МІНІСТЕРСТВО НАУКИ І ОСВІТИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
“ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ”
КАФЕДРА ПРОГРАМНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
УПРАВЛІННЯ

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ

до виконання індивідуального завдання з навчальної дисципліни
“Безпека програм та даних”

для студентів спеціальностей 122 “Комп’ютерні науки”,
121 “Інженерія програмного забезпечення”
денної форми навчання

Харків
НТУ «ХПІ»
2017

Методичні рекомендації до виконання індивідуального завдання з навчальної дисципліни “Безпека програм та даних” для студентів спеціальностей 122 “Комп’ютерні науки”, 121 “Інженерія програмного забезпечення” денної форми навчання// уклад. Євсеєв С.П., Шматко О.В., Іващенко О.В. – Харків: НТУ «ХПІ» – 2017 – 72 с.

Укладачі:

С.П. Євсеєв,

О.В. Шматко,

О.В. Іващенко

Рецензент:

Доцент ІС «ХНЕУ» Федорченко В. М.

Кафедра програмної інженерії та інформаційних технологій управління

ЗМІСТ

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, розміщені на значній відстані один від одного. Це викликає збільшення кількості вузлів мереж і кількості різних ліній зв’язку між ними, що, у свою чергу, підвищує ризик несанкціонованого підключення до мережі й доступу до конфіденційної інформації користувачів комп’ютерних систем і мереж (КСіМ). Внутрішньоплатижні банківські системи (ВПБС) які відносяться до складних многорівневих комунікаційних систем управління критичного призначення, порушення роботи приводить до втрати не тільки конфіденційної інформації банку, але й до економічних збитків, як банку, так і його клієнтів, що створює загальнонаціональну проблему.

Для протидії комп'ютерним злочинам або зменшення збитку від них необхідно грамотно вибирати заходи і засоби забезпечення захисту інформації від навмисного руйнування, крадіжки і несанкціонованого доступу. Необхідне знання основних законодавчих положень в цій області, організаційних, економічних і інших заходів забезпечення безпеки інформації.

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, яка висувається до них, є забезпечення користувачам потенційної можливості доступу до поділюваних ресурсів усіх комп'ютерів, об'єднаних у мережу.

До основних вимог функціонування глобальних обчислювальних систем (ГОС) відносяться: продуктивність, надійність, сумісність, керованість, захищеність, розширюваність і масштабованість. Основні вимоги і їх складові подані на рисунку 1.1.

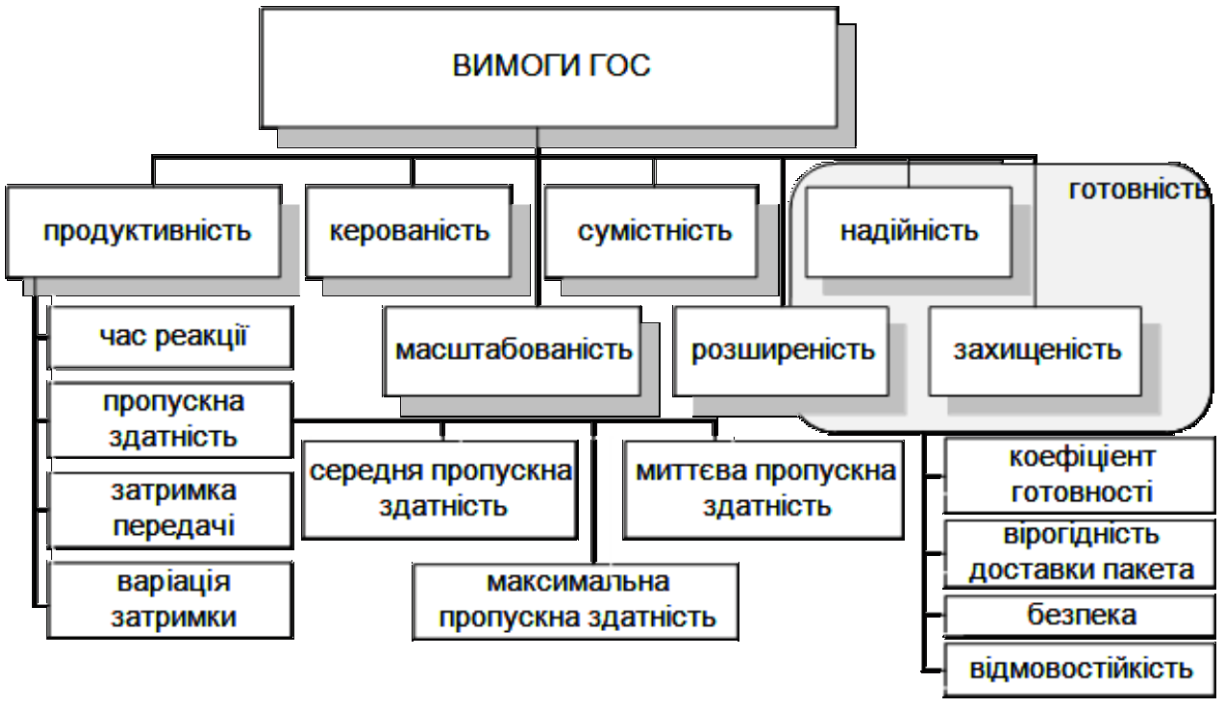

Рисунок 1.1 - Вимоги, які висуваються до обчислювальних мереж та систем

У цей час для оцінки функціонування локальних обчислювальних систем (ЛОС) і ГОС уведене поняття «якість обслуговування» (Quality of Service, Qps)

комп'ютерної мережі, що включає тільки дві найважливіші характеристики – продуктивність і надійність.

Проведений 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 здатності, показника часу затримки передачі і т. д.). Так, наприклад, технології Frame Relay і ATM дозволяють будувати мережі, що гарантують якість обслуговування за продуктивністю (показники середньої пропускної здатності, часу реакції, часу затримки та ін.).

Другий підхід полягає в 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 вповноважених користувачів ГОС якість обслуговування не гарантується, а гарантується тільки рівень їх привілеїв. Таке обслуговування називається обслуговуванням best effort – з найбільшим старанням. Проведений аналіз функціонування локальних мереж показує, що за таким принципом працюють ЛОС, побудовані на комутаторах з пріоритетом кадрів.

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

Основними характеристиками продуктивності є: час реакції, пропускна здатність, затримка передачі і її варіація.

Час реакції є інтегральною характеристикою продуктивності мережі й визначається як інтервал часу між виникненням запиту користувача до якої-небудь мережної служби й одержанням відповіді на цей запит.

Проведений аналіз даного показника показує, 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 розподіляється на час підготовки запитів на клієнтському комп'ютері, час передачі запитів між клієнтом і сервером через комунікаційне встаткування, час обробки запитів на сервері, час передачі відповідей від сервера клієнту і час обробки одержуваних від сервера відповідей на клієнтському комп'ютері.

Для визначення обсягу переданих даних за одиницю часу використовується пропускна здатність та її похідні (миттєва, максимальна і середня пропускні здатності).

При цьому середня пропускна здатність визначається як співвідношення загального обсягу переданих даних до часу їх передачі за тривалий проміжок часу (доба, місяць, рік), миттєва пропускна здатність визначається за дуже маленький проміжок часу (від 0,1 до 10^{-3} с) і максимальна пропускна здатність визначається як найбільша миттєва пропускна здатність, зафіксована протягом періоду спостереження.

Аналіз функціонування ГОС показує, що для проектування, настроювання й оптимізації використовуються такі показники, як середня й максимальна пропускні здатності. Для визначення якості мережі в цілому, не диференціюючи його за окремими сегментами або обладнаннями, використовується загальна пропускна здатність мережі, яка визначається як середня кількість інформації, переданої між усіма вузлами мережі в одиницю часу. Для визначення якості мережі так само використовують кількісний показник максимальної затримки передачі і її варіації.

Затримка передачі визначається 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.

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

Для опису передачі пакетів між кінцевими вузлами використовуються імовірнісні характеристики каналу зв'язку: імовірність доставки пакета вузлу призначення без викривлень, імовірність втрати пакета (за кожною із причин – переповнення буфера маршрутизатора, через розбіжність контрольної суми, через відсутність працездатного шляху до вузла призначення і т. д.), імовірність викривлення окремого біти переданих даних.

У показник загальної надійності включається безпека – здатність системи захистити дані від несанкціонованого доступу й відмовостійкість – здатність системи сховати від користувача її окремі елементи.

При проектуванні і модернізації ЛОС ураховуються додаткові вимоги до обчислювальних мереж:

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

Масштабованість (scalability) – можливість мережі нарощувати кількість вузлів і довжину зв'язків у дуже широких межах, при цьому зберігається показник продуктивності мережі.

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

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

Проведений аналіз працездатності ЛОС (ГОС) показує, що особливу складність представляє сполучення в одній мережі традиційного

комп’ютерного та мультимедійного трафіка. Для обліку складеного трафіка використовуються наступні додаткові параметри мережі:

Керованість – можливість централізовано контролювати стан основних елементів мережі, виявляти й розв’язувати проблеми, що виникають при роботі мережі, виконувати аналіз продуктивності й планувати розвиток мережі.

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

Сумісність або інтегрованість – можливість включення у ЛОС (ГОС) найрізноманітнішого програмного і апаратного забезпечення (різні операційні системи, що підтримують різні стеки комунікаційних протоколів, апаратні засоби й додатка від різних виробників).

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

Для оцінки надійності мережі використовуються основні характеристики складних систем: коефіцієнт готовності – проміжок часу, протягом якого система може бути використана; безпека – здатність системи захистити дані від несанкціонованого доступу й відмовостійкість – здатність системи працювати в умовах відмови деяких її елементів.

Проблема захисту комп’ютерних мереж від несанкціонованого доступу придбала особливу гостроту.

Розвиток комунікаційних технологій дозволяє будувати мережі розподіленої архітектури, що поєднують велику кількість сегментів, розташованих на значній відстані один від одного. Все це викликає збільшення числа вузлів мереж і кількості різних ліній зв’язку між ними, що, у свою чергу, 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, у системах керування великими фінансовими і промисловими організаціями, підприємствами енергетичного сектору, транспорту нових підходів до побудови протоколів і механізмів забезпечення безпеки інформаційних систем.

Природна вимога до безпеки і вірогідності оброблюваної та 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 втрат, збитку екології, життя і здоров'я людей.

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

Сучасні криптографічні засоби захисту інформації повинні забезпечувати своєчасну обробку величезних обсягів даних (десятки – сотні Мбіт/с) і задовольняти твердим вимогам з вірогідності і безпеки інформації.

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

1.2. Побудова класифікацій криптографічних засобів

При розробці підходів 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.

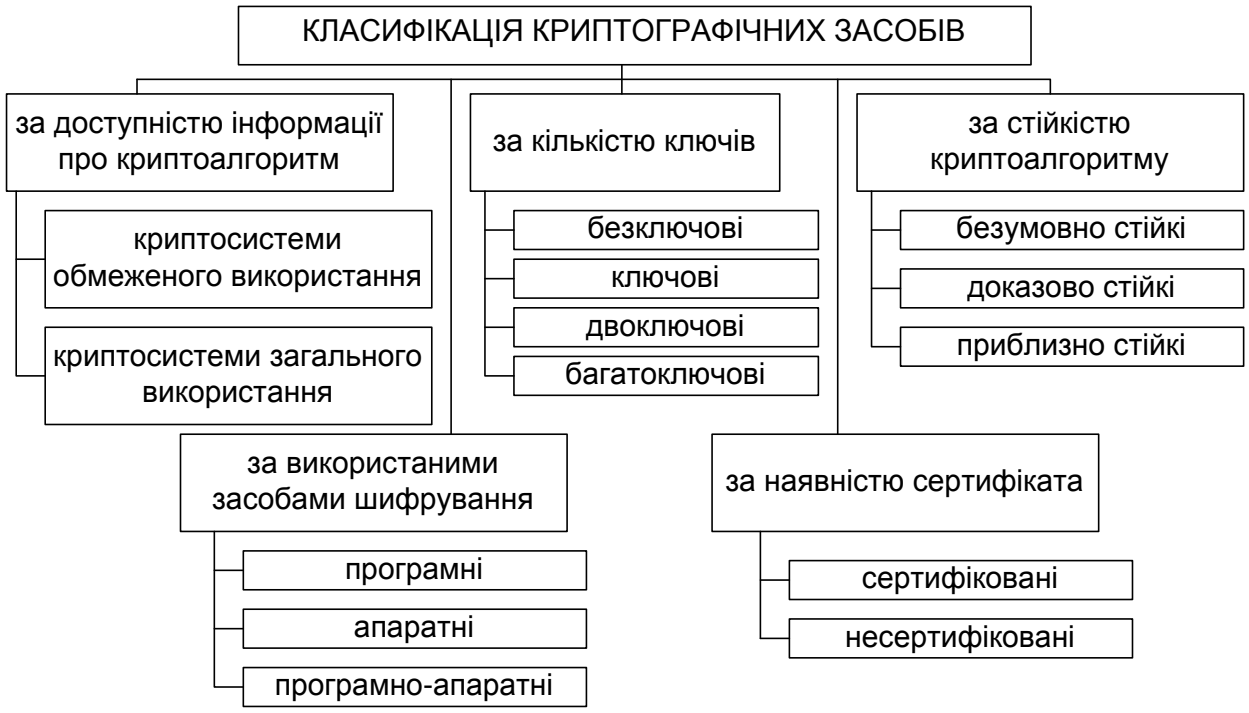

Рисунок 1.2 - Класифікація криптографічних засобів

Класифікація за доступністю інформації про криптоалгоритм

Пропонується наступна класифікація криптосистем:

криптосистеми обмеженого використання;

криптосистеми загального використання.

Криптографічна система називається *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 зводиться 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 називається її ключем. Такий ключ повинен вироблятися конкре-

тними користувачами 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 повинні проводитися в припущенні, що потенційному противнику відома вся інформація про криптосистему, за винятком використовуваного ключа.

Класифікація за кількістю ключів

За класифікаційною схемою криптосистеми підрозділяються на 3 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 застосовуються два види ключів: закриті (особисті) і відкриті.

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

Класифікація за стійкістю криптоалгоритма

Здатність криптосистеми протистояти атакам криптоаналитика називається стійкістю. Кількісно стійкість виміряється як складність найкращого алгоритму, що приводить криптоаналитика до успіху із прийнятною ймовірністю. Універсальний метод прямого перебору множини всіх можливих ключів дозволяє одержати оцінку зверху для стійкості алгоритму шифрування. Відносний очікуваний безпечний час визначається як напівдобуток кількості відкритих ключів і часу, необхідного криптоаналитику для того, щоб випробовувати кож-

ний ключ. Залежно від мети і можливостей криптоаналитика, змінюються й 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 степені захисту. За основу ставиться принципова можливість одержання з перехоплення деякої інформації про відкритий текст або використаний ключ**.** Існують *безумовностійкі* (або *теоретичностійкі*), *доказовостійкі*й, *приблизностійкі* 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 одержати деяку інформацію про них. Алгоритм безумовностійкий, якщо відновлення відкритого тексту неможливе при будь-якому обсязі шифртексту, отриманого криптоаналітиком. Безпека безумовностійких криптоалгоритмів заснована на доведених теоремах про неможливість розкриття ключа.

Стійкість *доказовостійких* криптоалгоритмів визначається 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 досяга-

ється збільшенням розміру математичного завдання або її заміною, що, як правило, тягне ланцюг змін в апаратурі, яка використовується для шифрування.

Приблизностійкі криптоалгоритми засновані на складності розв'язання приватного математичного завдання, яке не зводиться до добре відомих завдань і яку намагалися розв'язати один або кілька чоловік. Прикладами можуть служити блокові шифри. Приблизностійкі криптоалгоритми характеризуються порівняно малою вивченістю математичних завдань, на яких базується їх стійкість. Однак такі шифри мають велику гнучкість, що дозволяє при виявленні слабких місць не відмовлятися від алгоритмів, а проводити їх доробку.

Класифікація за використовуваними засобами

Розглянемо цю класифікацію в застосуванні до генераторів псевдовипадкових чисел. Для генерації ключової інформації, призначеної для використання в рамках симетричної криптосистеми, використовуються 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 і т. д.;

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 і якісних псевдовипадкових генераторів.

Кращий спосіб генерації множини випадкових бітів – витяг їх із природно випадкових подій реального світу. Часто такий метод вимагає наявності спеціальної апаратури, але можна реалізувати його й на комп'ютерах. У якості випадкових величин можна також розглядати інтервали між натисканнями клавіш клавіатури. Головний недолік подібних систем – можливі закономірності в послідовності, яка генерується. Використовувані фізичні процеси можуть бути ви-

падкові, 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 діючого 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 значимість електронних документів при обміні ними між користувачами дозволить використання *сертифікованих* криптоалгоритмів.

Класифікація криптоаналітичних атак

Наведена на рис. 1.3 класифікація дозволяє розрізняти криптоаналітичні атаки і їх наслідки одночасно за декількома параметрами.

Класифікація з доступу до відкритого й зашифрованого тексту

Перш ніж класифікувати атаки, введемо ряд позначень: відкритий текст будемо позначати буквою M, шифртекст – C (у якості M може виступати будь-яка послідовність бітів: текстовий файл і т. д.). Нехай для шифрування і розшифрування використовуються ключі k і $k^{/}$ відповідно (у симетричній криптографії $k = k^{/}$); позначимо функцію шифрування E_k, розшифрування – D_k. Тоді виконуються співвідношення $E_k(M) = C$, $D_k(C) = M$. Донедавна за критерієм доступу до відкритого і шифрованого тексту виділялося чотири основні типи криптоаналітичних атак. Однак останнім часом одним із найактуальних напрямів криптоаналізу стало здійснення атак, що використовують особливості реалізації та робочого середовища.

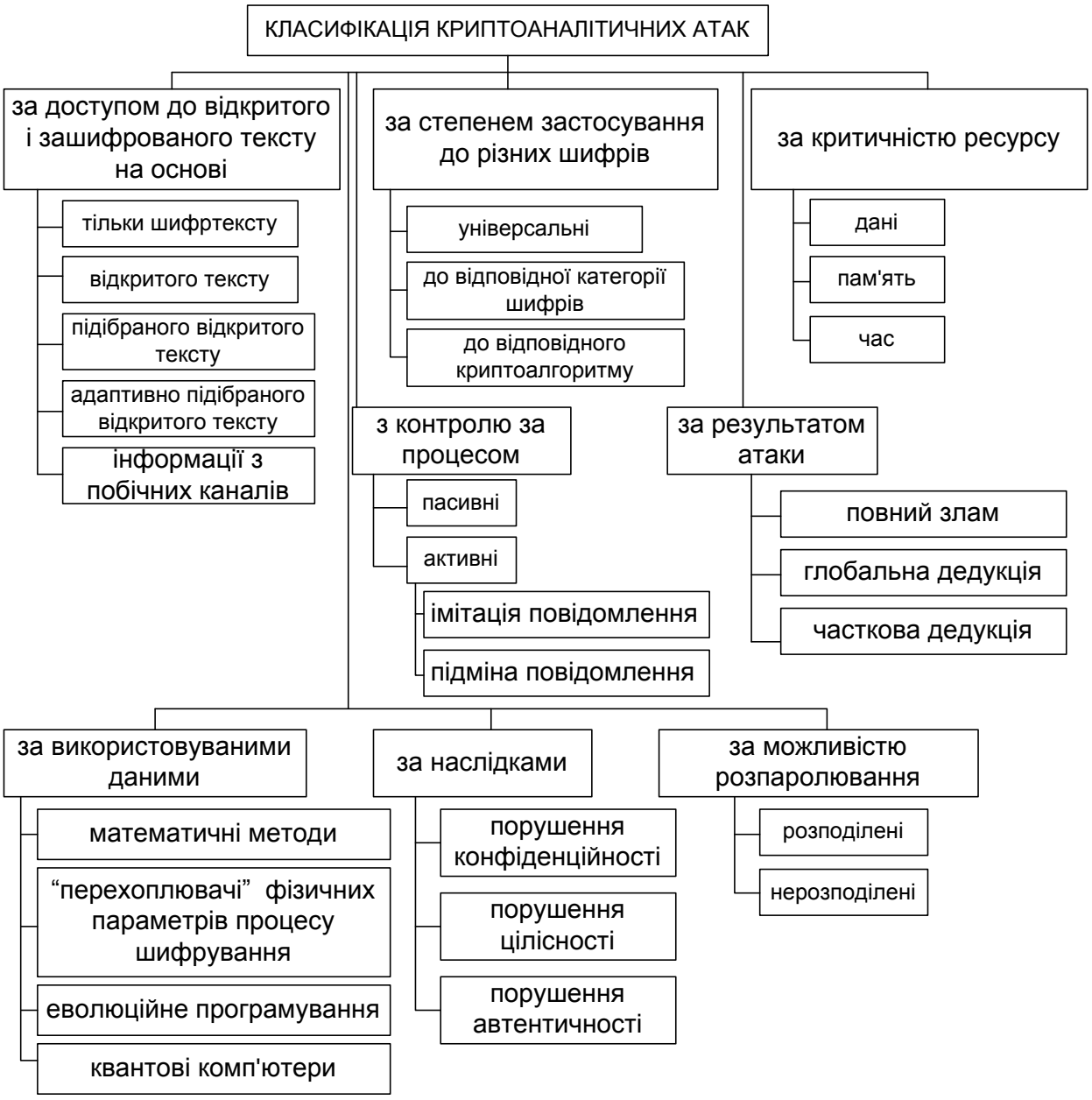

Рисунок 1.3 - Класифікація криптографічних атак

Атаки сторонніми або побічними каналами – це вид криптографічних атак, що використовують інформацію, отриману зі сторонніх або побічних каналів. У кожному випадку передбачається (згідно з фундаментальним допущенням Кірхгоффа, що криптоаналитик знає використовуваний алгоритм шифрування.

Атака на основі тільки шифртексту. Криптоаналитик розташовує шифртекстами c_1, ..., c_m, отриманими з невідомих відкритих текстів m_1,

...,m_mрізних 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 нездатності зробити це. У якості окремих випадків можливий збіг ключів або збіг відкритих текстів.

Атака на основі відкритого тексту. Криптоаналитик 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 нездатності 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 криптоаналитик має можливість вибору відкритих текстів m_1, ...,m_m. Мета атаки та ж, що й попередньої. Подібна атака можлива, наприклад, у випадку, коли криптоаналитик має доступ до шифратора передавальної сторони.

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

Атака на основі інформації з побічних каналів. Криптоаналитик має інформацію, яка може бути отримана з обладнання шифрування й не є при цьому ні відкритим текстом, ні шифртекстом.

Атаки з побічних каналів, у свою чергу, класифікуються за такими типами:

за контролем над обчислювальним процесом: *пасивній 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 (Electro-magnetic 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 світовім 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 передається каналами зв'язку в шифрованому виді, не повинне приводити до розсекречення іншої інформації, шифрованої на цьому ж 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 вважаються найнебезпечнішими.

Класифікація з контролю над процесом шифрування

До класу *пасивних* атак відносять дії противника, який «пасивно вивчає» шифровані повідомлення, може їх перехопити й піддати криптоаналізу з метою одержання інформації про відкритий текст або ключ. Однак сучасні технічні засоби дозволяють потенційному противнику «активно» втручатися в процес передачі повідомлення. Звичайно розрізняють два типи *активних* атак, які носять назви *імітації* й *підміни повідомлення*. *Атакаімітації* полягає в тому, що противник «вставляє» у канал зв'язку сфабриковане ним «шифроване повідомлення», яке насправді не передавалося від законного відправника до одержувача. При цьому противник розраховує на те, що одержувач сприйме це повідомлення як справжнє (автентичне). *Атакапідміни* полягає в тому, що противник,

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 служать імовірності успіху імітації й підміни відповідно. Ці ймовірності визначають шанси противника на успіх при нав'язуванні одержувачу неправильного повідомлення.

Класифікація за результатом атаки

Криптоаналіз ставить своїм завданням у різних умовах одержати додаткові відомості про ключ шифрування, щоб значно зменшити діапазон імовірних ключів. Результати криптоаналізу можуть варіюватися за степенями практичної застосовності. Шифр вважається зламаним, якщо в системі виявлене слабке місце, яке може бути використане для більш ефективного зламу, ніж метод повного перебору ключів ("brute-force approach"). Допустимо, для дешифрування тексту методом повного перебору потрібно перебрати 2^{128} можливих ключів; тоді винахід способу, що вимагає для дешифрування 2^{110} операцій з підбору ключа, буде вважатися зламом. Такі способи можуть вимагати нереалістично великих обсягів підібраного відкритого тексту або пам'яті ЕОМ. Під *зламом* розуміється лише підтвердження наявності уразливості криптоалгоритму, що свідчить про те, що властивості надійності шифру не відповідають заявленим характеристикам. Як правило, криптоаналіз починається зі спроб зламу спрощеної модифікації алгоритму, після чого результати поширюються на повноцінну версію. Криптограф Ларс Кнудсен [93] пропонує таку класифікацію успішних наслідків криптоаналізу блокових шифрів залежно від обсягу і якості секретної інформації, яку вдалося одержати:

повний злам – криптоаналитик отримує секретний ключ;

глобальна дедукція – криптоаналитик 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 одержує деяку інформацію про відкритий текст або ключ.

Класифікація за обсягом необхідних ресурсів

Атаки можна також класифікувати за обсягом ресурсів, необхідних для їх 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 криптоаналитика є розкриття більшої кількості шифрів (незалежно від того, чи прагне він цим завдати шкоди суспільству, попередити його про можливу небезпеку або просто одержати популярність), то для нього найкращою стратегією є розробка *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, при розв'язанні якого вдається використовувати багато методів тієї ж теорії складності, теорії чисел і алгебри, привело до появи методів криптоаналізу, застосованих до різних класів шифрів. Нарешті, існують атаки, що використовують деяку уразливість при проектуванні або реалізації конкретного шифру. Ці атаки не можуть бути в загальному випадку перенесені 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 математич-

не завдання, при 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 засновані на кореляції між значеннями *фізичних параметрів, вимірюваних у різні моменти під час обчислень* (споживання енергії, час обчислень, електромагнітне випромінювання і т. п.), і внутрішнім станом обчислювального обладнання, що мають відношення до секретного ключа. На практиці атаки побічними каналами на багато порядків більш ефективні, ніж традиційні атаки, засновані тільки на математичному аналізі. При цьому атаки 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. На даний момент методи, засновані на використанні нових інформаційних технологій (еволюційного програмування і квантових комп'ютерів), у криптоаналізі не привели до серйозних проривів у зламі шифрів і мають 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 одержати реакцію на виході. Завдання криптоаналізу – ідентифікація цієї системи, тобто визначення її структури на основі сигналів, що надходять на її вхід і одержуються на виході. Одним з інструментів розв'язання цього завдання можуть бути нейронні мережі. Генетичні алгоритми успішно застосовуються в криптоаналіз переставних і підставних шифрів.

Класифікація за наслідками атаки

Можливі наслідки реалізації атаки розглянемо з погляду порушення властивостей інформації – конфіденційності, цілісності й автентичності (доступнос-

ті). Можна виділити три стратегії дій, які може почати порушник у випадку успішної реалізації атаки.

Перехоплення інформації, переданої каналами зв'язку.

Модифікація інформації, переданої каналами зв'язку (підміна, неправильні повідомлення, блокування передачі і т. д.).

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, при оцінці ефективності методу криптоаналізу необхідно враховувати не тільки його часову і ємнісну складність, але й можливість распаралелювання на багатопроцесорній системі. Так, алгоритм Полларда має складність $O(\sqrt{n})$, однак *не піддається распаралелюванню*. У той же час метод повного перебору, який на однопроцесорній машині уступає за ефективністю методу Полларда, становить простий приклад методу криптоаналізу, що *допускає распаралелювання*.

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

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

2) виконання операції O_i;

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

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

Другий напрямок распаралелювання полягає в тому, що множина K розбивається на непересічні підмножини K_1, K_2 ..., K_Q. Система з Q машин

перебирає ключі так, що i-а машина здійснює перебір ключів з 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 при кожному черговому випробуванні кожний з N процесорів стартує з випадкової точки, то час випробування збільшиться, але схема значно спроститься. Середня кількість кроків випробування N процесорами (машинами) ключів з множини K у цьому випадку становить $\frac{|K|}{N}$. Реалізація такого паралелізму припускає різні розв'язання. Найбільш очевидне розв'язання – створення комп'ютерного вірусу для поширення програми-зломщика в глобальній мережі. Вірус повинен 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 зломщиків криптосистем

При оцінці 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 повинна вказувати:

категорії осіб, у числі яких може виявитися порушник;

припущення про кваліфікацію порушника і його технічну оснащеність;

можливі цілі порушника й очікуваний характер його дій.

За основу для розробки класифікаційної схеми була прийнята модель порушника, класифікація дозволяє при побудові моделі зломщика криптосистеми враховувати різні параметри й, тим самим, встановити залежність можливих сценаріїв атак від характеристик противника, з боку яких система піддається нападам. На рис. 1.4 наведена класифікація противника.

Рисунок 1.4 - Класифікація порушника криптосистем

Класифікація за технічною оснащеністю

На сьогоднішній день 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 в 1997 році на сайті www.distributed.net (проект «розподіленого зламу»), у якому на добровільній основі взяли участь більш 300 тисяч користувачів глобальної мережі, був успішно завершений за п’ять років (1 757 днів) – за цей час було перебрано 85 % всієї 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 криптоаналитика полягає у створенні нових і підвищенні ефективності існуючих методів аналізу стійкості крипто-

графічних 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 числа обслуговуючого персоналу. Якщо в ролі зломщиків виступають ненадійні співробітники компанії, то можливостей для здійснення атак з'являється набагато більше, ніж у будь-яких інших зломщиків.

Класифікація за рівнем підготовки

Кваліфікація зломщика визначається наявністю релевантних знань, умінь і навичок. Можна виділити чотири основні області, освоєння яких може бути корисним порушнику для здійснення атаки на криптосистему:

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

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

програмування – для розробки інструментальних засобів, що реалізують алгоритми криптоаналізу; створення вірусів для распаралелювання пошуків ключа й т. п.;

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

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

Градація противників за їх кваліфікацією може бути різною. Наприклад, в виділено три класи противника:

висококваліфікований зловмисник-професіонал;

кваліфікований зловмисник-непрофесіонал;

некваліфікований зловмисник-непрофесіонал.

Класифікація за первинною інформацією про засіб шифрування

Порушнику може бути відома інформація (у тому числі 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 можуть бути зламані. Це означає що, якщо для генерації ключів використовується криптографічний слабкий алгоритм, то незалежно від шифру, який використовується, вся система буде нестійкої. *Генератори випадкових чисел* – те місце, у якому часто ламаються криптографічні системи. Знаючи принцип витягу випадкових чисел, противник може значно скоротити область перебору можливих ключів системи.

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

Класифікація за можливістю кооперації

Останнім часом у зв'язку з розвитком мереж (зокрема, Інтернету) стало можливо ефективно використовувати метод «грубої сили» (перебору) шляхом распаралелювання операцій. Нерідко професійні хакери поєднуються у злочинні угрупування, що прагнуть до наживи й виконуючі розкрадають конфіденційну інформацію із замовлень конкуруючих 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 програма підключається до сервера, одержує від нього набір ключів для перебору й після закінчення роботи повертає результат. Програма може працювати у фоно-

вому режимі, у якості скринсейвера або активуватися ночами. Такий підхід застосуємо не тільки для зламу шифрів, але і для підбору двох текстів, що мають однакове значення хеш-функції, обчисленої зазначеним алгоритмом. На рис. 1.5 наведений приклад класифікації загроз інформації у загальному вигляді.

Рисунок 1.5 - Загрози інформації у критичних інформаційних системах і технологіях

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

При виборі криптосистеми необхідно проводити аналіз погроз безпеки в конкретній комп'ютерній системі, що передбачає оцінку стійкості до досить різноманітних типів криптоаналітичних нападів.

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

1.3. Побудова моделі порушника безпеки в КМіС

Спроба одержати несанкціонований доступ до комп'ютерних мереж з метою ознайомитися з ними, залишити записку, виконати, знищити, змінити або викрасти програму або іншу інформацію кваліфікується як *комп'ютерне піратство.* Як соціальне явище, подібні дії прослідковуються в останні 10 років, але при цьому спостерігається тенденція до їх стрімкого зростання по мірі збільшення кількості побутових комп'ютерів.

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

Однак комп'ютерні злочинці не цікавляться, наскільки добре здійснюється в цілому контроль у комп'ютерній системі; вони шукають єдину лазівку, яка приведе їх до бажаної мети. Для одержання інформації вони проявляють винахідливість, використовуючи психологічні фактори, детальне планування та активні дії. Необхідно розділити два визначення: хакер (hacker) і кракер (cracker). Основна відмінність полягає в постановці мети зламу комп'ютерних систем: перші ставлять дослідницькі завдання з оцінки і знаходження уразливостей з метою наступного підвищення надійності комп'ютерної системи. Кракери ж втручаються в систему з метою руйнуван-

ня, крадіжки, псування, модифікації інформації і роблять правопорушення з корисливими намірами швидкого збагачення.

Для запобігання можливих погроз необхідно не тільки забезпечити захист операційних систем, програмного забезпечення і контроль доступу, але й виявити категорії порушників і ті методи, які вони використовують.

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

шукачі пригод;

ідейні хакери;

хакери-професіонали;

ненадійні (неблагополучні) співробітники.

Шукач пригод, як правило, це студент, у якого рідко є продуманий план атаки. Він вибирає мету випадковим чином і звичайно відступає, зіштовхнувшись 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 же 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 атакуються. 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 й звичайно здійснюються в кілька етапів. Спочатку він збирає попередню інформацію (тип операційної системі (ОС), надаваємі сервіси й застосовуємі заходи захисту). Потім він становить план атаки з урахуванням зібраних даних і підбирає (або навіть розробляє) відповідні інструменти. Провівши атаку, він одержує закриту інформацію, і наре-

шті, знищує всі сліди своїх дій. Такий атакуючий професіонал звичайно добре фінансується й може працювати самому або у складі команди професіоналів.

Ненадійний (неблагополучний) співробітник своїми діями може доставити 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, як правило, менш твердий внутрішній захист. Він не так витончений у способах атаки, як промисловий шпигун, і тому частіше допускає помилки й тим самим може видати свою присутність. Однак у цьому випадку небезпека його несанкціонованого доступу до корпоративних даних багато вище, ніж будь-якого іншого зловмисника. Перераховані категорії порушників безпеки інформації можна згрупувати за їх кваліфікацією: *початківець* (шукач пригод), *фахівець* (ідейний хакер, ненадійний співробітник), *професіонал* (хакер-професіонал).

Порушник безпеки інформації, як правило, будучи фахівцем визначеної кваліфікації, намагається довідатися про комп'ютерні системи й мережі і, зокрема, про засоби їх захисту. Тому модель порушника визначає:

категорії осіб, у числі яких може виявитися порушник;

можливі цілі порушника і їх градації за степенями важливості й небезпеки;

припущення про його кваліфікації;

оцінка його технічної озброєності;

обмеження й припущення про характер його дій.

На рис. 1.6 наведена узагальнена модель порушника безпеки інформації.

Діапазон спонукальних мотивів одержання доступу до системи досить широкий: від бажання випробувати емоційний підйом при грі з комп'ютером до відчуття влади над ненависним менеджером. Займаються цим не тільки новачки, що бажають побавитися, але й професійні програмісти. Паролі вони добувають або в результаті підбору або шляхом обміну з іншими хакерами.

Частина з них, однак, починає не тільки переглядати файли, але й проявляти інтерес саме до їх змісту, а це вже являє серйозну загрозу, оскільки в цьому випадку важко відрізнити невинне баловство 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 у якості реваншу з метою послабити фірму як конкурента якої-небудь фірми.

Незадоволений керівником службовець створює одну із самих більших погроз обчислювальним системам колективного користування.

Рисунок 1.6 - Модель порушника безпеки інформації

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

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

які відносяться до злочинних угрупувань, що переслідують політичні цілі;

прагнучих одержати інформацію з метою промислового шпигунства;

хакерів або угрупування хакерів, що прагнуть до наживи.

Для здійснення несанкціонованого доступу в інформаційну систему потрібно, як правило, провести два підготовчі етапи:

зібрати відомості про систему;

виконати пробні спроби входження в систему.

Збір відомостей. Залежно від особистості зломщика і його похилостей можливі різні напрямки збору відомостей:

підбір співучасників;

аналіз періодичних видань, відомчих бюлетенів і документації;

перехоплення повідомлень електронної пошти;

підслуховування розмов, телексів, телефонів;

перехоплення інформації й електромагнітного випромінювання; організація крадіжок;

вимагання й хабар.

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

Підбір співучасників. Підбір співучасників заснований на підслуховуванні розмов у барах, фойє готелів, ресторанах, таксі, підключенні до телефонів і телексам, 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.

Витяг інформації з періодичних видань. Зломщики можуть почерпнути багато корисної інформації з газет і інших періодичних видань.

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

Телефонний канал доступу в таку систему звичайно вільний, хоча останнім часом системні оператори вимагають установки обладнань реєстрації користувачів електронної пошти. Аж до недавнього часу багато довідкових систем були оснащені блоками, через які зломщики могли витягати більші обсяги даних, а також ідентифікатори й паролі користувачів. 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. З метою одержання інформації про обчислювальну систему або отримання службових паролів зломщики можуть використовувати різноманітні способи. Наприклад, знайомлячись, вони представляються менеджерами; використовують запитальники, роздаючи їх у фойє

фірми й детально розпитуючи співробітників про комп'ютер-ну систему; дзвонять системному адміністратору 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 повинні пред'являти ідентифікаційний код або пароль.

Більш зловмисним, але, можливо, і більш успішним є метод «полювання за розумами», 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 росту, але, вважає себе гідним більш важливої й високооплачуваної посади; він може розкрити коди користувачів, паролі, указати слабкі місця в мережах зв'язку і т. д.

Аналіз роздруківок. Деякі зломщики одержали доступ, до ЕОМ просто вивчаючи роздруківки, і це один з найбільш ефективних і найменш ризикованих шляхів одержання 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 знищуються. Саме таким способом зломщики змогли одержати досить повну картину організації комп'ютерної системи, використовуючи викинуті роздруківки й незатребувані протоколи роботи системи, які співробітникам обчислювального центру представлялися невинними папірцями.

Перехоплення повідомлень в 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 – перехоплення усних повідомлень із використанням радіопередавачів, мікрофонів і мікрохвильових обладнань; підслуховування повідомлень, переданих з телефону, телексу й іншими каналами передачі даних; контроль електромагнітного ви-

промінювання від ПК; перехоплення супутникових або мікрохвильових передач.

Установкою радіопередавачів, мікрофонів і мікрохвильових обладнань або прослуховуванням ліній зв'язку звичайно займаються професійні зломщики, а також аматори й фахівці зі зв'язку. Останнім часом кількість випадків установки таких обладнань зросла. Улюбленими точками безконтрольного доступу також є телефонні лінії.

Передача даних з комутацією пакетів або з використанням широкосмугових ліній зв'язку зі швидкостями в тисячу й мільйони бод викликає інтерес у зломщиків і може бути перехоплена, щоб викрасти передані повідомлення, модифікувати їх зміст, затримати або вилучити.

1.4. Побудова моделі реалізації загроз безпеки в КМіС

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

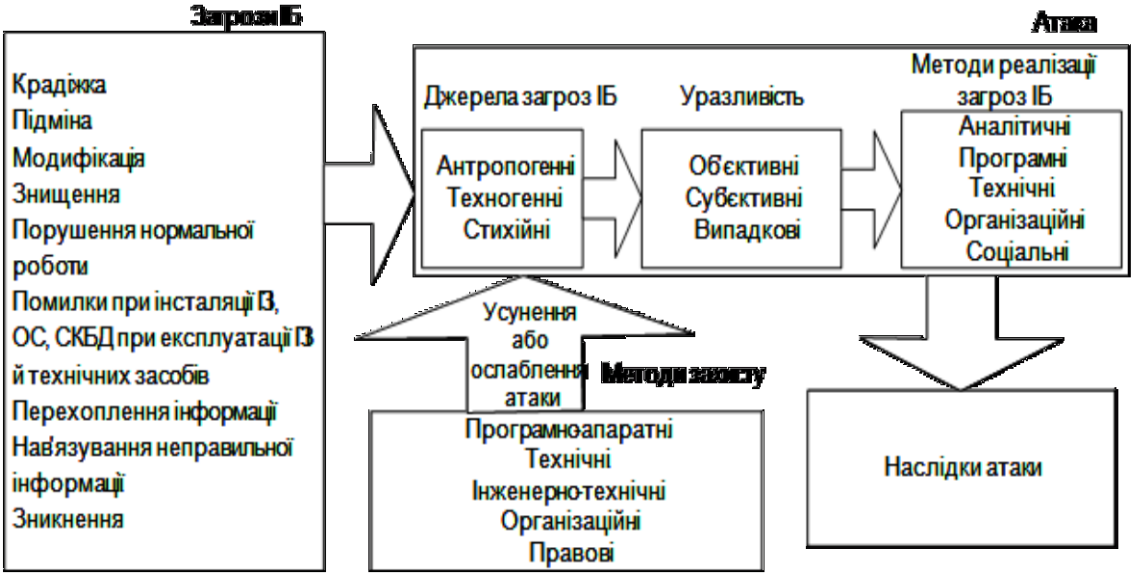

Рисунок 1.7 - Структурна схема моделі реалізації загроз інформаційних ресурсів в КМіС

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

Рисунок 1.8 - Мета і погрози безпеки інформації

Для опису моделі реалізації загроз інформаційних ресурсів зафіксуємо кінцеву множину суб'єктів, взаємодіючих з інформаційною системою – S, параметр N – кількість уразливих до атаки комп'ютерів (ПК); параметр D містить початкове значення середньої кількості атакованих комп'ютерів за обрану одиницю часу. Вважаємо, що Dє константою, обчислення враховують, що комп'ютер не може бути атакований двічі; a(t) – пропорція вразливих ПК, які були успішно атаковані 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:

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

Враховуючи, що N – константа і $n = d(\mathrm{Na}) = \mathrm{Nda}$,правильне таке рівняння:

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

у диференціальному вигляді:

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

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 в КМіС і моделей атак обраний функціональний тип математичних моделей, який називається моделями “чорної скриньки”. Математична модель є моделлю об’єкта, процесу або явища, що становить математичні закономірності, за допомогою яких описані основні характеристики об’єкта, який моделюємо, процесу або явища. Загальним для опису даних математичних моделей є процес формування криптограми.

Для цього зафіксуємо кінцеву множину $I = \{I_1, I_2, \ldots, I_m\}$ переданих пакетів, причому кожному пакету відповідає ймовірність $P\ (I_j)$. Розподіл ймовірностей випадкового процесу задається сукупним розподілом ймовірностей випадкових величин, тобто множиною ймовірностей $P^{\circ} = \{P\ (I_1), P\ (I_2), \ldots, P\ (I_m)\}$. Джерело ключів породжує потік ключів з множини К і/або К*. 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 ймовірність$P\ (K^i)$. Випадковий процес вироблення ключів задається множиною ймовірностей:

$$P^{K} = \{P\ (K_1), P\ (K_2), \ldots, P\ (K_k)\}$$

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

Вибір ключа K_i визначає конкретне відображення φ_i з множини відображень і криптограма формується: $E_l = \varphi_i(K_i, I_j)$.

Відмінність між активними і пасивними атаками полягає в тому, що при виконанні атак першого типу (активні атаки) порушник здійснює 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 одержання переданої інформації (розкриття вмісту повідомлень і аналіз потоку даних).

Оцінка степеня ефективності атаки може бути здійснена за рахунок проведення аналізу даних, якими володіє противник, його можливостей та інших параметрів пасивних атак. Основним методом оцінки можливостей противника при атаці є створення моделей атак.

1.5. Побудова математичної моделі пасивних атак у КМіС

Пасивні загрози випливають із прослуховування (несанкціонованого зчитування інформації) і не пов’язані з якою-небудь зміною інформації. Суть атаки полягає в тому, що порушник, визначивши факт виконання криптографічного протоколу, перехоплює всі дані, які були передані по каналу зв’язку . Тобто при передачі криптограми E_l в вузли приймання по деякому каналу порушник виконує моніторинг мережі.

При цьому порушник (криптоаналітик) зобов’язаний володіти всіма відкритими параметрами і даними, які використовуються суб’єктами s. У такому випадку криптоаналітик може провести криптоаналіз протоколу з 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 використовуються в протоколі, й інших характеристик протоколу. Узагальнена модель пасивних атак подана на рис. 1.9 – 1.10.

Рисунок 1.9 - Модель пасивних атак на інформаційні ресурси в КМіС

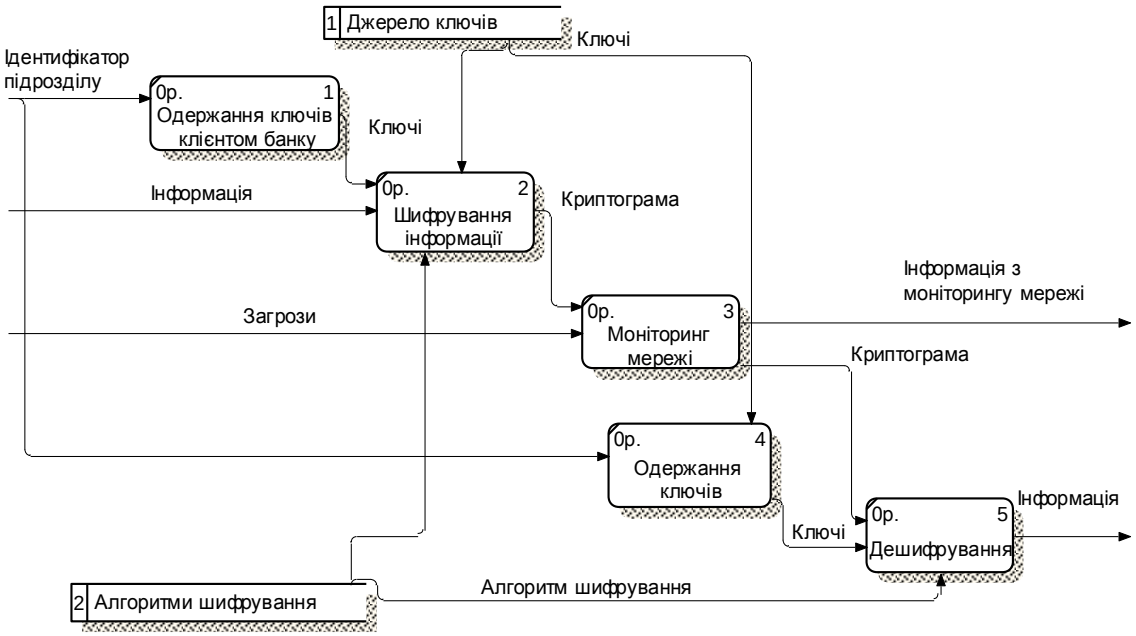

Рисунок 1.10 - Декомпозиція моделі пасивних атак

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

1.6. Побудова моделі активних атак у КМіС із блокуванням передачі інформації

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

Узагальнена модель активних атак із блокуванням передачі інформації подана на рис. 1.11 – 1.12. Одержувачем інформації в даній моделі є порушник.

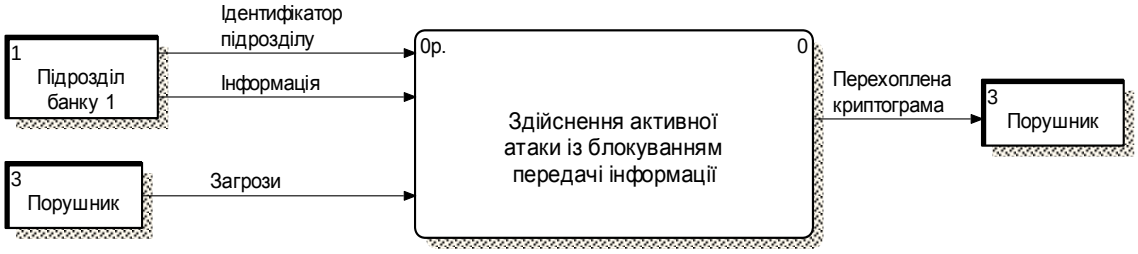

Рисунок 1.11 - Модель активних атак із блокуванням передачі інформації

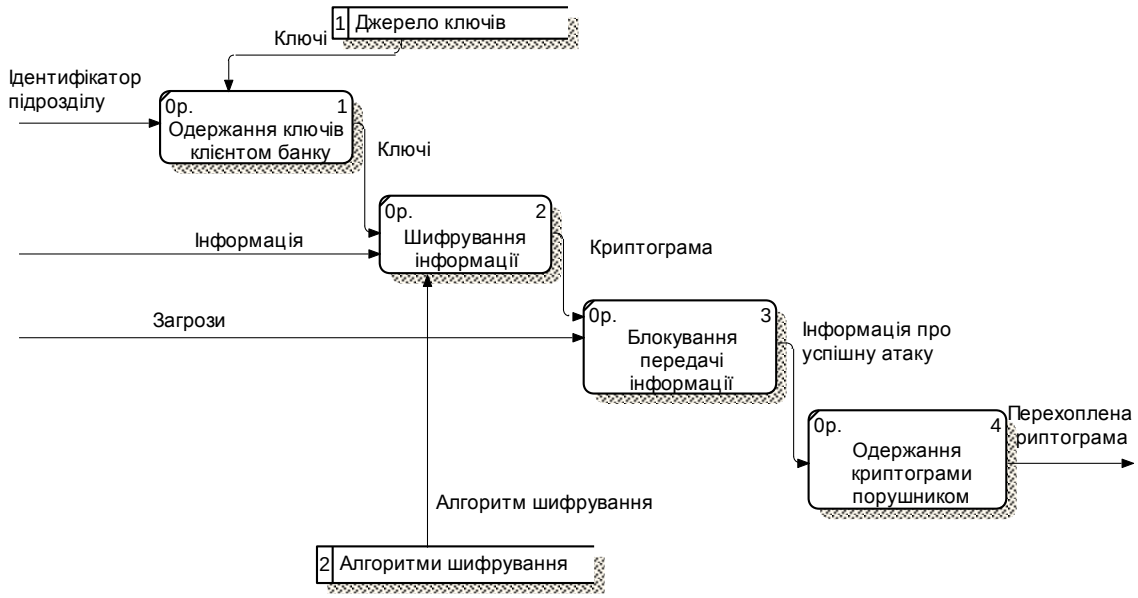

Рисунок 1.12 - Декомпозиція моделі активних атак із блокуванням передачі інформації

При реалізації даної 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

Суть атаки із внесенням перешкод полягає в тому, що порушник, визначивши факт виконання криптографічного протоколу, вносить деяку поми-

лку *e* й передає в вузол приймання криптограму (E_{l+e}). На прийомному кінці за допомогою зворотного відображення φ_i^{-1} (заданого ключем K_i*) із криптограми (E_{l+e}) відновлюється недостовірна інформація

$I_{je} = \varphi_i^{-1}(K_i^*, E_{l+e})$. Узагальнена модель активних атак із внесенням перешкод подана на рис.1.13 – 1.14.

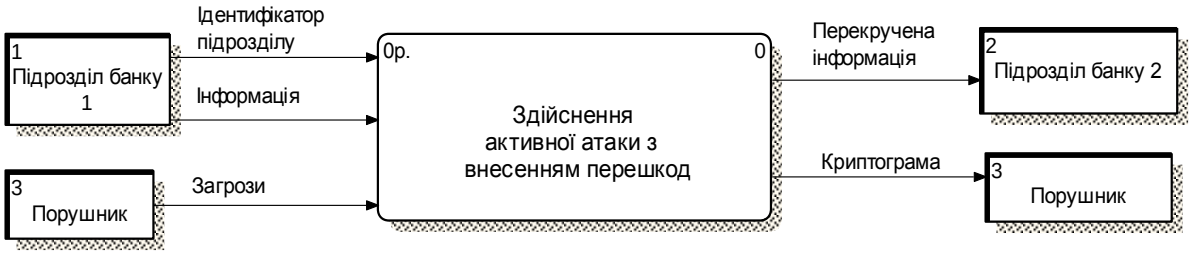

Рисунок 1.13 - Модель активних атак із внесення перешкод

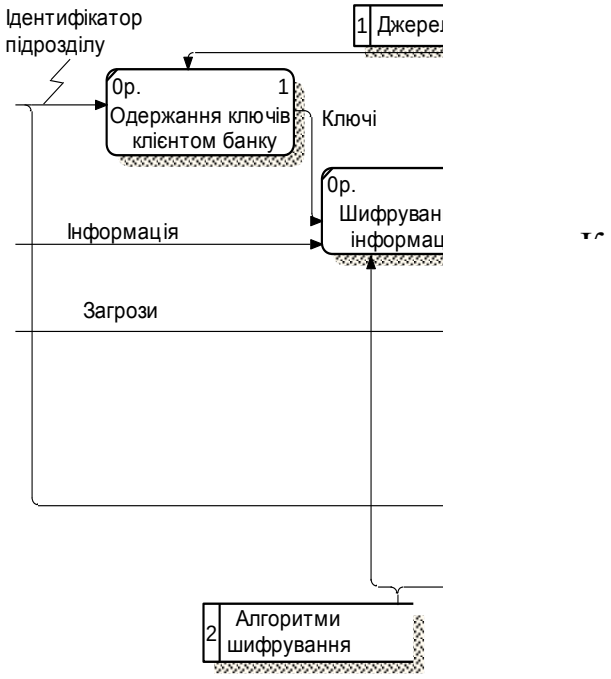

Рисунок 1.14 - Декомпозиція моделі активних атак із внесення перешкод

Реалізація даної атаки може призвести до збою або до одержання на прийомній стороні неправильної транзакції. Порушник може “керувати”

конфіденційною інформацією, результатом цього є економічний збиток клієнтів КМіС.

1.8. Побудова моделі активних атак “маскарад” у КМіС

Суть атаки “маскарад” полягає в тому, що користувач (або інша сутність – процес, підсистема і т. д.) передає інформацію від імені іншого користувача. Способи заміни ідентифікатора можуть бути різні, зазвичай вони визначаються помилками та особливостями мережних протоколів. Проте на прийомному вузлі таке повідомлення буде сприйняте як коректне, що може призвести до серйозних порушень роботи КМіС.

Розглянемо процес виконання атаки даного типу. Порушник, визначивши факт виконання криптографічного протоколу, перехоплює криптограму El. З її допомогою він може спробувати обчислити апостеріорні ймовірності різних можливих повідомлень:

$$P^{o|E_l} = \{P(I_1|E_l), P(I_2|E_l), \ldots, P(I_m|E_l)\};$$

і різних можливих ключів:

$$P^{K|E_l} = \{P(K_1|E_l), P(K_2|E_l), \ldots, P(K_k|E_l)\},$$

які могли бути використані при формуванні криптограми E_l.

Множини апостеріорних ймовірностей 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 приписані відповідні ймовірності. Одержавши 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 атака, як правило, пов’язана із спробами проникнення всередину периметра безпеки КМіС і часто реалізується хакерами.

Узагальнена модель активних атак “маскарад” подана на рис. 1.15- 1.16.

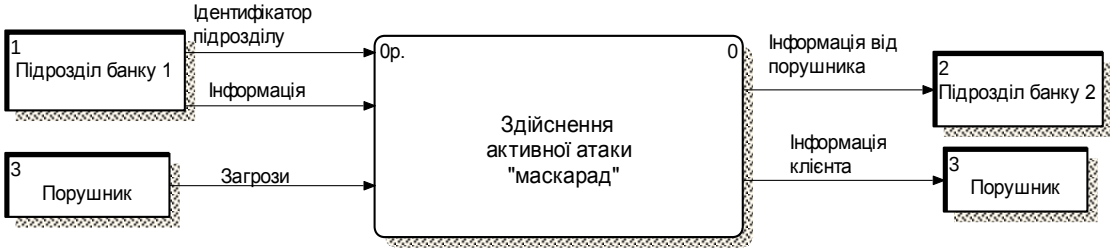

Рисунок 1.15 - Модель активних атак “маскарад”

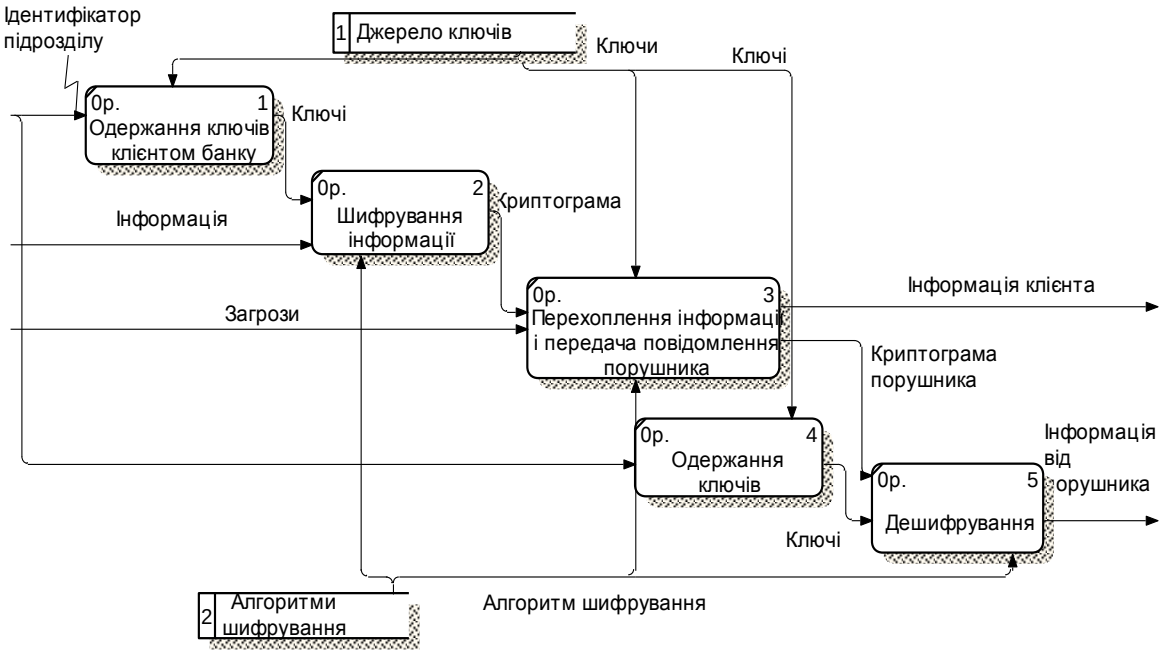

Рисунок 1.16 - Декомпозиція моделі активної атаки “маскарад”

При виконанні пасивної атаки порушник не впливає на протокол обміну інформацією в КМіС і намагається отримати інформацію про учасників протоколів за допомогою моніторингу мережі, тому пасивні атаки важко виявити. При активному розкритті криптопротоколів порушник намагається змінити протокол для власної потреби. Спроби виконання такого типу атаки

переслідує більш широкий набір задач: отримання інформації, погіршення роботи системи або отримання несанкціонованого доступу до ресурсів.

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

Оцінка ризику реалізації загроз безпеки заснована на захисті конфіденційних ресурсів, яка визначається за допомогою аналізу загроз, що діють на конкретний ресурс, уразливостей, через які дані загрози можуть бути реалізовані, і моделей атак.

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

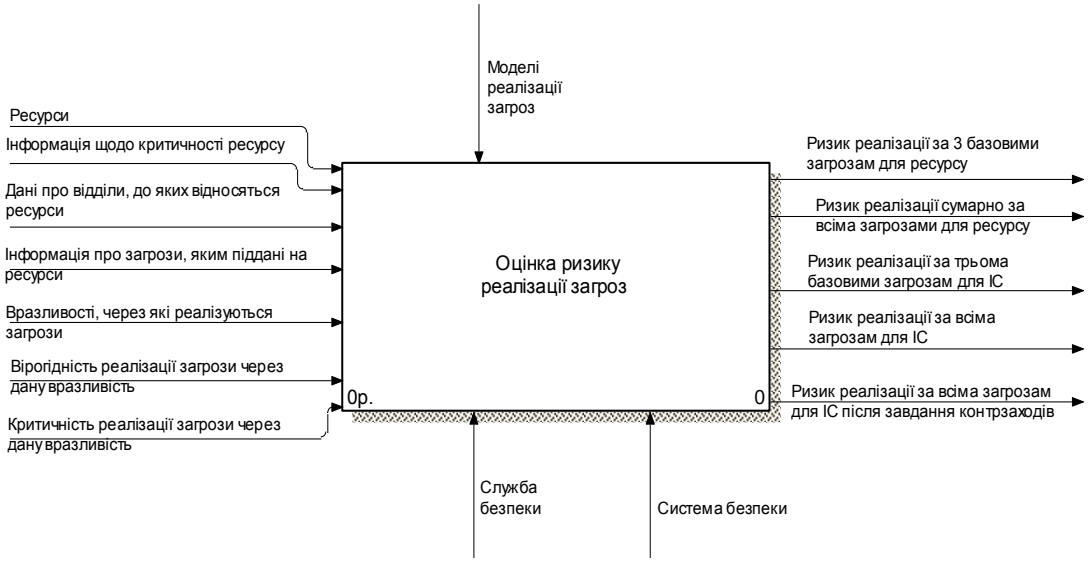

Рисунок 1.17 - Модель оцінки ризику реалізації загроз (контекстна діаграма)

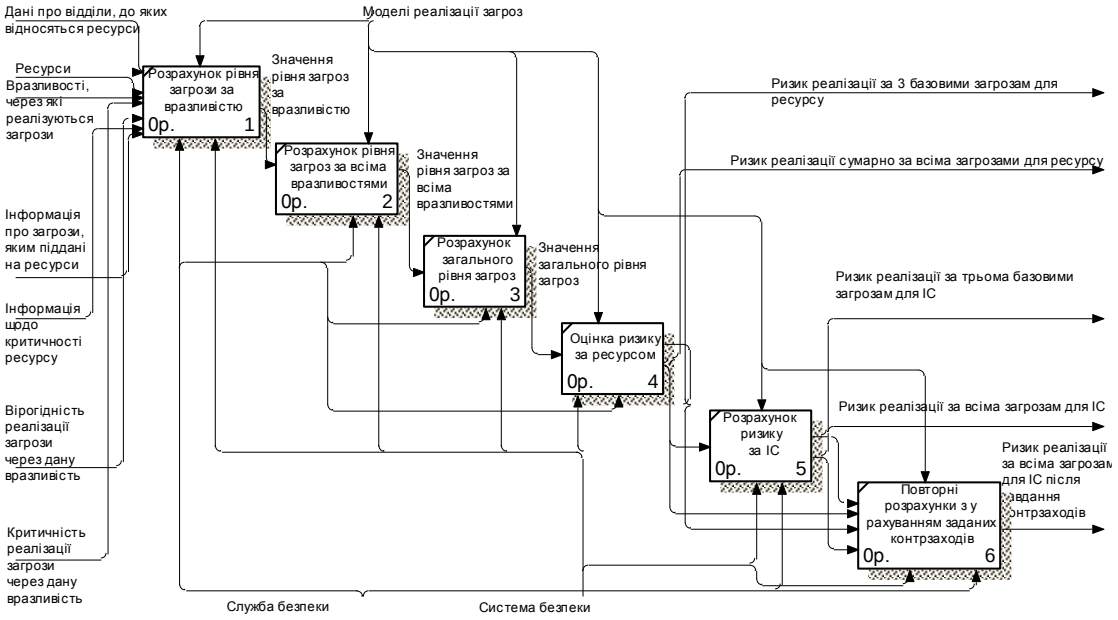

Рисунок 1.18 - Декомпозиція моделі оцінки ризику реалізації загроз

Для оцінки економічного збитку при реалізації загрози у телекомунікаційних системах пропонується використовувати узагальнену картку експерта-аналітика з захисту інформації, що дозволяє визначити найбільш уразливі місця, оцінити ризики та виробити комплекс заходів для забезпечення безпеки даних (табл. 1.1). При використанні картки експерта-аналітика вважаємо, що показник захищеності телекомунікаційних середнім систем Y_1= 5, тобто вони відносяться до систем із степенем вихідної захищеності.

На підставі ймовірностей загроз безпеки інформації (визначаються експертами-аналітиками) розраховується можливість її реалізації за формулою:

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

де Y_1 – степінь вихідної захищеності системи:

0 – для високої, 5 – для середньої, 10 – для низького степеня вихідної захищеності.

Y_2 – імовірність реалізації загрози:

0 – для малоймовірної загрози; 2 – для низької ймовірності загрози; 5 – для середньої ймовірності загрози; 10 – для високої ймовірності 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.

Таблиця 1.1 - Картка оцінки загроз безпеки телекомунікаційних систем

Найменування загрози	$\mathbf{Y_2}$	**Y**		**Методи протидії**	
				Технічні	**Організаційні**
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 адміністратора безпеки; Технологічний процес обробки; Акт встановлення засобів захисту; виключення електричних ліній які виходять за межі контрольованої зони ліній; розміщення трансформаторної підстанції в контрольованій зоні; контур заземлення

Продовження табл. 1.1

1	2	3		4	5
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 встановлення 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 ПО; настроювання засобів захисту; захист приміщення	Інструкція користувача; Інструкція адміністратора безпеки; технологічний процес обробки; Інструкція з антивірусного захисту; Акт встановлення засобів захисту; опломбування; сертифікація
Загрози ненавмисних дій користувачів і порушень безпеки функціонування ВПБС, через збої в програмному забезпеченні, а також від загроз (збоїв апаратури та електроживлення) і стихійного (ударів блискавок, пожеж, овеней і т.п.) характеру.	10	0,75	середня	Настроювання засобів захисту; доступ до встановлення режимів роботи засобів захисту надається тільки адміністратору безпеки; використання джерел безперебійного електроживлення; пожежна сигналізація; система захисту від НСД	Інструкція користувача; Інструкція адміністратора безпеки; резервне копіювання; Акт встановлення засобів захисту; дозвільна система допуску; технологічний процес обробки; 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 встановлення засобів захисту
Загрози перехоплення при передачі провідними (кабельними) лініями зв'язку	10	0,75	висока	Шифрування; фізичний захист каналу зв'язку	Пропускний режим; технологічний процес

1.10.Для оцінки ризику реалізації загроз у комунікаційних системах пропонується використовувати наступну методику:

На першому етапі розраховується *рівень загрози за уразливістю Th* на основі критичності та можливості реалізації загрози через дану уразливість. Рівень загрози показує, наскільки критичним є вплив даної загрози на ресурс із урахуванням імовірності її реалізації.

$$\mathrm{Th}_{c,I,a} = \frac{\mathrm{ER}_{c,I,a}}{100} P(V)_{c,I,a},$$

де $\mathrm{ER}_{c,I,a}$ – критичність реалізації загрози (%);

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

Під *критичністю реалізації загрози* (*ER*) розуміється степінь впливу реалізації загрози на ресурс, тобто як сильно реалізація загрози вплине на роботу ресурсу і складається з критичності реалізації загрози за конфіденційністю, цілісністю та доступністю (*Erc, Eri, Era*). Обчислюється одне або три значення залежно від кількості базових послуг безпеки. Отримується значення рівня загрози за уразливістю в інтервалі від 0 до 1. Під *базовими послугами безпеки* розуміється порушення конфіденційності, автентичності і цілісності даних.

На другому етапі розраховується *рівень загрози за всіма уразливостями Cth*, через які можлива реалізація даної загрози на ресурсі однієї з формул залежно від кількості використовуваних базових послуг у ВПБС:

для режиму з однією базовою послугою безпеки:

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

для режиму із трьома базовими послугами безпеки:

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

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

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

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

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

для режиму з однією базовою загрозою:

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

для режиму із трьома базовими загрозами:

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

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

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

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

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

$R = \mathrm{CThR} \cdot D$,

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

Під *критичністю ресурсу* (*D*) розуміється степінь значимості ресурсу для інформаційної системи, тобто як сильно реалізація загроз інформаційної безпеки на ресурс вплине на роботу інформаційної системи.

Залежно від обраного режиму роботи, може складатися із критичності ресурсу за конфіденційністю, цілісністю та автентичністю і визначається для режиму із трьома базовими послугами безпеки за формулами:

$$R_c = \mathrm{CThR}_c \cdot D_c$$

$$R_i = \mathrm{CThR}_i \cdot D_i$$

$$R_a = \mathrm{CThR}_a \cdot D_a$$

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

де$D_{a,\mathrm{ci}}$ – критичність ресурсу за 3 послугами безпеки;

R – сумарний ризик за трьома загрозами.

Таким чином, одержимо значення ризику за ресурсом в рівнях (заданих користувачем) або грошах.

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

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

або для режиму роботи в рівнях:

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

Для режиму роботи із трьома загрозами (у грошах):

$$\mathrm{CR}_{a,i,c} = \sum_{i=1}^{n} R_{i_i}$$

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

де $\mathrm{CR}_{a,i,c}$ – ризик системи з кожного виду загроз.

CR – ризик системи сумарна за трьома видам загроз,

або для режиму роботи в рівнях:

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

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

Таким чином, пропонуєма методика дозволяє оцінити економічний збиток при реалізації загрози на ВПБС при використанні, як окремих засобів захисту, так і при комплексному забезпечені захисту банківських транзакцій. Для аналізу ефективності використання засобів захисту пропонується оцінити введений "контрзахід" (E) за виразом:

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

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.

Розглянемо розрахунки ризиків для однієї послуги інформаційної безпеки, так як, для інших послуг ризик розраховується аналогічно на прикладі критичних систем управління комерційного банку.

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

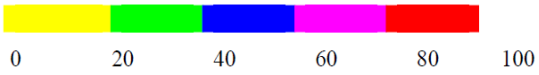

Рисунок 1.19 - Шкала оцінки критичності ресурсу

Критичність ресурсу визначається відповідно до цінності збереженої в системі інформації, при цьому під *цінністю інформації* розуміється той позитивний ефект, який може бути отриманий при її використанні на розглянутому інтервалі часу.

Визначимо значення критичності сервера банку рівне 100%, тому що втрата конфіденційної інформації, що перебуває на сервері, приводить до її втрати і відповідно руйнуванню всієї ВПБС в цілому. Відповідно до розроб-

леного алгоритму проводимо розрахунки при виникненні різних загроз (табл. 1.2).

Таблиця 1.2 - Загрози та уразливості в ВПБС

Загрози	Уразливості	$P(V)$	ER,%
Загроза 1. Розкрадання апаратних засобів, носіїв інформації шляхом фізичного доступу до них	Уразливість1. Відсутність регламенту доступу в приміщення з ресурсами, що містять банківську (конфіденційну) інформацію	0,35	70
	Уразливість2. Існуюча система спостереження охоплює не всі важливі об'єкти	0,35	70
Загроза 2. Несанкціонований доступ каналами зв'язку	Відсутність міжмережного екрана	0,75	70
Загроза 3. Збій електроживлення	Відсутність джерела безперебійного електроживлення	0,75	40

Результати розрахунків оцінки ризику ресурсу представлені в табл. 1.3.

Таблиця 1.3 - Результати розрахунків оцінки ризику ресурсу

Загроза/уразливість	Th	Cth	Cthr	R,%
Загроза1/уразливість1	0,245	0,43	0,8105	81,05
Загроза1/уразливість2	0,245			
Загроза2/уразливість	0,525	0,525		
Загроза3/уразливість	0,3	0,3		

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

2. ОСНОВНІ ПРИНЦИПИ ЗАХИСТУ ІНФОРМАЦІЇ ПРИ ПІДКЛЮЧЕННІ ДО МЕРЕЖІ ІНТЕРНЕТ

Для підключення мережі організації (будь-який) до мережі Інтернет необхідно прийняти ряд певних організаційно-технічних заходів для її захисту.

При побудові захисту варто виходити з того, що будь-який захист ускладнює використання системи, що, за прямим призначенням обмежує функціональні можливості, споживає обчислювальні й трудові ресурси, вимагає фінансових витрат на створення та експлуатацію. Чим вище захист, тим дорожчою у побудові та обслуговуванні стає система і тим менш зручною для безпосередніх користувачів.

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

2.1. Firewall (Брандмауер)

Основним загальновизнаним засобом такого захисту є міжмережний екран (Брандмауер). Міжмережний екран установлюється між мережею та Internet і виконує роль мережного фільтра (рис. 2.1).

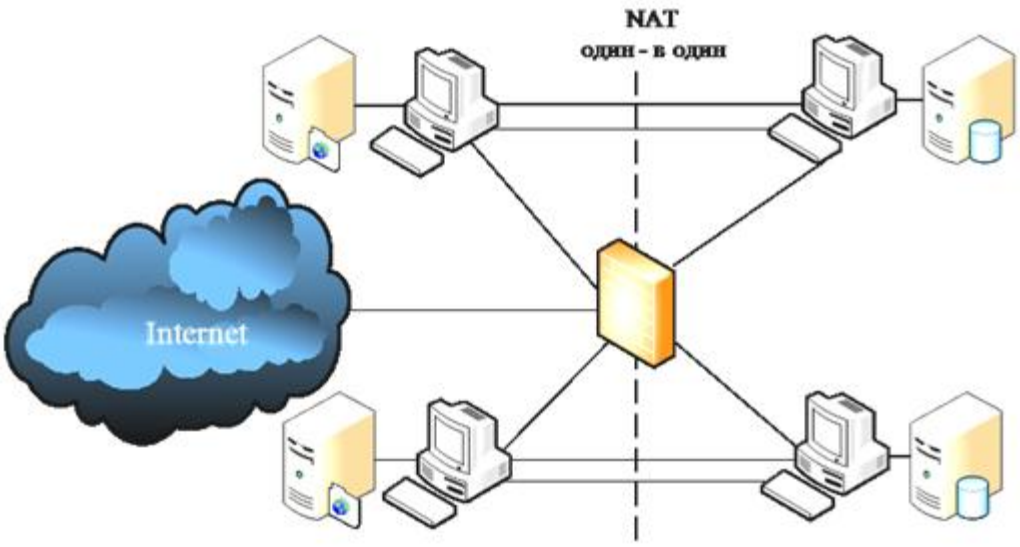

Рисунок 2.1 - Встановлення брандмауера у локальній мережі

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

Допустимість того або іншого трафіка визначається мережним адміністратором відповідно до політики інформаційної безпеки організації. (Наприклад, може бути дозволений доступ із частини комп'ютерів мережі до web та ftp-серверів Internet і двонаправлений доступ між Internet та поштовим сервером, але при цьому заборонені всі інші протоколи й напрямки трафіка).

Таким чином, міжмережний екран фізично розташовується на місці мережного шлюзу (маршрутизатора), логічно представляється доцільним сполучити їх функції в одному пристрої. Це дозволяє одним засобом захистити й локальну мережу і безпосередньо сам шлюз. Така опція передбачена для маршрутизаторів компанії Cisco Systems (Firewall Feature Set). Однак дане правило є необов'язковим і міжмережний екран може бути поданий окремим пристроєм.

У найпростішому випадку виконання функцій міжмережного екрана можна організувати за допомогою мережного фільтра на основі аркушів дос-

тупу (access-lists). Аркуші доступу визначають правила, за якими або дозволяється, або забороняється проходження трафіка з певними ознаками від одного мережного інтерфейсу маршрутизатора до іншого усередині самого маршрутизатора. Як ознаки можуть використовуватися *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 аркушів доступу порівняно із сьогоднішнім міжмережним екраном полягає у тому, що вони дозволяють створити статичний однобічний фільтр, тоді як мережне з'єднання становить динамічний процес. Аркуші доступу не дозволяють контролювати параметри IP-пакета, що залежать від попередніх пакетів. Звідси виникає складність застосування аркушів 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 мережної атаки, як "викрадення з'єднання", або "хай-джекінг".

У Firewall Feature Set зазначені проблеми вирішуються за допомогою того, що він відслідковує кожне мережне з'єднання окремо і контролює весь процес у динаміку. При встановленні нового TCP-сеансу міжмережний екран створює для нього новий процес, що контролює правильність з'єднання до самого моменту його завершення. При цьому кожний пакет на транспортному рівні перевіряється на відповідність попередній, а всі "підозрілі" пакети відбраковуються. 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.

Іншими словами, у настроюваннях міжмережного екрана задаються правила для проходження трафіка від одного інтерфейсу до іншого, для кожного напрямку й кожного тракту окремо. Якщо правило дозволяє проходження IP-пакета від інтерфейсу внутрішньої мережі до Internet-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 вичерпаний час очікування, тунель закривається, і обіг ззовні до внутрішнього комп’ютера буде відкинутий. З цієї ж причини екран не пропустить пакети у зворотному напрямку, якщо ініціатором з’єднання є зовнішній комп’ютер.

Крім того, міжмережний екран, на відміну від аркушів доступу, може контролювати зміст IP-пакетів у полі даних і відбраковувати пакети, що містять потенційно-небезпечні коди, наприклад, java-апліти. Є міжмережні екрани, здатні виявити в IP-пакетах ознаки відомих мережних 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 вище й засоби керування iptables. Через те що Linux є безкоштовною ОС, витрати на побудову такого міжмережного екрана зводяться до придбання звичайного персонального комп’ютера із двома мережними інтерфейсами.Проте Linux дозволяє побудувати досить надійний і гнучкий мережний фільтр, що розпізнає окремі прапори в службових полях IP-пакета.

2.1. NAT

Другою цеглинкою забезпечення захищеності мережі є “заміна мережної адреси” – Network Address Translation, або NAT. Вона становить заміну в IP-пакеті реальної адреси комп’ютера внутрішньої мережі на будь-яку іншу задану адресу при посиланні його в зовнішню мережу. Завдяки цьому для внутрішньої мережі стає можливим використання діапазонів адрес, які не застосовуються в Internet (наприклад, 10.0.0.0 – 10.255.255.255). Це дозволяє запобігти прямому обігу ззовні до внутрішніх комп’ютерів і приховує структуру мережі. Існує кілька різновидів NAT.

Найпростіша й найбільш марна з погляду захисту – це трансляція фіксованої внутрішньої адреси у фіксовану зовнішню. При цьому противник безперешкодно «бачить» такий комп’ютер у зовнішній мережі, тому що йому

однозначно відповідає певна зовнішня адреса. Однак вона необхідна при організації сервера, до якого потрібно забезпечити доступ ззовні (Рисунок 2.2).

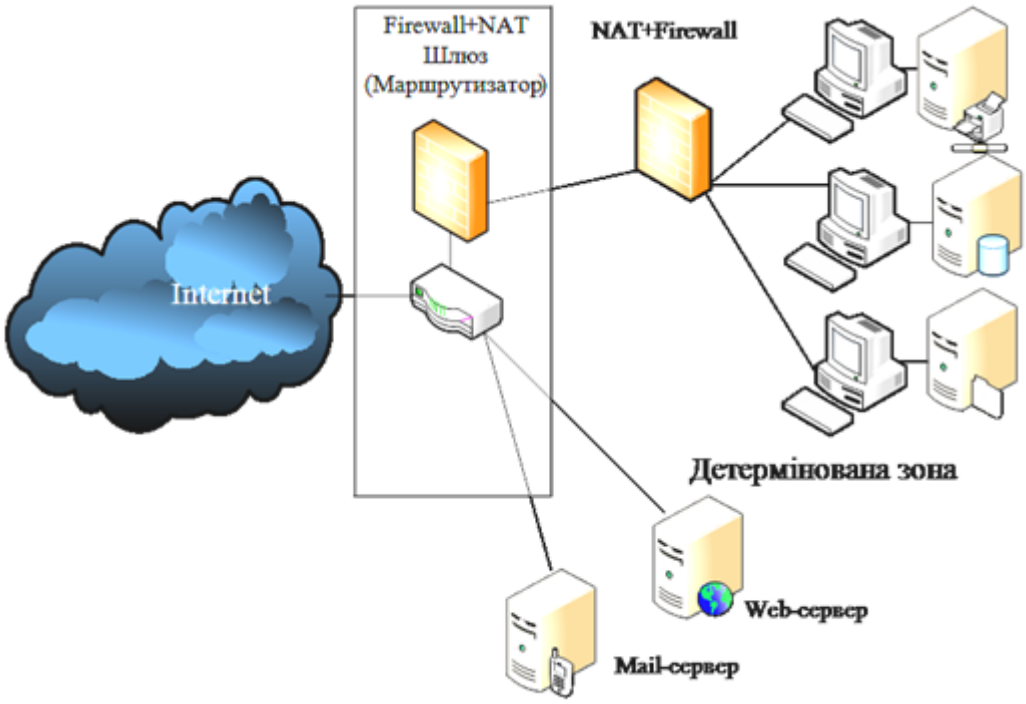

Рисунок 2.2 - Трансляція фіксованої внутрішньої адреси
у фіксовану зовнішню

Друга форма NAT – це трансляція групи внутрішніх адрес в одну зовнішню. При цьому всі внутрішні комп'ютери можуть працювати з Internet одночасно, а маршрутизатор розрізняє, кому яка відповідь перетранслюється 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). Якщо противник, навіть бачить трафік, що виходить із внутрішньої мережі, то він не може визначити, від якого комп'ютера він виходить. Крім того, це виключає можливість ініціативного обігу ззовні до внутрішнього комп'ютера, тому що для маршрутизатора в цьому випадку відсутнє правило прив'язки зовнішньої ад-

реси до внутрішньої. Зокрема виключається можливість сканування ззовні внутрішньої мережі.

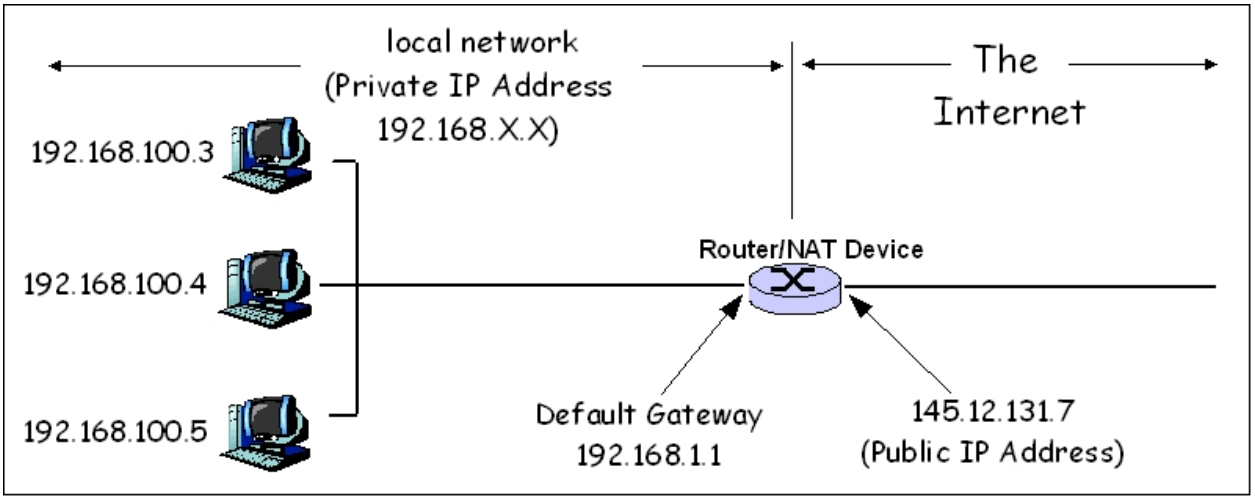

Рисунок 2.3 - Трансляція групи внутрішніх адрес в одну зовнішню

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

2.3. Демілітаризована зона

Як правило, організації потрібно мати у себе деякі мережні ресурси, до яких відкритий доступ з Internet. Звичайно це поштовий, dns і web-сервери. Механізм їх роботи допускає, що до них повинен бути дозволений вільний або слабко обмежений обіг з Internet. Відповідно ймовірність їх зламу вища, ніж інших комп'ютерів мережі. Із цієї причини розміщати їх усередині зони, яка захищається, недоцільно з погляду безпеки, тому що у випадку 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 міжмережним екраном, що забезпечує захист внутрішніх комп'ютерів. Логічну область їх розміщення називають демілітаризованою зоною (рис. 2.4).

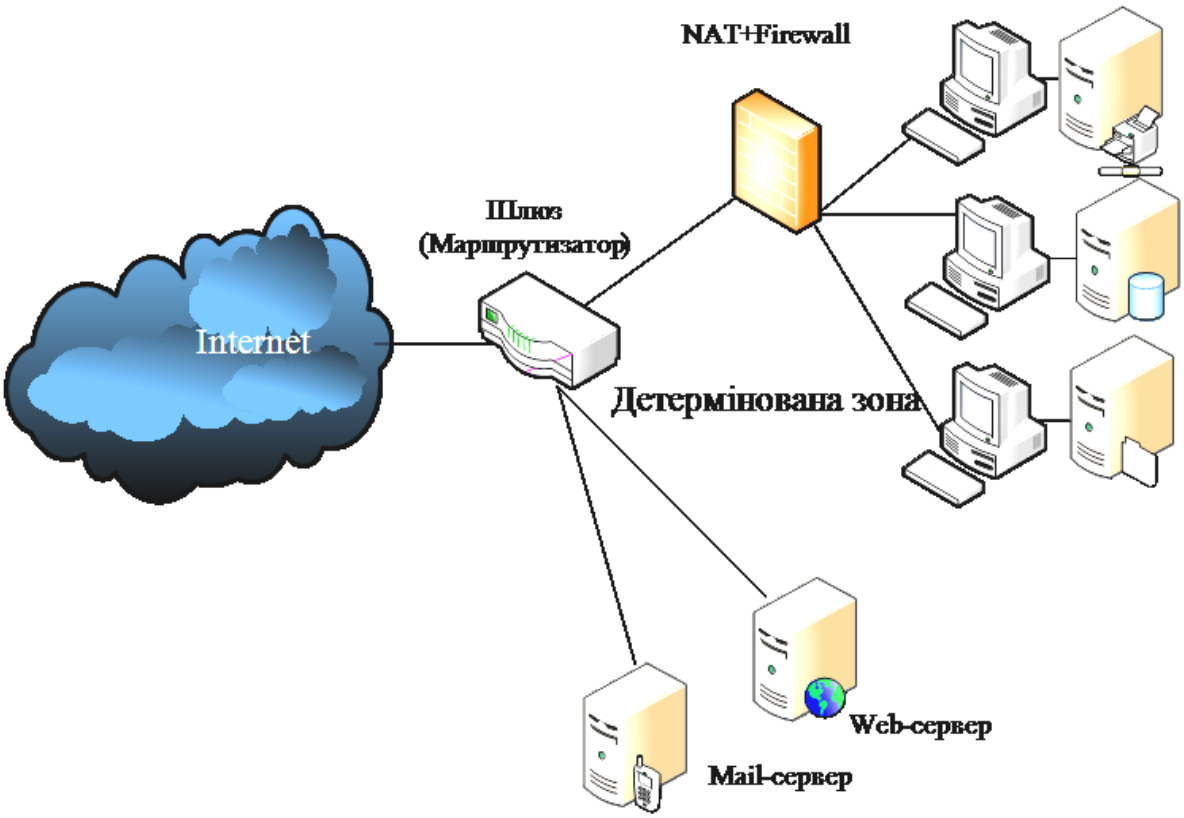

Рисунок 2.4 - Демілітаризована зона

2.4. Другий firewall

З рис. 2.4 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. При правильному настроюванні обох міжмережних екранів противнику буде вже набагато сутужніше дістатися до внутрішньої мережі організації. Наявність другого міжмережного екрана ускладнює конфігурування мережного встаткування й настроювання роботи всіх елементів мережі. Для додаткового підвищення захищеності можна використати *Firewall*-и різних виробників. Тоді якщо в одному з них буде виявлена вразливість, інший не до-

зволить противнику безперешкодно проникнути у мережу, як це мало б місце при використанні *Firewall*-ів одного типу.

Особливо варто підкреслити, що можливість мережного доступу до шлюзів і до міжмережних екранів, щоб уникнути зловмисного використання, повинна бути відключена. З погляду безпеки пристрої, які знаходяться на стражі мережі, повинні конфігуруватися й адмініструватися тільки через консольний порт локально (рис. 2.5).

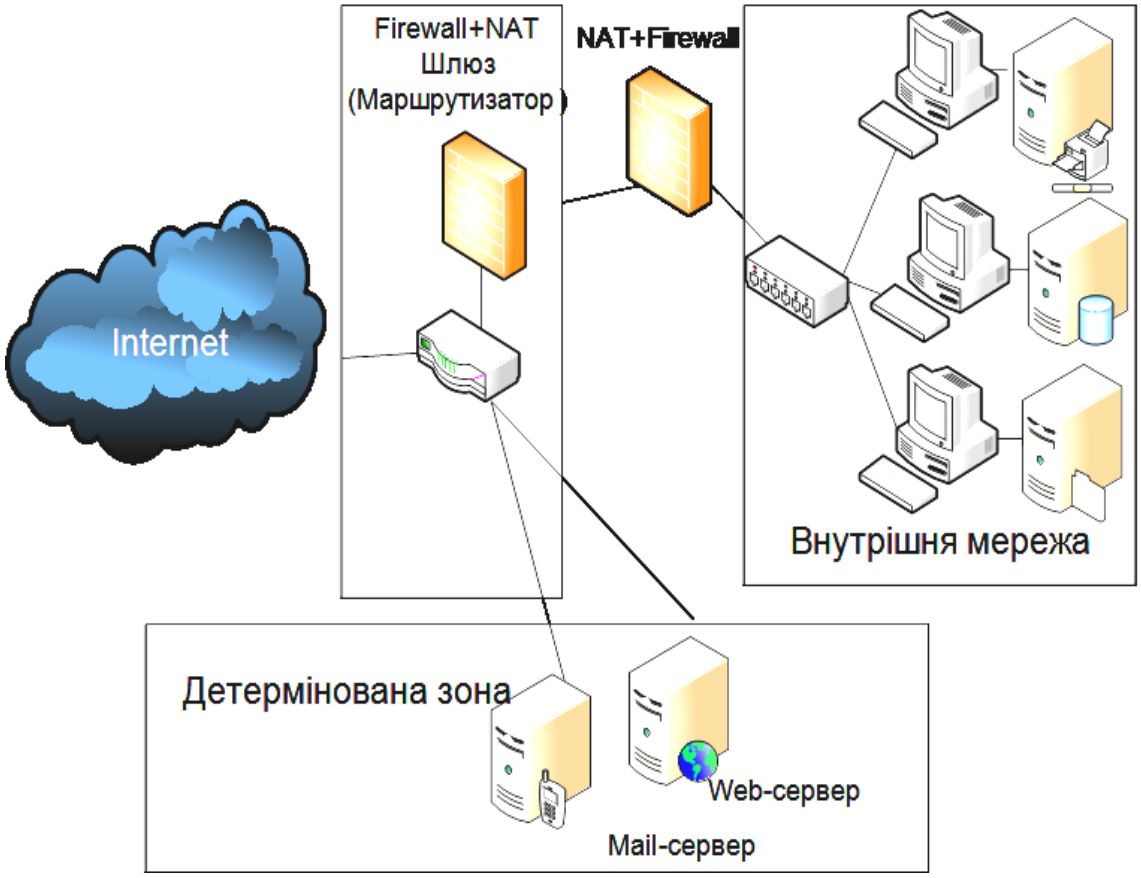

Рисунок 2.5 - Локально-консольний порт для серверів

Схема, запропонована на рис. 2.5, може бути дещо вдосконалена. Для цього необхідно використати граничний маршрутизатор із двома Ethernet-портами (рис. 2.6).

2.5. Proxy-сервер

Використання так званого “посередника” (proxy-сервера) також підвищує рівень захищеності мережі, тому що виключає необхідність прямого виходу в Internet комп’ютерів користувачів. При цьому також стає можливим більш строгий контроль за даними в IP-пакетах на рівні мережних додатків. Proxy-сервер працює як посередник між користувальницьким додатком і вилученим мережним ресурсом в Internet. Схематично сутність його роботи показана на рис. 2.6.

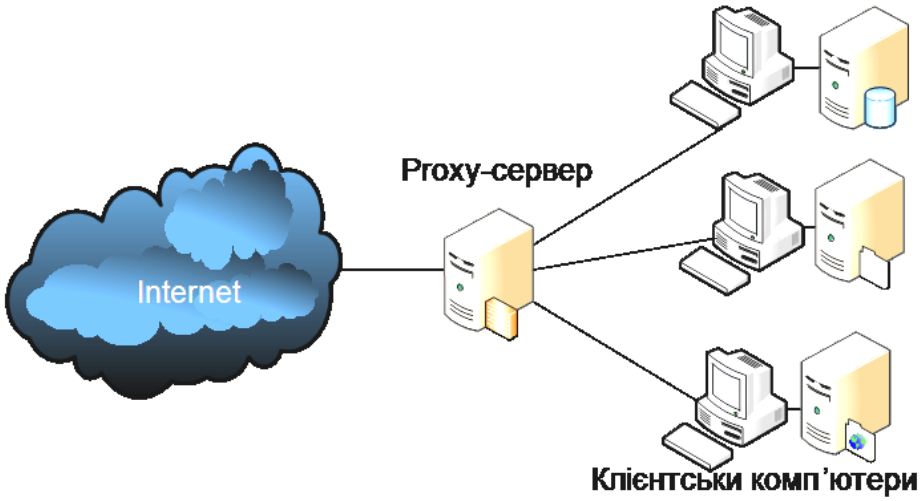

Рисунок 2.6- Proxy-сервер

Proxy-сервер складається ніби із двох частин, клієнтської і серверної. Клієнтська частина дивиться у сторону Internet, серверна – у сторону клієнтського комп’ютера. Коли клієнтський комп’ютер звертається до вилученого сайта через *proxy*-сервер, його клієнтський мережний додаток взаємодіє із серверною частиною *proxy*-сервера. При цьому *proxy*-сервер на рівні додатка передає клієнтський запит своєї клієнтської частини, і вона вже від імені *proxy*-сервера надсилає даний запит на вилучений сайт. Тобто *IP*-пакет що відправлений має адресу *proxy*-сервера.

Потім отримана відповідь передається у зворотну сторону від клієнтської частини *proxy*-сервера його серверної частини, з якою безпосере-

дньо взаємодіє користувальницький комп'ютер. Таким чином, пряме з'єднання клієнтських комп'ютерів з вилученим сайтом виключається. Усередині *proxy*-сервера передача даних між клієнтською частиною й серверною відбувається вже не на транспортному рівні, а на рівні протоколу додатка, ніж забезпечується легкість контролю команд і даних на відповідність установленим стандартам. Крім того, це дозволяє забезпечити досить надійний контроль проти передачі зловмисних кодів усередині даних. Навіть у випадку успішної атаки з боку Internet за відкритими протоколами у цьому випадку буде ушкоджений тільки *proxy*-сервер, що не представляє інформаційної цінності, а користувальницькі комп'ютери будуть залишатися в безпеці ще якийсь час.

Через те що *proxy*-сервер працює тільки за декількома відомими протоколами (HTTP, FTP та інших) 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.

2.6. Другий mail-сервер

Залишати *mail-сервер* у демілітаризованій зоні з однієї сторони небажано, тому що на ньому фактично зберігається поштова база даних з перепискою локальних користувачів, а демілітаризована зона не може забезпечити належного рівня захисту мережним 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.

Внаслідок цього доречним рішенням є використання двох поштових серверів. Основний сервер установлюється усередині мережі, яка захищена, і його не видно для зовнішнього світу. Всі локальні користувачі поштової системи заводяться на нього і мають до нього прямий доступ. Відповідно вся вхідна кореспонденція зберігається на ньому у поштових скриньках локаль-

них користувачів. Відправлення електронної пошти також здійснюється через нього.

Другий, або зовнішній, поштовий сервер установлюється в демілітаризованій зоні й забезпечує взаємодію по e-mail з Internet. Він настроюється таким чином, щоб всю 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 жоден аркуш не відкладається для довгострокового зберігання. Тому якщо він виявиться зламаним зловмисником, то противник не одержить доступу до накопиченої переписки. Проте після зламу противник одержує можливість перехоплення й читання транзитної пошти. Тому потрібен ретельний контроль за подібною ситуацією й негайне вживання заходів при підозрі на НСД (несанаційного доступу).

Перевагою такої схеми є те, що навіть зі зламаного зовнішнього поштового сервера не так просто дістатися до внутрішньої захищеної мережі. Обмін даними між зовнішніми й внутрішнім поштовими серверами відбувається через міжмережний екран з єдиним дозволеним портом (SMTP) за єдиною дозволеною парою адрес. Звертання до інших комп'ютерів і по інших протоколах буде блокуватися. 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 досить встановити покажчик на інфікований конверт, щоб вірус активізувався. Але більш небезпечним є те, що механізм роботи поштових вірусів може бути використаний зловмисником для закидання в область мережного "троянського коня", якими захищається. Він дозволить противнику таємно скачувати дані з вашої мережі та здобути всю інформацію, що цікавить. Тому забезпеченню антивірусного захисту трак-

ту доставки пошти у внутрішню мережу варто приділити досить серйозну увагу.

Існує ряд програмних засобів, призначених для контролю кореспонденції на поштових серверах на предмет наявності в ній вірусів у процесі прийому й пересилання електронної пошти.

Принцип її роботи полягає в тому, що вся пошта, що проходить через сервер, спочатку перенаправляється спеціальному користувачу, у ролі якого виступає антивірусний процес. Він сканує зміст кожного аркуша на наявність у ньому фрагментів відомих вірусів. Якщо аркуш містить щось схоже на вірус, воно вилучається із процесу передачі й, залежно від настроювань антивірусу, піддається заданій обробці. Повідомлення про виявлений вірус відсилаються відправнику й одержувачу інфікованого аркушу, а також на ім'я зазначених адміністраторів системи. Після перевірки аркуші, що не викликають підозри, відсилаються за призначенням.

Тим самим на рівні поштового сервера ставиться надійний захист відомим вірусам у 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 сайта. Інакше мережа може стати уразливою для знову створених вірусів.

2.7. Log-сервер

Загальновідомий механізм протоколювання системних подій на серверах і клієнтських робочих станціях. Розроблювачі програмного забезпечення включають у свої продукти фрагменти коду, які на ту або іншу подію генерують відповідні текстові повідомлення, що посилають операційній системі. Система збирає дані повідомлення в log-файлах, які потім можуть аналізуватися адміністратором або користувачем з метою з'ясування, які події відбувалися в системі деякий час потому. Це дозволяє, наприклад, з'ясувати, чому не запускається та або інша програма, або чому припинив функціонувати певний сервіс. Дуже корисні log-файли для пошуку слідів зламу системи й від-

відування її несанкціонованими гостями. Через те що злом, як правило, супроводжується множиною заборонених дій, це породжує велику кількість системних повідомлень, що осідають в log-файлах. Із цієї причини 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 проникнули, як довго в ній перебували, ніж встигли покористуватися. Або навіть просто переконатися, що все добре.

Тому обов'язковою умовою для мережі, підключеної до Internet, є наявність у ній окремого log-сервера.

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 міжмережні екрани. Збираючи такі повідомлення на спеціально виділеному сервері, ми забезпечуємо їм схоронність від рук противника. Тому для мінімізації ймовірності зламу log-сервер повинен бути призначений тільки для збору *log*-повідомлень. Він не повинен виконувати будь-яких інших функцій і виконувати інші мережні додатки, крім syslogd. У цьому випадку 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 наступна схема підключення локальної мережі до Internet (рис. 2.7).

Таким чином, проведений аналіз способів захисту комп'ютерних мереж при підключені їх до глобальної мережі Інтернет показав, що для забезпечення захисту при обміні інформацією абоненти локальної мережі повинні використовувати принципи і засоби безпеки в комплексі з організаційними заходами. Це дозволить надійно захистити від атак як активних, так і пасивних противників.

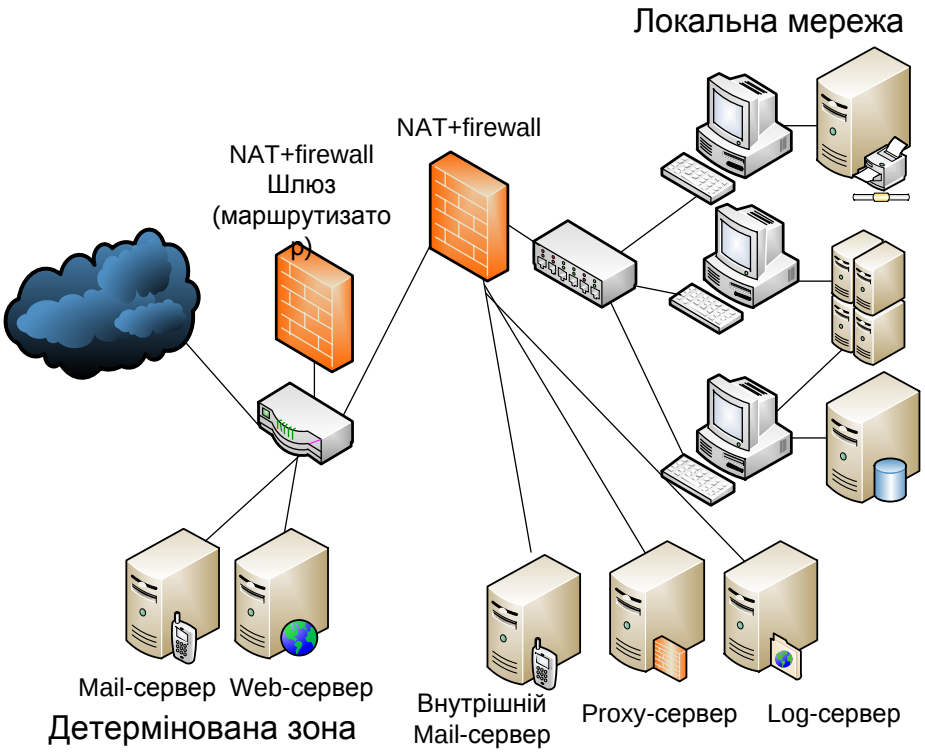

Рисунок 2.7 - Схема з *Log-сервером*

3. ЗАВДАННЯ

Графічне. Побудувати за допомогою MSVizio структурну схему побудови корпоративної мережі компанії

У корпоративній мережі компанії, що розташовується в 2-х будинках (4 поверхи та 2 поверхи відповідно), кількість ПК і мережеві технології визначені у табл. 3.1. Розробити структурну схему захисту корпоративної мереж компанії, обґрунтувати та запропонувати необхідні протоколи каналів зв'язку, і програмно-апаратні засоби для забезпечення конфіденційного обміну інформацією між користувачами другого будинку; забезпечити надійний захист при виході користувачів до мережі Internet. Програмно-апаратні засоби забезпечення безпеки при підключені до Internet визначені у табл. 3.2.

Розрахункове. Провести розрахунки ризику інформаційної безпеки при підключені до мережі та можливості проведення активної (пасивної) атаки.

Оформлення завдання здійснювати у відповідності до Системи стандартів з організації навчального процесу (ТЕКСТОВІ ДОКУМЕНТИ У СФЕРІ НАВЧАЛЬНОГО ПРОЦЕСУ. Загальні вимоги до виконання. СТВУЗ-ХПІ-3.01-2010). Загальний обсяг до 15 сторінок. Варіант завдання для кожного студента визначається у відповідності за номером у Журналі академічної групи.

Таблиця 3.1 - Кількість ПК і мережеві технології

№ варіанту	**Кількість ПК 1 будинок**	**Мережеві технології**	**Кількість ПК 2 будинок**	**Мережеві технології**
1	8	Ethernet	FDDI	6
2	10	100AnyLAN	WiFi	4
3	6	Token Ring	Fast Ethernet	8
4	12	WiFi	Token Ring	12
5	14	Ethernet	WiFi	14
6	20	100AnyLAN	Token Ring	16
7	8	Fast Ethernet	100AnyLAN	20
8	6	Ethernet	FDDI	8
9	4	100AnyLAN	WiFi	10
10	8	Token Ring	Fast Ethernet	6
11	12	WiFi	Token Ring	12

Продовження таблиці 3.1

12	14	Ethernet	WiFi	14
13	16	100AnyLAN	Token Ring	20
14	20	Fast Ethernet	100AnyLAN	8
15	8	Ethernet	FDDI	6
16	10	100AnyLAN	WiFi	4
17	6	Token Ring	Fast Ethernet	8
18	12	WiFi	Token Ring	12
19	14	Ethernet	WiFi	14
20	20	100AnyLAN	Token Ring	16
21	8	Fast Ethernet	100AnyLAN	20
22	6	Token Ring	Fast Ethernet	8
23	12	WiFi	Token Ring	12
24	14	Ethernet	WiFi	14
25	20	100AnyLAN	Token Ring	16

Таблиця 3.2 - Програмно-апаратні засоби забезпечення безпеки при підключені до Internet

№ варіанту	**Програмне забезпечення**	**№ варіанту**	**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

Навчальне видання

Методичні рекомендації

до виконання індивідуального завдання з навчальної дисципліни

“Безпека програм та даних”

для студентів спеціальностей 122 “Комп’ютерні науки”,

121 “Інженерія програмного забезпечення”

денної форми навчання

Укладачі:

Євсеєв Сергій Петрович,

Шматко Олександр Віталійович,

Іващенко Оксана Віталіївна

Відповідальний за випуск С.П. Євсеєв

Роботу до видання рекомендував В. М. Федорченко

Видавець і виготовлювач

Видавничий центр НТУ «ХПІ»,

вул. Кирпичова, 2, м.Харків-2, 61002

Свідоцтво про державну реєстрацію ДК № 3657 від 24.12.2009 р.