують, і він може працювати сам або у складі команди професіоналів.

Ненадійний (неблагополучний) співробітник своїми діями може завдати стільки ж проблем (буває й більше), скільки промисловий шпигун, до того ж його присутність, звичайно, складніше виявити. Крім того, йому доводиться долати не зовнішній захист мережі, а тільки, переважно, менш твердий внутрішній захист. Він не такий витончений у способах атаки, як промисловий шпигун, і тому частіше допускає помилок і тим самим може видати свою присутність. Однак у цьому разі небезпека його несанкціонованого доступу до корпоративних даних набагато вища, ніж

будь-якого іншого зловмисника. Перелічені категорії порушників безпеки інформації можна згрупувати за їхньою кваліфікацією: *початківець* (шукач пригод), *фахівець* (ідейний хакер, ненадійний співробітник), *професіонал* (хакер-професіонал).

Порушник безпеки інформації, переважно, будучи фахівцем визначеної кваліфікації, намагається довідатися про комп'ютерні системи й мережі та, зокрема, про засоби їхнього захисту. Тому модель порушника визначає:

категорії осіб, серед яких може виявитися порушник;

можливі цілі порушника і їхню градацію за ступенями важливості й небезпеки;

припущення про його кваліфікацію;

оцінку його технічної озброєності;

обмеження та припущення про характер його дій.

На рис. 1.6 наведено узагальнену модель порушника безпеки інформації.

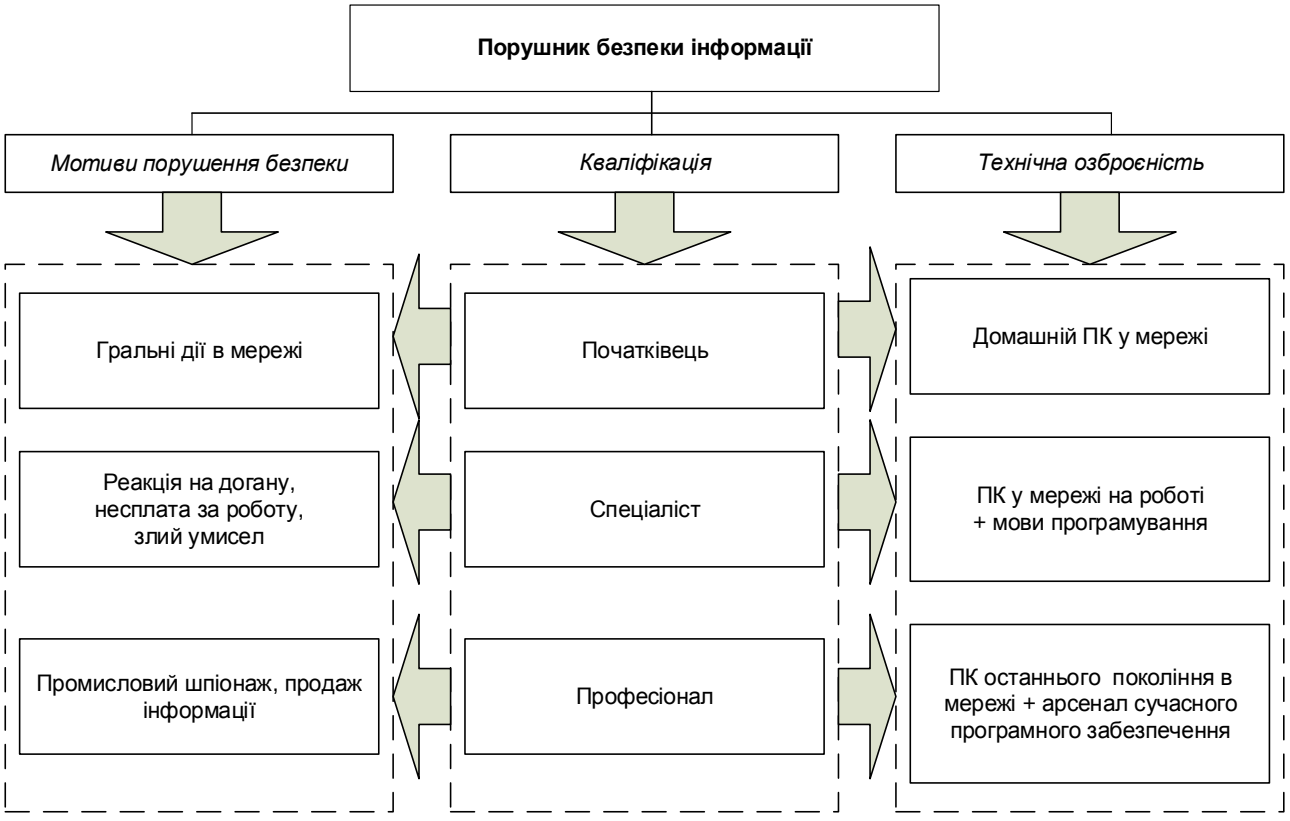


Рис. 1.6. **Модель порушника безпеки інформації**

Діапазон спонукальних мотивів дістання доступу до системи досить широкий: від бажання випробувати емоційний підйом під час гри з комп'ютером до відчуття влади над ненависним менеджером. Займа-

ються цим не тільки новачки, що бажають побавитися, але й професійні програмісти. Паролі вони здобувають або в результаті підбору або шляхом обміну з іншими хакерами.

Частина з них, однак, починає не тільки переглядати файли, але й виявляти інтерес саме до їхнього змісту, а це вже становить серйозну загрозу, оскільки в цьому разі важко відрізнити невинні пустощі від злочинних дій.

Донедавна викликали занепокоєння випадки, коли незадоволені керівником службовці, зловживаючи своїм положенням, псували системи, допускаючи до них сторонніх або залишаючи системи без догляду в робочому стані.

Спонукальними мотивами таких дій є:

реакція на догану або зауваження з боку керівника;

невдоволення тим, що фірма не оплатила понаднормові години роботи (хоча найчастіше понаднормова робота виникає через неефективне використання робочого часу);

злий намір як реванш, із метою послабити фірму як конкурента якої-небудь фірми.

Незадоволений керівником службовець створює одну із найбільших загроз обчислювальним системам колективного користування.

Професійні хакери – це комп'ютерні фанати, що прекрасно знають обчислювальну техніку і системи зв'язку. Вони витратили масу часу на обмірковування способів проникнення в системи та ще більше, експериментуючи із самими системами. Для входження в систему професіонали найчастіше використовують деяку систематику й експерименти, а не розраховують на удачу або здогад. Їхня мета – виявити й подолати захист, вивчити можливості обчислювальної установки й потім вийти, упевнившись у можливості досягнення своєї мети.

Завдяки високій кваліфікації, ці люди розуміють, що ступінь ризику малий, тому що відсутні мотиви руйнування або розкрадання. До категорії хакерів-професіоналів звичайно зараховують таких осіб:

які належать до злочинних угруповань, що дбають про політичні цілі;

які прагнуть отримати інформацію, із метою промислового шпигунства;

хакерів або угруповання хакерів, що прагнуть до наживи.

Для здійснення несанкціонованого доступу до інформаційної системи потрібно, переважно, провести два підготовчі етапи:

зібрати відомості про систему;

виконати пробні спроби входження в систему.

Збір відомостей. Залежно від особистості зломника і його схильностей можливі різні напрями збирання відомостей:

підбір співучасників;

аналіз періодичних видань, відомчих бюлетенів і документації;

перехоплення повідомлень електронної пошти;

прослуховування розмов, телексів, телефонів;

перехоплення інформації й електромагнітного випромінювання; організація крадіжок;

вимагання й хабар.

Багато власників систем часто не уявляють, яку підготовчу роботу має виконати порушник, щоб проникнути в ту або ту комп'ютерну систему. Тому вони самовпевнено вважають, що єдине, що необхідно зробити, – це захистити файл, надавши йому пароль, і забувають, що будь-яка інформація про ті або ті слабкі місця системи може допомогти зломнику знайти лазівку й обійти пароль, діставши доступ до файлу. Таким чином, інформація стає легкодоступною, якщо зломник знає, де й що дивитися.

Підбір співучасників. Підбір співучасників засновано на прослуховуванні розмов у барах, фойє готелів, ресторанах, таксі, підключенні до телефонів і телексів, вивченні змісту загублених портфелів і документів. Більшу й корисну інформацію можна витягти, якщо трапляється можливість підсісти до групи програмістів. Цей спосіб часто використовують репортери й професійні агенти.

Витягування інформації з періодичних видань. Зломники можуть почерпнути багато корисної інформації з газет та інших періодичних видань.

Перехоплення повідомлень електронної пошти. Звичайно для підключення до електронної пошти використовують побутовий комп'ютер із модемом для зв'язку з державною телефонною мережею.

Телефонний канал доступу в таку систему звичайно вільний, хоча останнім часом системні оператори вимагають установки обладнання реєстрації користувачів електронної пошти. Аж до недавнього часу багато довідкових систем було оснащено блоками, через які зломники могли витягати більші обсяги даних, а також ідентифікатори й паролі користу-

вачів. Зараз немає нічого незвичайного в тому, що блоки, установлені кракерами, можуть бути зашифровані й тільки окремі члени злочинних угруповань можуть зчитувати з них інформацію.

Зав'язування знайомств. Із метою отримання інформації про обчислювальну систему або отримання службових паролів зломники можуть використовувати різноманітні способи. Наприклад, знайомлячись, вони представляються менеджерами; використовують опитувальники, роздаючи їх у фойє фірми й детально розпитуючи співробітників про комп'ютерну систему; дзвонять системному адміністраторові в обідній час із проханням нагадати нібито забутий пароль; прогулюються в будинку, спостерігаючи за доступом до системи; установлюють контакти з незайнятими в цей момент службовцями охорони, яким відвідувачі при вході в будинок фірми мають пред'являти ідентифікаційний код або пароль.

Більш зловмисним, але, можливо, і більш успішним є метод "полювання за разумами", коли на фірму приходить людина, яка бажає працювати системним програмістом або інженером зв'язку, і просить дати йому консультацію. Дивно, як багато інформації може передати службовець, який не має перспективи зростання, але вважає себе гідним більш важливої та високооплачуваної посади; він може розкрити коди користувачів, паролі, указати слабкі місця в мережах зв'язку тощо.

Аналіз роздруківок. Деякі зломники дістали доступ до комп'ютера, просто вивчаючи роздруківки, і це один із найбільш ефективних і найменш ризикованих шляхів отримання конфіденційної інформації. Численні фірми втрачають інформацію зі своїх комп'ютерних систем, по-перше, помилково думаючи, що вона не містить конфіденційної інформації, і, по-друге, помилково вважаючи, що всі чорнові роздруківки сумлінно знищують. Саме таким способом зломники змогли з'ясувати досить повну картину організації комп'ютерної системи, використовуючи викинуті роздруківки й незатребувані протоколи роботи системи, які співробітникам обчислювального центру представлялися невинними папірцями.

Перехоплення повідомлень у каналах зв'язку. На сьогодні кількість фірм, оснащених обчислювальною технікою, постійно зростає, тому перехоплення повідомлень стало досить реальною загрозою й для комерційного світу. Спектр можливих перехоплень досить широкий – це перехоплення усних повідомлень із використанням радіопередавачів, мікрофонів і мікрохвильових обладнань; прослуховування повідомлень, пере-

даних із телефону, телексу й іншими каналами передавання даних; контроль за електромагнітним випромінюванням від ПК; перехоплення супутникових або мікрохвильових передач.

Установленням радіопередавачів, мікрофонів і мікрохвильового обладнання або прослуховуванням ліній зв'язку звичайно займаються професійні зломщики, а також аматори та фахівці зі зв'язку. Останнім часом кількість випадків установлення такого обладнання зросла. Улюбленими точками безконтрольного доступу також є телефонні лінії.

Передавання даних із комутацією пакетів або з використанням широкосмугових ліній зв'язку зі швидкостями тисяча та мільйони бодів викликає інтерес у зломників і може бути перехоплена, щоб викрасти передані повідомлення, модифікувати їхній зміст, затримати або вилучити.

1.4. Побудова моделі реалізації загроз безпеки у КміС

Моделювання процесу реалізації загроз КміС доцільно здійснювати на основі розгляду логічного ланцюжка: "загрози – джерело загрози – метод реалізації – уразливість – наслідки". На рис. 1.7 подано структурна схема моделі реалізації загроз інформаційних ресурсів у КміС.

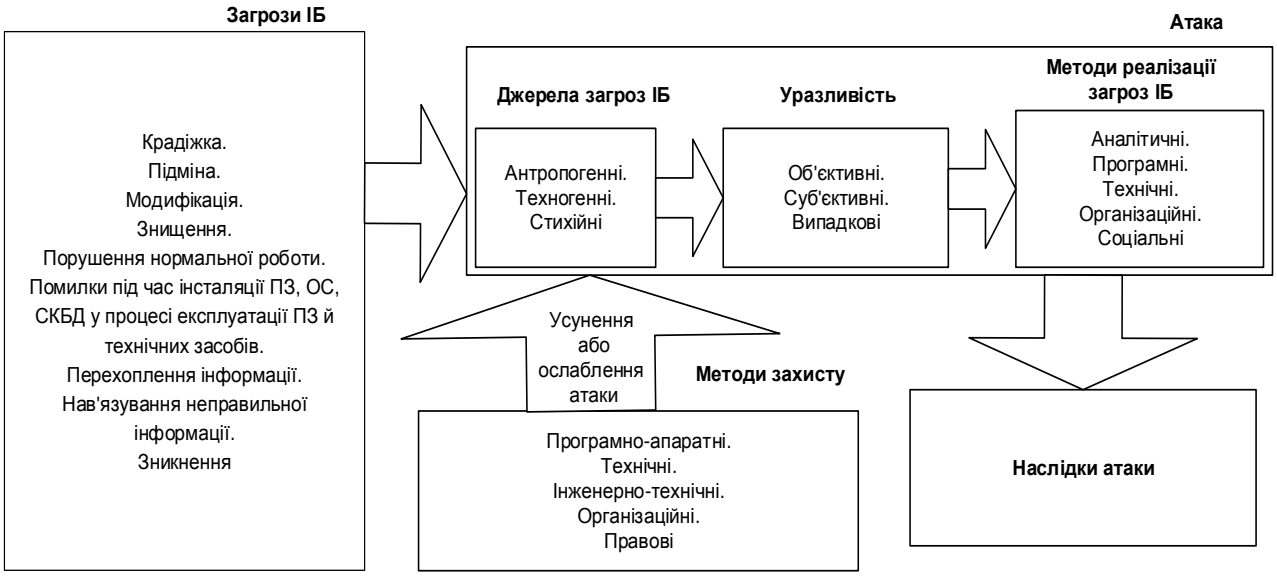


Рис. 1.7. **Структурна схема моделі реалізації загроз інформаційних ресурсів в КміС**

Аналіз негативних наслідків реалізації погроз передбачає обов'язкову ідентифікацію (наприклад, присвоєння унікального коду) можливих джерел загроз, уразливостей, що сприяють їхній появі та методів реалізації, тобто класифікацію (рис. 1.8).

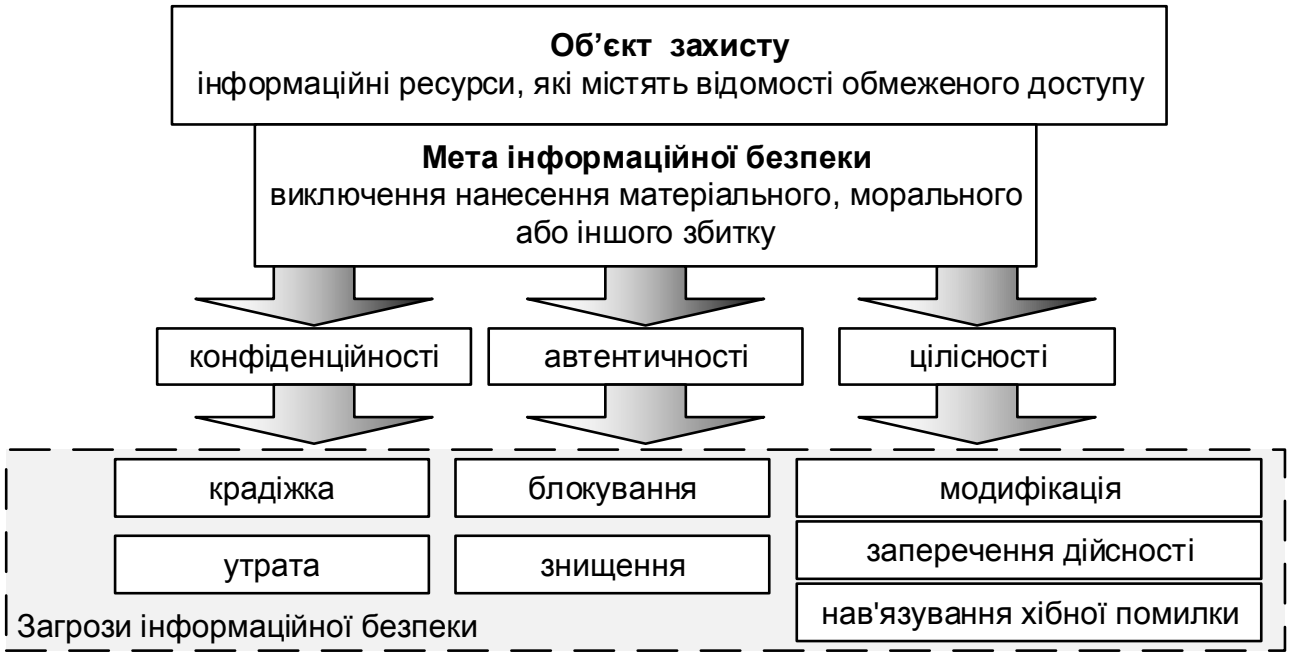


Рис. 1.8. **Мета і погрози безпеки інформації**

Для опису моделі реалізації загроз інформаційних ресурсів зафіксуйте кінцеву множину суб'єктів, взаємодійних з інформаційною системою – S, параметр N – кількість уразливих до атаки комп'ютерів (ПК); параметр D містить початкове значення середньої кількості атакованих комп'ютерів за вибрану одиницю часу. Уважають, що D є константою, обчислення враховують, що комп'ютер не може бути атаковано двічі; a(t) – пропорція вразливих ПК, які було успішно атаковано за час t, $N \cdot a(t)$ – загальна кількість успішно атакованих комп'ютерів, за час t зроблено не більше $D(1-a(t))$ нових успішних атак. Кількість захоплених комп'ютерів за період часу $d(t)$ дорівнює:

$$n = aN \cdot D(1-a)dt.$$

Ураховуючи, що N – константа і $n = d(Na) = Nda$, правильним буде таке рівняння:

$$Nda = aN \cdot D(1-a)dt,$$

у диференціальному вигляді:

$$\frac{da}{dt} = Da(1-a),$$

має таке рішення:

$$a = \frac{e^{D(t-T)}}{1+e^{D(t-T)}},$$

де T – часовий параметр, що характеризує найбільше зростання атак.

Для побудови загальної структури підсистеми безпеки інформаційної безпеки у КміС і моделей атак вибрано функціональний тип математичних моделей, який називають моделями “чорної скриньки”. Математична модель є моделлю об’єкта, процесу або явища, що становить математичні закономірності, за допомогою яких описано основні характеристики об’єкта, який моделюють, процесу або явища. Загальним для опису цих математичних моделей є процес формування криптограми.

Для цього зафіксують кінцеву множину $I = \{I_1, I_2, ..., I_m\}$ переданих пакетів, причому кожному пакетів відповідає ймовірність $P^*(I_j)$. Розподіл імовірностей випадкового процесу задають сукупним розподілом імовірностей випадкових величин, тобто множиною ймовірностей $P^*_o = \left\{P^*\left(I_1\right), P^*\left(I_2\right), ..., P^*\left(I_m\right)\right\}$. Джерело ключів породжує потік ключів із множини K і/або K^*. Кожному ключу $K_i \in K = \{K_1, K_2, \ldots, K_k\}$ відповідає деяка ймовірність $P^*(K_i)$, а кожному $K_i^* \in K^* = \{K_1^*, K_2^*, \ldots, K_k^*\}$ відповідає імовірність $P^*(K^*_i)$. Випадковий процес вироблення ключів задається множиною імовірностей:

$$P^*_K = \left\{P^*\left(K_1\right), P^*\left(K_2\right), ..., P^*\left(K_k\right)\right\}$$

$$P^*_{K^*} = \left\{P^*\left(K_1^*\right), P^*\left(K_2^*\right), ..., P^*\left(K_k^*\right)\right\}.$$

Вибір ключа K_i визначає конкретне відображення φ_i із множини відображень і формує криптограму: $E_I = \varphi_i(K_i, I_j)$.

Відмінність між активними й пасивними атаками полягає в тому, що під час здійснення атак першого типу (активні атаки) порушник виконує активні дії, тобто дії, пов’язані зі зміною потоку даних або зі створенням фальшивих потоків (імітація, відтворення, модифікація повідомлень або перешкоди в обслуговуванні). Метою другого типу атак (пасивні атаки) є отримання переданої інформації (розкриття вмісту повідомлень і аналіз потоку даних).

Оцінювання ступеня ефективності атаки може бути здійснено за рахунок аналізу даних, якими володіє противник, його можливостей та інших параметрів пасивних атак. Основним методом оцінювання можливостей противника під час атак є створення моделей атак.

1.5. Побудова моделі пасивних атак у КміС

Пасивні загрози випливають із прослуховування (несанкціонованого зчитування інформації) і не пов'язані з якою-небудь зміною інформації. Сутність атаки полягає в тому, що порушник, визначивши факт виконання криптографічного протоколу, перехоплює всі дані, які було передано каналом зв'язку, тобто під час передавання криптограми E_l у вузли приймання деяким каналом порушник виконує моніторинг мережі.

Водночас порушник (криптоаналітик) зобов'язаний володіти всіма відкритими параметрами й даними, які використовуються суб'єкти *s*. У такому разі криптоаналітик може зробити криптоаналіз протоколу, із метою визначення сеансових або довгострокових ключів, які використовуються суб'єктами-учасниками протоколу.

Криптоаналіз протоколу залежить від типу протоколу, кількості й типу ключів, математичного апарату, які використовують у протоколі, та інших характеристик протоколу. Узагальнену модель пасивних атак подано на рис. 1.9 і 1.10.

Рис. 1.9. **Модель пасивних атак на інформаційні ресурси у КміС**

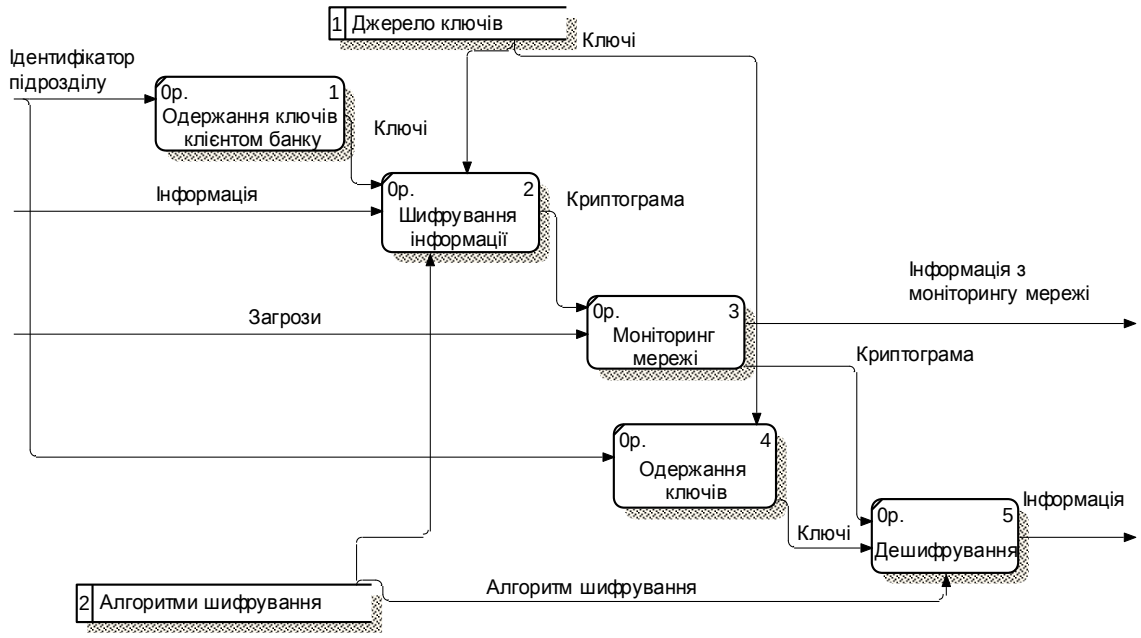


Рис. 1.10. **Декомпозиція моделі пасивних атак**

Криптоаналіз є рішенням математичного завдання, із метою визначення самого повідомлення або деяких особистих ключів суб'єктів-учасників протоколу.

1.6. Побудова моделі активних атак у КміС із блокуванням передавання інформації

Сутність атаки із блокуванням передавання інформації полягає в тому, що порушник, визначивши факт виконання криптографічного протоколу, блокує передавання інформації, у результаті чого криптограма не досягає прийомної сторони.

Узагальнена модель активних атак із блокуванням передавання інформації подано на рис. 1.11 і 1.12. Одержувачем інформації в цій моделі є порушник.

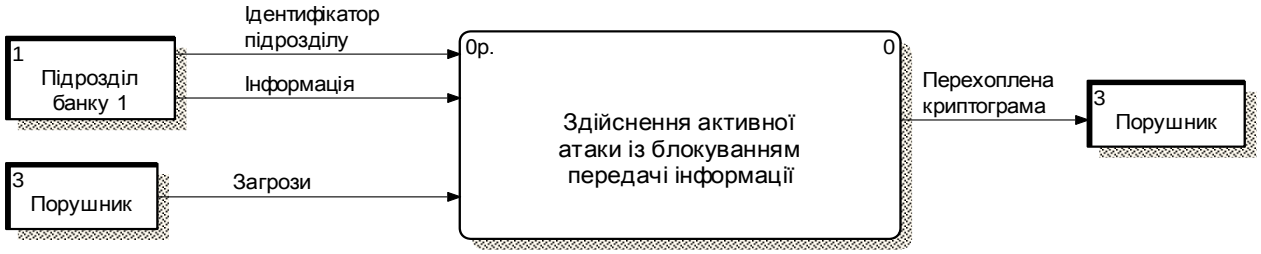


Рис. 1.11. **Модель активних атак із блокуванням передаванняі інформації**

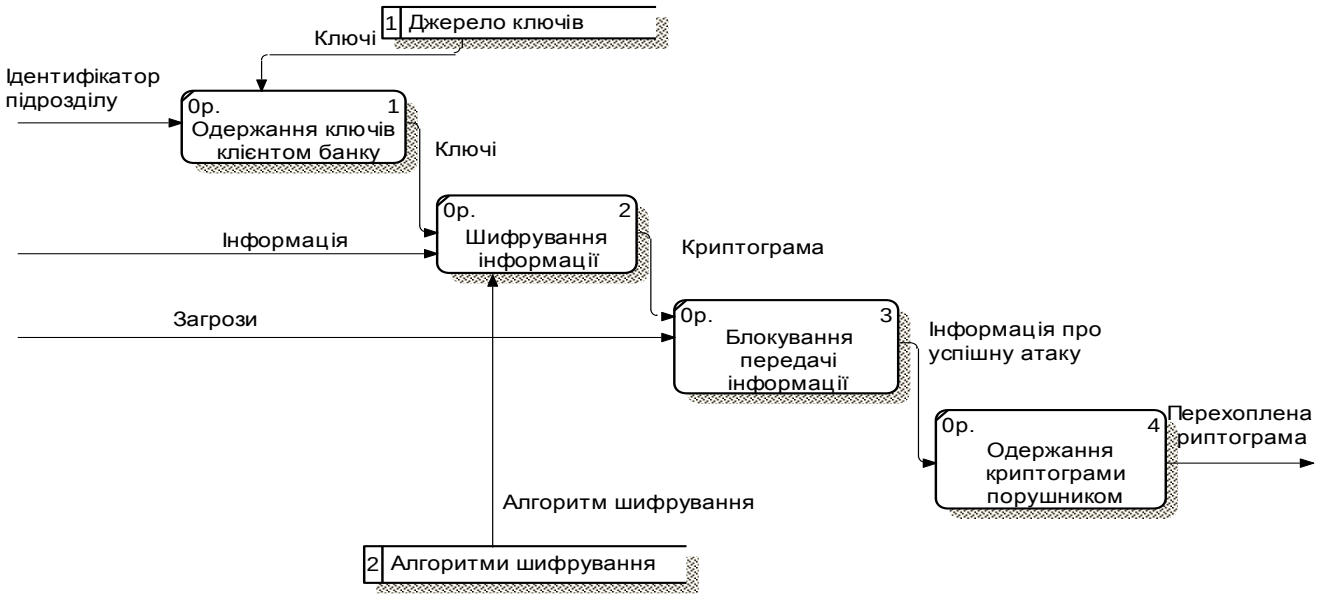


Рис. 1.12. **Декомпозиція моделі активних атак із блокуванням передавання інформації**

Під час реалізації цієї атаки необхідні дані не досягають пункту призначення або досягають занадто пізно, що призводить до втрати конфіденційної банківської інформації.

1.7. Побудова моделі активних атак у КміС із внесенням перешкод

Сутність атаки із внесенням перешкод полягає в тому, що порушник, визначивши факт виконання криптографічного протоколу, уносить деяку помилку *e* й передає у вузол приймання криптограму (E_{I+e}). На прийомному кінці за допомогою зворотного відображення φ_i^{-1} (заданого ключем K_i^*) із криптограми (E_{I+e}) відновлюється недостовірна інформація $I_{je} = \varphi_i^{-1}(K_i^*, E_{I+e})$.

Узагальнену модель активних атак із внесенням перешкод подана на рис.1.13 і 1.14.

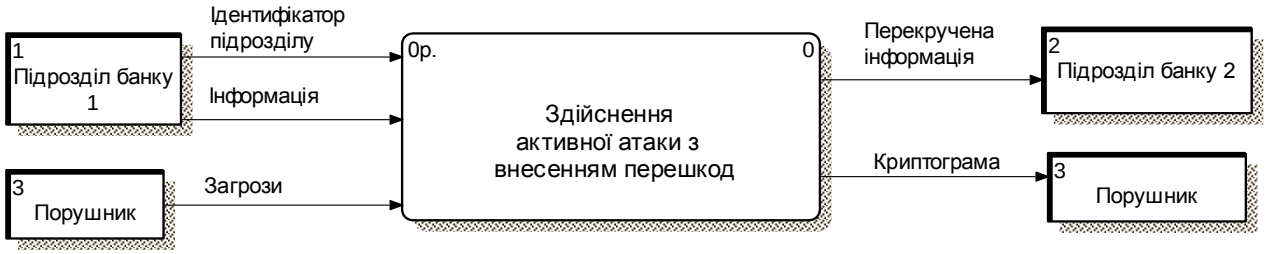


Рис. 1.13. **Модель активних атак із внесенням перешкод**

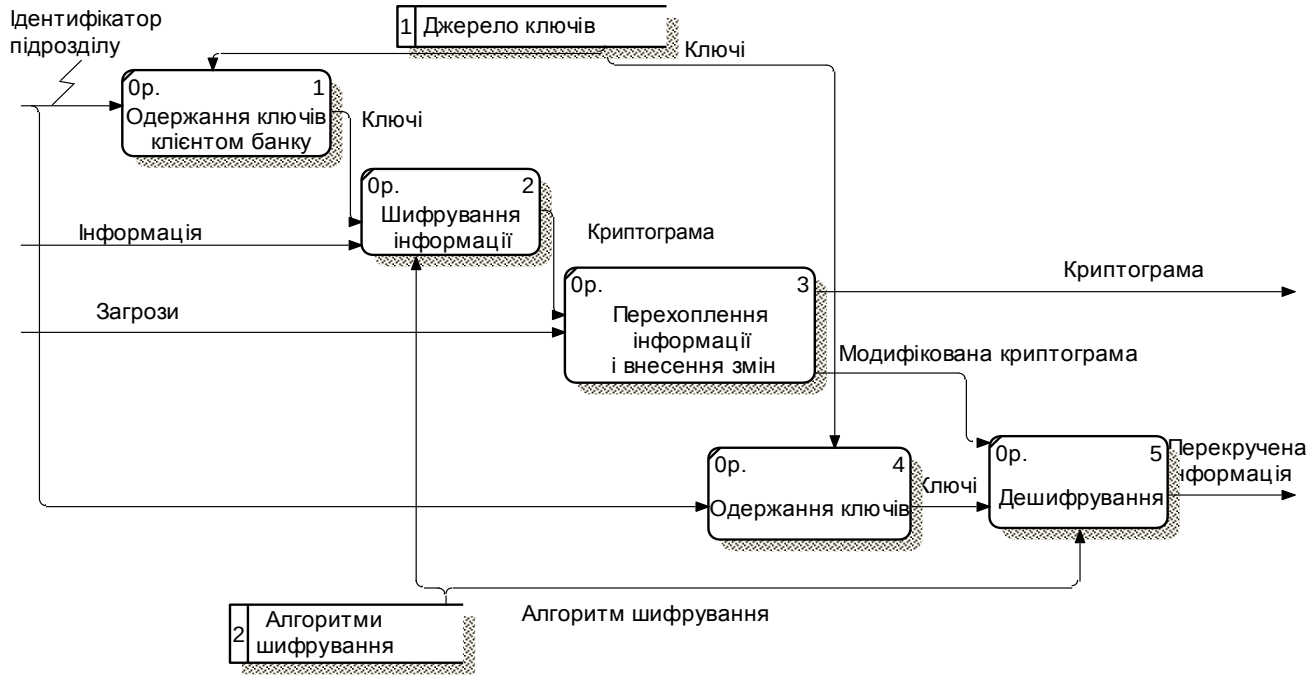


Рис. 1.14. **Декомпозиція моделі активних атак із внесенням перешкод**

Реалізація цієї атаки може призвести до перебою або до отримання на прийомній стороні неправильної транзакції. Порушник може “управляти” конфіденційною інформацією, результатом цього є економічний збиток клієнтів КміС.

1.8. Побудова моделі активних атак “маскарад” у КміС

Сутність атаки “маскарад” полягає в тому, що користувач (або інший суб'єкт – процес, підсистема та ін.) передає інформацію від імені іншого користувача. Способи заміни ідентифікатора можуть бути різні, зазвичай їх визначають за помилками та особливостями мережних протоколів. Проте на прийомному вузлі таке повідомлення буде сприйняте як коректне, що може призвести до серйозних порушень роботи КміС.

Розгляньмо процес здійснення атаки цього типу. Порушник, визначивши факт виконання криптографічного протоколу, перехоплює криптограму E_l. Із її допомогою він може спробувати обчислити апостеріорні ймовірності різних можливих повідомлень:

$$P^*_{o|E_l} = \left\{P^*\left(I_1|E_l\right), P^*\left(I_2|E_l\right), ..., P^*\left(I_m|E_l\right)\right\}$$

і різних можливих ключів:

$$P^*_{K|E_l} = \left\{P^*\left(K_1|E_l\right), P^*\left(K_2|E_l\right), ..., P^*\left(K_k|E_l\right)\right\},$$

які могли бути використані під час формування криптограми E_l.

Множини апостеріорних імовірностей утворюють апостеріорні знання порушника про ключі $K = \{K_1, K_2, \ldots, K_k\}$ і про інформацію $I = \{I_1, I_2, \ldots, I_m\}$ після перехоплення криптограми E_l. Фактично множини $P^*_{K|E_l}$ і $P^*_{M|E_l}$ є множинами припущень, яким приписано відповідні ймовірності. Отримавши необхідну інформацію, формує криптограму з недостовірною інформацією E_l $e=\varphi_i(K_i, I_{je})$ і передає її на вузлі приймання.

На прийомному кінці за допомогою зворотного відображення φ_i^{-1} (заданого ключем K_i^*) із криптограми E_{le} відновлюється недостовірна інформація, передана порушником:

$$I_{je} = \varphi_i^{-1}(K_i^*, E_{le}),\ I_{je} \neq I_j.$$

Такого типу атаку, переважно, пов'язано зі спробами проникнення всередину периметра безпеки КміС і часто реалізується хакерами.

Узагальнену модель активних атак "маскарад" подано на рис. 1.15 і 1.16.

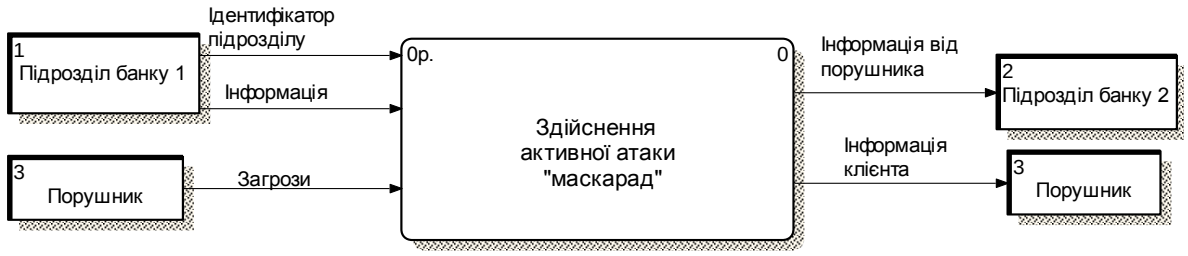


Рис. 1.15. **Модель активних атак "маскарад"**

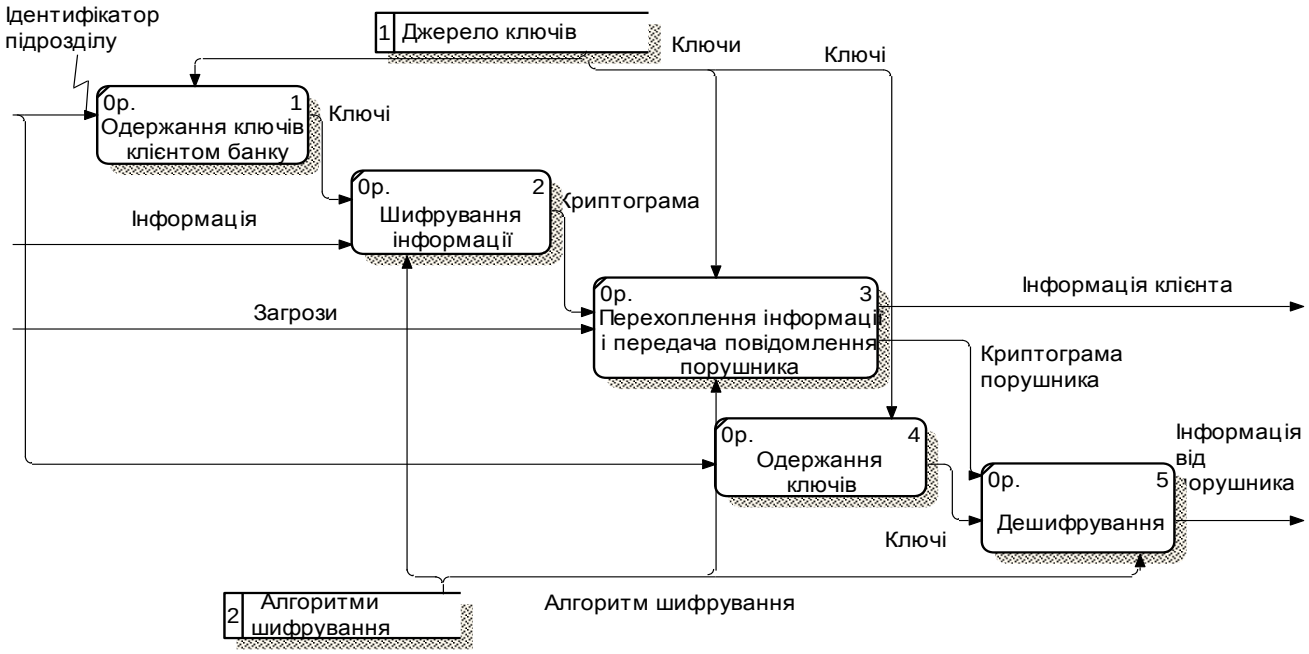


Рис. 1.16. **Декомпозиція моделі активної атаки “маскарад”**

Під час здійснення пасивної атаки порушник не впливає на протокол обміну інформацією у КміС і намагається отримати інформацію про учасників протоколів за допомогою моніторингу мережі, тому пасивні атаки важко виявити. Під час активного розкриття криптопротоколів порушник намагається змінити протокол для власної потреби. Спроби здійснення такого типу атаки мають на меті більш широкий набір завдань: отримання інформації, погіршення роботи системи або отримання несанкціонованого доступу до ресурсів.

1.9. Побудова та аналіз моделі оцінювання ризику реалізації загроз безпеки комунікаційних систем

Оцінювання ризику реалізації загроз безпеки засновано на захисті конфіденційних ресурсів, яку визначають за допомогою аналізу загроз, що діють на конкретний ресурс, уразливостей, через які ці загрози може бути реалізовано, і моделей атак.

Для побудови моделі оцінювання ризику реалізації загроз безпеки телекомунікаційних систем вибрано функціональний тип математичних моделей, названий моделями “чорного ящика”. Ці моделі побудовано, відповідно до методології IDEF0 з використанням Case-засобу Bpwin (рис. 1.17 – 1.18).

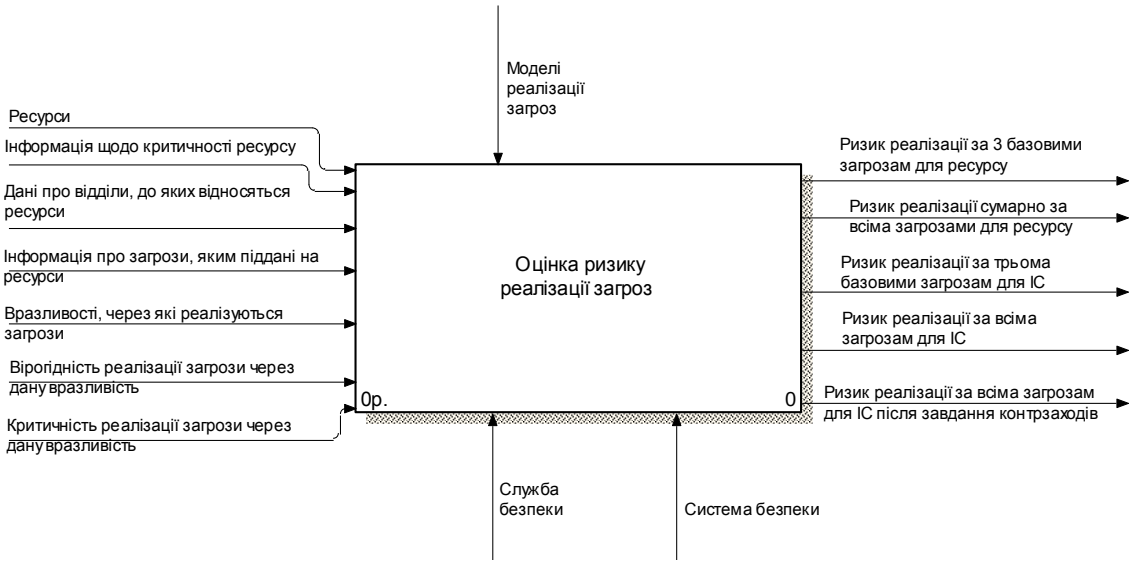


Рис. 1.17. **Модель оцінювання ризику реалізації загроз** (контекстна діаграма)

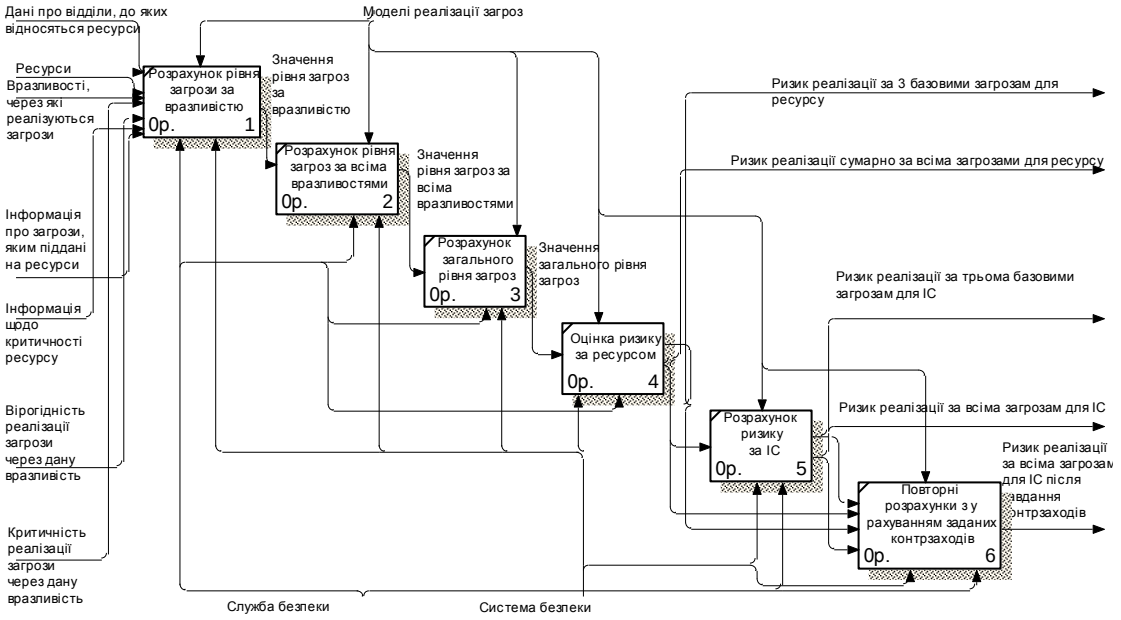


Рис. 1.18. **Декомпозиція моделі оцінювання ризику реалізації загроз**

Для оцінювання економічного збитку під час реалізації загрози в телекомунікаційних системах пропонують використовувати узагальнену картку експерта-аналітика із захисту інформації, що дозволяє визначити найбільш уразливі місця, оцінити ризики та виробити комплекс заходів для забезпечення безпеки даних (табл. 1.1). Під час використання картки експерта-аналітика вважають, що середній показник захищеності телекомунікаційних систем Y_1 = 5, тобто вони належать до систем зі ступенем вихідної захищеності.

Таблиця 1.1

Картка оцінки загроз безпеки телекомунікаційних систем

Назви загрози	Y_2	Y		Методи протидії	
				технічні	організаційні
1	2	3	4	5	6
Загрози навмисного електромагнітного впливу на її елементи	5	0,5	Середня	Екранування будинків і приміщень, ТЗ	Видалення від мережі контрольованої зони
Загрози витоку по технічних каналах	5	0,5	Середня	Генератор шуму за ланцюгом електроживлення генератори просторового зашумлення	Інструкції користувача та адміністра-тора безпеки; технологічний процес оброблення; акт встановлення засобів захисту; виключення електричних ліній, які виходять за межі контрольованої зони ліній; розміщення трансформаторної підстанції в контрольованій зоні; контур заземлення
Загрози несанкціонованого доступу до інформації					
Загрози знищення, розкрадання апаратних засобів носіїв інформації шляхом фізичного доступу до них	2	0,35	Середня	Охоронна сигналізація; ґрати на вікна; металеві двері; кодовий замок; шифрування даних; охоронна сигналізація; зберігання в сейфі коштовних ресурсів; шифрування даних	Пропускний режим; охорона; акт установлення засобів захисту; облік носіїв інформації; інструкції користувача та адміністратора безпеки
Загрози розкрадання, несанкціонованої модифікації або блокування інформації за рахунок НСД із застосуванням програмно-апаратних і програмних засобів	10	0,75	Висока	Антивірусне ПЗ; настроювання засобів захисту; захист приміщення	Інструкція користувача; інструкція адміністратора безпеки; технологічний процес оброблення; інструкція з антивірусного захисту; акт встановлення засобів захисту; апломбування; сертифікація

Закінчення табл. 1.1

1	2	3	4	5	6
Загрози ненавмисних дій користувачів і порушень безпеки функціонування ВПБС, через перебої у програмному забезпеченні, а також від загроз (перебоїв апаратури та електроживлення) і стихійного (ударів блискавок, пожеж, повеней і т.ін.) характеру	10	0,75	Середня	Настроювання засобів захисту; доступ до встановлення режимів роботи засобів захисту надано тільки адміністратору безпеки; використання джерел безперебійного електроживлення; пожежна сигналізація; система захисту від НСД	Інструкція користувача; інструкція адміністратора безпеки; резервне копіювання; акт установлення засобів захисту; дозвільна система допуску; технологічний процес оброблення; договір про не розголошення банківської інформації
Загрози несанкціонованого доступу каналами зв'язку	10	0,75	Висока	Міжмережний екран	Технологічний процес; інструкція користувача та адміністратора безпеки; акт установлення засобів захисту
Загрози перехоплення під час передавання провідними (кабельними) лініями зв'язку	10	0,75	Висока	Шифрування; фізичний захист каналу зв'язку	Пропускний режим; технологічний процес

На підставі імовірностей загроз безпеки інформації (визначаються експертами-аналітиками) розраховують можливість її реалізації за такою формулою:

$$Y = \frac{Y_1 + Y_2}{20},$$

де Y_1 – ступінь вихідної захищеності системи: 0 – для високої, 5 – для середньої, 10 – для низького ступеня вихідної захищеності;

Y_2 – імовірність реалізації загрози: 0 – для малоймовірної загрози; 2 – для низької імовірності загрози; 5 – для середньої імовірності загрози; 10 – для високої імовірності загрози.

Y – можливість реалізації загрози: $0 < Y < 0{,}3$ – низька; $0{,}3 < Y < 0{,}6$ – середня; $0{,}6 < Y < 0{,}8$ – висока; $Y > 0{,}8$ – дуже висока.

1.10. Оцінювання ризику реалізації загроз у комунікаційних системах

Пропонують використовувати таку методику.

На першому етапі розраховують **рівень загрози за уразливістю *Th*** на основі критичності та можливості реалізації загрози через цю вразливість. Рівень загрози показує, наскільки критичним є вплив цієї загрози на ресурс із урахуванням імовірності її реалізації.

$$Th_{c,I,a} = \frac{ER_{c,I,a}}{100} P(V)_{c,I,a},$$

де $ER_{c,I,a}$ – критичність реалізації загрози (%);

$P(V)_{c,I,a}$ – можливість реалізації загрози через цю вразливість.

Під **критичністю реалізації загро*зи* (*ER*)** розуміють ступінь впливу реалізації загрози на ресурс, тобто як сильно реалізація загрози вплине на роботу ресурсу, вона складається із критичності реалізації загрози за конфіденційністю, цілісністю та доступністю (*Erc, Eri, Era*). Обчислюють одне або три значення, залежно від кількості базових послуг безпеки. Знаходять значення рівня загрози за вразливістю в інтервалі від 0 до 1. Під *базовими послугами безпеки* розуміють порушення конфіденційності, автентичності та цілісності даних.

На другому етапі розраховують **рівень загрози за всіма вразливостям*и* *Cth***, через які можлива реалізація цієї загрози на ресурсі однією з формул, залежно від кількості використовуваних базових послуг у ВПБС:

для режиму з однією базовою послугою безпеки:

$$CTh = 1 - \prod_{i=1}^{n} (1 - Th);$$

для режиму із трьома базовими послугами безпеки:

$$CTh_c = 1 - \prod_{i=1}^{n} (1 - Th_c);$$

$$CTh_i = 1 - \prod_{i=1}^{n} (1 - Th_i);$$

$$CTh_a = 1 - \prod_{i=1}^{n} (1 - Th_a).$$

Значення *рівня* загрози за всіма вразливостями перебуває в інтервалі від 0 до 1.

Аналогічно розраховують **загальний рівень загроз за ресурсом *Cthr*** (ураховуючи всі загрози, що діють на ресурс):

для режиму з однією базовою загрозою:

$$CThR = 1 - \prod_{i=1}^{n} (1 - Th);$$

для режиму із трьома базовими загрозами:

$$CThR_c = 1 - \prod_{i=1}^{n} (1 - Th_c);$$

$$CThR_i = 1 - \prod_{i=1}^{n} (1 - Th_i);$$

$$CThR_a = 1 - \prod_{i=1}^{n} (1 - Th_a).$$

Значення загального рівня загрози знаходять в інтервалі від 0 до 1.

На третьому етапі розраховується **ризик за ресурсом *R*** для режиму з однією базовою загрозою:

$$R = CThR \cdot D,$$

де *D* – критичність ресурсу (задається в грошах або у рівнях).

Під **критичністю ресурсу (*D*)** розуміють ступінь значущості ресурсу для інформаційної системи, тобто як сильно реалізація загроз інформаційної безпеки на ресурс вплине на роботу інформаційної системи.

Залежно від вибраного режиму роботи, він може складатися із критичності ресурсу за конфіденційністю, цілісністю та автентичністю, його визначають для режиму із трьома базовими послугами безпеки за такими формулами:

$$R_c = CThR_c \cdot D_c;$$
$$R_i = CThR_i \cdot D_i;$$
$$R_a = CThR_a \cdot D_a;$$

$$R = (1 - \prod_{i=1}^{3}(1 - \frac{R_i}{100})) \cdot 100.$$

де $D_{a,ci}$ – критичність ресурсу за трьома послугами безпеки;

R – сумарний ризик за трьома загрозами.

Таким чином, знаходять значення ризику за ресурсом у рівнях (заданих користувачем) або грошах.

На четвертому етапі розраховуємо **економічний ризик у ВПБС *CR*** для режиму з однією базовою загрозою (у грошах):

$$CR = \sum_{i=1}^{n} R_i ;$$

або для режиму роботи в рівнях:

$$CR = (1 - \prod_{i=1}^{n}(1 - \frac{R_i}{100})) \cdot 100.$$

Для режиму роботи із трьома загрозами (у грошах):

$$CR_{a,i,c} = \sum_{i=1}^{n} R_{ii} ;$$

$$CR = \sum_{i=1}^{3} CR_{a,i,c} ,$$

де $CR_{a,i,c}$ – ризик системи з кожного виду загроз;

CR – ризик системи сумарна за трьома видам загроз

або для режиму роботи в рівнях:

$$CR_{a,i,c} = (1 - \prod_{i=1}^{n}(1 - \frac{R_i}{100})) \cdot 100;$$

$$CR = (1 - \prod_{i=1}^{n}(1 - \frac{R_{i,a,c}}{100})) \cdot 100.$$

Таким чином, запропонлвана методика дозволяє оцінити економічний збиток під час реалізації загрози на ВПБС у ході використання, як окремих засобів захисту, так і під час комплексного забезпечення захисту банківських транзакцій. Для аналізу ефективності використання засобів захисту пропонують оцінити введений “контрзахід” *E* за виразом:

$$E = \frac{R_{old} - R_{new}}{R_{old}},$$

де R_{old} – значення ризику без обліку контрзаходу;

R_{new} – значення ризику з урахуванням заданого контрзаходу.

1.11. Приклад розрахунків ризику інформаційної безпеки у ВПБС

Розгляньмо розрахунки ризиків для однієї послуги інформаційної безпеки, оскільки для інших послуг ризик розраховують аналогічно на прикладі критичних систем управління комерційного банку.

Ресурсом є сервер, критичність якого оцінюють за шкалою від 0 до 100 % (рис. 1.19).

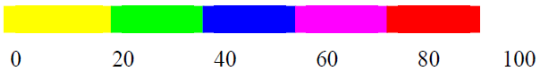


Рис. 1.19. **Шкала оцінки критичності ресурсу**

Критичність ресурсу визначають, відповідно до цінності збереженої в системі інформації, під **цінністю інформації** розуміють той позитивний ефект, який може бути отримано під час її використання на розглянутому інтервалі часу.

Обчисліть значення критичності сервера банку, що дорівнює 100 %, тому що втрата конфіденційної інформації, що перебуває на сервері, приводить до її втрати та відповідно руйнуванню всієї ВПБС загалому. Відповідно до розробленого алгоритму, роблять розрахунки під час виникнення різних загроз (табл. 1.2).

Таблиця 1.2

Загрози та вразливості у ВПБС

Загрози	Уразливості	P(V)	ER,%
1. Розкрадання апаратних засобів, носіїв інформації шляхом фізичного доступу до них	1. Відсутність регламенту доступу до приміщення з ресурсами, що містять банківську (конфіденційну) інформацію	0,35	70
	2. Наявна система спостереження охоплює не всі важливі об'єкти	0,35	70
2. Несанкціонований доступ каналами зв'язку	3. Відсутність міжмережного екрана	0,75	70
3. Перебій електроживлення	4. Відсутність джерела безперебійного електроживлення	0,75	40

Результати розрахунків оцінки ризику ресурсу наведено в табл. 1.3.

Таблиця 1.3

Результати розрахунків оцінки ризику ресурсу

Загроза/уразливість	Th	Cth	Cthr	R,%
Загроза 1/уразливість 1	0,245	0,43	0,8105	81,05
Загроза 1/уразливість 2	0,245			
Загроза 2/уразливість 3	0,525	0,525		
Загроза 3/уразливість 4	0,3	0,3		

Таким чином, ризик сервера, розрахований за моделлю загроз безпеки ВПБС і методикою оцінювання ризику реалізації загроз, становить 81,05 %, що свідчить про необхідність у вживанні комплексу заходів щодо забезпечення захисту цього сервера за допомогою відповідних криптографічних алгоритмів.

2. Основні принципи захисту інформації під час підключення до мережі інтернет

Для підключення мережі організації (будь-якої) до мережі інтернет необхідно вжити ряд певних організаційно-технічних заходів для її захисту.

Під час побудови системи захисту варто виходити з того, що будь-який захист ускладнює використання системи, що за прямим призначенням обмежує функціональні можливості, споживає обчислювальні та трудові ресурси, потребує фінансових витрат на створення та експлуа-

тацію. Чим надійніший захист, тим дорожчою в ході побудови та обслуговування стає система і тим менш зручною для безпосередніх користувачів.

Тому захищаючи мережу варто виходити з доцільної вартості захисту. Тобто витрати на захист мають бути пропорційні цінності ресурсу, що захищає. Є ряд основних принципів, що дозволяють організувати досить безпечне підключення до інтернет порівняно простими засобами.

2.1. Firewall (Брандмауер)

Основним загальновизнаним засобом такого захисту є міжмережевий екран (Брандмауер).

Міжмережевий екран установлюють між мережею та інтернет і він виконує роль мережевого фільтра (рис. 2.1).

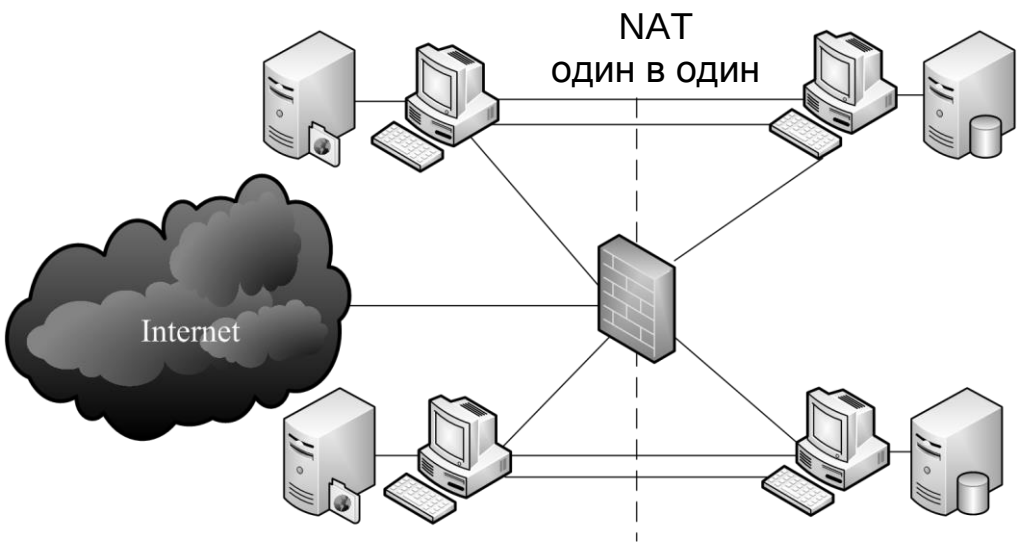


Рис. 2.1. **Установлення брандмауера в локальній мережі**

Його настроюють таким чином, щоб пропускати допустимий трафік від користувачів мережі до служб Internet і назад, і обмежити трафік із боку інтернет до мережі, яка потребує захисту, тільки необхідними службами, наприклад: smtp, dns, ntp.

Допустимість того або того трафіка визначено мережним адміністратором, відповідно до політики інформаційної безпеки організації. (Наприклад, може бути дозволено доступ із частини комп'ютерів мережі до web та ftp-серверів інтернеті двоспрямований доступ між інтернет та поштовим сервером, але водночас заборонено всі інші протоколи й напрямки трафіка).

Таким чином, міжмережевий екран фізично розташовують на місці мережного шлюзу (маршрутизатора), логічно є доцільним сполучити їхні функції в одному пристрої. Це дозволяє одним засобом захистити й локальну мережу і безпосередньо сам шлюз. Таку опцію передбачено для маршрутизаторів компанії Cisco Systems (Firewall Feature Set). Однак це правило є необов'язковим і міжмережний екран може бути подано окремим пристроєм.

У найпростішому випадку виконання функцій міжмережного екрана можна організувати за допомогою мережного фільтра на основі сторінокдоступу (access-lists). Сторінки доступу визначають правила, за якими або дозволено, або заборонено проходження трафіка з певними ознаками від одного мережного інтерфейсу маршрутизатора до іншого усередині самого маршрутизатора. Як ознаки можуть використовувати *IP*-адреси або діапазон, *IP-адреса* джерела й приймача, тип протоколу, номер порту призначення або відправлення, ряд інших службових ознак *IP*-пакета.

Відмінність і недолік сторінок доступу, порівняно із сучасним міжмережевим екраном полягає в тому, що вони дозволяють створити статичний однобічний фільтр, тоді як мережеве з'єднання становить динамічний процес. Сторінки доступу не дозволяють контролювати параметри *IP-пакета*, що залежать від попередніх пакетів. Звідси виникає складність застосування сторінок доступу для тонкого настроювання фільтрації трафіка в точній відповідності із прийнятою політикою безпеки. Зокрема, із цієї причини аркуші доступу не в змозі захистити від такого різновиду мережевої атаки, як "викрадення з'єднання", або "хай-джекінг".

У Firewall Feature Set зазначені проблеми вирішують за допомогою того, що він відстежує кожне мережне з'єднання окремо і контролює весь процес у динаміці. Під час встановлення нового TCP-сеансу міжмережевий екран створює для нього новий процес, що контролює правильність з'єднання до самого моменту його завершення. Д того ж кожний пакет на транспортному рівні перевіряють на відповідність попередньому, а всі "підозрілі" пакети відбраковують. Завдяки цьому стає можливим досить легко організувати фільтр для доступу внутрішнього комп'ютера до зовнішнього, але не дозволяє зовнішньому комп'ютеру самостійно звернутися до внутрішнього.

Інакше кажучи, у настроюваннях міжмережевого екрана задають правила для проходження трафіка від одного інтерфейсу до іншого, для кожного напрямку й кожного тракту окремо. Якщо правило дозволяє прохо-

дження *IP-пакета* від інтерфейсу внутрішньої мережі до інтернет-інтерфейсу, то на підставі такого пакета формується логічний тунель у маршрутизаторі, через який уже можуть пройти відповідні пакети від зовнішнього одержувача. Як тільки з'єднання закрите або вичерпано час очікування, тунель закривається, і обіг ззовні до внутрішнього комп'ютера буде відкинуто. Із цієї ж причини екран не пропустить пакети у зворотному напрямку, якщо ініціатором з'єднання є зовнішній комп'ютер.

Крім того, міжмережевий екран, на відміну від сторінок доступу, може контролювати зміст *IP-пакетів* у полі даних і відбраковувати пакети, що містять потенційно небезпечні коди, наприклад, java-апліти. Є міжмережеві екрани, здатні виявити в *IP-пакетах* ознаки відомих мережевих атак і перервати таке з'єднання, але це вже досить дорогі системи.

З найбільш дешевих систем слід зазначити *Firewall* на основі ядра операційної системи Linux версії 2.4.20 і вищої й засоби управління iptables. Через те що Linux є безкоштовною ОС, витрати на побудову такого міжмережевого екрана зведено до придбання звичайного персонального комп'ютера із двома мережевими інтерфейсами. Проте Linux дозволяє побудувати досить надійний і гнучкий мережевий фільтр, що розпізнає окремі прапорці у службових полях *IP-пакета*.

2.2. NAT

Другою цеглинкою забезпечення захищеності мережі є "заміна мережевої адреси" – Network Address Translation, або NAT. Вона становить заміну в *IP-пакеті* реальної адреси комп'ютера внутрішньої мережі на будь-яку іншу задану адресу під час посилання його в зовнішню мережу. Завдяки цьому для внутрішньої мережі стає можливим використання діапазонів адрес, які не застосовують в інтернет (наприклад, 10.0.0.0 – 10.255.255.255). Це дозволяє запобігти прямому обігу ззовні до внутрішніх комп'ютерів і приховує структуру мережі. Є кілька різновидів NAT.

Найпростіша й найбільш марна з погляду захисту – це трансляція фіксованої внутрішньої адреси у фіксовану зовнішню. До того ж противник безперешкодно "бачить" такий комп'ютер у зовнішній мережі, тому що йому однозначно відповідає певна зовнішня адреса. Однак вона необхідна під час організації сервера, до якого потрібно забезпечити доступ ззовні (рис. 2.2).

Друга форма NAT – це трансляція групи внутрішніх адрес в одну зовнішню. У цьому разі всі внутрішні комп'ютери можуть працювати з

Internet одночасно, а маршрутизатор розрізняє, кому яка відповідь перетрансльовується за службовими даними *TCP*-з'єднання. У зовнішній мережі створюється враження, що до неї звертається тільки один комп'ютер. Така заміна істотно ускладнює життя противнику, тому що повністю приховує внутрішні комп'ютери й перешкоджає "обчисленню" жертви (рис. 2.3). Противник, навіть бачачи трафік, що виходить із внутрішньої мережі, не може визначити, від якого комп'ютера він виходить.

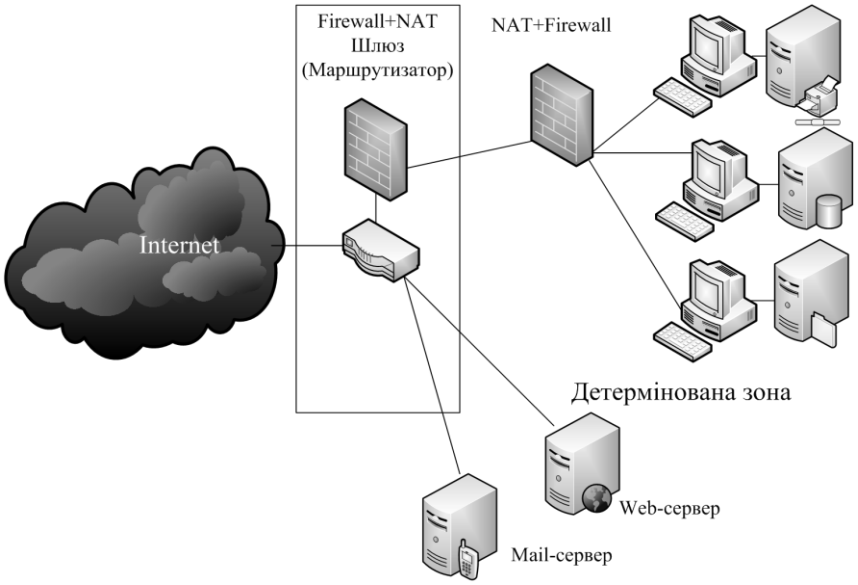


Рис. 2.2. **Трансляція фіксованої внутрішньої адреси у фіксовану зовнішню**

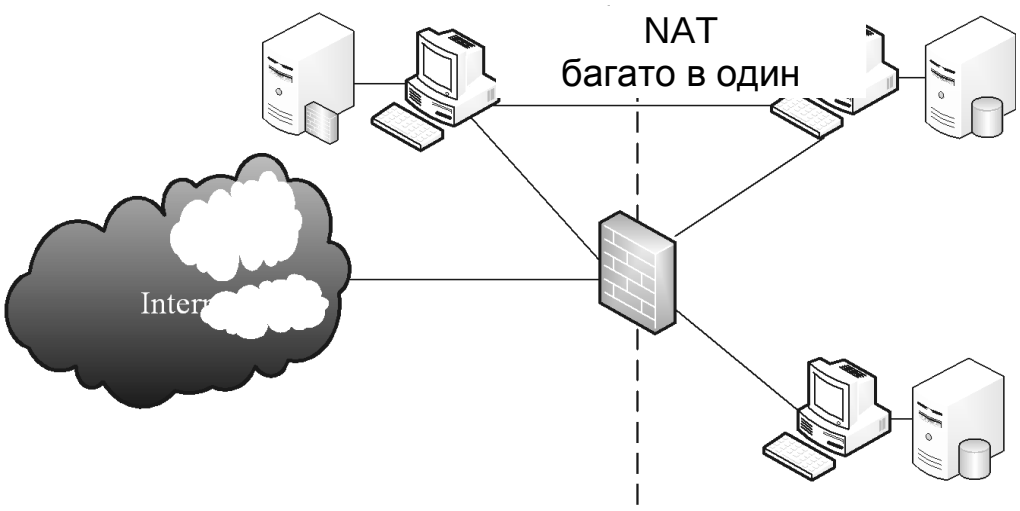


Рис. 2.3. **Трансляція групи внутрішніх адрес в одну зовнішню**

Крім того, це виключає можливість ініціативного обігу ззовні до внутрішнього комп'ютера, тому що для маршрутизатора в цьому разі відсутнє

правило прив'язування зовнішньої адреси до внутрішньої. Зокрема виключено можливість сканування іззовні внутрішньої мережі.

Третя форма NAT – це використання для заміни внутрішніх адрес не однієї адреси, а будь-якої з виділених адрес, тобто, внутрішній комп'ютер, виходячи в інтернет, отримує вільну в цей момент адресу з бази даних (БД). Водночас адреси підмінюють динамічно, і кожне нове *TCP*-з'єднання може бути встановлено з іншою *IP-адресою*. Це також створює додаткові труднощі противнику, тому що позбавляє його можливості атакувати будь-який внутрішній комп'ютер прицільно. Сказане щодо другої форми NAT є справедливим і для третьої форми. Якщо запит приходить іззовні, то маршрутизатор не в змозі зв'язати адресу із БД з адресою мережі. Тому такий запит не досягне мети.

2.3. Демілітаризована зона

Переважно, організації потрібно мати в себе деякі мережеві ресурси, до яких відкритий доступ з Internet. Звичайно це поштовий, dns- і web-сервери. Механізм їхньої роботи допускає, що до них має бути дозволено вільний або слабко обмежений обіг з інтернет. Відповідно імовірність їхнього зламу вища, ніж інших комп'ютерів мережі. Із цієї причини розміщати їх усередині зони, яку захищено, недоцільно з погляду безпеки, тому що в разі зламу вони можуть стати воротами для атаки внутрішніх комп'ютерів. Для мінімізації ризику і збереження функціональності такі сервери встановлюють за основним шлюзом мережі, але перед міжмережевим екраном, що забезпечує захист внутрішніх комп'ютерів. Логічну область їхнього розміщення називають **демілітаризованою зоною** (рис. 2.4).

2.4. Другий firewall

Із рис. 2.5 видно, що ніщо не заважає встановити другий Firewall на основному шлюзі мережі. Це є логічним рішенням і дозволяє одночасно підвищити рівень захисту внутрішньої мережі й захистити сервери демілітаризованої зони. У разі правильного настроювання обох міжмережевих екранів противнику буде вже набагато сутужніше дістатися до внутрішньої мережі організації. Наявність другого міжмережевого екрана ускладнює конфігурування мережевого устаткування й настроювання роботи всіх елементів мережі. Для додаткового підвищення захищеності можна використати Firewall-и різних виробників. Тоді якщо в одному з них

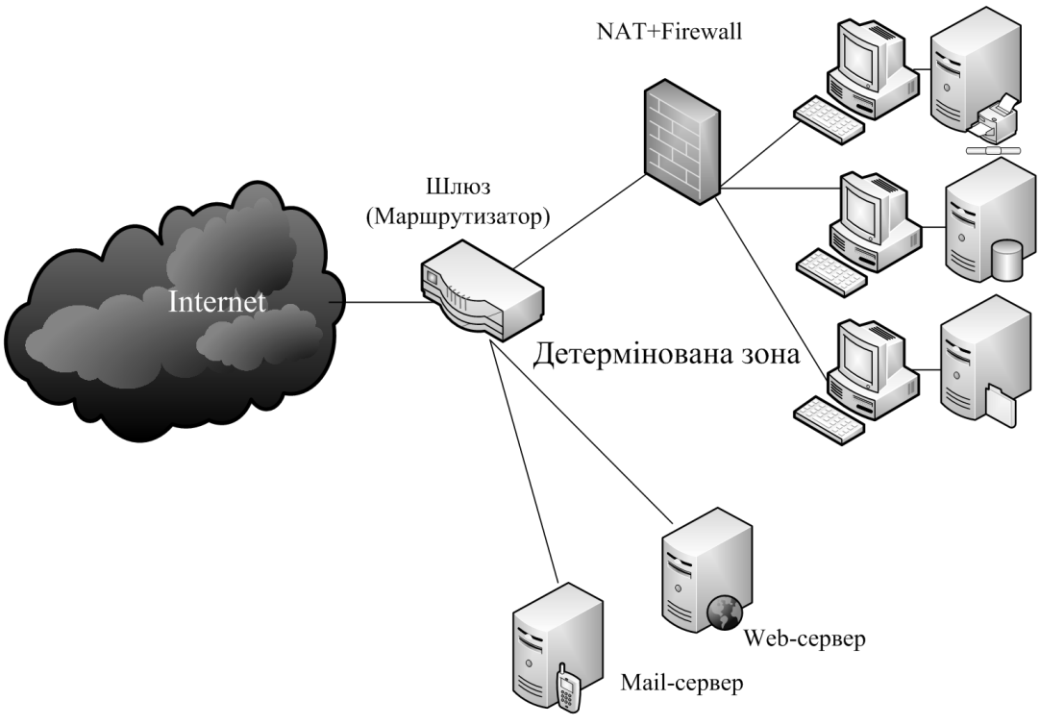


Рис. 2.4. **Демілітаризована зона**

буде виявлено вразливість, інший не дозволить противнику безперешкодно проникнути в мережу, як це мало б місце під час використання Firewall-ів одного типу.

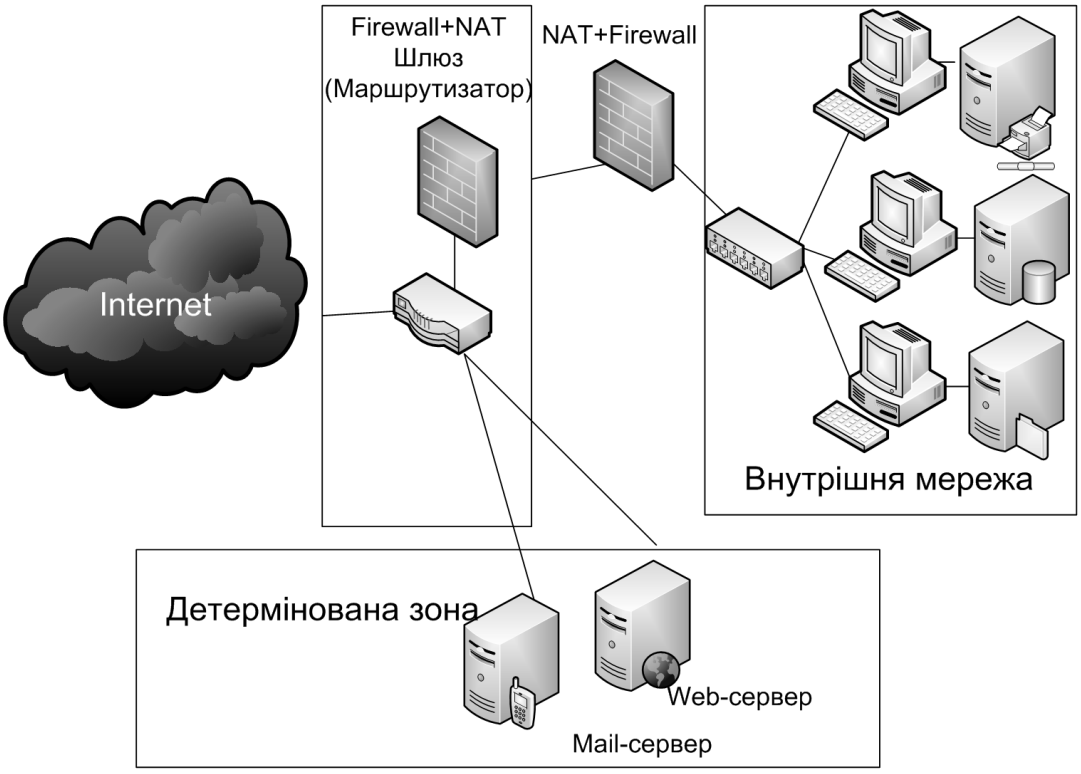


Рис. 2.5. **Локально-консольний порт для серверів**

Особливо варто підкреслити, що можливість мережевого доступу до шлюзів і до міжмережевих екранів, щоб уникнути зловмисного використання, має бути виключена. Із погляду безпеки пристрої, які перебувають на варті мережі, мають конфігурувати й адмініструвати тільки через консольний порт локально (рис. 2.5).

Схему, запропоновану на рис. 2.5, може бути дещо вдосконалено. Для цього необхідно використати граничний маршрутизатор із двома Ethernet-портами (рис. 2.6).

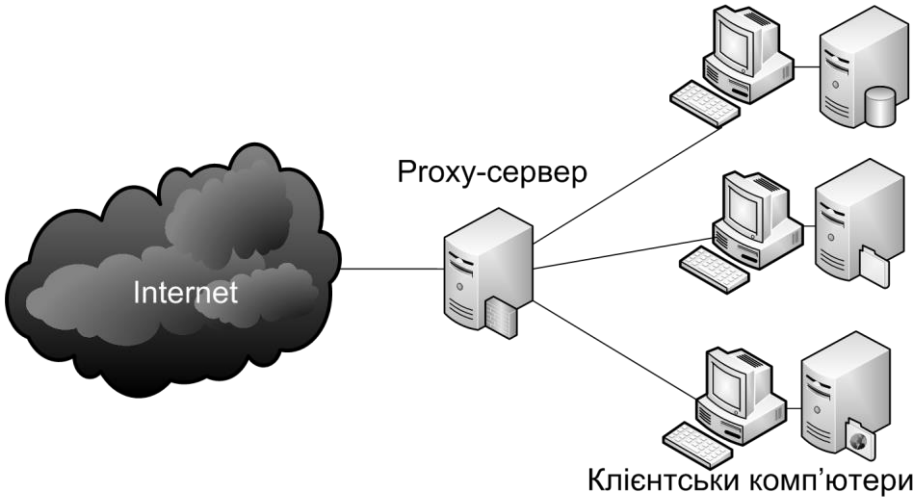


Рис. 2.6. **Proxy-сервер**

2.5. Proxy-сервер

Використання так званого "посередника" (*Proxy-сервера*) також підвищує рівень захищеності мережі, тому що виключає необхідність у прямому виході в інтернет комп'ютерів користувачів. Водночас також стає можливим більш суворий контроль за даними в *IP-пакетах* на рівні мережевих додатків. *Proxy-сервер* працює як посередник між додатком користувача і вилученим мережевим ресурсом в інтернет. Схематично сутність його роботи показано на рис. 2.6.

Proxy-сервер складається ніби із двох частин, клієнтської та серверної. Клієнтська частина дивиться в бік інтернет, серверна – в бік клієнтського комп'ютера. Коли клієнтський комп'ютер звертається до вилученого сайту через *Proxy-сервер*, його клієнтський мережевий додаток взаємодіє із серверною частиною *Proxy-сервера*.

Водночас *Proxy-сервер* на рівні додатка передає клієнтський запит своєї клієнтської частини, і вона вже від імені *Proxy-сервера* надсилає цей

запит на вилучений сайт. Тобто відправлений *IP*-пакет має адресу *Proxy-сервера*.

Потім отриману відповідь передають у зворотний бік від клієнтської частини *Proxy-сервера* його серверної частини, із якою безпосередньо взаємодіє комп'ютер користувача. Таким чином, пряме з'єднання клієнтських комп'ютерів з вилученим сайтом виключено. Усередині *Proxy-сервера* передавання даних між клієнтською частиною й серверною відбувається вже не на транспортному рівні, а на рівні протоколу додатка, цим забезпечено легкість контролю команд і даних на відповідність установленим стандартам. Крім того, це дозволяє забезпечити досить надійний контроль за передавання зловмисних кодів усередині даних. Навіть у разі успішної атаки з боку інтернет за відкритими протоколами у цьому випадку буде ушкоджено тільки *Proxy-сервер*, що не становить інформаційну цінність, а комп'ютери користувачів будуть залишатися в безпеці ще якийсь час.

Через те що *Proxy-сервер* працює тільки за декількома відомими протоколами (HTTP, FTP та ін.) і не пропускає через себе інші пакети, він сильно обмежує можливості противника з використання мережних "троянських коней" для закріплення на будь-якому з користувальницьких комп'ютерів.

Залишати *mail-сервер* у демілітаризованій зоні з одного боку небажано, тому що на ньому фактично зберігається поштова база даних із перепискою локальних користувачів, а демілітаризована зона не може забезпечити належного рівня захисту мережевим ресурсам. З іншого боку, якщо сховати *mail-сервер* усередині локальної мережі, то він або не зможе взаємодіяти із зовнішнім середовищем, або буде становити ворота із зовнішнього середовища у внутрішню локальну мережу, якими потенційно зможе скористатися противник.

Унаслідок цього доречним рішенням є використання двох поштових серверів. Основний сервер установлюють усередині мережі, яка захищена, і його не видно для зовнішнього світу. Усі локальні користувачі поштової системи заводять на нього і мають до нього прямий доступ. Відповідно, уся вхідна кореспонденція зберігається на ньому в поштових скриньках локальних користувачів. Відправлення електронної пошти також здійснюють через нього.

Другий, або зовнішній, поштовий сервер установлюють у демілітаризованій зоні, він забезпечує взаємодію *e-mail* з інтернет. Його настро-

ють таким чином, щоб усю пошту, що приходить на ім'я користувачів організації, відразу пересилати на внутрішній поштовий сервер. У такий спосіб у його поштовій базі даних немає ні одного облікового запису користувачів організації і жодну сторінку не відкладають для довгострокового зберігання. Тому якщо він виявиться зламаним зловмисником, то противник не дістане доступу до накопиченої переписки. Проте після зламу противник дістає можливість перехоплення й читання транзитної пошти. Тому потрібен ретельний контроль за подібною ситуацією й негайне вживання заходів за підозри на несанаційнований доступ (НСД).

Перевагою такої схеми є те, що навіть зі зламаного зовнішнього поштового сервера не так просто дістатися до внутрішньої захищеної мережі. Обмін даними між зовнішніми та внутрішнім поштовими серверами відбувається через міжмережний екран із єдиним дозволеним портом (SMTP) за єдиною дозволеною парою адрес. Звертання до інших комп'ютерів і за іншими протоколами буде заблоковано. Тому впливати з нього прямо на комп'ютери користувачів внутрішньої мережі неможливо.

2.7. Антивірусний захист поштової системи

Операційна система Windows дуже вразлива перед деякими різновидами поштових вірусів. Користувачу буває достатньо встановити покажчик на інфікований конверт, щоб вірус активізувався. Але більш небезпечним є те, що механізм роботи поштових вірусів може бути використано зловмисником для закидання в область мережевого "троянського коня", якими захищається. Він дозволить противнику таємно скачувати дані з вашої мережі та здобути всю інформацію, що цікавить. Тому забезпеченню антивірусного захисту тракту доставлення пошти у внутрішню мережу варто приділити досить серйозну увагу.

Є ряд програмних засобів, призначених для контролю за кореспонденцією на поштових серверах щодо наявності в ній вірусів у процесі приймання й пересилання електронної пошти.

Принцип її роботи полягає в тому, що всю пошту, що проходить через сервер, спочатку переспрямовують спеціальному користувачеві, роль якого виконує антивірусний процес. Він сканує зміст кожної сторінки на наявність у ньому фрагментів відомих вірусів. Якщо сторінка містить щось схоже на вірус, його вилучають із процесу передавання й, залежно від настроювань антивірусу, піддають заданій обробці. Повідомлення про виявлений вірус відсилають відправнику й одержувачу інфікованої сторінки, а також на ім'я

зазначених адміністраторів системи. Після перевірки сторінки, що не викликають підозри, відсилають за призначенням.

Тим самим на рівні поштового сервера ставлять надійний захист відомим вірусам в електронній пошті. Через те що антивірусна програма розпізнає тільки віруси, сигнатури яких перебувають у її базі даних, необхідно регулярно обновляти антивірусну базу даних з офіційного сайту. Інакше мережа може стати вразливою для знову створених вірусів.

2.8. Log-сервер

Log-сервер – це загальновідомий механізм протоколювання системних подій на серверах і клієнтських робочих станціях. Розроблювачі програмного забезпечення включають у свої продукти фрагменти коду, які на ту або ту подію генерують відповідні текстові повідомлення, що посилають операційній системі. Система збирає дані повідомлення в log-файлах, які потім можуть аналізуватися адміністратором або користувачем, із метою з'ясування, які події відбувалися в системі деякий час потому. Це дозволяє, наприклад, з'ясувати, чому не запускається та або та програма, або чому припинив функціонувати певний сервіс. Дуже корисні log-файли для пошуку слідів зламу системи й відвідування її несанкціонованими гостями. Через те що злам, переважно, супроводжено безліччю заборонених дій, це породжує велику кількість системних повідомлень, що осідають у log-файлах. Через це противник завжди прагне стерти сліди своєї присутності, або видаливши log-файли, або їх підчистивши. В обох випадках адміністратору після цього буде важко зрозуміти, що ж відбулося в системі насправді: яким чином у неї проникли, як довго в ній перебували, перш ніж встигли покористуватися. Або навіть просто переконатися, що все добре.

Тому обов'язковою умовою для мережі, підключеної до інтернет, є наявність у ній окремого *Log-серв*ера.

Принцип його роботи полягає в тому, що кожна операційна система може посилати повідомлення про системні події за UDP-протоколом на вилучений сервер. Це можуть робити також маршрутизатори й міжмережеві екрани. Збираючи такі повідомлення на спеціально виділеному сервері, забезпечують їм схоронність від рук противника. Тому для мінімізації імовірності зламу *Log-сервер* має бути призначено тільки для збирання log-повідомлень. Він не має виконувати будь-яких інших функцій і виконувати інші мережеві додатки, крім syslogd. У цьому разі після зламу будь-яких

комп'ютерів мережі на *Log-сервері* залишаться відповідні повідомлення, знищити які противник уже не зможе.

Таким чином, у результаті найбільш оптимальної є така схема підключення локальної мережі до інтернет (рис. 2.7).

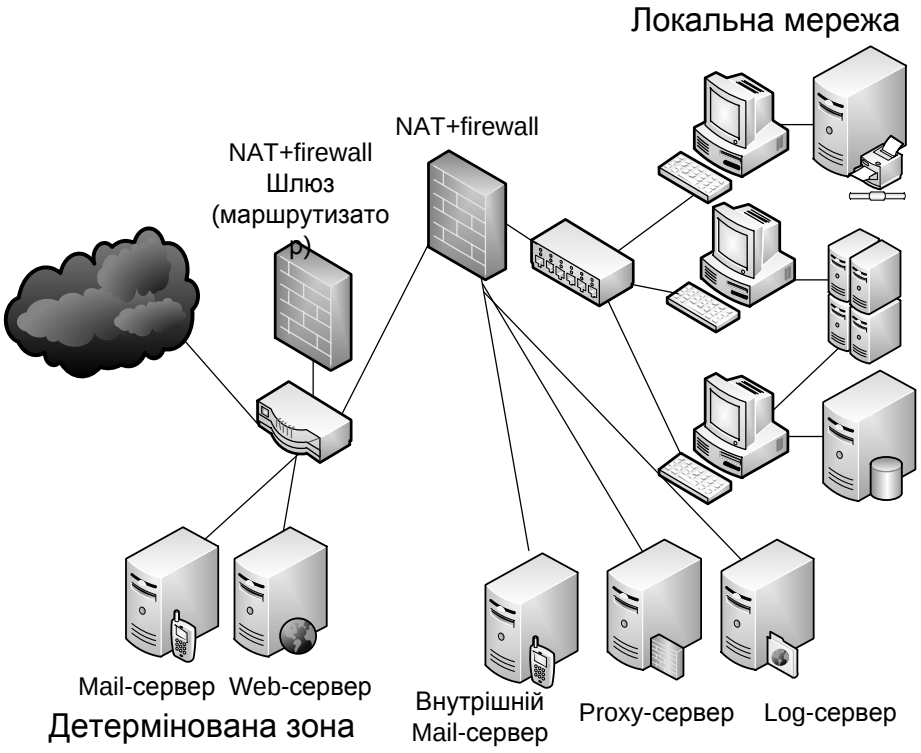


Рис. 2.7. **Схема з Log-сервером**

Таким чином, зроблений аналіз способів захисту комп'ютерних мереж під час підключення їх до глобальної мережі інтернет показав, що для забезпечення захисту під час обміну інформацією абоненти локальної мережі мають використовувати принципи й засоби безпеки в комплексі з організаційними заходами. Це дозволить надійно захистити від атак як активних, так і пасивних противників.

3. Виконання завдання

3.1. Графічне завдання

Розробіть за допомогою Packet Tracer структурну схему побудови корпоративної мережі компанії.

У корпоративній мережі компанії, що розташовується у двох будинках (4 поверхи та 2 поверхи, відповідно), кількість комп'ютерів і мережеві технології визначено в табл. 3.1.

Таблиця 3.1

Кількість ПК і мережеві технології

№ варіанта	Кількість комп'ютерів 1-й будинок	Мережеві технології	Кількість комп'ютерів 2-й будинок	Мережеві технології
1	8	Ethernet	6	FDDI
2	10	100AnyLAN	4	WiFi
3	6	Token Ring	8	Fast Ethernet
4	12	WiFi	12	Token Ring
5	14	Ethernet	14	WiFi
6	20	100AnyLAN	16	Token Ring
7	8	Fast Ethernet	20	100AnyLAN
8	6	Ethernet	8	FDDI
9	4	100AnyLAN	10	WiFi
10	8	Token Ring	6	Fast Ethernet
11	12	WiFi	12	Token Ring
12	14	Ethernet	14	WiFi
13	16	100AnyLAN	20	Token Ring
14	20	Fast Ethernet	8	100AnyLAN
15	8	Ethernet	6	FDDI
16	10	100AnyLAN	4	WiFi
17	6	Token Ring	8	Fast Ethernet
18	12	WiFi	12	Token Ring
19	14	Ethernet	14	WiFi
20	20	100AnyLAN	16	Token Ring
21	8	Fast Ethernet	20	100AnyLAN
22	6	Token Ring	8	Fast Ethernet
23	12	WiFi	12	Token Ring
24	14	Ethernet	14	WiFi
25	20	100AnyLAN	16	Token Ring

Розробіть структурну схему захисту корпоративної мережі компанії, обґрунтуйте та запропонуйте необхідні протоколи каналів зв’язку і програмно-апаратні засоби для забезпечення конфіденційного обміну інформацією між користувачами другого будинку; забезпечте надійний захист під час входу користувачів до мережі інтернет. Програмно-апаратні засоби забезпечення безпеки під час підключення до інтернет наведено в табл. 3.2.

Таблиця 3.2

Програмно-апаратні засоби забезпечення безпеки під час підключення до інтернет

№ варіанта	Програмне забезпечення	№ варіанта	Програмне забезпечення
1, 3, 5, 19	NAT-2, Proxy-сервер	8, 10, 12, 22	Демілітаризована зона, NAT-3
2, 4, 6, 20	Демілітаризована зона, Log-сервер	13, 15, 17, 23	2 Mail-сервери, NAT-1
7, 9, 11, 21	NAT-1 + Firewall, Proxy-сервер	14, 16, 18, 24, 25	Log-сервер, Proxy-сервер

3.2. Розрахункове завдання

Проведіть розрахунки ризику інформаційної безпеки при підключенні до мережі та можливості проведення активної (пасивної) атаки.

Варіант завдання для кожного студента визначається у відповідності за номером у Журналі академічної групи.

Рекомендована література

1. Вимоги до оформлення курсових і дипломних проєктів: методичні рекомендації для студентів галузі знань 12 "Інформаційні технології" / уклад. А. А. Гаврилова, С. П. Євсеєв, Г. П. Коц та ін. – Харків : ХНЕУ ім. С. Кузнеця, 2018. – 49 с.

2. Постников В. М., Спиридонов С. Б. Методы выбора весовых коэффициентов локальных критериев / В. М. Постников, С. Б. Спиридонов, 2016. – М. : *Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана".* – Вып. 3. – С. 267 – 287.

3. The development of the method of multifactor authentication based on hybrid crypto-code constructions on defective codes / S. Yevseiev at al., Восточно-европейский журнал передовых технологий, 2017. – № 5/9(89). – С. 19 – 36.

4. Банк данных угроз безопасности информации. [Электронный ресурс]. – Режим доступа: http://bdu.fstec.ru/vul.

5. Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України, [Електронний ресурс]: Постанова НБУ від 28.09.2017р. № 95. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/en/v0095500-17/page.

Додатки

Додаток А

Символи кирилиці (альтернативна кодова таблиця ASCII)

Символи	Десяткові	Двійкові	Символи	Десяткові	Двійкові
А	192	11000000	б	225	11100001
Б	193	11000001	в	226	11100010
В	194	11000010	г	227	11100011
Г	195	11000011	д	228	11100100
Д	196	11000100	е	229	11100101
Е	197	11000101	ж	230	11100110
Ж	198	11000110	з	231	11100111
З	199	11000111	и	232	11101000
И	200	11001000	й	277	11101001
Й	201	11001001	к	234	11101010
К	202	11001010	л	235	11101011
Л	203	11001011	м	236	11101100
М	204	11001100	н	237	11101101
Н	205	11001101	о	238	11101110
О	206	11001110	п	239	11101111
П	207	11001111	р	240	11110000
Р	208	11010000	с	241	11110001
С	209	11010001	т	242	11110010
Т	210	11010010	у	243	11110011
У	211	11010011	ф	244	11110100
Ф	212	11010100	х	245	11110101
Х	213	11010101	ц	246	11110110
Ц	214	11010110	ч	247	11110111
Ч	215	11010111	ш	248	11111000
Ш	216	11011000	щ	249	11111001
Щ	217	11011001	ъ	250	11111010
Ъ	218	11011010	ы	251	11111011
Ы	219	11011011	ь	252	11111100
Ь	220	11011100	э	253	11111101
Э	221	11011101	ю	254	11111110
Ю	222	11011110	я	255	11111111
Я	223	11011111	пробел	32	00100000
а	224	11100000			

Додаток Б

Алгоритм шифрування ДСТУ 28147-89

Міждержавний стандарт шифрування ДСТУ 28147-89 передбачає 4 режими роботи:

- режим простої заміни;
- режим гамування;
- режим гамування зі зворотним зв'язком;
- режим вироблення імітовставки.

Проста заміна

Режим простої заміни є основою для всіх інших режимів. Довжина блока – 64 біти, довжина ключа – 256 бітів, кількість підключів – 32, довжина підключа – 32 біти, кількість циклів – 32.

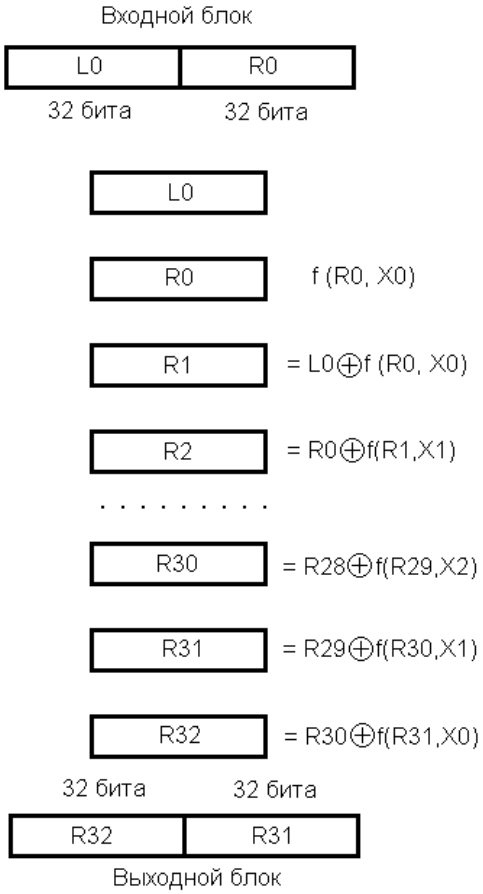
Відкриті дані, що підлягають зашифруванню, розподіляють на 64-бітові блоки, які обробляють незалежно один від одного (оскільки блоки даних шифрують, незалежно один від одного, під час зашифрування двох однакових блоків відкритого тексту виходять однакові блоки шифротекста і навпаки). Схему оброблення 64-бітного блоку показано на рис. А1 і А2.

Процедура шифрування 64-бітного блока включає 32 цикли. У кожному циклі використовують свій підключ, який виробляють з основного ключа. Розмір масиву відкритих або зашифрованих даних, що піддається, відповідно, зашифруванню або розшифруванню, має бути кратний 64 бітам, після виконання операції розмір визначеного масиву даних не змінюється.

Режим *простої заміни* застосовують для шифрування короткої, ключової інформації.

У режимах гамування виробляють гаму шифру блоками по 64 біти із застосуванням ДСТУ у режимі простої заміни. У першому режимі гама не залежить від шифрованих даних, у другому – залежить від шифроблоків.

Режим вироблення імітовставки призначено для виявлення випадкових або навмисних спотворень даних. Імітовставку виробляють (за допомогою перших 16 циклів ДСТУ у режимі простої заміни) із відкритих даних та ключа і додають при передаванні каналом зв'язку до блоків зашифрованих даних.



де ⊕ – складання за модулем 2.

Рис. А1. **Алгоритм шифрування ДСТУ 28147-89 (режим простої заміни)**

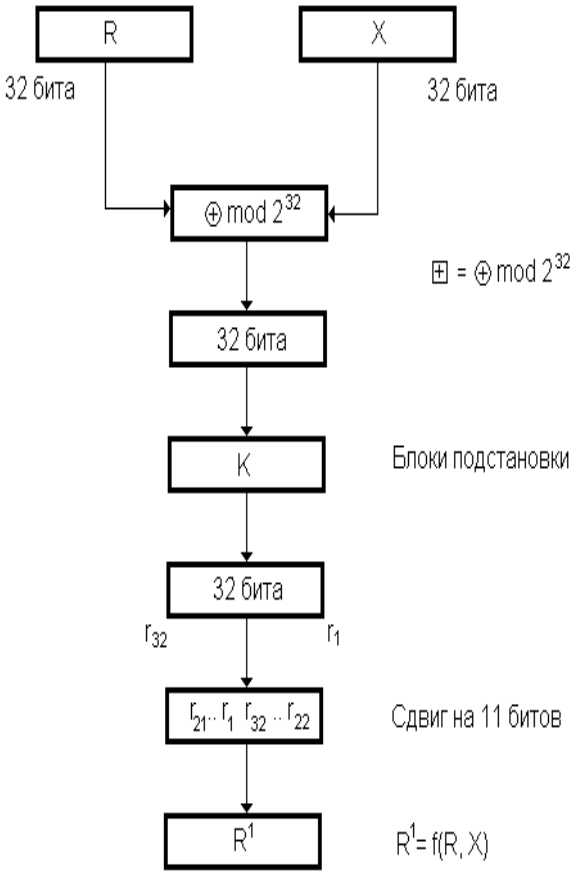


Рис. А2. **Функція перетворення *f(R,X)* в алгоритмі ДСТУ 28147-89**

Додаток В

Блок підстановки в алгоритмі шифрування ДСТУ 28147-89

	8	7	6	5	4	3	2	1
0	1	13	4	6	7	5	14	4
1	15	11	11	12	13	8	11	10
2	13	4	10	7	10	1	4	9
3	0	1	0	1	1	13	12	2
4	5	3	7	5	0	10	6	13
5	7	15	2	15	8	3	13	8
6	10	5	1	13	9	4	15	0
7	4	9	13	8	15	2	10	14
8	9	0	3	4	14	14	2	6
9	2	10	6	10	4	15	3	11
10	3	14	8	9	6	12	8	1
11	14	7	5	14	12	7	1	12
12	6	6	9	0	11	6	0	7
13	11	8	12	3	2	0	7	15
14	8	2	15	11	5	9	5	5
15	12	12	14	2	3	11	9	3

Приклад. Нехай 32-бітна послідовність має такий вигляд:

1001	1011	1100	0101	1110	0100	0000	1001

Розподіліть вхідну послідовність на 8 блоків по 4 біти. Шостий блок 1100 пропускайте через 6-й вузол підстановки за таким правилом: перетворіть двійкове число 1100 до десяткового вигляду – 12. Заповнення 12-го рядка для 6-го вузла підстановки дорівнює 9, що у двійковому вигляді є 1001. Таким чином, 4-бітний блок 1100 замінено на 1001. Решта блоку замінюють аналогічно.

8	7	6	5	4	3	2	1	номер вузла
1001	1011	1100	0101	1110	0100	0000	1001	вхід
9	11	12	5	14	4	0	9	адреса
2	7	9	15	5	10	14	11	заповнення
0010	0111	1001	1111	0101	1010	1110	1011	результат

Вихідна послідовність має такий вигляд:

010	111	001	111	101	010	110	011

Додаток Г

Алгоритм шифрування RSA

Алгоритм шифрування RSA належить до криптографічних систем із відкритим ключем. Криптосистеми з відкритим ключем (асиметричні криптосистеми) було розроблено у 2-й пол. 1970-х рр. В асиметричних криптосистемах процедури прямого і зворотнього криптоперетворень виконують на різних ключах і не мають між собою очевидних і легко простежуваних зв'язків, які дозволяють за одним ключем визначити інший. У такій схемі знання тільки ключа шифрування не дозволяє розшифрувати повідомлення, тому він не є секретним елементом шифру і його зазвичай публікує учасник обміну для того, щоб будь-який бажаючий міг послати йому шифрування повідомлення.

Принцип функціонування асиметричної криптосистеми полягає в такому:

- користувач А генерує два ключі – відкритий (незасекречений) і секретний та передає відкритий ключ по незахищеним каналам користувачу Б;
- користувач Б шифрує повідомлення, використовуючи відкритий ключ шифрування користувача А;
- користувач Б посилає зашифроване повідомлення користувачу А незахищеним каналом;
- користувач А отримує зашифроване повідомлення і дешифрує його, використовуючи свій секретний ключ.

Пари {відкритий ключ; секретний ключ} обчислюють за допомогою спеціальних алгоритмів, причому жоден ключ не може бути виведено з іншого.

Криптографічна система RSA (Rivest–Shamir–Adleman)

Авторами алгоритму RSA, запропонованого 1977 р., є Р. Ріверст (Rivest), А. Шамір (Shamir) і А. Адлеман (Adleman). Надійність алгоритму ґрунтується на складності факторизації (розкладання на множники) великих чисел і труднощах обчислення дискретних алгоритмів (знаходження x за відомих a, b і n із рівняння $a^x = b \pmod n$).

Алгоритм RSA складається із трьох частин: генерації ключів, шифрування та розшифрування.

1. Генерація ключів. Виберіть два великі різні прості числа p і q (натуральне число є простим, якщо воно ділиться тільки на себе та на 1) і знайдіть їхній добуток $n = pq$.

Обчисліть функцію Ейлера $\varphi(n)$ за такою формулою:

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

Алгоритм шифрування RSA

Закритий ключ d обирають з умов $d < \varphi(n)$ та d взаємно просто з $\varphi(n)$, тобто d і $\varphi(n)$ не мають загальних дільників.

Відкритий ключ e обирають з умов $e < \varphi(n)$ та $de = 1 (mod\ \varphi(n))$.

Остання умова означає, що різниця $(de - 1)$ має ділитися на $\varphi(n)$ без залишку. Для визначення числа e необхідно підібрати таке число k, що $(de - 1) = \varphi(n)\bullet k$.

В алгоритмі RSA (e, n) – відкритий ключ, (d, n) – секретний ключ.

2. Шифрування. Вхідне повідомлення розподіляють на блоки M_i однакової довжини. Кожен блок подають у вигляді великого десяткового числа, меншого n, і шифрують окремо. Шифрування блока M (M – десяткове число) здійснюють за такою формулою:

$$M^e = C\ (mod\ n),$$

де C – шифроблок, відповідний блоку відкритого повідомлення M. Шифроблоки поєднують в шифрограму.

3. Розшифрування. Під час розшифрування шифрограму розподіляють на блоки відомої довжини та кожен шифроблок розшифровують окремо за такою формулою:

$$C^d = M\ (mod\ n).$$

Додаток Д

Таблиця простих чисел

1	2	3	5	7
11	13	17	19	23
29	31	37	41	43
47	53	59	61	67
71	73	79	83	89
97	101	103	107	109
113	127	131	137	139
149	151	157	163	167
173	179	181	191	193
197	199	211	223	227
229	233	239	241	251
257	263	269	271	277
281	283	293	307	311
313	317	331	337	347
349	353	359	367	373
379	383	389	397	401
409	419	421	431	433
439	443	449	457	461
463	467	479	487	491
499	503	509	521	523
541	547	557	563	569
571	577	587	593	599

Додаток Е

Функція гешування

Функцією гешування (геш-функцією) називають перетворення даних, що переводять рядок бітів *M* довільної довжини в рядок бітів *h(M*) деякої фіксованої довжини (кілька десятків або сотень біт).

Геш-функція *h(M)* має задовольняти такі умови:

1) геш-функція *h(M)* має бути чутливою до будь-яких змін вхідної послідовності *M*;

2) для цього значення *h(M)* має бути неможливо знайти значення *M*;

3) для цього значення *h(M)* має бути неможливо знайти значення $M' \neq M$ таке, що $h(M') = h(M)$.

Ситуація, за якої для різних вхідних послідовностей *M*, *M'* збігаються значення їхніх геш-образів: *h(M) = h(M')*, називають колізією.

Під час побудові геш-образу вхідну послідовність *M* розподіляють на блоки M_i фіксованої довжини й обробляють по блоках за такою формулою:

$$H_i = f(H_{i-1}, M_i).$$

Геш-значення, що обчислюють під час уведення останнього блока повідомлення, стає геш-значенням (геш-образом) усього повідомлення.

Як приклад розгляньте спрощений варіант геш-функції з рекомендацій МККТТ X.509:

$$H_i = (H_{i-1} + M_i)^2 \bmod n ,$$

де $n = p \cdot q$, *p* та *q* – великі прості числа;

H_0 – довільне початкове заповнення;

M_i – *i*-й блок повідомлення $M = M_1 M_2 \ldots M_k$.

Додаток Ж

Електронний цифровий підпис

Цифровий підпис у цифрових документах відіграє ту ж роль, що й підпис, поставлений від руки в документах на папері: це дані, що приєднують до переданого повідомлення, які підтверджують, що власник підпису уклав або засвідчив це повідомлення. Одержувач повідомлення за допомогою цифрового підпису може перевірити, що автором повідомлення є саме власник підпису і що у процесі передавання не було порушено цілісність отриманих даних.

Під час розроблення механізму цифрового підпису слід виконати такі наступні завдання:

- створити підпис таким чином, щоб його неможливо було підробити;
- мати можливість перевірки того, що підпис дійсно належить указаному власнику;
- мати можливість запобігти відмові від підпису.

Класична схема створення цифрового підпису

Під час створення цифрового підпису за класичною схемою відправник:

1) застосовує до вихідного повідомлення геш-функцію;
2) обчислює цифровий підпис за геш-образом повідомлення з використанням секретного ключа створення підпису;
3) формує нове повідомлення, що складається з вихідного повідомлення і доданого до нього цифрового підпису.

Отримавши підписане повідомлення, одержувач:

1) відділяє цифровий підпис від основного повідомлення;
2) застосовує до основного повідомленням геш-функцію;
3) із використанням відкритого ключа перевірки підпису витягує геш-образ повідомлення з цифрового підпису;
4) перевіряє відповідність обчисленого геш-образу повідомлення (п. 2) і витягнутого із цифрового підпису. Якщо геш-образи збігаються, то підпис визнають справжнім.

Схема підпису RSA

Криптосистему з відкритим ключем RSA можна використовувати не тільки для шифрування, але й для побудови схеми цифрового підпису.

Для створення підпису повідомлення *M* відправник:

1) обчислює геш-образ $r = h(M)$ повідомлення *M* за допомогою деякої геш-функції;

2) зашифровує отриманий геш-образ *r* на своєму секретному ключі (d,n), тобто обчислює значення $s = r^d \bmod n$, яке і є підписом.

Для перевірки підпису одержувач:

1) розшифровує підпис *s* на відкритому ключі (e, n) відправника, тобто обчислює $r' = (s^e \bullet \bmod n)$ і таким чином відновлює передбачуваний геш-образ r' повідомлення *M*;

2) обчислює геш-образ $h(M) = r$ повідомлення *M* за допомогою тієї ж самої геш-функції, яку використовував відправник;

3) порівнює знайдені значення *r* та r'. Якщо вони збігаються, то підпис правильний, відправник дійсно є тим, за кого себе видає, і повідомлення не було змінено під час передавання.

ЗМІСТ

НАВЧАЛЬНЕ ВИДАННЯ

Методичні рекомендації щодо написання курсових проєктів для студентів зі спеціальності 125 "Кібербезпека" першого (бакалаврського) рівня

Укладачі: **Євсеєв** Сергій Петрович
Король Ольга Григорівна
Гаврилова Алла Андріївна
Коц Григорій Павлович

Самостійне електронне текстове мережеве видання

Відповідальний за випуск *С. П. Євсеєв*

Редактор *О. Г. Доценко*

Коректор

План 2020 р. Поз. № 79 ЕВ Обсяг 85 с.

Видавець і виготовлювач – видавництво ХНЕУ ім. С. Кузнеця, 61001, м. Харків, просп. Науки, 9-А

Свідоцтво про внесення суб'єкта видавничої справи до Державного реєстру ДК № 4853 від 20.02.2015 р.