

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ЕКОНОМІКО-ТЕХНОЛОГІЧНИЙ
УНІВЕРСИТЕТ ТРАНСПОРТУ

Гончарова Л.Л.
Возненко А.Д.
Стасюк О.І.
Коваль Ю.О.

ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ
В ТЕЛЕКОМУНІКАЦІЙНИХ
ТА КОМП'ЮТЕРНИХ МЕРЕЖАХ

2013

РЕЦЕНЗЕНТИ

Корченко О. Г. Завідувач кафедри «Безпеки інформаційних технологій» проф., доктор техн. наук, Національний авіаційний університет;

Танкевич С. М. Провідний науковий співробітник, проф., доктор техн. наук Інституту електродинаміки Національної академії наук України;

Віноградов М.А. проф. кафедри «Інформаційних технологій» Національного авіаційного університету, проф., доктор техн. наук.

*Рекомендовано Міністерством освіти і науки України
як навчальний посібник для студентів вищих навчальних закладів.
Лист № 1/11-6357 від 01.04.13*

Гончарова Л.Л., Возненко А.Д., Стасюк О.І., Коваль Ю.О.

Основи захисту інформації в телекомунікаційних та комп'ютерних мережах. – К., 2013. – 435 с., іл.160.

У навчальному посібнику викладено основні поняття організації безпеки інформаційних ресурсів. Розглянуті способи побудови інформаційно-комунікаційних систем та мереж на основі сучасних способів передачі і обробки інформації, а також режими роботи бездротових систем та мереж. Проведено класифікацію методів та засобів несанкціонованого доступу до інформаційних ресурсів. Викладено загальні поняття криптографічного аналізу і способи захисту інформації в інформаційних системах та мережах за допомогою криптографічних методів. Широко викладено засоби захисту інформації від несанкціонованого доступу. Розглянуто технологічні аспекти захисту інформації від руйнівних програмних впливів. Наводяться нормативно-правові методи інформаційної безпеки з урахуванням вітчизняних та міжнародних стандартів. Всі матеріали які надруковані в даному навчальному посібнику надані виключно для використання в освітніх цілях.

Автори висловлюють велику подяку доктору техн. наук, проф. О.К. Юдіну і доктору техн. наук, проф. О.Г. Корченко (Національний авіаційний університет) за консультації, рецензування і представлені результати наукових досліджень в галузі захисту інформації для навчального посібника. С.О. Пархоменко за розробку дизайну обкладинки.

Навчальний посібник призначено для студентів технічних спеціальностей вищих навчальних закладів, аспірантів, наукових та інженерно-технічних працівників з напрямку 050202 – «Автоматизація та комп'ютерно-інтегровані технології».

ЗМІСТ

Вступ.....	5
Розділ 1. БЕЗПЕКА ІНФОРМАЦІЙНИХ РЕСУРСІВ.....	7
1.1. Визначення.....	7
1.2. Загрози інформаційній безпеці.....	14
1.3. Моделі порушень інформаційних ресурсів.....	18
1.4. Методи і засоби організації інформаційної безпеки.....	23
1.5. Інформаційна система як об'єкт захисту.....	24
1.6. Атаки на інформаційні ресурси системи.....	30
1.7. Рівні захисту інформаційних систем.....	47
1.8. Основні принципи захисту інформації.....	50
Розділ 2. ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ СИСТЕМИ ТА МЕРЕЖІ.....	53
2.1. Визначення інформаційно-комунікаційних систем.....	53
2.2. Модель взаємодії відкритих системи OSI.....	59
2.3. Організація інформаційних систем передачі даних.....	71
2.4. Ієрархічна технологія серверної взаємодії.....	80
2.5. Організація взаємодії Web-навігаторів.....	87
2.6. Розподілена обробка інформації на основі мігруючих програм.....	90
2.7. Організація системи доступу до баз даних.....	95
2.8. Сучасні систем серверної взаємодії.....	99
2.9. Комп'ютерні мережі моніторингу режимів систем електропостачання залізниць.....	101
Розділ 3. ЗАХИСТ ДАНИХ У БЕЗДРОТОВИХ СИСТЕМАХ ПЕРЕДАЧІ.....	110
3.1. Особливості передачі інформації в бездротових мережах.....	110
3.2. Завадостійкі способи кодування в каналах безпроводного зв'язку.....	116
3.3. Організація мереж бездротового зв'язку.....	120
3.4. Супутникові інформаційні системи.....	133
3.5. Організація множинного доступу до інформаційних ресурсів.....	142
Розділ 4. ОРГАНІЗАЦІЯ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ.....	158
4.1. Основи криптографічного захисту.....	158
4.2. Криптографічні методи.....	163
4.3. Шифрування інформації в каналах зв'язку з використанням ключів.....	174
4.4. Алгоритми організації цифрового підпису.....	177
4.5. Алгоритми з використанням ключів.....	180
4.6. Криптографічний захист інформаційно-комунікаційних систем.....	200

Розділ 5. ОСНОВИ ЗАХИСТУ ВІД РУЙНІВНИХ ПРОГРАМНИХ ВПЛИВІВ.....	218
5.1. Захист програмного забезпечення. Класифікація загроз.....	218
5.2 Класифікація комп'ютерних вірусів.....	226
5.3 Методи та засоби захисту програмного забезпечення.....	235
5.4. Методи боротьби з вірусами.....	240
5.5.Захист програмного забезпечення від реасемблерів та налагоджувачів.....	246
5.6 Системний підхід до захисту ПЗ.....	250
Розділ 6. ЗАГАЛЬНІ ПОЛОЖЕННЯ ЗАХИСТУ ІНФОМАЦІЇ НА ОСНОВІ МІЖНАРОДНИХ СТАНДАРТІВ.....	257
6.1.Безпека інформаційних ресурсів у ІКСМ.....	259
6.2. Організація технічного захисту інформації.....	261
6.3.Методика і критерії оцінки захищеності інформації.....	267
6.4.Захист інформації на базі ISO/IEC.....	272
6.5. Задачі організації безпеки інформації.....	283
6.6. Управління доступом і забезпечення цілісності програмного забезпечення.....	289
СПИСОК ЛІТЕРАТУРИ.....	307

ВСТУП

Сучасний рівень розвитку виробництва характеризується широким впровадженням перспективних комп'ютерних технологій в різних сферах людської діяльності. Нові інформаційні технології активно впроваджуються в усі сфери діяльності держави. Інформаційні мережі обслуговують і управляють банківськими системами, космічними об'єктами, контролюють роботу атомних електростанцій, а також розподіляють електроенергію. В цьому плані показовим є електричне господарство залізничного транспорту України безпека руху якого тісно пов'язана з організацією високого рівня надійності та ефективності функціонування силового електричного обладнання тягових підстанцій, що тісно пов'язано з інформатизацією та інтелектуалізацією систем керування електропостачанням. Інформатизація технологічних процесів виробництва є характерною рисою існування сучасного суспільства. Інформаційно-комунікаційні системи передачі даних є основою обміну інформаційними ресурсами, завдяки яким здійснюється зберігання, передача й обробка інформації, а також надання послуг споживачам з умов впровадження найсучасніших технологій. Широке впровадження корпоративних інформаційно-комунікаційних систем і мереж є основою сучасного функціонування організацій та підприємств. Такий підхід відкриває можливість підвищити ефективність діяльності компаній за рахунок використання більш оперативної й повної інформації, а також розширяє нові можливості для взаємодії з потенційними клієнтами за допомогою загальнодоступних глобальних інформаційних мереж. Новітні інформаційно-комунікаційні технології відкрили можливість об'єднати корпоративні мережі в глобальне інформаційне середовище. Це призвело до появи такого унікального явища, як глобальні інформаційні системи та мережі передачі даних. Концепція організації інформаційно-комунікаційних мереж є логічним результатом розвитку інформаційних технологій та їх упровадження в усі сфери діяльності сучасного суспільства. Основна функція інформаційно-комунікаційних систем та мереж в умовах функціонування інтегрованих інформаційних комплексів полягає в організації оперативного та надійного обміну інформацією між абонентами, а також у скороченні витрат на передачу даних. Разом з перевагами застосування глобальних інтегрованих інформаційних систем та мереж передачі даних з'явилися дуже небезпечні ризики, стосовно взаємодії з відкритим і неконтрольованим зовнішнім інформаційним середовищем. Стало очевидним, що надійність функціонування інтегрованих інформаційних комплексів залежить не тільки від рівня захисту інформаційних даних в системі від несанкціонованого доступу, а також характеризується рівнем застосування сучасних технологій та методів захисту інформації від зовнішнього середовища і руйнівних програмних впливів. Досвід застосування комп'ютерних засобів і технологій управління виробництвом стимулював проведення нових наукових досліджень в сфері розробки нових принципів організації і

методів синтезу систем комплексного захисту інформації. Цей факт є дуже важливим при вирішенні спектру завдань, пов'язаних із керуванням електропостачання залізниць за допомогою комп'ютеризованих систем, високий рівень захисту інформації в яких дозволяє покращити якість функціонування електричних мереж, що надзвичайно важливо при значній фізичній зношеності енергетичного обладнання, збільшити терміни експлуатації системи електропостачання на тягу, забезпечити можливість своєчасного виконання регламентних і ремонтних робіт і, як наслідок, значно збільшити рівень безпеки руху залізничного транспорту України. Рішення цієї проблеми тісно пов'язано з необхідністю при створенні сучасних інтегрованих інформаційних комплексів, побудові, впровадженні й супроводу систем захисту інформації дотримуватись вимог державних і міжнародних стандартів. Важливість проблеми організації безпеки інформаційних технологій, обумовлені такими причинами:

- різким збільшення обсягів інформаційних потоків даних, що обробляється і передається каналами зв'язку та значним зростанням потужності сучасних автоматизованих комплексів;
- високим темпом росту сучасних інформаційних технологій у всіх сферах діяльності суспільства, і як наслідок, зростання кількості розподілених баз даних різного призначення й інтеграції до сучасного інформаційного простору;
- поширенню сучасних комутативних та безкомутативних мережних технологій і значному розширенню кількості джерел інформації та кола користувачів, які мають безпосередній доступ до інформаційних ресурсів та широкого спектру послуг, що надаються інформаційними системами.

В рамках навчального посібника під безпекою інтегрованих інформаційних систем будемо розуміти стан захищеності таких властивостей інформаційних ресурсів як цілісності, доступності і конфіденційності, що в комплексі забезпечують нормальний процес функціонування та гарантованого надання встановленого переліку послуг. Автори висловлюють велику подяку доктору техн. наук, проф. О.К. Юдіну і доктору техн. наук, проф. О.Г. Корченко (Національний авіаційний університет) за консультації, рецензування і представлені для навчального посібника результати наукових досліджень в галузі захисту інформації. Всі матеріали які надруковані в даному навчальному посібнику надані виключно для використання в освітніх цілях.

Розділ 1. БЕЗПЕКА ІНФОРМАЦІЙНИХ РЕСУРСІВ

1.1 . Визначення

Інформаційна безпека – це стан захищеності потреб інформації особистістю, суспільством і державою, при якому забезпечується їхнє існування і прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз [1-15].

Слід відзначити, що задоволення потреб в інформації призводить до оволодіння відомостями про навколишній світ та процеси, що протікають в ньому, тобто інформованості особистості, суспільства та держави. Стан інформованості визначає ступінь адекватності сприйняття суб'єктами навколишньої дійсності і як наслідок – обґрунтованість рішень та дій, що приймаються.

Інформаційну безпеку можна поділити на такі поняття щодо забезпечення стану захищеності:

- особистості, суспільства, держави від впливу неякісної інформації;
- інформації та інформаційних ресурсів від несанкціонованого впливу сторонніх осіб;
- інформаційних прав і свобод людини і громадянина.

Інформаційна безпека – це одна із сторін розгляду інформаційних відносин у межах інформаційного законодавства з позицій захисту життєво важливих інтересів особистості, суспільства, держави та акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами.

Інформаційне середовище [information environment] – сфера діяльності суб'єктів, пов'язана зі створенням, перетворенням і використанням інформації. Інформаційне середовище умовно поділяється на три основні предметні частини:

- створення і розповсюдження інформації;
- формування інформаційних ресурсів, підготовка інформаційних продуктів, надання інформаційних послуг;
- споживання інформації;
- створення і застосування інформаційних систем, інформаційних технологій і засобів їхнього забезпечення;
- створення і застосування засобів і механізмів інформаційної безпеки.

Об'єктами інформаційної безпеки [information security object] є свідомість, психіка людей; інформаційні системи та мережі різного масштабу і різного призначення. До соціальних об'єктів інформаційної безпеки звичайно відносять особистість, колектив, суспільство, державу, світове товариство.

Суб'єкти інформаційної безпеки [information security subject] – держава, що здійснює свої функції через відповідні органи; громадяни; суспільні або інші організації та об'єднання що володіють

повноваженнями із забезпечення інформаційної безпеки у відповідності до законодавства.

Інтереси особистості в інформаційній сфері полягають: в реалізації конституційних прав людини та громадянина на доступ до інформації, на використання інформації в інтересах здійснення не забороненої законом діяльності, фізичного, духовного та інтелектуального розвитку; в захисті інформації, що забезпечує особисту безпеку.

Інтереси суспільства в інформаційній сфері полягають у:

- забезпеченні інтересів особистості в цій сфері;
- зміцненні демократії;
- створенні правової соціальної держави;
- досягненні та підтриманні суспільного спокою;
- духовному відновленні держави.

Інтереси держави в інформаційній сфері полягають у створенні умов:

- для гармонійного розвитку державної інформаційної інфраструктури;
- для реалізації конституційних прав і свобод людини та громадянина в галузі одержання інформації та користування нею з метою забезпечення непорушності конституційного ладу, суверенітету та територіальної цілісності держави, політичної, економічної та соціальної стабільності, у безумовному забезпеченні законності та правопорядку, розвитку рівноправного та взаємовигідного міжнародного співробітництва.

Інформаційне забезпечення інформаційної безпеки [information support information security] включає збирання (добування) відомостей про дестабілізуючі фактори та інформаційні загрози, їхнє оброблення, обмін інформацією між органами керування і силами та засобами системи інформаційної безпеки.

Інформаційний захист [infosecurity] досягається шляхом внесення в порядку законодавчої ініціативи законопроектів, здійснення судового захисту, проведення оперативних заходів силами і засобами інформаційної безпеки.

Інформаційна кооперація [information cooperation] (лат. cooperatio, від соорего – співробітничая) – форма забезпечення інформаційної безпеки між рівноправними суб'єктами інформаційного процесу (фізичними, юридичними, міжнародними), яка включає сукупність їхніх взаємоузгоджених дій, спрямованих на одержання відомостей про дестабілізуючі фактори, дестабілізуючі й інформаційні загрози та захист від них доступними законними способами і засобами.

Для конкретної особистості такими способами і засобами можуть бути:

- судовий захист прав і свобод у використанні інформації;
- адміністративний захист її життєво важливих інтересів у інформованості з боку територіальних або відомчих органів інформаційної безпеки;

– автономний захист своїх прав і свобод в основному із застосуванням технічних засобів захисту, особистої, сімейної і професійної таємниці.

Це ж характерно і для суспільних об'єднань, організацій (підприємств). Разом із тим, при наявності у них власних органів інформаційної безпеки суттєво розширюються їхні можливості у сфері автономного захисту.

Інформаційна зброя – сукупність спеціально організованої інформації та інформаційних технологій, яка дозволяє цілеспрямовано змінювати (знищувати, спотворювати), копіювати, блокувати інформацію, долати системи захисту, обмежувати допуск законних користувачів, здійснювати дезінформацію, порушувати функціонування носіїв інформації, дезорганізовувати роботу технічних засобів комп'ютерних систем та інформаційно-обчислювальних мереж, що застосовується в ході інформаційної війни (боротьби) для досягнення поставлених цілей.

За метою використання така інформаційна зброя поділяється на інформаційну зброю атаки та інформаційну зброю забезпечення.

Інформаційна зброя інформаційно-комунікаційних систем та мереж (ІКСМ) – інформаційна зброя, за допомогою якої здійснюється вплив на інформацію, що зберігається, оброблюється і передається в інформаційно-комунікаційних системах та мережах і (або) порушуються інформаційні технології, що застосовуються в ІКСМ.

У складі інформаційної зброї ІКСМ можна виділити чотири основних види засобів інформаційних впливів:

- засоби порушення конфіденційності інформації;
- засоби порушення цілісності інформації;
- засоби порушення доступності інформації;
- засоби психологічного впливу на абонентів ІКСМ.

Успішне застосування інформаційної зброї забезпечення дозволяє здійснювати деструктивні впливи на інформацію, що зберігається, обробляється й передається в мережах обміну інформацією, з використанням інформаційної зброї ІКСМ.

За способом реалізації інформаційну зброю поділяють на три великих класи:

- інформаційна алгоритмічна (математична) зброя;
- інформаційна програмна зброя;
- інформаційна апаратна зброя.

Інформаційна алгоритмічна (математична) зброя – це вид інформаційної зброї до якого, звичайно, відносять:

- алгоритми, що використовують сполучення санкціонованих дій для здійснення несанкціонованого доступу до інформаційних ресурсів;
- алгоритми застосування санкціонованого (легального) програмного забезпечення і програмні засоби несанкціонованого доступу для здійснення незаконного доступу до інформаційних ресурсів.

До **інформаційної програмної зброї** відносять програми з потенційно небезпечними наслідками своєї роботи для інформаційних ресурсів мережі обміну інформацією.

Програми з потенційно небезпечними наслідками – це окремі програми, які мають спроможність виконувати будь-яку непросту множину наступних функцій:

- приховування ознак своєї присутності в програмно-апаратному середовищі мережі обміну інформацією;
- здатність до самодублювання, асоціювання себе з іншими програмами і (або) перенесення своїх фрагментів в інші ділянки оперативної або зовнішньої пам'яті;
- руйнування (спотворення довільним чином) кодів програм в оперативній пам'яті;
- збереження фрагментів інформації з оперативної пам'яті в деякій ділянці зовнішньої пам'яті прямого доступу (локальної або віддаленої);
- спотворення довільним чином, блокування і (або) підміни масивів інформації, що виводиться у зовнішню пам'ять або в канал зв'язку, утворених в результаті роботи прикладних програм, або масивів даних, що уже знаходяться у зовнішній пам'яті;
- блокування інформаційного обміну в телекомунікаційних мережах, фальсифікування інформації в каналах державного та воєнного управління;
- нейтралізація роботи тестових програм і систем захисту інформаційних ресурсів.

Програми з потенційно небезпечними наслідками умовно поділяють на такі класи:

- комп'ютерні віруси;
- засоби несанкціонованого доступу;
- програмні закладки.

Комп'ютерні віруси [computer viruses] (від лат. virus – отрута) – це спеціальні програми, які здатні самочинно розмножуватися, створюючи свої копії, і поширюватися, модифікуючи (заражаючи) інші програми шляхом приєднання до них для наступного одержання управління та відтворення нових копій.

Після запуску заражених програм вірус може виконувати різні небажані дії, що порушують цілісність інформації та (або) режим роботи засобів обчислювальної техніки: псування файлів та каталогів, модифікування програмного забезпечення, спотворення результатів обчислень, засмічування або стирання пам'яті, створення завад при роботі ЕОМ, наприклад, різних аудіо- та відеоефектів.

Для комп'ютерних вірусів принципове значення мають такі класифікаційні ознаки: об'єкт впливу (зараження); спосіб зараження об'єкта; принцип маскування; деструктивні можливості.

За видом об'єкта зараження комп'ютерні віруси поділяються на завантажувальні віруси, файлові віруси, завантажувально-файлові віруси, макровіруси.

За способом зараження комп'ютерні віруси поділяються на резидентні і нерезидентні.

За способом маскування – на поліморфні віруси, віруси-невидимки (стелс-віруси) та комбіновані віруси.

За деструктивними можливостями – на безпечні віруси й віруси, що виконують деструктивні функції.

Комп'ютерні віруси можуть розмножуватися, впроваджуватися у програми, передаватися лініями зв'язку, мережами обміну інформацією, виводити з ладу системи керування і т. ін.

Засоби несанкціонованого доступу – клас програм з потенційно небезпечними наслідками, для яких обов'язковим є виконання наступних функцій:

- руйнування (спотворення довільним чином) кодів програм в оперативній пам'яті;
- збереження фрагментів інформації з оперативної пам'яті в деякій ділянці зовнішньої пам'яті прямого доступу (локальної або віддаленої);
- спотворення довільним чином, блокування і (або) підміни масивів інформації, що виводиться у зовнішню пам'ять або в канал зв'язку, утворених в результаті роботи прикладних програм, або масивів даних, що уже знаходяться у зовнішній пам'яті;
- нейтралізація роботи тестових програм і систем захисту інформаційних ресурсів.

До засобів несанкціонованого доступу належить будь-яке позаштатне програмне забезпечення ІКСМ, яке злоумисник може використати для порушення цілісності операційної системи або обчислювального середовища. Часто цей тип програмного забезпечення використовується для аналізу систем захисту, з метою їхнього подолання й реалізації несанкціонованого доступу до інформаційних ресурсів мереж обміну інформацією.

Відмітною ознакою (відносно програмних закладок) засобів несанкціонованого доступу є наявність функцій подолання захисту.

Програмні закладки [program bag] відносяться до програм з потенційно небезпечними наслідками:

- руйнування (спотворення довільним чином) кодів програм в оперативній пам'яті;
- збереження фрагментів інформації з оперативної пам'яті в деякій ділянці зовнішньої пам'яті прямого доступу (локальної або віддаленої);
- спотворення довільним чином, блокування і (або) підміни масивів інформації, що виводиться у зовнішню пам'ять або в канал зв'язку, утворених в результаті роботи прикладних програм, або масивів даних, що уже знаходяться у зовнішній пам'яті. Відмітною ознакою (відносно засобів несанкціонованого доступу) є відсутність функцій подолання захисту [32].

Виділяють декілька видів програмних закладок:

- троянські програми;
- логічні бомби;

- програмні пастки;
- програмні хробаки.

До **Троянських програм [Trojan program]** відносяться програмні закладки, які мають законний доступ до системи, проте виконують також і приховані (неоголошені) функції.

Так, Троянські програми в доповнення до основних (проектних і документованих) надають додаткові, але не описані в документації функціональні можливості, спрямовані на те, щоб обійти контроль доступу і привести до несанкціонованого знищення, блокування, модифікації або копіювання інформації, порушення роботи ІКСМ, системи або їхні мережі.

Ці можливості можуть самоліквідуватись, що робить неможливим їхнє виявлення, або ж можуть реалізуватись постійно, але існувати потай. Найбільш небезпечним є опосередкований вплив, при якому «Троянський кінь» діє в межах повноважень одного користувача, але в інтересах іншого користувача, встановити особу якого інколи неможливо.

Впровадження Троянських програм в автоматизовані системи керування інформаційними системами та мережами здійснюється такими засобами:

- використанням віддалених атак;
- впровадженням програмних закладок в операційні системи та програмне забезпечення, що поставляються на експорт;
- агентурним шляхом.

Програмні закладки можна також класифікувати у відповідності до мети створення та за способом доставки в систему. За метою створення:

- програмні закладки класу «дослідник»;
- програмні закладки класу «перехоплювач»;
- програмні закладки класу «руйнівник»;
- програмні класу «активна завада».

За способом доставки в систему:

- закладки, асоційовані з програмно-апаратним середовищем (BIOS). У даному випадку асоціюванням [associate] (лат. associatio – сполучення, з'єднання, від associō – з'єдную) розуміють інтеграція коду програми з потенційно небезпечними наслідками або її частини в код іншої програми таким чином, щоб при деяких умовах керування передавалося на код програми з потенційно небезпечними наслідками;
- закладки, асоційовані з програмами первинного завантаження (знаходяться в Master Boot або Record BOOT – секторах активних розділів);
- закладки, асоційовані із завантаженням драйверів, командного інтерпретатора, мережних драйверів (завантаженням операційної системи);
- закладки, асоційовані з прикладним програмним забезпеченням загального призначення (вбудовані в клавіатурні й екранні драйвери, програми тестування ПЕОМ, утиліти й оболонки типу NORTON);
- модулі, що виконуються, які містять тільки код закладки (як правило, впроваджуються в пакетні файли типу BAT);

- модулі-імітатори, що співпадають з деякими програмами, що потребують введення конфіденційної інформації, за зовнішнім виглядом;
- закладки, що маскуються під програмні засоби оптимізаційного призначення (архіватори, прискорювачі і т. ін.);
- закладки, що маскуються під програмні засоби ігрового й розважального призначення (як правило використовуються для первинного впровадження закладок типу «дослідник»).

Як засоби інформаційної зброї програмні закладки мають достатньо специфічну форму реалізації процедури нападу, виконання функцій і дослідження систем захисту (наприклад, паролів доступу) елементів обчислювального середовища.

Інформаційна апаратна зброя включає апаратні засоби, призначені для виконання функцій інформаційної зброї. Прикладом інформаційної апаратної зброї можуть бути апаратні закладки, які впроваджуються в ПЕОМ, що готуються на експорт та їхнє периферійне обладнання. Апаратні закладки маскуються під звичайні пристрої мікроелектроніки і застосовуються для збирання, оброблення й передавання конфіденційної інформації.

Інформаційна боротьба [information struggle] – це боротьба з використанням спеціальних способів і засобів для впливу на інформаційну сферу (середовище) конфронтуючої сторони, а також для захисту власної інформаційної сфери в інтересах досягнення поставленої мети. Інформаційна боротьба може бути як самостійним видом, так і складовою частиною будь-якого іншого різновиду боротьби (збройної, ідеологічної, економічної і т. ін.). Вона ведеться постійно, як у мирний, так і у воєнний час. Масштаби інформаційної боротьби настільки великі, що її підготовка і ведення повинні носити плановий, систематичний характер, заснований на глибоких знаннях законів і закономірностей інформаційної боротьби [12].

Теорія інформаційної боротьби [information struggle theory] представляє систему знань про характер, закони, закономірності, ця база є головною при розробці фундаментальних положень теорії інформаційної боротьби та визначення напрямків її розвитку.

Оскільки основними завданнями інформаційної боротьби є ураження об'єктів інформаційного середовища противника та захист власної інформації, то структура теорії інформаційної боротьби повинна включати загальні основи теорії інформаційної боротьби, теорію ураження інформації і теорію захисту інформації.

Теорія захисту інформації [data protection theory] – складова частина теорії інформаційної боротьби включає загальні положення, що визначають: предмет, завдання і зміст теорії; об'єкти й елементи захисту інформації; основні фактори, що впливають на зміст і ефективність захисту інформації, а також визначає та вивчає загрози інформації і методологічні основи її захисту, систему показників оцінки ефективності захисту інформації, загальну математичну модель захисту інформації, організаційно-технічні і правові основи захисту інформації.

1.2 . Загрози інформаційній безпеці

Основні загрози інформаційній безпеці [information security threat]

– сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства і держави в інформаційній сфері.

Основні загрози інформаційній безпеці можна розділити на три групи:

- загрози впливу неякісної інформації (недостовірної, фальшивої, дезінформації) на особистість, суспільство, державу;
- загрози несанкціонованого і неправомірного впливу сторонніх осіб на інформацію і інформаційні ресурси (на виробництво інформації, інформаційні ресурси, на системи їхнього формування і використання);
- загрози інформаційним правам і свободам особистості (праву на виробництво, розповсюдження, пошук, одержання, передавання і використання інформації; праву на інтелектуальну власність на інформацію і речову власність на документовану інформацію; праву на особисту таємницю; праву на захист честі і достоїнства й т. ін.).

Фактори загроз за видовою ознакою поділяються на політичні, економічні та організаційно-технічні [8-16]:

Дестабілізуючі фактори інформаційної безпеки [destabilizing factor] – явища та процеси природного і штучного походження, що породжують інформаційні загрози.

Джерелами дестабілізуючих факторів можуть бути як окремі особи, так і організації та їхні об'єднання.

Особливу групу джерел складають інформаційні системи і мережі, оскільки вони одночасно є знаряддям приведення в дію інформаційних загроз, каналом їхнього проникнення у свідомість особистості або суспільну свідомість і генератором спонтанних загроз, що виникають внаслідок технічних несправностей та інших причин.

Джерелом дестабілізуючих факторів може бути також природне середовище.

Кожному джерелу властиві певні види дестабілізуючих факторів, які можна представити двома групами: міждержавні дестабілізуючі фактори і внутрідержавні дестабілізуючі фактори.

Сукупність джерел разом із властивими їм видами дестабілізуючих формують цілий спектр інформаційних загроз, що впливають на стан інформованості особистості, суспільства і держави. До них відносяться: викрадення, знищення, втрата, приховування, спотворення, розголошення, фальсифікація, компрометація корисної (істинної) інформації, а також фабрикавання, розповсюдження і впровадження дезінформації.

Політичні фактори загроз інформаційній безпеці:

- зміни геополітичної обстановки внаслідок фундаментальних змін у різноманітних регіонах світу, зведення до мінімуму ймовірності світової ядерної війни;
- інформаційна експансія розвинених країн, які здійснюють глобальний моніторинг світових політичних, економічних, воєнних,

екологічних та інших процесів, та розповсюджують інформацію з метою здобуття односторонніх переваг;

- становлення нової державності в пострадянських країнах на основі принципів демократії, законності, інформаційної відкритості;
- знищення колишньої командно-адміністративної системи державного управління, а також системи забезпечення безпеки;
- порушення інформаційних зв'язків;
- прагнення країн до більш тісного співробітництва із закордонними країнами в процесі проведення реформ на основі максимальної відкритості сторін;
- низька загальна правова та інформаційна культура сторін.

Економічні фактори загроз безпеці інформації:

- перехід на ринкові відносини в економіці, поява на ринку великої кількості вітчизняних та зарубіжних комерційних структур – виробників та споживачів інформації, засобів інформатизації та захисту інформації, включення інформаційної продукції в систему товарних відносин;
- критичний стан вітчизняних галузей промисловості, яка виробляє засоби інформатизації та захисту інформації;
- розширення кооперації із зарубіжними країнами в розвитку інформаційної інфраструктури.

Організаційно-технічні фактори загроз інформаційній безпеці:

- недостатня нормативно-правова база у сфері інформаційних відносин, у тому числі в галузі забезпечення інформаційної безпеки;
- недостатнє регулювання державою процесів функціонування та розвитку ринку засобів інформатизації, інформаційних продуктів та послуг;
- широке використання у сфері державного управління та кредитно-фінансової сфери незахищених від витоку інформації каналів;
- зростання обсягів інформації, яка передається відкритими каналами зв'язку;
- загострення криміногенної обстановки, зростання числа комп'ютерних злочинів, особливо в кредитно-фінансовій сфері.

Локальні фактори загроз інформаційній безпеці:

- перехоплення електронних випромінювань;
- застосування пристроїв підслуховування, або закладок;
- дистанційне фотографування;
- розкрадання носіїв інформації та промислових відходів;
- копіювання носіїв інформації з подоланням заходів захисту;
- незаконне приєднання до апаратури та ліній зв'язку;
- впровадження та використання комп'ютерних вірусів і т. ін.

Загрози у інформаційно-комунікаційних системах та мережах передачі даних:

- протиправне збирання і використання інформації;
- порушення технології обробки інформації;

- впровадження в апаратні і програмні вироби компонентів, що реалізують функції, не передбачені документацією на ці вироби;
- розробка і поширення програм, що порушують нормальне функціонування інформаційних та інформаційно-телекомунікаційних систем, у тому числі систем захисту інформації;
- радіоелектронний вплив з метою виведення з ладу, пошкодження чи руйнування засобів і систем обробки інформації, телекомунікації зв'язку;
- вплив на парольно-ключові системи захисту автоматизованих систем обробки і передачі інформації;
- компрометація ключів і засобів криптографічного захисту інформації;
- витік інформації технічними каналами;
- впровадження електронних пристроїв для перехоплення інформації в технічні засоби обробки, зберігання і передачі інформації з каналів зв'язку, а також у службові приміщення органів державної влади, підприємств, установ та організацій усіх форм власності;
- знищення, пошкодження, руйнування чи розкрадання машинних та інших носіїв інформації;
- перехоплення інформації в мережах передачі даних та лініях зв'язку, дешифрування цієї інформації і нав'язування хибної інформації;
- використання несертифікованих вітчизняних і закордонних інформаційних технологій, засобів захисту інформації, засобів інформатизації, телекомунікації зв'язку при створенні і розвитку інформаційної інфраструктури України;
- несанкціонований доступ до інформації, що знаходиться в банках і базах даних;
- порушення законних обмежень на поширення інформації.

Канал витоку інформації – сукупність джерела інформації, матеріального носія або середовища поширення, що несе зазначену інформацію сигналу й засобу виділення інформації із сигналу або носія [51-59].

Одним з основних властивостей каналу є місце розташування засобу виділення інформації із сигналу або носія, що може розташовуватися в межах контрольованої зони, або поза нею (рис. 1.1.).

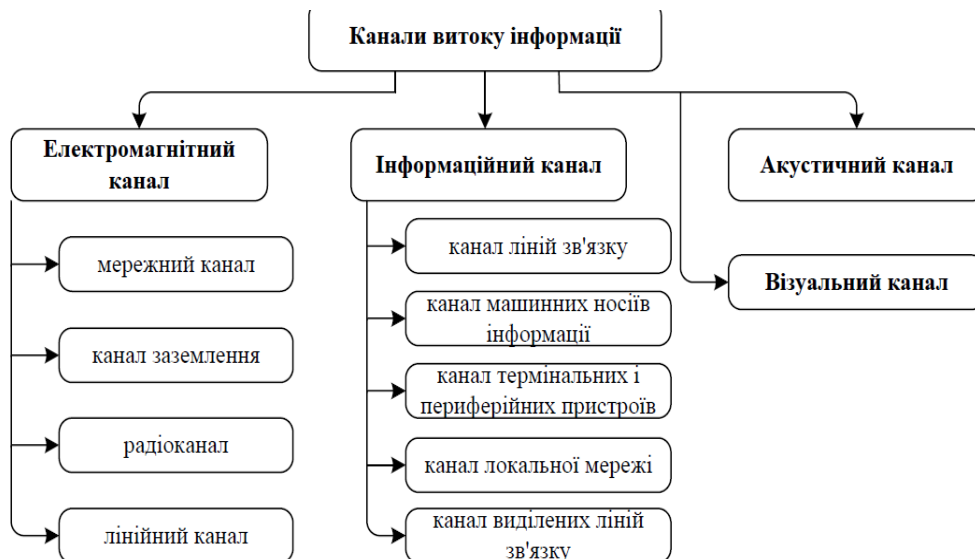


Рис 1.1. Класифікація каналів витоку інформації

Виділяють такі канали витоку:

1. Електромагнітний канал. Причиною його виникнення є електромагнітне поле, пов'язане із проходженням електричного струму в апаратних компонентах автоматизованої системи (АС). Електромагнітне поле може індукціювати струм в близько розташованих провідних лініях (наведення). Електромагнітний канал у свою чергу поділяються на такі канали:

- радіоканал (високочастотне випромінювання);
- мережний канал (наведення на мережу електроживлення);
- канал заземлення (наведення на проведення заземлення);
- лінійний канал (наведення на лінії зв'язку між комп'ютерними системами).

2. Акустичний (віброакустичний) канал. Пов'язаний з поширенням звукових хвиль у повітрі або пружних коливаннях в інших середовищах, що виникають при роботі пристроїв відображення інформації АС.

3. Візуальний канал. Пов'язаний з можливістю візуального спостереження зломисником за роботою пристроїв відображення інформації АС без проникнення в приміщення, де розташовані компоненти системи. Як засіб одержання інформації в цьому випадку можуть розглядатися фотокамери, відеокамери й т.п.

4. Інформаційний канал. Пов'язаний з доступом до елементів АС, носіїв інформації, програмного забезпечення (у тому числі до операційних систем), а також з підключенням до ліній зв'язку. Інформаційний канал може бути розділений на канали:

- канал ліній зв'язку;
- канал виділених ліній зв'язку;
- канал локальної мережі;
- канал машинних носіїв інформації;
- канал термінальних і периферійних пристроїв.

1.3. Моделі порушень інформаційних ресурсів

Інформаційні ресурси інформаційно-керуючих систем та мереж, у першу чергу розподілені бази даних та знань є привабливими, з точки зору розташованої на них інформації, не тільки для авторизованих користувачів інформаційної системи, а також для окремих осіб або певних груп осіб, які прагнуть бути її користувачами. Ця привабливість обумовлена характером і обсягом інформації, що вводиться, обробляється, зберігається та циркулює в ІКСМ [44].

Якщо та або інша особа – користувач ресурсами ІКСМ здійснює спробу несанкціонованого (не авторизованого) доступу до інформаційних ресурсів системи (з метою: ознайомлення, модифікації, знищення, зміни режимів використання або загального функціонування системи тощо), то такий користувач є порушником.

Порушення з боку цих осіб можуть бути як ненавмисними, так і зловмисними. Особливу небезпеку варто очікувати від зловмисних порушників, які в силу тих або інших причин перебувають під впливом:

- кримінальних осіб та їх угруповань;
- бізнесменів, комерсантів та їх об'єднань;
- політичних діячів і партій;
- агентів спецслужб інших держав, або самі входять у їх склад.

Припустимим характером дій з боку цих порушників варто вважати бажання й прагнення одержати необхідні для порушника дані для подальшого використання, модифікації або знищення з метою досягнення певних умов для себе, своїх підприємств, прихильників або конкурентів.

Крім того, необхідно враховувати, що використання ресурсів ІКСМ, насамперед інформаційних, і їх модифікація або знищення можуть бути здійснені порушником (зловмисниками) навмисно, або ненавмисно (неправильні, непередбачені дії без злих намірів, внаслідок недбалості тощо). При цьому порушники можуть бути внутрішніми (із числа співробітників, користувачів ІКСМ) або зовнішніми (сторонні особи чи особи, які перебувають за межами контрольованої зони, або проникли в її межі несанкціонованим шляхом).

Кваліфікація порушника

Варто очікувати, що порушники мають певний рівень кваліфікації, достатній для успішної реалізації загроз ресурсам ІКСМ, тобто:

- володіють інформацією щодо функціональних особливостей ІКСМ, уміють користуватися штатними засобами;
- володіють високим рівнем знань і досвідом роботи в обслуговуванні ідентичних засобів ІКСМ;
- володіють високим рівнем знань в галузі обчислювальної техніки й програмування на мовах розробки програмних засобів ІКСМ, проектуванню й експлуатації подібних до ІКСМ систем;
- володіють інформацією щодо функцій і механізмів захисту, які реалізовані як у системі захисту інформації ІКСМ, так і у функціях і механізмах захисту, що вбудовані в базове й прикладне програмне

забезпечення. За рівнем можливостей, які надаються штатною інфраструктурою інформаційної мережі, виділяють чотири рівні порушників. Класифікація ієрархічна, тобто кожний наступний рівень містить у собі функціональні можливості попереднього рівня:

- перший рівень відповідає найбільш низькому рівню можливостей порушника у системі – можливістю запуску фіксованого набору програм, які реалізують певні функції з обробки інформації;

- другий рівень визначається можливістю створення й запуску власних програм з новими функціями обробки і подальшого одержання потрібної порушнику інформації;

- третій рівень визначається можливістю управління функціонуванням ІКСМ, тобто впливом на базове програмне забезпечення системи, а також на склад і конфігурацію технічного забезпечення інформаційної системи;

- четвертий рівень визначається інтегрованим обсягом можливостей співробітників, які здійснюють: розробку, впровадження й експлуатацію технічних засобів інформаційної системи, а також можливістю введення до складу інформаційної системи власних технічних засобів з новими функціями, щодо обробки і отримання інформації.

Ступінь ризику

Нижче наводиться приблизний перелік персоналу ІКСМ й відповідний ступінь ризику щодо можливої реалізації загроз та нанесення шкоди залежно від зазначених робочих функцій працівників:

- найбільший ризик: системний адміністратор; адміністратор бази даних; адміністратор безпеки;

- високий ризик: оператор системи; оператор введення й підготовки даних; менеджер обробки даних; системний програміст;

- середній ризик: інженер системи; менеджер програмного забезпечення;

- обмежений ризик: прикладний програміст; інженер і оператор зв'язку; інженер по устаткуванню; оператор периферійного устаткування; бібліотекар системних магнітних носіїв; користувач-програміст; користувач-операціоніст.

- низький ризик: інженер по периферійному устаткуванню; бібліотекар магнітних носіїв користувачів.

Цілі і мета порушника:

- особиста авторизація, тобто одержати особисті легальні атрибути доступу, з бажано найширшими правами щодо доступу до ресурсів ІКСМ, з метою їхнього використання, одержання необхідної інформації в потрібному обсязі, ознайомлення з конфіденційною інформацією, одержання можливості її модифікації або знищення у відповідності зі своїми намірами;

- авторизувати інших осіб, які б мали можливість одержати легальні атрибути доступу, з бажано найширшими правами щодо доступу до ресурсів ІКСМ з метою їхнього використання, одержання необхідної

інформації в потрібному обсязі, ознайомлення з конфіденційною інформацією, одержання можливості її модифікації або знищення у відповідності зі своїми намірами;

– знайти прихильників або довірених осіб серед персоналу або користувачів ІКСМ, які мають можливість одержувати легальні атрибути доступу до ресурсів ІКСМ з метою їхнього використання, одержання необхідної інформації в потрібному обсязі, ознайомлення з конфіденційною інформацією, одержання можливості її модифікації або знищення у відповідності зі своїми намірами.

При відсутності можливості або безуспішності реалізації вищенаведених дій порушник може мати наміри:

1. Одержання атрибутів доступу авторизованих користувачів шляхом використання технічних засобів, крадіжок, купівлі, або одержання іншим шляхом.

2. Проникнення на місця розміщення тих або інших компонентів, елементів або ресурсів ІКСМ (обчислювальних ресурсів, інформаційних ресурсів, базового й прикладного програмного забезпечення й програмного забезпечення системи технічного захисту інформації (ТЗІ), включаючи носії резервні копії, ресурсів введення/виводу інформації, телекомунікаційного устаткування, включаючи мережу передачі даних) шляхом подолання будівельних конструкцій, охорони або охоронної сигналізації та ін.

3. Зміни режимів функціонування ІКСМ, її ресурсів та послуг системи.

4. Установки фізичних засобів у місцях розміщення елементів ІКСМ (технічних закладок) чи інших засобів технічної розвідки (у тому числі і віддалених, наприклад, в елементах комунікаційної мережі зв'язку) для перехвату інформації.

5. Установки фізичних засобів у місцях розміщення елементів ІКСМ (технічних закладок) або інших засобів (у тому числі й віддалених, наприклад в елементах комунікаційної мережі зв'язку) для генерації хибних сигналів, інформаційних символів або спотворених повідомлень.

6. Установки програмних засобів (програмних закладок або вірусів), копіювання інформації з метою її використання.

7. Установки програмних засобів (програмних закладок або вірусів) для модифікації системного програмного забезпечення, так і інформації ІКСМ, шляхом введення програмних вірусів, спотворених сигналів, інформаційних символів або хибних повідомлень з метою перевантаження систем і порушення, таким чином, доступності компонентів ІКСМ.

8. Здійснення спроб несанкціонованого доступу до обчислювальних та інформаційних ресурсів, базового й прикладного програмного забезпечення.

9. Здійснення спроб несанкціонованого доступу до системи захисту інформації, як частини ІКСМ, так і до її телекомунікаційної підсистеми, шляхом подолання системи управління доступом.

Рівень знань порушника

Порушник може знати:

- склад, розміщення, функціональні особливості, умови й режими функціонування елементів ІКСМ, включаючи траси прокладених або можливих ліній зв'язку, комунікаційних мереж зв'язку й трафіки відповідних каналів передачі даних;
- порядок, засоби й режими здійснення охорони елементів ІКСМ, місця їх розміщення і навколишню територію;
- порядок, засоби й режими здійснення організаційно-правових і технічних заходів захисту ресурсів ІКСМ;
- основні закономірності формування в ІКСМ баз даних і потоків запитів до них.
- за характером дій зловмисник може здійснювати: активні або пасивні дії, стосовно ресурсів і функціональних властивостей захищеності інформаційних об'єктів ІКСМ.

Під активною загрозою розуміється спроба навмисної несанкціонованої зміни стану функціонування ІКСМ, а під пасивною загрозою – спроба несанкціонованого проникнення в систему без зміни її стану.

Класифікація за характером дій

За характером дій порушників можна класифікувати на:

- випадкових порушників – авторизованих користувачів, які порушили політику безпеки тієї або іншої послуги ненавмисно, а помилково, шляхом виконання непередбачених дій з об'єктом захисту, шляхом випадкового подолання засобів управління доступом тощо;
- терплячих зловмисників – авторизованих користувачів, які порушили політику безпеки тієї або іншої послуги навмисно, але без рішучих дій, маскуючись, шляхом підбору атрибутів доступу інших користувачів з метою схованого подолання засобів управління доступом тощо;
- рішучих зловмисників, які мають на меті порушити ту або іншу властивість інформації. Зловмисники прагнуть перебороти: засоби організаційного обмеження доступу, охоронної сигналізації, керування доступом до фізичних ресурсів, елементи будівельних конструкцій, тощо і одержати можливість фізичного доступу до засобів обробки, зберігання або передачі інформаційних ресурсів з метою виводу їх з ладу, зміни режимів функціонування, крадіжки носіїв інформації та ін.;
- зловмисників, які використовують засоби віддаленого доступу до інформаційних об'єктів з умов: витоку інформації технічними каналами, реалізації спеціальних впливів на інформацію з технічних каналів, впливу на мережне устаткування локальних або розподілених мереж, у тому числі й засоби телекомунікаційних мереж (АТС і лінії зв'язку), які використовуються елементами ІКСМ.

Дії порушників можуть бути спрямованими на порушення функціональних властивостей захищеності інформаційних об'єктів, зокрема на порушення:

- конфіденційності, цілісності й доступності інформаційних об'єктів;
- функцій спостереження за діяльністю користувачів і процесів, однозначної ідентифікації користувачів, ресурсів і процесів.

Така класифікація дає можливість чітко визначити методи та засоби запобігання несанкціонованим діям порушників, а також визначити організаційно-правові заходи, які потрібні для побудови комплексної системи захисту інформації.

Порушники можуть використовувати такі методи та засоби:

- агентурні методи одержання відомостей через підкуплених користувачів і персонал, а також через прихильників чи довірених осіб з числа штатних працівників або таких, які мають доступ до ресурсів ІКСМ;
- пасивні технічні засоби перехоплення інформаційних сигналів;
- штатні засоби ІКСМ або недоліки проектування системи захисту інформації від НСД;
- методи й засоби активного впливу на елементи ІКСМ, які змінюють конфігурацію ІКСМ (підключення додаткових або модифікація штатних технічних засобів, підключення або «врізання» у канали передачі даних, впровадження й використання спеціального ПЗ і т.п.).

За місцем здійснення порушень дії зловмисника можна класифікувати:

- без одержання доступу на контрольовану територію із використанням технічних засобів віддаленого доступу через засоби: Internet, електронної пошти, модемного зв'язку чи дистанційної розвідки (наприклад: по оптичних, акустичних каналах, каналах побічних електромагнітних випромінювань і т. ін.), або з використанням засобів одержання інформації з мережі передачі даних (наприклад: шляхом підключення або «врізання» у лінії зв'язку);
- з одержанням доступу на контрольовану територію ІКСМ або до робочих місць кінцевих користувачів, але без доступу до технічних засобів ІКСМ, також з використанням технічних засобів дистанційної розвідки з подальшим несанкціонованим доступом до будинків, або приміщень, у яких розміщені елементи ІКСМ;
- з одержанням доступу до робочих місць кінцевих користувачів ІКСМ з подальшим несанкціонованим доступом до пристроїв введення/виводу інформації, копіювання, до каналного або каналотворюючого устаткування й до інших елементів ІКСМ;
- з одержанням доступу до засобів управління ІКСМ і засобів управління комплексною системою захисту інформації з подальшими розширеними можливостями доступу до ресурсів ІКСМ та послуг системи.

1.4. Методи і засоби організації інформаційної безпеки

Забезпечення інформаційної безпеки – сукупність заходів, призначених для досягнення стану захищеності потреб особистостей, суспільства і держави в обробці, зберіганні та поширенні інформації.

Держава здійснює свої заходи через відповідні органи, а громадяни, суспільні організації і об'єднання, що мають відповідні повноваження, у відповідності із законодавством. В основу забезпечення інформаційної безпеки держави повинні бути покладені такі принципи [37]:

- законність, дотримання балансу інтересів особистості, суспільства і держави;

- взаємна відповідальність суб'єктів забезпечення інформаційної безпеки;

- інтеграція систем національної і міжнародної безпеки.

Специфічними принципами забезпечення інформаційної безпеки є:

- превентивний характер проведення її заходів по відношенню до заходів інших видів безпеки;

- адекватна інформованість об'єктів безпеки, у тому числі і міжнародних.

Адекватна інформованість об'єктів безпеки означає, що всі вони мають право володіти інформацією про явища і процеси, що їх цікавлять, обмежене тільки законодавчо з метою охорони особистої, сімейної, професійної, комерційної та державної таємниці, а також моралі.

Права та свободи суспільства в питаннях пошуку, володіння та розповсюдження інформації повинні регулюватися законодавчими актами, які видаються щодо специфіки діяльності суспільних об'єднань та організацій або змісту інформації. Наприклад, адекватна інформованість суспільства про його матеріальні цінності досягається у сфері створення норм та правозастосування законодавства про захист комерційної таємниці. Права та свободи суспільства в духовній сфері повинні захищати законодавчі акти, які визначають порядок освіти та функціонування освітніх, просвітницьких, культурних, релігійних організацій, а також засобів масової інформації. В основі прав і свобод держави у сфері її інформованості з питань світової політики, економіки, науки, ресурсів, екології, оборони тощо лежать діючі норми та принципи міждержавного права. Головним слід вважати принцип рівної безпеки. Стосовно інформаційної сфери можна говорити про її трансформацію в принцип адекватної інформованості держав світового співтовариства, який передбачає право кожної держави на інформаційну безпеку, забезпечення інформаційної безпеки усіх членів співтовариства в рівній мірі, врахування інтересів усіх сторін без будь-якої дискримінації, виключення односторонніх переваг, відмова від дій, що наносять шкоду іншій державі. Законодавча база, яка визначає перелік відомостей, що віднесені до державної таємниці, механізм та порядок її захисту повинні розроблюватися виходячи із наведеного принципу, а також багатосторонніх угод держав, які входять до міжнародної системи

інформаційної безпеки. Формування останньої буде, очевидно, справою далекої перспективи, яка ознаменує собою вищий рівень прояву довіри та зацікавленості держав світового співтовариства в забезпеченні виконання на практиці принципу адекватної інформованості. Така система повинна стати підсистемою у системі колективної безпеки.

Органи (служби) інформаційної безпеки можуть створюватися (на законодавчих засадах) і в недержавних структурах для захисту своїх потреб в забезпеченні необхідною інформацією. Дані органи на основі укладення відповідних угод можуть бути приєднані до єдиної державної системи інформаційної безпеки.

На теперішній час окремі елементи системи інформаційної безпеки створені та функціонують (органи зовнішньої розвідки, інформаційні служби різноманітних міністерств, система технічного та криптографічного захисту інформації держави і т. ін.). Проте для їхнього функціонування ще недостатня правова база. Зміст діяльності органів інформаційної безпеки також ще не в повній мірі відповідає покладеним на них завданням. Це пояснюється в першу чергу недостатнім опрацюванням питань, що стосуються форм і способів забезпечення інформаційної безпеки.

1.5 Інформаційна система як об'єкт захисту.

Інформаційна боротьба розглядається як одна з форм забезпечення інформаційної безпеки від інформаційних навмисних загроз. Ведеться державними органами інформаційної безпеки з формуваннями, що мають різноманітний (суспільний) стан (фізичні особи, юридичні особи, суб'єкти міжнародного права) і зловмисно створюють інформаційні загрози життєво важливим інтересам особистості, суспільства і держави. Інформаційна боротьба включає комплекс заходів інформаційного забезпечення, інформаційного захисту й інформаційної протидії, що здійснюються за єдиним замислом і планом з метою захоплення і утримання інформаційної переваги [90].

Інформаційний захист [infosecurity] – це сукупність заходів від інформаційної протидії противника, які включають дії з деблокування інформації, необхідної для вирішення завдань управління, і блокування дезінформації, що розповсюджується і упродовжується в систему управління.

Радіоелектронний захист [radio electronic protection] – це сукупність заходів забезпечення стійкої роботи засобів управління і розвідки в умовах ведення противником радіоелектронної боротьби, застосування розвідувально-ударних комплексів, самонавідної зброї та усунення взаємного впливу радіоелектронних засобів.

Для інформаційних систем як об'єктів безпеки властиві такі наступні характеристики, як: конфіденційність, доступність та цілісність інформації (даних) в інформаційній системі [67].

Конфіденційність [confidentiality, privacy] (від лат. confidential – довір'я) – це властивість не підлягати розголошенню.

Конфіденційність інформації (даних) в інформаційній системі – це властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і (або) процесом інформаційної системи. Інформація зберігає конфіденційність, якщо дотримуються встановлені правила ознайомлення з нею.

Доступність [availability] у загальному сенсі представляється як можливість доступу до інформаційних ресурсів при їх обробці, зберіганні та передачі.

Для інформаційної системи – це властивість ресурсу системи, яка полягає в тому, що користувач і (або) процес, який володіє відповідними повноваженнями, може використовувати ресурс відповідно до правил, встановлених політикою безпеки, не очікуючи довше заданого (малого) проміжку часу, тобто коли він знаходиться у вигляді, необхідному користувачеві, і в той час, коли він йому необхідний.

Доступність даних [data confidentiality] в інформаційній системі – це властивість даних, що полягає у можливості їхнього отримання користувачем або програмою. Визначається рядом факторів: можливістю працювати за терміналом, володінням паролем, знанням мови запитів та ін.

Цілісність [integrity] – це внутрішня єдність, зв'язаність усіх частин інформаційних ресурсів при їх обробці, зберіганні та передачі, як одного цілого в інформаційній системі. Тобто, це стан даних, або інформаційної системи, коли дані та програми використовуються встановленим чином, що забезпечує:

- стійку роботу системи;
- автоматичне відновлення у випадку виявлення системою потенційної помилки;
- автоматичне використання альтернативних компонентів замість тих, що вийшли з ладу.

Для інформаційної системи можна розглядати такі поняття як цілісність даних, цілісність інформації, цілісність бази даних, цілісність інформаційної системи.

Цілісність даних [data integrity] в інформаційній системі – це стан, при якому дані, що зберігаються в системі, в точності відповідають даним у вихідних документах; властивість, що має відношення до набору даних і означає, що дані не можуть бути змінені або зруйновані без санкції на доступ. Цілісність даних вважається збереженою, якщо дані не спотворені і не зруйновані (стерті).

Семантична цілісність даних [semantic data integrity] – це стан даних, коли вони зберігають свій інформаційний зміст та однозначність інтерпретації в умовах випадкових впливів.

Цілісність інформації [information integrity] – це властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і (або) процесом. Інформація зберігає

цілісність, якщо дотримуються встановлені правила її модифікації (видалення).

Цілісність бази даних [database integrity] – це стан бази даних, коли всі значення даних правильні в тому сенсі, що відображають стан реального світу (в межах заданих обмежень по точності та часовій узгодженості) і підпорядковуються правилам взаємного непротиворіччя. Підтримка цілісності бази даних містить перевірку цілісності і відновлення з будь-якого неправильного стану, яке може бути виявлено; це входить у функції адміністратора бази даних.

Цілісність системи [system integrity] – це властивість системи, яка полягає в тому, що жоден її компонент не може бути усунений, модифікований або доданий з порушенням політики безпеки.

Захищена інформаційна система – інформаційна система, яка для певних умов експлуатації забезпечує безпеку (конфіденційність, цілісність) інформації, що функціонує в системі, та підтримує свою працездатність в умовах впливу на неї заданої множини загроз.

Для інформаційної системи властиві такі види загроз: загрози порушення конфіденційності, загрози порушення цілісності, загрози порушення працездатності (доступності).

Загрози порушення конфіденційності спрямовані на розголошення інформації з обмеженим доступом.

Загрози порушення працездатності (доступності) спрямовані на створення ситуацій, коли в результаті навмисних дій знижується працездатність обчислювальної системи, або її ресурси стають недоступними.

Загрози порушення цілісності полягають у спотворенні або зміні неавторизованим користувачем інформації, що зберігається або передається. Цілісність інформації може бути порушена як зловмисником, так і в результаті об'єктивних впливів із сторони середовища експлуатації системи.

Вважають, що забезпечення безпеки інформації повинно носити комплексний характер. Усе більше фахівців пропонують свої рішення в галузі забезпечення безпеки інформаційних ресурсів як комплексні. Проте організація забезпечення безпеки інформації повинна носити не просто комплексний характер, але ще й ґрунтуватися на всебічному аналізі можливих негативних наслідків, при якому важливо не проігнорувати суттєві аспекти.

Насамперед заходи забезпечення інформаційної безпеки в організації спрямовуються тільки на те, щоб не допустити збитків від втрати конфіденційної інформації. Відповідно до цього уже передбачається наявність цінної інформації, через втрату якої організація може понести збитки. А якщо є цінна інформація, то звичайно ж є можливість здійснення будь-яких дій, які можуть нанести шкоду цій інформації. Усі шкідливі дії можуть бути здійсненими тільки при наявності будь-яких слабких місць.

А якщо є дії, то є найвища загроза їх здійснення, а також наявні джерела, з яких ці загрози можуть виходити [12, 29].

Виникає наступний ланцюжок: джерело загрози – фактор (вразливість) – загроза (дія) – наслідки (атака).

Загроза (дія) – це можлива небезпека (потенційна або така, що існує реально) вчинення будь-якого діяння (дії або бездіяльності), спрямованого проти об'єкта захисту (інформаційних ресурсів), яке наносить збиток власнику або користувачу, що проявляється як небезпека спотворення або втрати інформації.

Фактор (уразливість) – це властиві об'єкту інформатизації причини, які призводять до порушення безпеки інформації на конкретному об'єкті та зумовлені вадами процесу функціонування об'єкта інформатизації, властивостями архітектури інформаційно-телекомунікаційної системи, протоколами обміну та інтерфейсами, що застосовуються програмним забезпеченням і апаратними засобами, умовами експлуатації.

Наслідки (атака) – це можливі наслідки реалізації загрози (можливі дії) при взаємодії джерела загрози через наявні фактори (уразливості).

Атака – це завжди пара «джерело-фактор», що реалізує загрозу та призводить до збитків.

Прояви збитків, як категорія класифікації загроз, можуть бути різноманітні:

- моральні й матеріальні збитки ділової репутації організації;
- моральні, фізичні або матеріальні збитки, зв'язані з розголошенням персональних даних окремих осіб;
- матеріальні (фінансові) збитки від розголошення конфіденційної інформації;
- матеріальні (фінансові) збитки від необхідності відновлення порушених інформаційних ресурсів;
- матеріальні збитки (втрати) від неможливості виконання взятих на себе зобов'язань перед третьою стороною;
- моральні та матеріальні збитки від дезорганізації діяльності організації;
- матеріальні та моральні збитки від порушення міжнародних відносин.

Слід відзначити, що збитки можуть бути спричинені як будь-яким суб'єктом (у цьому випадку відбувається правопорушення), так і наслідком незалежного від суб'єкта прояву (стихійних випадків, або інших впливів, таких як прояви техногенних властивостей цивілізації).

У першому випадку наявна вина суб'єкта, яка визначає спричинену шкоду як склад злочину, що здійснюється із злими намірами (навмисно) або через необережність, і спричинені збитки повинні класифікуватися як склад злочину відповідно до кримінального права.

У другому випадку збитки носять імовірнісний характер і повинні бути співставлені як мінімум із тим ризиком, який обговорюється цивільним, адміністративним або арбітражним правом, як предмет

розгляду. І визначення цього, хто саме є причиною збитків, є другим за важливістю (після спроби цього не допустити) питанням для потерпілого.

В теорії права під збитками розуміють невігідні для власника майнові наслідки, що виникли внаслідок правопорушення. Збитки виражаються у зменшенні майна, або у недоодержанні прибутку, який був би одержаний при відсутності правопорушення (втрачена вигода). Якщо розглядати як суб'єкт, що спричинив збитки, будь-яку особистість, категорія «збитки» є справедливою тільки у тому випадку, коли можна довести, що вони спричинені, тобто діяння особистості необхідно кваліфікувати в термінах правових актів як склад злочину. Тому, при класифікації загроз безпеці інформації у цьому випадку доцільно враховувати вимоги діючого кримінального права, які визначають склад злочину.

Для прикладу можна розглянути приклади складів злочину, які визначаються кримінальними кодексами в багатьох державах.

Копіювання комп'ютерної інформації – це повторювання та стійке збереження інформації на машинному або іншому носіїві.

Знищення – це зовнішній вплив на майно, у результаті якого воно припиняє своє існування або приходить у повну непридатність для використання за цільовим призначенням. Знищене майно не може бути відновлене шляхом ремонту або реставрації та повністю виводиться з господарського обігу.

Знищення комп'ютерної інформації – стирання її у пам'яті ЕОМ.

Пошкодження – змінювання властивостей майна, при якому суттєво погіршується його стан, втрачається значна частина його корисних властивостей і воно стає повністю або частково непридатним для цільового використання.

Модифікація комп'ютерної інформації – внесення будь-яких змін, окрім пов'язаних з адаптацією програми для ЕОМ або баз даних.

Блокування комп'ютерної інформації – штучне утруднення доступу користувачів до інформації, не пов'язане з її знищенням.

Несанкціоноване знищення, блокування, модифікація, копіювання інформації – будь-які не дозволені законом, власником або компетентним користувачем указаних дій з інформацією.

Обман (заперечення автентичності, нав'язування хибної інформації) – навмисне спотворення або приховування істини з метою введення в оману особу, у веденні якої знаходиться майно, і таким чином домагатися від неї добровільної передачі майна, а також повідомлення з цією метою свідомо неправдивих відомостей.

Якщо розглядати як суб'єкт, що спричинив збитки, будь-яке природне або техногенне явище під збитками можна розуміти невігідні для власника майнові наслідки, викликані цими явищами, і які можуть бути компенсовані за рахунок третьої сторони (страхування ризиків настання події) або за рахунок власних засобів власника інформації.

Виходячи з попередніх міркувань можна виділити три основні види загроз безпеці інформації: загрози безпеці інформації при забезпеченні конфіденційності, доступності та цілісності.

Загрози безпеці інформації при забезпеченні конфіденційності:

- крадіжка (копіювання) інформації та засобів її оброблення;
- втрата (ненавмисна втрата, витік) інформації та засобів її оброблення.

Загрози безпеці інформації при забезпеченні доступності:

- блокування інформації;
- знищення інформації та засобів її оброблення.
- загрози безпеці інформації при забезпеченні цілісності:
- модифікація (спотворення) інформації;
- заперечення автентичності інформації;
- нав'язування фальшивої інформації.

Носіями загроз безпеці інформації є джерела загроз. Джерелами загроз можуть бути як суб'єкти (особистість), так і об'єктивні прояви. Причому, джерела загроз можуть знаходитися як усередині організації – внутрішні джерела, так і ззовні її – зовнішні джерела. Поділ джерел на суб'єктивні та об'єктивні виправдане виходячи з попередніх міркувань стосовно вини або ризику збитку інформації. А поділ на внутрішні та зовнішні джерела виправданий тому, що для однієї й тієї ж загрози методи відбивання для внутрішніх і зовнішніх загроз можуть бути різними.

Усі джерела загроз безпеці інформації можна розділити на три групи:

- обумовлені діями суб'єкта (антропогенні джерела загроз);
- обумовлені технічними засобами (техногенні джерела загроз);
- обумовлені стихійними джерелами.

Внутрішні суб'єкти (джерела), як правило, представляють собою висококваліфікованих спеціалістів у галузі розробки та експлуатації програмного забезпечення та технічних засобів, знайомі зі специфікою завдань, що вирішуються, структурою та основними функціями та принципами роботи програмно-апаратних засобів захисту інформації, мають можливість використання штатного обладнання та технічних засобів мережі.

Друга група містить джерела загроз, що визначаються технічною діяльністю людини та розвитком цивілізації. Проте наслідки, викликані такою діяльністю, вийшли з-під контролю людини та діють самі по собі. Людство дійсно стає все більше залежним від техніки, і джерела загроз, які безпосередньо залежать від властивостей техніки, менше прогнозовані і тому потребують особливої уваги. Даний клас джерел загроз безпеці інформації є особливо актуальним у сучасних умовах, так як очікується різке зростання числа техногенних катастроф, викликаних фізичним та морально застарілим станом існуючого обладнання, а також відсутністю коштів на його оновлення. Технічні засоби, що є джерелами потенційних загроз безпеці інформації, також можуть бути зовнішніми та внутрішніми.

Третя група джерел загроз об'єднує обставини, що складають непереборну силу, тобто такі обставини, які носять об'єктивний і абсолютний характер, що розповсюджується на всіх. До непереборної сили в законодавстві та договірній практиці відносять стихійні лиха або інші обставини, які неможливо передбачити або їм запобігти або можливо передбачити, але не можливо запобігти їм при сучасному рівні знань і можливостей людини. Такі джерела загроз абсолютно не піддаються прогнозуванню, і тому заходи захисту від них повинні застосовуватися завжди. Стихійні джерела потенційних загроз інформаційній безпеці, як правило, є зовнішніми по відношенню до об'єкта захисту. Під ними розуміють, насамперед, природні катаклізми.

Напрями забезпечення безпеки інформації – це нормативно-правові категорії, орієнтовані на забезпечення комплексного захисту інформації від внутрішніх та зовнішніх загроз на державному рівні, на рівні підприємства або організації, на рівні окремої особистості.

З урахуванням практики, що склалася на теперішній час, виділяють такі напрями захисту інформації [80]:

- **правовий захист** – це спеціальні закони, інші нормативні акти, правила, процедури та заходи, що забезпечують захист інформації на правовій основі;

- **організаційний захист** – це регламентація виробничої діяльності та взаємовідносин виконавців на нормативно-правовій основі, яка виключає або послаблює нанесення будь-яких збитків виконавцям;

- **інженерно-технічний захист** – це використання різноманітних технічних засобів, що перешкоджають нанесенню збитків.

Крім того, заходи захисту, орієнтовані на забезпечення безпеки інформації, можуть бути охарактеризовані цілим рядом параметрів, що відображають, окрім напрямів, орієнтацію на об'єкти захисту, характер загроз, способи дій, їх розповсюдження, охоплення та масштабність.

Так, за характером загроз заходи захисту орієнтовані на захист інформації від розголошення, витоку та несанкціонованого доступу. За способом дії їх можна поділити на попередження, виявлення, припинення та відновлення збитків або інших утрат. За охопленням заходи захисту можуть розповсюджуватися на територію, будівлю, приміщення, апаратуру або окремі елементи апаратури. Масштабність заходів захисту характеризується як об'єктовий, груповий або індивідуальний захист.

1.6. Атаки на інформаційні ресурси системи

Проблема несанкціонованого доступу (НСД) до ресурсів інформаційних систем загострювалась із розвитком інформаційних технологій і тотального використання комп'ютерних мереж у всіх сферах діяльності суспільства. Розв'язання завдань розробки та вибору відповідних ефективних методів і засобів захисту значною мірою залежить від низки чинників, пов'язаних із самим процесом несанкціонованого доступу [29-31].

Реалізація загроз здійснюється шляхом атак на ресурси ІС, а суттєвим чинником впливу на успіх атакуючих дій є рівень уразливості системи.

Вирішення задач розробки та вибору відповідних ефективних методів і засобів захисту від таких дій значною мірою залежить від низки чинників, пов'язаних із самим процесом атаки та його різномірністю.

Базовими ознаками, за якими можна характеризувати весь спектр атак, є (рис. 1.2):

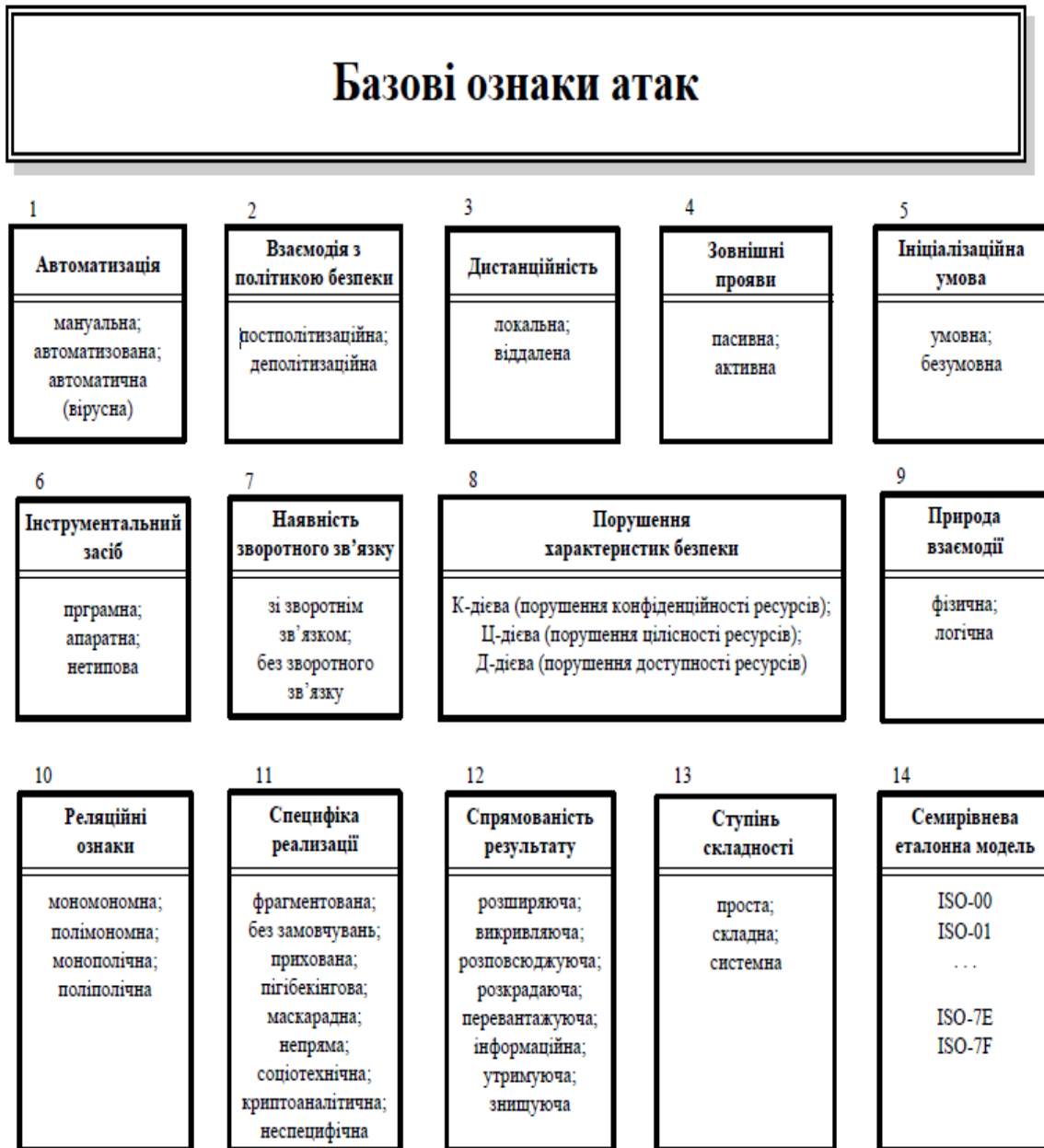


Рис. 1.2. Класифікація атак

- автоматизація;
- взаємодія з політикою безпеки;
- дистанційність;
- зовнішні прояви;
- ініціалізаційна умова;

- інструментальні засоби;
- наявність зворотного зв'язку;
- порушення характеристик безпеки;
- природа взаємодії;
- реляційні ознаки;
- специфіка реалізації;
- спрямованість результату;
- ступінь складності;
- семирівнева еталонна модель.

Відповідно до кожної ознаки розглянемо класи атак. За автоматизацією:

- мануальна;
- автоматизована;
- автоматична (вірусна). *Мануальна атака* (підглядання, збирання сміття, вилучення інформаційних носіїв, підміна положень вмикачів режимів тощо) реалізується за прямою участю людини без використання будь-яких спеціальних засобів (рис. 1.3).

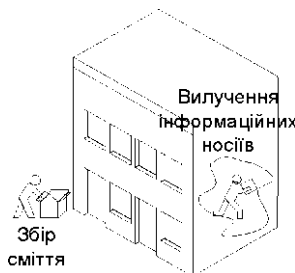


Рис. 1.3. Приклад мануальної атаки

Автоматизована атака здійснюється за постійною участю оператора з використанням широкого спектру програмних і апаратних засобів та пов'язана з суперзапіном, снупінгом, сніфінгом, підключенням додаткових терміналів, використанням торів тощо. Наприклад (рис. 1.4), неавторизована сторона атакує за допомогою апаратних та програмних засобів

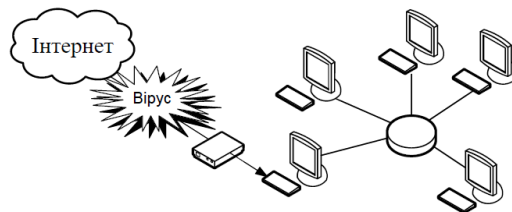


Рис. 1.4. Приклад автоматичної атаки

(наприклад, шляхом використання утиліти віддаленого керування), робочу станцію при прямому підключенні до мережі. мережевих аналізу.

Автоматична атака реалізується без участі людини і, як правило, з використанням спеціалізованих програмних засобів, функціонування яких

базується на вірусних технологіях, наприклад, зараження комп'ютера вірусом під час його підключення до глобальної мережі Internet (рис. 1.5).

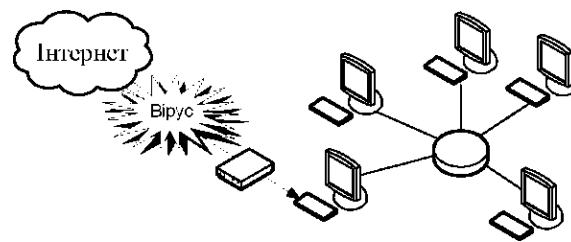


Рис. 1.5. Приклад автоматичної атаки

За взаємодією з політикою безпеки:

- постполітизаційна;
- деполітизаційна.

Постполітизаційна атака заснована на використанні недоліків у вже реалізованій політиці безпеки. Такими недоліками можуть бути невірно побудовані правила розмежування доступу, використання програмних і апаратних засобів з недостатнім рівнем захищеності, прорахунки при блокуванні каналів витоку інформації з обмеженим доступом тощо. Наприклад, якщо користувачу та адміністратору мережі надані однакові права доступу до сервера, то неавторизована сторона, що одержала права доступу Користувача 1, зможе реалізувати атаку на інформаційні ресурси на рівні прав адміністратора (рис. 1.6,а).

Деполітизаційна атака пов'язана з помилками і недбалістю, які мають місце при реалізації заходів із забезпеченням вже існуючої політики безпеки. Це, в першу чергу, пов'язане з людським чинником і залежить від належної адміністративної підтримки, коректності виконання функцій захисту, своєчасного реагування на нештатні ситуації тощо. Наприклад, якщо Користувач залишає без нагляду робочий комп'ютер, не дотримуючись політики безпеки (не закінчує сеанс роботи чи не блокує комп'ютер), то неавторизована сторона за час його відсутності має доступ до інформаційних ресурсів (Рис. 1.6,б). Якщо атака на ресурс здійснюється в локальованій області його розташування (локальна обчислювальна мережа, робоча станція, принтер, носій інформації, ОС, додатки тощо), то вона є локальна, а у протилежному випадку – віддалена. Наприклад, локальна атака може бути реалізована всередині сегмента (фізичного об'єднання станцій за допомогою комутаційних пристроїв не вище каналного рівня), при цьому джерело атаки і ресурс, що піддався атакуючій дії, будуть знаходитись в межах одного сегмента. Наприклад (рис. 1.6,аб) локальна атака реалізовується неавторизованою стороною в одному сегменті мережі, а відділена відбувається через мережу Internet.

Міжсегментна атака може бути прикладом віддаленої атаки, коли джерело і ресурс знаходяться в різних сегментах комп'ютерної мережі інформаційних ресурсів через невиконання Користувачем функцій захисту (рис. 1.6,б) мережі, наприклад, кампусної. У першому випадку ініціатором атаки зазвичай буває легальний користувач, який, наприклад, із файл-

сервера через робочу станцію здійснює копіювання конфіденційних даних на позаштатний носій інформації.

За зовнішнім проявом:

- пасивна;
- активна.

В результаті своєї дії (наприклад, візуального перегляду даних з терміналу) *пасивна атака* не здійснює безпосереднього впливу на ресурси і може не порушити їх базові характеристики безпеки, наприклад, при перехопленні зашифрованих даних.

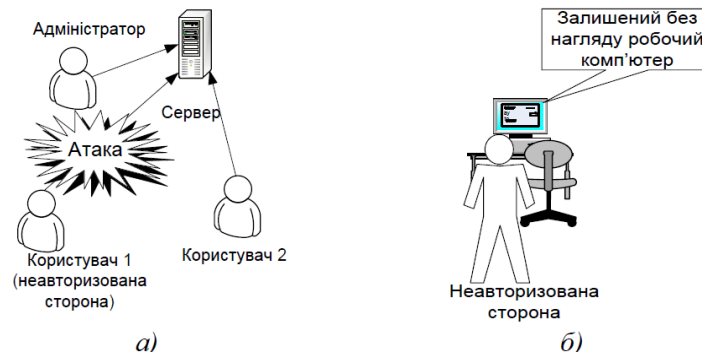


Рис. 1.6. Приклад постполітизаційної і деполітизаційної атаки

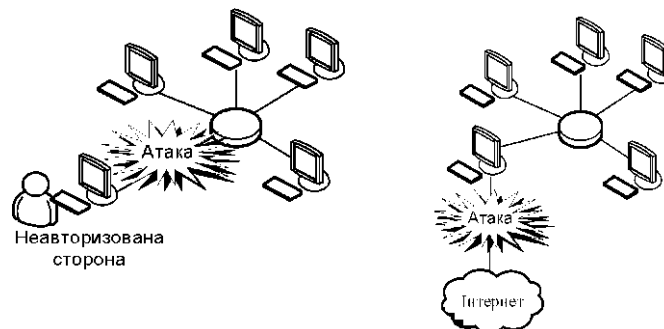


Рис. 1.7. Реалізація локальної та віддаленої атаки

У результаті *активної атаки* на ресурси ІС здійснюється безпосередній вплив (зміна конфігурації, порушення функціональності та ін.) і порушуються їх базові характеристики безпеки.

Наприклад, перехоплення супутникового сигналу (рис. 1.8) без його модифікації відноситься до пасивної атаки.

Перехоплення повідомлення неавторизованою стороною з подальшою його модифікацією (рис. 1.9) належить до активної атаки.

За ініціалізаційною умовою:

- умовна;
- безумовна.

Умовна атака ініціалізується у випадку виникнення певної події (механізм логічної бомби) і в свою чергу може поділятися на пасивну і активну. Прикладом ініціалізації *пасивної умовної атаки* може бути

передача від потенційної цілі запиту певного типу, який і буде умовою початку атаки. У цьому випадку, наприклад, такою умовою можуть бути DNS- і ARP - запити в стеку протоколів TCP/IP.



Рис. 1.8. Реалізація пасивної атаки

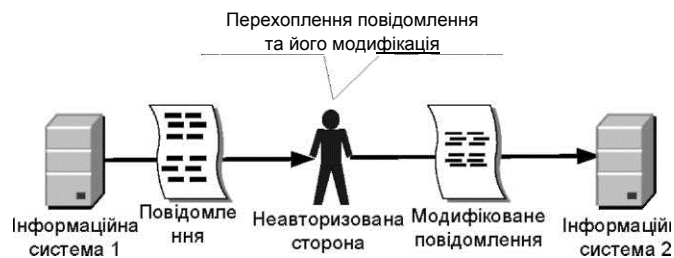


Рис. 1.9. Реалізація активної атаки

За *активною умовною атакою* здійснюється постійний моніторинг стану окремих ресурсів ІС і при певній їх зміні формується сигнал ініціалізації. Прикладом такого стану може бути подія, пов'язана з перериванням сеансу роботи користувача з сервером без стандартної команди, наприклад, LOGOFF. Момент ініціалізації безумовної атаки не супроводжується певною зміною стану ресурсів і визначається джерелом атаки.

За використанням інструментальним засобом:

- програмна;
- апаратна;
- нетипова.

Програмна атака ґрунтується на спеціальних мікро- або макрокодованих засобах (наприклад, суперзапінгових утилітах, внутрішніх командах, сценаріях автоматизації тощо), які функціонують в межах ІС для реалізації своїх функцій.

Наприклад, віддалений комп'ютер (рис. 1.10) відправляє повідомлення на робочу станцію, до якої не санкціоновано підключається неавторизована сторона за допомогою портативного комп'ютера і реалізує зараження цієї станції вірусом, який модифікує це повідомлення.



Рис. 1.10. Реалізація програмної атаки

Апаратна атака засновується на різноманітних механічних, електричних, електромеханічних, електронних, електронно-механічних та інших пристроях, які використовуються автономно чи в поєднанні з іншою апаратурою для виконання відповідних функцій. Наприклад, в кімнаті для нарад (рис. 1.11) може бути встановлений «жучок» для прослуховування конфіденційних розмов. Цей приклад є характерним для апаратної атаки.



Рис. 1.11. Реалізація апаратної атаки

Нетипова атака реалізується на підґрунті таких засобів, які не відносяться до апаратних або програмних, наприклад, вибухівка, радіоактивні матеріали, кислоти, луги, комахи, гризуни тощо.

За наявності зворотного зв'язку (з ресурсом, що піддався атаці):

- зі зворотнім зв'язком;
- без зворотного зв'язку.

У процесі реалізації *атаки зі зворотнім зв'язком* здійснюється отримання від атакованого ресурсу відповіді, які необхідні, наприклад, для подальшого продовження зазначеного процесу на більш ефективному рівні, який досягається завдяки аналізу реакцій об'єкта атаки на певні зміни.

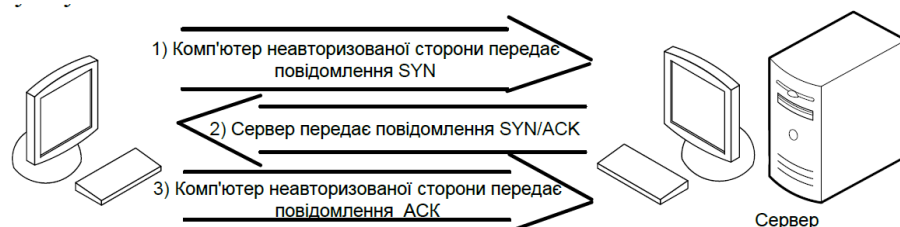


Рис.

1.12. Реалізація атаки із зворотним зв'язком

Прикладом атаки зі зворотнім зв'язком є сканування портів спеціальним програмним забезпеченням. Під час сканування на порти сервера відправляється пакет синхронізації SYN. Якщо на це повідомлення (рис. 1.12) приходиться відповідь (зворотній зв'язок) у вигляді пакету

SYN/ACK, то це означає, що сканований порт знаходиться у стані очікування і можна виконувати наступну дію.

Атака без зворотного зв'язку реалізує свої дії незалежно від реакції атакованого ресурсу. Найбільш яскравим прикладом такої атаки є відмова в обслуговуванні, наприклад, перевантаження маршрутизатора (рис. 1.13), що призводить до його блокування.

За порушенням базових характеристик безпеки ресурсів ІС:

- К-дієва (порушення конфіденційності ресурсів);
- Ц-дієва (порушення цілісності ресурсів);
- Д-дієва (порушення доступності ресурсів).



Рис. 1.13. Реалізація атаки без зворотного зв'язку

Якщо в процесі атаки порушуються різні характеристики безпеки, то результируючий тип буде комбінований на базі основних, наприклад, КЦД-дієва атака, що порушує конфіденційність, цілісність і доступність ресурсів ІС.

За природою взаємодії (з ресурсами ІС):

- фізична;
- логічна.

Для першої характерна *фізична* форма взаємодії, яка проявляється у вигляді різного роду прямих блокувань, пошкоджень, проникнень, крадіжок тощо, наприклад, розмикання електричних з'єднань, пошкодження носіїв інформації, розукомплектовування, подолання фізичного кордону захисту, підслуховування, перехоплення побічних електромагнітних випромінювань і наведень тощо. Прикладом фізичної атаки може бути перехоплення побічних електромагнітних випромінювань з монітора комп'ютера спеціалізованою апаратурою (рис. 1.14).

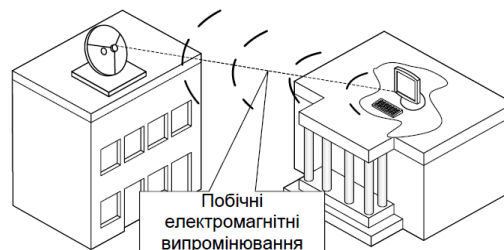


Рис. 1.14. Реалізація фізичної атаки

Для другої не властива пряма фізична взаємодія з ресурсами і вона в основному пов'язана з логікою подій, наприклад, аналізом протоколів, перевантаженням, визначенням паролів, захопленням сеансів тощо.

Прикладом *логічної атаки* може бути перехоплення сеансу зв'язку (рис. 1.15).

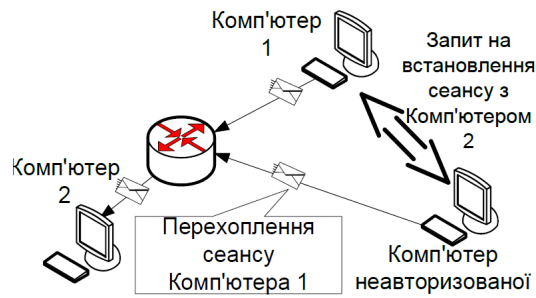


Рис. 1.15. Приклад логічної атаки

Мономономна атака реалізується із одного джерела на один конкретний ресурс. Часто таку атаку називають нерозподіленою, наприклад, мономономною атакою може бути віддалене управління (рис. 1.16) або сканування портів комп'ютера з визначеною IP-адресою.

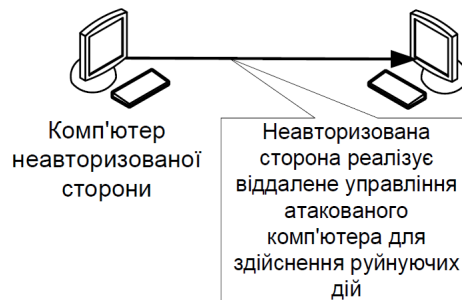


Рис. 1.16. Приклад реалізації мономономної атаки

Полімономна атака здійснюється одночасно з декількох джерел (два і більше) на один ресурс і націлена на досягнення однієї конкретної мети. Таку атаку часто називають розподіленою (рис. 1.17).

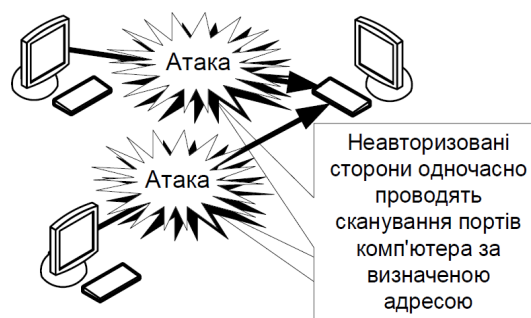


Рис. 1.17. Приклад реалізації полімономної атаки

Монополічна атака реалізується із одного джерела одночасно на множину ресурсів (два і більше) і направлена на досягнення конкретної мети (рис. 1.18).

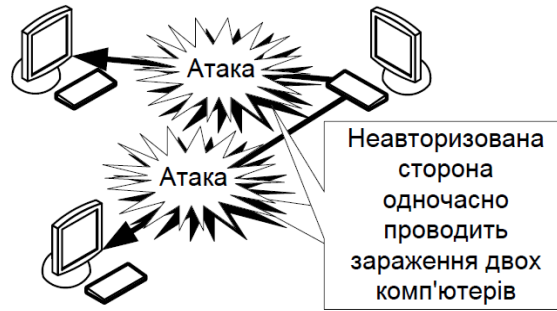


Рис. 1.18. Приклад монополічної атаки

Приклад такої атаки може бути заснований на широкомовному передаванні повідомлення від джерела на всі комп'ютери сегмента, адреси яких знаходяться під одною маскою підмережі. Поліполічна атака поєднує у собі полімономну і монополічну технології, за якими множина джерел здійснює атаку на множину ресурсів з метою досягнення однієї конкретної мети (рис. 1.19).

За специфікою реалізації:

- фрагментована;
- без замовчувань;
- прихована;
- пігібекінгова;
- маскарадна;
- непряма;
- соціотехнічна;
- криптоаналітична;
- неспецифічна.

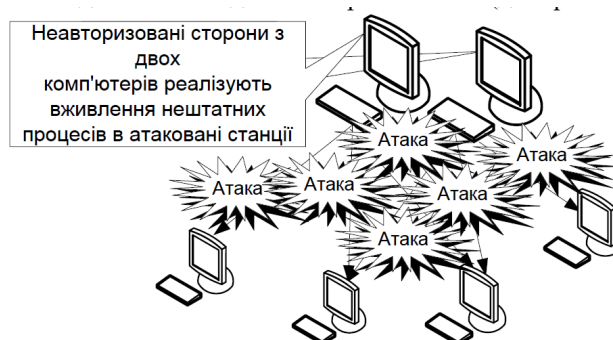


Рис. 1.19. Приклад поліполічної атаки

Фрагментована атака базується на принципі декомпозиції і поетапної реалізації, наприклад, на основі використання механізму розбиття IP-пакетів (на множину більш мілкіших) і подальшого їх передавання (рис. 1.20). Такий підхід дозволяє обходити системи виявлення атак, які не розраховані на протидію декомпозиційним.

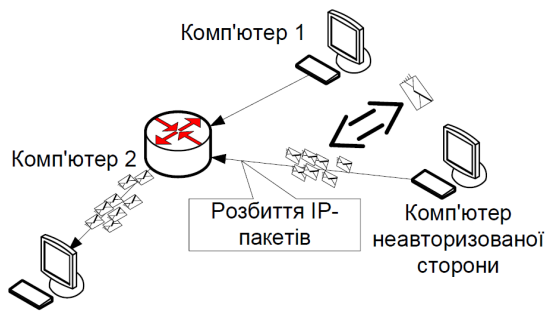


Рис. 1.20. Приклад фрагментованої атаки

Атака, яка реалізується без використання значень за замовчуванням (наприклад, програмна закладка Back Orifice за замовчуванням використовує порт 31337, але це значення може бути змінено наприклад на 31336), орієнтована на подолання систем виявлення атак, які засновуються на сигнатурних (шаблонних) технологіях за аналогією з антивірусними програмами, призначеними для захисту від сигнатурних вірусів.

Прихована атака використовує різноманітні заходи (підміна контрольних сум, перехоплення даних, модифікація ядра операційної системи, використання стандартних або схожих до стандартних імен тощо), які дозволяють залишатися невиявленими в локалізованій області атакованого ресурсу. Технологія прихованої атаки за своєю ідеологією подібна до технології стелс-вірусів.

Пігібекінгова атака заснована на несанкціонованому одержанні доступу до тимчасово неконтрольованого ресурсу, наприклад, шляхом проникнення до інформаційної системи в результаті тимчасової відсутності або після некоректного завершення сеансу роботи легального користувача.

Маскарадна атака заснована на формуванні такої поведінки порушника, яка дозволяє йому видати себе за легальне джерело, наприклад, шляхом обману (spoofing) атакувати обчислювальну мережу (з протоколом TCP/IP) привласнюючи IP-адресу, за допомогою якої обходиться система захисту.

Непряма атака заснована на тому, що напад здійснюється через третю особу (посередника), а істинне джерело нападу залишається невідомим, при цьому часто використовуються маскарадні технології (див. рис. 1.21).

Наприклад, скориставшись варіантом нападу з атакуючих дій, для виключення можливості виявлення реального джерела, порушник проводить або переспрямовує свій трафік через чужий комп'ютер, який для атакованого ресурсу і буде вихідним джерелом.

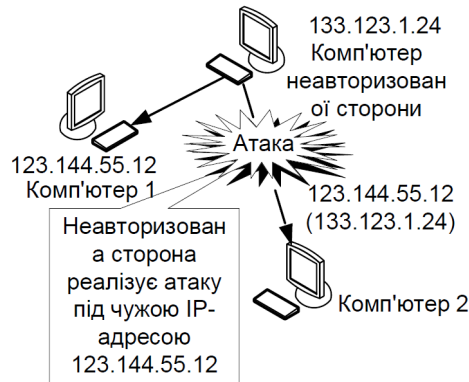


Рис. 1.21. Приклад реалізації непрямої атаки

Соціотехнічна (соціоінжинірингова) атака пов'язана з отриманням даних (наприклад, імен користувачів, паролів, телефонних номерів віддаленого доступу тощо) від атакованих людей у процесі інформаційного обміну (рис. 1.22).

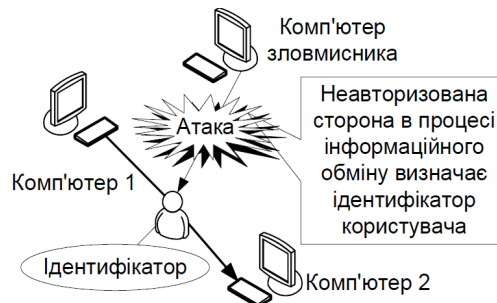


Рис. 1.22. Приклад соціотехнічної атаки

Криптоаналітична атака заснована на використанні широкого спектру криптоаналітичних методів та засобів для зламування ресурсів, захищених різними криптографічними засобами.

До *неспецифічних категорій* відносяться атаки, які не мають вищезазначених особливостей реалізації, при цьому слід враховувати, що технології атак постійно розвиваються і дана ознака може бути розширена.

За спрямованістю результату:

- розширююча;
- викривляюча;
- розповсюджуюча;
- розкрадаюча;
- перевантажуюча;
- інформаційна;
- утримуюча;
- знищуюча.

Розширююча атака (рис. 1.23) орієнтована на одержання більших повноважень на права доступу до ресурсу, наприклад, на вхід в локальну обчислювальну мережу з правами адміністратора, отримання доступу на запис до полів баз даних, зміну атрибутів файлів тощо.

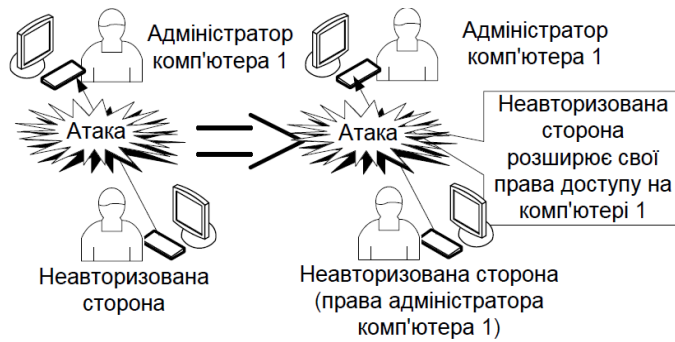


Рис. 1.23. Приклад реалізації розширюючої атаки

Викривляюча атака пов'язана зі здійсненням будь-яких прямих змін в цільовому ресурсі, наприклад, підробка полів баз даних, підміна інформаційних носіїв, зміна часу і дати тощо.

Розповсюджуюча атака спрямована на отримання доступу до ресурсу та його розкриття без відповідних на це повноважень, наприклад, несанкціоноване одержання файлу даних з пароллями і їх публікація на хакерських сайтах або розсилання серед абонентів обчислювальної мережі.

Розкрадаюча атака направлена на використання ресурсу без нанесення прямого збитку, наприклад, без зниження якості обслуговування користувачів здійснити тимчасове вилучення частини пам'яті (для розширення можливостей іншої системи), завантаження телекомунікаційних каналів, використання робочої станції або мережевого сервісу тощо.

Перевантажуюча атака спрямована на завантаження ресурсу до такого рівня, що він втрачає властивість щодо його використання. Результатом такої атаки може бути «неможливість використання», «перевантаження», «перешкоджання використанню», «відмова в обслуговуванні» тощо. Прикладом такої атаки (рис. 1.24) може бути перевантаження маршрутизатора.

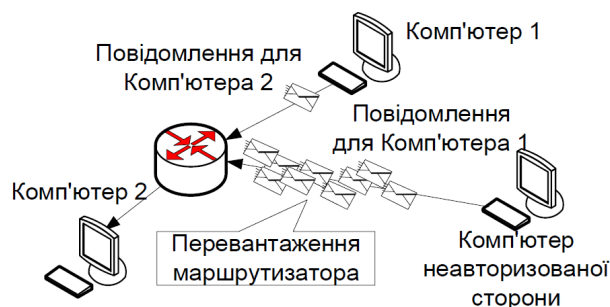


Рис. 1.24. Реалізація перевантажуючого НСД

Інформаційна атака пов'язана зі збиранням необхідних даних (як правило для реалізації подальших дій) і не передбачає прямого впливу на ресурс, наприклад, одержання інформації в результаті аналізу публікацій, використання системних утиліт для виявлення активних робочих станцій, сервісів тощо (рис. 1.25).

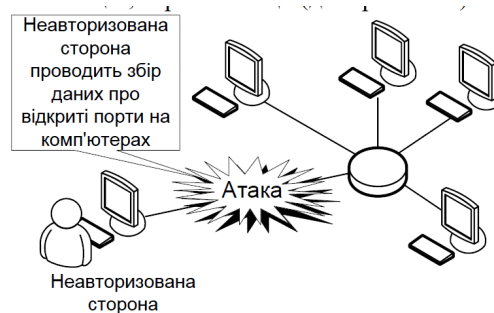


Рис. 1.25. Приклад інформаційної атаки

Утримуюча атака призначена для тимчасової затримки ресурсу з метою зниження його актуальності, наприклад, притримування шини знищуюча атака орієнтована на безповоротну ліквідацію ресурсу, наприклад, вилучення файлу, дроблення інформаційного носія, низькорівневе форматування жорсткого диску з метою знищення даних тощо (рис. 1.26).

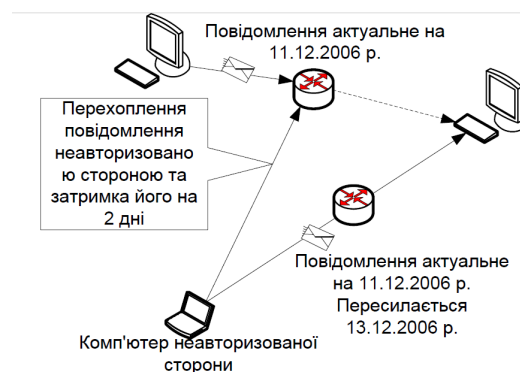


Рис. 1.26. Приклад утримуючої атаки

Знищуюча атака орієнтована на безповоротну ліквідацію ресурсу, наприклад, вилучення файлу, дроблення інформаційного носія, низькорівневе форматування жорсткого диску з метою знищення даних тощо (рис. 1.27).

За ступенем складності:

- проста;
- складна.

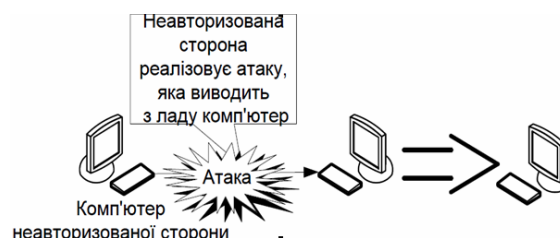


Рис. 1.27. Приклад знищуючої атаки

Проста атака (рис. 1.28) є нескладною в реалізації діями, направленними на виконання окремих процедур, наприклад, сканування

портів, аналіз трафіку, пошук активних робочих станцій, віддалене управління тощо.

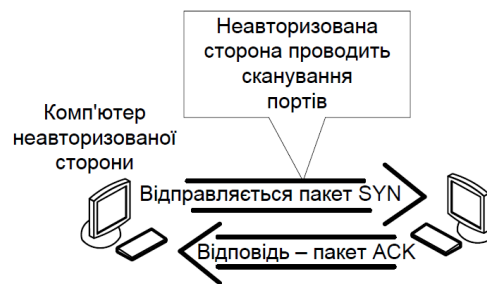


Рис. 1.28. Приклад простої атаки

Складна атака є комбінацією простих і призначена для реалізації низки необхідних функцій, наприклад, виявлення активної робочої станції і здійснення віддаленого управління нею.

Системна атака будується на основі сформованого системного підходу з багатокроковою комбінацією дій та використанням простих атак для ефективною реалізації спеціально направленою комплексу функцій, наприклад, пошук активних робочих станцій, моніторинг трафіку, сканування, зламування ОС і робочих додатків, несанкціоноване копіювання даних та замітання слідів.

Міжнародна організація стандартизації (ISO) запропонувала семирівневу еталонну модель з метою розмежування функцій різних протоколів у процесі передачі інформації від одного абонента іншому. Таких класів функцій виділено сім. Вони отримали назву рівнів, кожний з яких виконує певні задачі в процесі передачі блоку інформації, причому відповідний рівень зі сторони приймача виконує перетворення, зворотні тим, що зроблені на тому самому рівні на передавальній стороні (джерелі). У цьому зв'язку атака за семирівневою еталонною моделлю можна визначити на таких рівнях:

- фізичний, що кодується параметром $K0(2) = 20$;
- канальний, що кодується параметром $K1(2) = 21$;
- мережевий, що кодується параметром $K2(2) = 2^2$;
- транспортний, що кодується параметром $K3(2) = 23$;
- сеансовий, що кодується параметром $K4(2) = 24$;
- представлення даних, що кодується параметром $K5(2) = 25$;
- прикладний, що кодується параметром $K6(2) = 2^6$.

На *фізичному рівні* забезпечуються необхідні механічні, електричні, функціональні і процедурні характеристики для встановлення, підтримки і розмикання фізичного з'єднання. На *канальному рівні* забезпечуються функціональні і процедурні засоби для встановлення, підтримки і вивільнення ліній передавання даних між абонентами мережі (наприклад, терміналами і вузлами мережі). На *мережевому рівні* забезпечуються функціональні і процедурні засоби для обміну службовою інформацією між двома об'єктами транспортного рівня мережі (тобто пристроями, що

підтримують протоколи на транспортному рівні за допомогою мережевого з'єднання). Гарантує незалежність поводження об'єктів транспортного рівня від схеми маршрутизації і комутації. На *транспортному рівні* забезпечується оптимізація комутаційного обслуговування (підтримуваного реалізацією більш низьких рівнів зв'язку) шляхом забезпечення прозорих передач даних між абонентами в рамках сеансу. На *сеансовому рівні* здійснюється забезпечення на логічному рівні обслуговування двох «пов'язаних» на *рівні представлення даних* об'єктів мережі і керування введенням діалогу між ними шляхом синхронізації повідомлень.

На *рівні представлення даних* забезпечується сукупність службових операцій, які можна вибрати на *прикладному рівні* для інтерпретації переданих і одержуваних даних. Ці службові операції містять керування інформаційним обміном, відображення даних і керування структурованими даними. Службові операції цього рівня являють собою основу всієї семирівневої моделі і дозволяють пов'язувати в одне ціле термінали і засоби обчислювальної техніки будь-яких типів.

На *прикладному рівні* забезпечується безпосередня підтримка прикладних процесів і програм кінцевого користувача і керування взаємодії цих програм з різними об'єктами мережі передачі даних. Визначення класу атаки за даною ознакою наступне – ISO-K, де $K = K_{(2)0} + K_{(2)1} + K_{(2)2} + K_{(2)3} + K_{(2)4} + K_{(2)5} + K_{(2)6}$ – двійковий код. Для зручності K будемо представляти у шістнадцятковому коді (K (16)). Наприклад, якщо за цією класифікацією атака записана як ISO-3A (де $3A_{(16)} = 0111010 = 2^5 + 2^4 + 2^3 + 2^1 = K5 + K4 + K3 + K1$), то вона інтерпретує реалізацію на рівні каналному, транспортному, сеансовому і представлення даних, а, наприклад, запис ISO-00 означає, що клас атаки не підтримується семирівневою еталонною моделлю.

Не важко помітити, що атаки, які класифікуються за ознаковим принципом, можуть у кожному конкретному випадку при визначенні загального класу містити не тільки одну, але і більше компонент кожної з ознак. Слід зазначити, що з появою нових методів і засобів реалізації несанкціонованих дій, ознаки такої класифікації можуть бути розширені. При практичному використанні класифікації, наприклад, таку атаку, як сканування портів, можна визначити як: автоматизована, 12• 13• 14• 15• 16• 17• • 16• 17• 18• 19• 20• 21• • 20• 21• 22• 23• 24or рамна, зі зворотним зв'язком, K-дієва, логічна, мономонна, неспецифічна, інформаційна, проста, ISO-36.

За допомогою даної класифікації можна здійснювати (відповідну їй) формалізацію можливостей систем протидії для підвищення ефективності їхнього вибору і формуванні вимог при їхній розробці.

З НСД пов'язані такі поняття, як доступ та перехоплення. Під доступом (access) розуміють взаємодію між ресурсами інформаційних систем, що забезпечує передачу інформації між такими ресурсами, а в процесі доступу до інформації (access to information) реалізуються,

зокрема, її копіювання, модифікація, знищення, ініціалізація тощо. Розрізняють несанкціонований та санкціонований доступи. Якщо доступ до ресурсів системи здійснюється, наприклад, з порушенням або поза правилами розмежування доступу, то такий доступ – несанкціонований. Однією з базових дій, що породжує НСД, є перехоплення (*intercept*), під яким розуміють несанкціоноване одержання інформації незаконним підключенням до каналів зв'язку (наприклад, пряме перехоплення) чи візуально (наприклад, підглядання), або за допомогою радіотехнічних засобів (наприклад, непряме перехоплення).

За дією на інформацію розрізняють активне і пасивне перехоплення, а за типом підключення:

- пряме;
- непряме.

Активне перехоплення (*active eavesdropping*) – це таке перехоплення, під час якого в супротивника є можливість не тільки перехоплювати повідомлення, а й впливати на нього, наприклад, затримувати або вилучати сигнали, що передаються каналами зв'язку.

Пасивне перехоплення (*passive tapping*) – отримання інформації з можливістю тільки спостерігати за обміном повідомленнями (наприклад, з метою виявлення різної системної інформації в обчислювальній мережі (ОМ)), не впливаючи на нього.

Пряме перехоплення (*direct eavesdropping*) – перехоплення інформації безпосереднім підімкненням (наприклад, додаткового терміналу) до лінії зв'язку. Пряме перехоплення можна виявляти перевіркою лінії зв'язку.

Непряме перехоплення (*indirect eavesdropping*) – перехоплення інформації (наприклад, індуктивних хвиль) без використання безпосереднього підключення до лінії зв'язку (*threat*). Таке перехоплення важко виявити, оскільки немає безпосереднього приєднання термінального обладнання до лінії зв'язку.

1.7. Рівні захисту інформаційних систем

Побудова надійного захисту інформаційної системи неможлива без попереднього аналізу можливих загроз безпеки системи [83]. Цей аналіз повинен складатися з таких етапів:

- виявлення характеру інформації, яка зберігається в системі;
- оцінки цінності інформації, яка зберігається в системі;
- побудови моделі зловмисника;
- визначення та класифікації загроз інформації в системі (несанкціоноване зчитування, несанкціонована модифікація і т.д.);
- визначення затрат часу і матеріальних ресурсів на злам системи, припустимих для зловмисників;
- оцінки припустимих витрат часу, засобів і ресурсів системи на організацію її захисту.

Проблеми інформаційної безпеки вирішуються, як правило, з допомогою створення спеціалізованих систем захисту інформації, які повинні забезпечувати безпеку інформаційної системи від несанкціонованого доступу (НСД) до інформаційних ресурсів. Система захисту інформації є інструментом адміністраторів інформаційної безпеки, які виконують функції із забезпечення захисту інформаційної системи і контролю її захищеності.

Система захисту інформації повинна виконувати такі функції:

- реєстрація і облік користувачів, носіїв інформації, інформаційних масивів;
- забезпечення цілісності системного та прикладного програмного забезпечення та інформації яка оброблюється;
- захист комерційної таємниці, включаючи використання сертифікованих засобів криптографічного захисту;
- створення захищеного електронного документообігу з використанням сертифікованих засобів криптографічні перетворення і електронного цифрового підпису;
- централізоване управління системою захисту інформації;
- управління доступом;
- забезпечення ефективного антивірусного захисту, тощо.

Комплекс вимог, які висуваються до системи безпеки, передбачає функціональне навантаження на кожний з наведених на рис. 1.29. рівнів. Організація захисту на фізичному рівні повинна зменшити можливість несанкціонованих дій сторонніх осіб і персоналу підприємства, а також понизити вплив техногенних джерел.

Захист на технологічному рівні (програмний продукт і технічні засоби обробки інформації). Система захисту на цьому рівні повинна бути автономною, але забезпечувати реалізацію єдиної політики безпеки і будуватись на основі використання сукупності вбудованих систем захисту операційної системи і систем управління базами даних та знань.

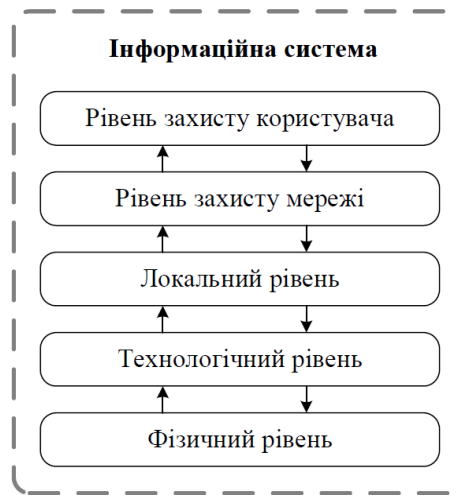


Рис. 1.29. Рівні захисту інформаційної системи

На локальному рівні організується розподілення інформаційних ресурсів ІС на сегменти за рівнями конфіденційності по територіальному і функціональному принципам, а також виділяється в окремий сегмент засоби обробки конфіденційної інформації. Підвищенню рівня захищеності сприяє обмеження і мінімізація кількості точок входу/виходу (точок взаємодії) між сегментами, створення надійної оболонки по периметру сегментів і інформаційної системи в цілому, організація захищеного обміну інформацією між сегментами.

На мережевому рівні організується захищений інформаційний обмін даними між автоматизованими робочими місцями, а також створюється надійна оболонка фізичного захисту периметра розташування ІКСМ в цілому. Система захисту на цьому рівні повинна будуватись з урахуванням реалізації захисту на попередніх рівнях.

На рівні користувача повинно бути забезпечено допуск тільки авторизованих абонентів до роботи в інформаційній системі, створено захисну оболонку навколо її елементів, а також організовано індивідуальне захищене середовище діяльності кожного користувача.

Залежно від призначення і характеру задач з обробки інформації можна виділити три основні види експлуатації інформаційно-комунікаційних систем, що мають принципове значення для складу посадовців і характеру доступу до інформації з:

- **закритим доступом** – організація-споживач використовує інформаційну систему повністю в своїх інтересах, при цьому обслуговуючий персонал, включаючи технічний і оперативний склад, є співробітниками даної організації;

- **обмеженим доступом** – організація-споживач обчислювальної системи поєднує свої інтереси з інтересами інших організацій і приватних осіб;

- **відкритим доступом** – організація-споживач обчислювальної мережі надає послуги населенню.

Назва «Система з відкритим доступом» умовна в тому значенні, що будь-яка людина може скористатися послугами даної системи. Насправді ж кожна інформаційна система (ІС) має і внутрішню частину, яка стосується обробки її власної інформації, яка може бути закритою для сторонніх осіб [84].

Усі загрози безпеки, спрямовані проти програмних і технічних засобів інформаційної системи, впливають на безпеку інформаційних ресурсів і призводять до порушення основних властивостей інформації, яка зберігається і обробляється в системі. Як правило, загрози інформаційній безпеці розрізняються за способом їх реалізації.

Дослідження і аналіз численних випадків впливів на інформацію і несанкціонованого доступу до неї показують, що їх можна розділити на випадкові і навмисні.

Навмисні загрози можуть бути реалізовані шляхом довготривалої масованої атаки несанкціонованими запитами або вірусами тощо. Наслідки такі: руйнування (втрата) інформації, модифікація (зміна інформації на помилкову, яка коректна за формою і змістом, але має інший сенс) і ознайомлення з нею сторонніх осіб. Ціна вказаних подій може бути досить високою. Попередження зазначених наслідків в інформаційній системі є основною метою створення системи безпеки інформації, розроблення та вдосконалення існуючих методів захисту інформації в інформаційно-комунікаційних системах та мережах.

Для вирішення поставленої задачі доцільно навести найбільш повну класифікацію загроз і шляхів їх реалізації в ІКСМ.

Можна виділити такі основні класи загроз безпеці, які спрямовані проти інформаційних ресурсів:

- загрози конфіденційності даних і програм;
- загрози цілісності даних, програм, апаратури;
- загрози доступності даних;
- загрози відмови від виконання трансакцій.

Оцінка вразливості інформаційної системи і побудова моделі впливів припускають вивчення всіх варіантів реалізації перерахованих вище загроз і виявлення наслідків, до яких вони призводять.

1.8. Основні принципи захисту інформації

Захист інформації від НСД є складовою частиною загальної проблеми забезпечення захисту інформації в ІКСМ. В загальному випадку комплекс програмно-технічних засобів та організаційних рішень по захисту інформації в ІКСМ реалізується в рамках системи захисту інформації від НСД, яка умовно складається з таких чотирьох підсистем [79]:

- управління доступом до ІКСМ, до її послуг та ресурсів;
- реєстрація і облік користувачів, послуг, інформаційних ресурсів;
- криптографічного захисту;
- забезпечення цілісності інформаційних потоків, інформаційних ресурсів та програмного забезпечення.

Закриття каналів несанкціонованого отримання інформації повинно починатися з контролю доступу користувачів до ресурсів ІКСМ. Ця задача вирішується на основі ряду принципів:

Принцип виправданості доступу – користувач повинен мати достатню «форму допуску» для отримання інформації того рівня конфіденційності, що він вимагає, і ця інформація дійсно необхідна йому для виконання його виробничих функцій.

Принцип достатньої глибини контролю доступу. Засоби захисту інформації повинні включати механізми контролю доступу до всіх видів інформаційних і програмних ресурсів ІКСМ, які у відповідності з принципом виправданості доступу слід розмежовувати між користувачами.

Принцип розмежування інформаційних потоків. Для попередження порушення інформаційної безпеки, яке, наприклад, може мати місце при запису секретної інформації на несекретні носії і в несекретні файли, її передачі програмам і процесам, які не призначені для обробки секретної інформації, а також при передачі секретної інформації по незахищених каналах зв'язку, необхідно здійснювати відповідне розмежування інформаційних потоків.

Принцип персональної відповідальності. Кожний користувач повинен нести персональну відповідальність за свою діяльність в системі, включаючи будь-які операції з конфіденційною інформацією і можливі порушення її захисту.

Принцип цілісності засобів захисту. Даний принцип передбачає, що засоби захисту інформації в ІКСМ повинні чітко виконувати свої функції у відповідності з переліченими принципами і бути ізольованими від користувачів, а для свого супроводу повинні включати спеціальний захищений інтерфейс для засобів контролю, сигналізації про спроби порушення захисту інформації і впливу на процеси в системі.

Реалізація перелічених принципів здійснюється з допомогою так званого «монітору звернень», який контролює будь-які запити до даних чи програм з боку користувачів (чи їх програм) за установленими для них видами доступу до цих даних і програм. Схематично такий монітор можна представити у вигляді, показаному на рис. 1.30.

Практичне створення монітору звернень, як видно з наведеного рисунку, передбачає розробку конкретних правил розмежування доступу у вигляді так званої моделі захисту інформації.

Найбільш розповсюджена модель отримала назву – багаторівнева модель захисту Белла Ла Падула. Основою цієї моделі є поняття рівня конфіденційності (форми допуску) і категорії (прикладної області) суб'єкта і об'єкта доступу. На основі присвоєних кожному суб'єкту і об'єкту доступу конкретних рівнів і категорій в моделі визначаються їх рівні безпеки, а потім встановлюється їх взаємодія. При цьому в моделі приймається, що один рівень безпеки домінує над іншим тоді і тільки тоді, коли відповідний йому рівень конфіденційності більше чи дорівнює конфіденційності іншого, а множина категорій включає множину категорій другого.

Розмежування і контроль доступу до інформації

Розмежування доступу в ІКСМ полягає в розділенні інформації на частини і організації доступу до неї користувачів відповідно до їх функціональних обов'язків і повноважень.

Задача такого розмежування доступу до інформації: скорочення кількості користувачів, що не мають до неї відношення при виконанні своїх функцій, тобто захист інформації від порушника серед законних користувачів. Розмежування доступу користувачів ІКСМ може здійснюватися за такими параметрами:

- виглядом, характером, призначенням, ступенем важливості і секретності інформації;
- способами її обробки: обчислення, запис, внесення змін, виконання команди;
- умовним номером терміналу; часом обробки й ін.

При проектуванні ІКСМ на її базі проводяться розробка і реалізація функціональних задач по розмежуванню і контролю доступу до апаратури і інформації як в рамках інформаційної системи в цілому, так і до відокремлених інформаційних ресурсів;



Рис. 1.30. Структура монітору звернень

- розробка апаратних засобів ідентифікації та аутентифікації користувачів та ресурсів системи;

- розробка програмних засобів контролю і управління розмежуванням доступу;
- розробка окремої експлуатаційної документації на засоби ідентифікації, аутентифікації, розмежування і контролю доступу.

Запитання для самоконтролю:

1. Дайте визначення інформаційній безпеці.
2. Назвіть об'єкти інформаційної безпеки.
3. Визначте інтереси держави в інформаційній сфері.
4. Перерахуйте основні загрози інформаційним ресурсам ІКСМ.
5. Назвіть основні локальні фактори загроз інформаційній безпеці.
6. Які існують канали витоку інформації?
7. Основні характеристики побудови моделі порушника.
8. Основні положення методів і засобів забезпечення інформаційної безпеки.
9. Дайте визначення, що таке комп'ютерні віруси.
10. Розкрийте поняття «цілісність».
11. Розкрийте поняття «доступність».
12. Розкрийте поняття конфіденційності інформації.
13. Назвіть основні напрями забезпечення безпеки інформації.
14. Як класифікуються атаки за автоматизацією системи?
15. Як класифікуються атаки за ініціалізаційною умовою?
16. Як реалізується атаки зі зворотним зв'язком?
17. Чи можливо реалізувати монономні атаки з кількох джерел?
18. На чому ґрунтується пігібекінгові атаки?
19. Що можна віднести до неспецифічних категорій НСД?
20. Як класифікуються атаки за засобами захисту від НСД?
21. Що відноситься до засобів несанкціонованого доступу?
22. Розкрийте поняття «інформаційна боротьба».
23. Назвіть основні характеристики інформаційної системи.
24. Розкрийте зміст моделі системи захисту інформації.
25. Якими показниками може бути оцінено якість розподілу доступу?
26. Назвіть основні принципи та рівні захисту інформаційних систем.
27. Які існують основні принципи захисту інформації?

Розділ 2. ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ СИСТЕМИ ТА МЕРЕЖІ

Впровадження та інтеграція інформаційно-комунікаційних систем та мереж потребує високого рівня технічних і соціальних вимог до якості інформаційних ресурсів та безпосередньо до систем передачі, обробки і відображення даних. Базовими властивостями інформаційних ресурсів є їх цілісність, конфіденційність і доступність. Випадкові, а також штучні завади, спотворюють інформаційні потоки, які надходять від джерела повідомлення до споживача, що призводить до втрати цілісності даних. Спотворення основних властивостей інформації при її передачі чи обробці, веде до неякісних процедур прийняття рішень або зовсім унеможливорює цей процес у всіх сферах діяльності розвинутого суспільства.

Базовою функцією інформаційних систем передачі даних є здійснення процесів оперативного та надійного обміну інформацією між джерелом повідомлення та його користувачем, а також у забезпеченні ефективності функціонування інформаційної системи мінімізації часу передачі інформації з умов зростання її обсягів при фіксованій вірогідності інформаційного потоку. Інформаційні системи передачі даних є базовою платформою сучасного процесу інформатизації суспільства, що активно впливає на стан національної безпеки держави.

2.1. Визначення інформаційно-комунікаційних систем

Інформаційно-комунікаційна система (та мережа, ІКСМ) – це інтегрований комплекс організаційно-технічних заходів та взаємопов'язаних і взаємоузгоджених комунікаційних, програмно-апаратних і програмних компонентів, які забезпечують достовірну передачу інформації від джерела повідомлення до споживача.

Вивчення мережі в цілому потребує знання принципів роботи та характеристик її окремих елементів: комп'ютерів, комунікаційного устаткування, операційних систем, мережних додатків і т. ін.

Багаторівневою моделлю інформаційно-комунікаційної системи називається повний інтегрований комплекс середовища та комунікаційних й програмно-апаратних засобів, що застосовується з метою достовірної передачі інформаційних потоків від джерела повідомлення до споживача.

Перший (апаратний) рівень – основа будь-якої мережі, створена стандартизованими комп'ютерними платформами й використовується з метою автоматизованої обробки даних.

Другий рівень – комунікаційне устаткування зазначеної інформаційно-комунікаційної мережі.

Не зважаючи на те, що комп'ютери і є центральними елементами обробки даних у мережах, не менш важливу роль в організації мережі відіграють комунікаційні пристрої. Кабельні системи, повторювачі, мости, комутатори, маршрутизатори й модульні концентратори – усі ці складові перетворилися з допоміжних компонентів мережі на основні як за впливом

на характеристики мережі, так і за вартістю. Сьогодні комунікаційний пристрій може бути складним спеціалізованим мультипроцесором, який потрібно конфігурувати, оптимізувати й адмініструвати. Для вивчення принципів роботи комунікаційного устаткування необхідно знання великої кількості протоколів, використовуваних як у локальних, так і у глобальних мережах.

Третій рівень – операційні системи (ОС), які створюють та забезпечують програмну платформу мережі.

Від того, які концепції управління локальними та розподіленими ресурсами покладено в основу мережної ОС, залежить ефективність роботи всієї мережі. При проектуванні мережі важливо враховувати:

- оптимальність взаємодії даної операційної системи з іншими ОС мережі;
- можливості забезпечення безпеки інформації і захищеності даних;
- можливість нарощувати кількість користувачів (складність мережі);
- можливість адаптації чи інсталяції на інші типи обчислювальних платформ тощо.

Четвертий рівень – рівень мережних засобів – утворюють мережні додатки, такі як мережні бази даних, поштові системи, засоби архівації даних, системи автоматизації колективної роботи і т. ін.

Важливо уявляти діапазон можливостей, що надаються додатками для різних сфер застосування, а також знати, наскільки вони сумісні з іншими мережними додатками й операційними системами.

При об'єднанні в мережу великої кількості користувачів постає цілий комплекс технічних питань. Проектування мережі передусім передбачає розв'язання задачі про її топологію – спосіб організації фізичних зв'язків між елементами мережі.

Топологією інформаційно-комунікаційної мережі називається конфігурація графа, вершинам якого відповідають користувачі (комп'ютери) мережі (іноді й інше устаткування, наприклад концентратори), а ребрам - фізичні зв'язки між ними.

Комп'ютери, які підключені до мережі, часто називають станціями або вузлами мережі.

Повнозв'язана топологія відповідає мережі, в якій кожний комп'ютер мережі пов'язаний з усіма іншими (рис. 2.1,а).

Топології мереж (а – повнозв'язана топологія, б – комірчаста топологія, в – загальна шина, г – топологія зірка, д – розширена зірка, е – кільцева топологія).

Комірчаста топологія (рис. 2.1,б) утворюється з повнозв'язаної вилученням деяких можливих зв'язків.

Загальна шина (рис. 2.1,в) – поширена топологія для локальних мереж. У цьому разі комп'ютери підключаються до одного коаксіального кабелю. Передана інформація може поширюватись в обидва боки.

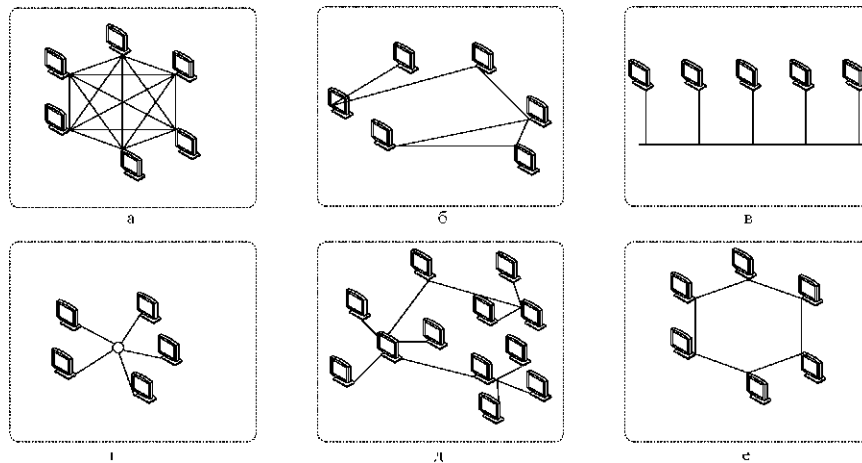


Рис. 2.1. Види топологій інформаційно-комунікаційних мереж

Застосування загальної шини знижує вартість проводки, уніфікує підключення різних модулів, забезпечує можливість миттєвого широкомовного звернення до всіх станцій мережі. Недолік загальної шини полягає в її низькій надійності: будь-який дефект кабелю або якого-небудь з численних роз'ємів повністю паралізує всю мережу. Їй притаманна також невисока продуктивність, оскільки за такого способу підключення в кожний момент часу тільки один комп'ютер може передавати дані в мережу. Тому пропускна здатність каналу зв'язку завжди розподіляється тут між усіма вузлами мережі.

Топологія зірка (рис. 2.1,г). – У цьому разі кожний комп'ютер підключається окремим кабелем до загального пристрою, названого концентратором, який міститься в центрі мережі.

Розширена зірка (ієрархічна топологія) (рис. 2.1,д) – топологія мережі з використанням кількох концентраторів, ієрархічно з'єднаних між собою зв'язками типу зірка. Нині розширена зірка є найпоширенішим типом топології зв'язків як у локальних, так і в глобальних мережах.

Кільцева топологія (рис. 2.1,е) – топологія мережі, в якій дані передаються по кільцю від одного комп'ютера до іншого, як правило, в одному напрямі.

Невеликі мережі здебільшого мають типову топологію – зірка, кільце або загальна шина, для великих мереж характерна наявність довільних зв'язків між комп'ютерами. У таких мережах можна виділити окремі довільно зв'язані фрагменти (підмережі), що мають типову топологію, тому їх називають **мережами з мішаною топологією**.

Мережева технологія – це узгоджений набір стандартних протоколів та програмно-апаратних засобів, що їх реалізують (наприклад, мережевих адаптерів, драйверів, кабелів і роз'ємів), достатніх для побудови та функціонування інформаційно-комунікаційної мережі.

Однією з найбільш розвинених мережевих технологій є технологія Ethernet. Протоколи, на основі яких будується мережа певної технології (у вузькому сенсі), спеціально розроблялися для спільної роботи користувачів (абонентів), тому від розробника мережі не вимагається

додаткових зусиль щодо організації її взаємодії. Іноді мережні технології називають базовими, маючи на увазі те, що на їх основі будується базис будь-якої мережі.

Головний принцип, покладений в основу Ethernet, – випадковий метод доступу до середовища передачі даних та загальних інформаційних ресурсів (CSMA/CD). Як середовище може використовуватися товстий або тонкий коаксіальний кабель, вита пара, оптоволокно або радіохвилі для передачі інформаційних потоків.

Сутність випадкового методу доступу: користувач у мережі Ethernet може передавати дані по мережі тільки тоді, коли мережа вільна, тобто коли ніякий інший користувач (комп'ютер) у даний момент не обмінюється даними. Тому важливою частиною технології Ethernet є процедура визначення доступності середовища.

Після того як комп'ютер переконався, що мережа вільна, він починає передачу, «захоплюючи» при цьому середовище. Час монопольного використання середовища одним вузлом обмежується часом передачі одного кадру.

Кадр (фрейм) – це одиниця даних, якою обмінюються користувачі (комп'ютери) у мережі Ethernet. Кадр має фіксований формат і разом із полем даних містить різну службову інформацію (наприклад, адресу одержувача і адресу відправника).

Іноді може виникати ситуація, коли одночасно два або більше користувачів вирішують, що мережа вільна, і починають передавати інформацію. Така ситуація називається колізією – перешкоджанням достовірній передачі даних по мережі. У стандарті Ethernet передбачено алгоритм виявлення і коректної обробки колізій. Імовірність виникнення колізії залежить від інтенсивності мережного трафіку. Після виявлення колізії мережні адаптери, які намагалися передати свої кадри, припиняють передачу і після паузи випадкової тривалості намагаються знову отримати доступ до середовища й передати той кадр, який викликав колізію.

У мережах з невеликою кількістю користувачів найчастіше використовується одна з базових топологій – загальна шина, кільце, зірка або мішана топологія. Усі перелічені топології мають властивість однорідності, тобто всі комп'ютери в такій мережі мають однакові права щодо доступу до інших комп'ютерів (за винятком центрального комп'ютера при з'єднанні зірка). Така однорідність структури спрощує процедуру нарощування кількості комп'ютерів, полегшує обслуговування та експлуатацію мережі.

Проте при побудові великих мереж однорідна структура зв'язків перетворюється з переваги на недолік. У таких мережах використання типових структур породжує різні обмеження, найважливішими з яких є: обмеження на довжину зв'язку між вузлами; обмеження на кількість вузлів у мережі; обмеження на інтенсивність трафіку, що породжується вузлами мережі. Наприклад, технологія Ethernet на тонкому коаксіальному кабелі дає змогу використовувати кабель завдовжки не більш як 185 м, до якого

можна підключити не більш як 30 комп'ютерів. Для зняття цих обмежень використовуються спеціальні методи структуризації мережі та спеціальне устаткування, що створює структуру – повторювачі, концентратори, мости, комутатори, маршрутизатори. Устаткування такого роду також називають комунікаційним, маючи на увазі, що за його допомогою окремі сегменти мережі взаємодіють між собою.

Повторювач (repeater) – комунікаційний пристрій, використовуваний для фізичного з'єднання різних сегментів локальної мережі з метою збільшення загальної довжини мережі. Повторювач передає сигнали, що приходять з одного сегмента мережі в інші її сегменти (рис. 2.2). Повторювач дає змогу подолати обмеження на довжину ліній зв'язку за рахунок підвищення якості переданого сигналу – відновлення його потужності та амплітуди, поліпшення фронтів і т. ін.

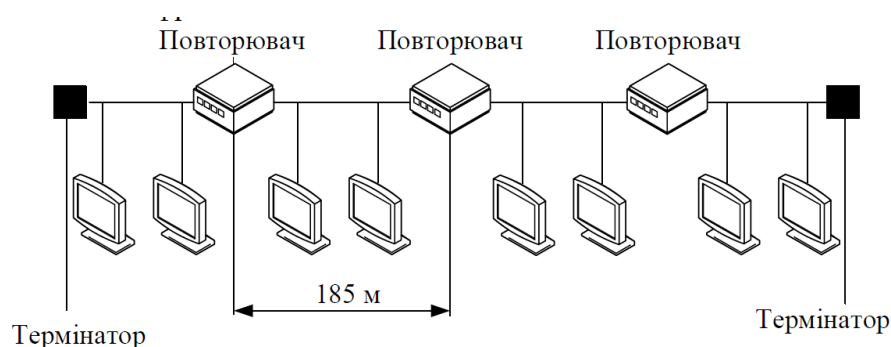


Рис. 2.2. Повторювач для розширення мережі Ethernet

Концентратори характерні для всіх базових технологій локальних мереж.

Концентратор інформаційно-комунікаційної мережі – комунікаційне устаткування, функцією якого є безпосереднє спрямування переданої користувачем інформації одному або решті комп'ютерів мережі.

Зауважимо, що в роботі концентраторів будь-яких технологій багато спільного – вони повторюють сигнали, що прийшли з одного з їхніх портів, на інших своїх портах. Різниця полягає в тому, на яких саме портах повторюються вхідні сигнали. Концентратор завжди змінює фізичну топологію мережі, але при цьому може залишати без зміни її логічну топологію. Фізична структуризація мережі за допомогою концентраторів корисна не тільки для збільшення відстані між вузлами мережі, а й для підвищення її надійності [13, 16]. Фізична структуризація мережі корисна в багатьох розуміннях, проте в ряді випадків, коли йдеться про мережі великого і середнього розміру, неможливо обійтися без логічної структуризації мережі. Найважливішою проблемою, що не вирішується шляхом фізичної структуризації, залишається проблема перерозподілу переданого трафіку між різними фізичними сегментами мережі. Вирішення проблеми полягає у відмові від ідеї єдиного однорідного розподіленого середовища.

Логічна структуризація мережі – це процес поділу мережі на сегменти з локалізованим трафіком. Для логічної структуризації мережі використовуються такі комунікаційні пристрої, як мости, комутатори, маршрутизатори і шлюзи.

Міст поділяє передавальне середовище мережі на частини (логічні сегменти), передаючи інформацію з одного сегмента в інший тільки в тому разі, якщо така передача справді необхідна, тобто якщо адреса комп'ютера призначення належить іншій підмережі.

Тим самим міст ізолює трафік однієї підмережі від трафіку інших, підвищуючи загальну продуктивність передачі даних у мережі.

На рис. 2.3 зображено мережу, яку було сформовано на базі мережі з центральним концентратором його заміною на міст. Мережі робочих груп 1 і 2 складаються з поодиноких логічних сегментів, а мережа групи 3 – із двох логічних сегментів. Кожний логічний сегмент, побудований на базі концентратора, має просту фізичну структуру, утворену відрізками кабелю, які пов'язують комп'ютери з портами концентратора.

Мости використовують для локалізації трафіку та апаратної адресації комп'ютерів. Це ускладнює розпізнавання належності того чи іншого користувача до певного логічного сегмента – сама адреса не містить жодної інформації з цього приводу.

Комутатор (switch, switching hub) за принципом обробки кадрів не відрізняється від моста.

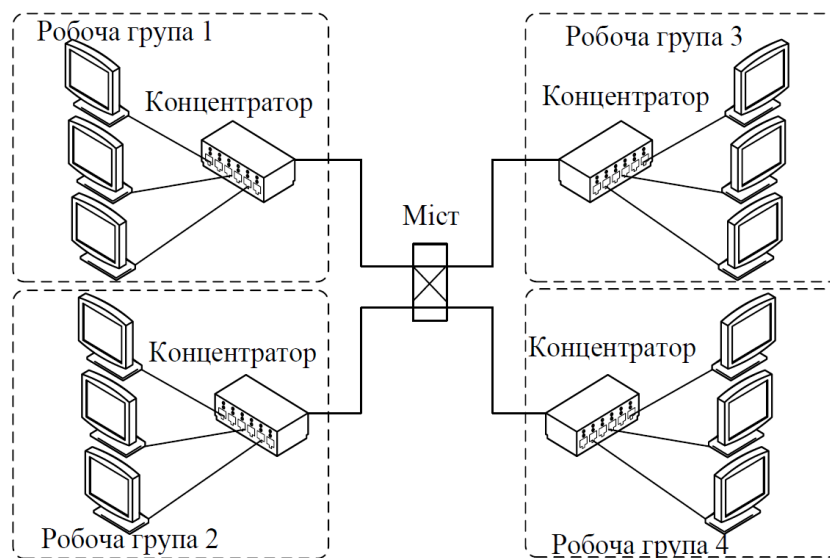


Рис. 2.3. Логічна структуризація мережі з використанням моста

Але він є свого роду комунікаційним мультипроцесором, оскільки кожний його порт обладнано спеціалізованим процесором, який обробляє кадри згідно з алгоритмом моста незалежно від процесорів інших портів.

За рахунок цього загальна продуктивність комутатора вища за продуктивність традиційного моста, що має один процесорний блок. Можна сказати, що комутатори – це мости нового покоління, які

обробляють кадри в паралельному режимі. Обмеження, пов'язані із застосуванням мостів і комутаторів за топологією зв'язків, а також низкою інших параметрів, привели до того, що в ряді комунікаційних пристроїв з'явився ще один тип устаткування – маршрутизатор (router). Маршрутизатори надійніше й ефективніше, ніж мости, ізолюють трафік окремих частин мережі один від одного.

Маршрутизатор – це комунікаційне устаткування, яке збирає інформацію про топологію міжмережевих з'єднань і на її підставі пересилає пакети мережного рівня в мережу призначення.

Маршрутизатори утворюють логічні сегменти за допомогою явної адресації, оскільки використовують не прості апаратні, а складні числові адреси. У цих адресах є поле номера мережі, так що всі комп'ютери, в яких значення цього поля однакове, належать до одного сегмента, який у цьому разі називають підмережею (subnet). Іншою дуже важливою характеристикою маршрутизаторів є їхня здатність зв'язувати в єдину мережу підмережі, побудовані з використанням різних мережних технологій.

Поряд із переліченими пристроями окремі частини мережі може сполучати шлюз (gateway). Зазвичай основною причиною, з якої в мережі використовують шлюз, є необхідність об'єднати мережі з різними типами системного і прикладного програмного забезпечення, а не потреба локалізувати трафік. Проте забезпечення шлюзом локалізації трафіку є, по суті, деяким побічним ефектом. Великі мережі практично ніколи не будуються без логічної структуризації. Для окремих сегментів і підмереж характерні типові однорідні топології базових технологій, і для їх об'єднання завжди використовується устаткування, що забезпечує локалізацію трафіку: мости, комутатори, маршрутизатори та шлюзи.

Для спрощення структури більшість мереж організовуються в набори рівнів, кожний наступний з яких зводиться над попереднім. Кількість рівнів, їх назви, зміст і призначення різняться від мережі до мережі. Проте в усіх мережах метою кожного рівня є надання деякого сервісу для рівнів, розташованих вище.

2.2. Модель взаємодії відкритих системи OSI

На початку 1980-х років такі міжнародні організації зі стандартизації, як ISO, ITU-T та деякі інші, розробили модель, що відіграла значну роль у розвитку інформаційних мереж. Ця модель називається моделлю взаємодії відкритих систем (Open System Interconnection – OSI), або моделлю OSI. Модель OSI визначає різні рівні взаємодії систем, дає їм стандартні імена і вказує, які функції має виконувати кожний рівень [82-91].

У моделі ISO/OSI (рис. 2.4) засоби взаємодії поділяються на сім рівнів: прикладний, представницький, сеансовий, транспортний, мережний, каналний і фізичний. Кожен рівень має справу з одним визначеним аспектом взаємодії мережних пристроїв.

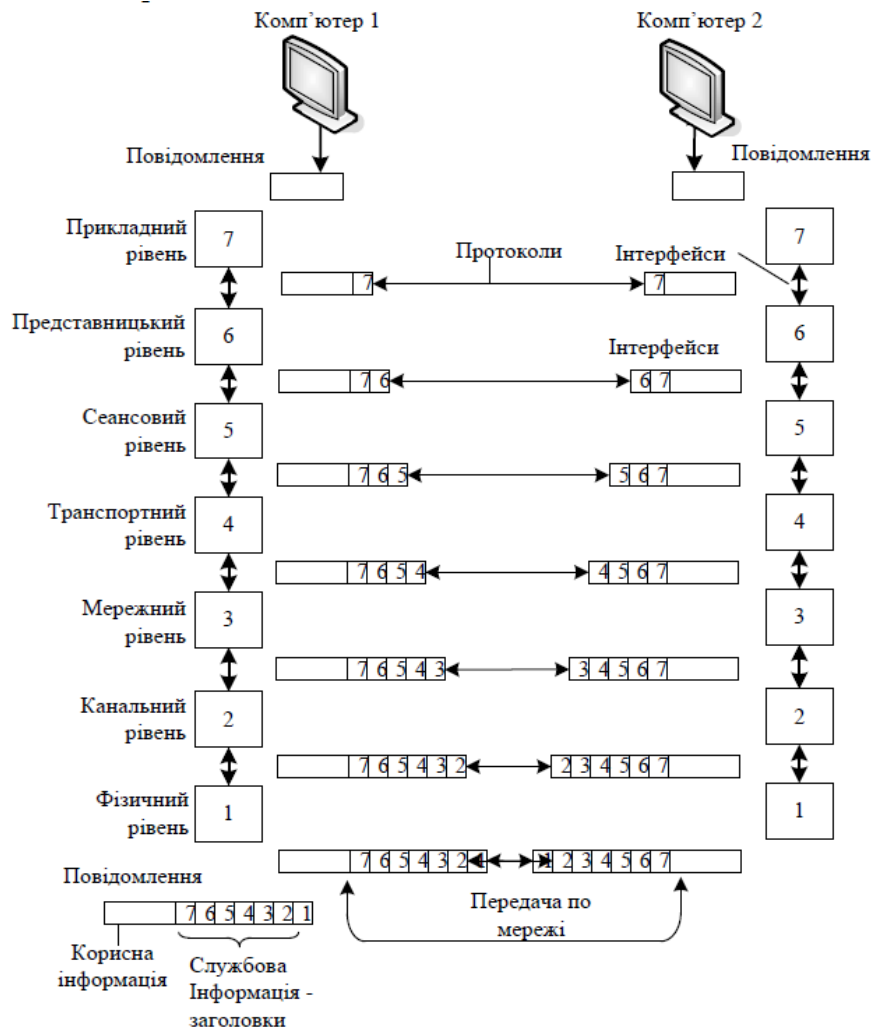


Рис. 2.4. Модель взаємодії відкритих систем ISO/OSI

Модель OSI описує тільки системні засоби взаємодії, що реалізуються операційною системою, системними утилітами, системними апаратними засобами. Модель не містить засобів взаємодії додатків кінцевих користувачів. Отже, нехай додаток звертається із запитом до прикладного рівня, наприклад до файлової служби.

На підставі цього запиту програмне забезпечення прикладного рівня формує повідомлення стандартного формату. Звичайне повідомлення складається із заголовка і поля даних. Заголовок містить службову інформацію, яку необхідно передати через мережу прикладному рівню машини – адресата, щоб повідомити його, яку роботу потрібно виконати. Після формування повідомлення прикладний рівень спрямовує його вниз по стеку представницького рівня. Протокол представницького рівня на підставі інформації, отриманої із заголовка прикладного рівня, виконує необхідні дії і додає до повідомлення власну службову інформацію.

Отримане в результаті повідомлення передається вниз на сеансовий рівень, який, у свою чергу, додає свій заголовок і т.д. (Деякі реалізації протоколів розміщують службову інформацію не тільки на початку повідомлення у вигляді заголовка, а й у кінці у вигляді так званого кінцевика.) Нарешті, повідомлення досягає нижнього, фізичного рівня,

який власне і передає його по лініях зв'язку машині-адресатові. До цього моменту повідомлення «обростає» заголовками всіх рівнів (рис. 2.5).

Коли повідомлення по мережі надходить на машину-адресат, воно приймається її фізичним рівнем і послідовно переміщується вгору з рівня на рівень. Кожний рівень аналізує й обробляє заголовок свого рівня, виконуючи відповідні даному рівню функції, а потім вилучає цей заголовок і передає

У моделі OSI розрізняють два основні типи протоколів. Перша група протоколів – протоколи зі встановленням з'єднання (connection-oriented), в яких перед обміном даними відправник і одержувач мають спочатку встановити з'єднання і, можливо, вибрати деякі параметри протоколу, які вони використовуватимуть при обміні даними. Після завершення діалогу вони мають розірвати це з'єднання. Телефон – це приклад взаємодії, що ґрунтується на встановленні з'єднання.

Друга група протоколів – протоколи без попереднього встановлення з'єднання (connectionless). Такі протоколи називаються також дейтаграмними протоколами. Відправник просто передає повідомлення, коли воно готове. При взаємодії комп'ютерів використовуються протоколи обох типів.

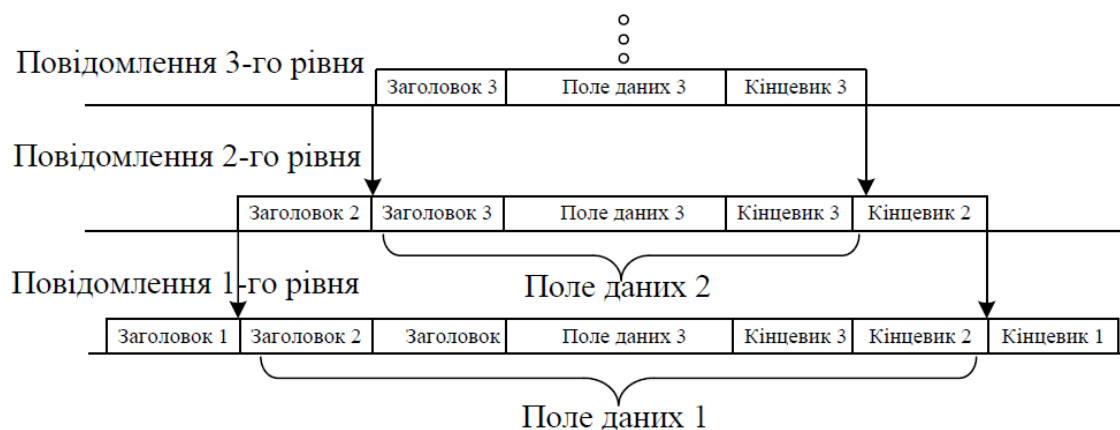


Рис. 2.5. Структура повідомлень різних рівнів моделі ISO/OSI повідомлення вищого рівня.

Функції рівнів моделі OSI. Фізичний рівень (I). Фізичний рівень має справу з передачею бітів по фізичних каналах зв'язку, таких наприклад, як коаксіальний кабель, вита пара, оптоволоконний кабель або цифровий територіальний канал. Цього рівня стосуються характеристики фізичних середовищ передачі даних, такі як смуга пропускання, завадостійкість, хвильовий опір і т. ін. На цьому самому рівні визначаються характеристики електричних сигналів, що передають дискретну інформацію, наприклад, крутизна фронтів імпульсів, рівні напруги або струму переданого сигналу, тип кодування, швидкість передачі сигналів. Окрім цього, тут стандартизуються типи роз'ємів і призначення кожного контакту.

Функції фізичного рівня реалізуються у всіх пристроях, підключених до мережі. З боку комп'ютера функції фізичного рівня виконуються мережним адаптером або послідовним портом.

Канальний рівень (2). На фізичному рівні пересилаються біти інформації. При цьому не враховується, що в деяких мережах, в яких лінії зв'язку використовуються (розділяються) за часом кількома парами комп'ютерів, які взаємодіють, фізичне середовище передачі може бути зайнятим. Тому одним із завдань канального рівня є перевірка доступності середовища передачі. Іншим завданням канального рівня є реалізація механізмів виявлення і корекції помилок. Для цього на канальному рівні біти групуються в набори, які називають кадрами (frames). Канальний рівень забезпечує коректність передачі кожного кадру, розміщуючи спеціальну послідовність бітів на початку і в кінці кожного кадру для його виділення, а також обчислює контрольну суму, обробляючи всі байти кадру певним способом і додаючи контрольну суму до кадру. Коли кадр приходить по мережі, одержувач знову обчислює контрольну суму отриманих даних і порівнює результат з контрольною сумою з кадру. Якщо вони збігаються, кадр вважається за дійсне повідомлення та приймається. Якщо ж контрольні суми не збігаються, то фіксується помилка.

Канальний рівень може не тільки виявляти помилки, а й виправляти їх за рахунок повторної передачі пошкоджених кадрів. Необхідно зазначити, що функція виправлення помилок не є обов'язковою для канального рівня, тому в деяких протоколах цього рівня вона відсутня, наприклад в Ethernet і frame relay.

У локальних мережах протоколи канального рівня використовуються комп'ютерами, мостами, комутаторами і маршрутизаторами. У комп'ютерах функції канального рівня реалізуються спільними зусиллями мережних адаптерів і їхніх драйверів.

У глобальних мережах, які рідко мають регулярну топологію, канальний рівень часто забезпечує обмін повідомленнями тільки між двома сусідніми комп'ютерами, з'єднаними індивідуальною лінією зв'язку. Прикладами протоколів «точка-точка» (як часто називають такі протоколи) можуть служити широко розповсюджені протоколи PPP і LAR-V. У таких випадках для доставляння повідомлень між кінцевими вузлами через усю мережу використовуються засоби мережного рівня.

Мережний рівень (3). Мережевий рівень слугує для утворення єдиної транспортної системи, об'єднуючи кілька мереж, причому ці мережі можуть використовувати абсолютно різні принципи передачі повідомлень між кінцевими вузлами і мати довільну структуру зв'язків. Функції мережевого рівня доволі різноманітні. Почнемо їх розгляд на прикладі об'єднання локальних мереж.

Протоколи канального рівня локальних мереж забезпечують доставляння даних між будь-якими вузлами тільки в мережі з відповідною типовою топологією, наприклад топологією ієрархічної зірки. Це дуже

жорстке обмеження, яке не дає змоги будувати мережі з розвиненою структурою, наприклад мережі, які об'єднують кілька мереж підприємства в єдину мережу, або високонадійні мережі, в яких існують надлишкові зв'язки між вузлами. Можна було б ускладнювати протоколи канального рівня для підтримки петлеподібних надлишкових зв'язків, але принцип розподілу обов'язків між рівнями приводить до іншого рішення. Щоб, з одного боку, зберегти простоту процедур передачі даних для типових топологій, а з другого – припустити використання довільних топологій, вводиться додатковий мережний рівень.

На мережевому рівні сам термін «мережа» наділяють специфічним значенням. У цьому разі під мережею розуміється сукупність комп'ютерів, з'єднаних між собою відповідно до однієї зі стандартних типових топологій, які використовують для передачі даних один із протоколів канального рівня, визначений для цієї топології.

У середині мережі доставляння даних забезпечується відповідним канальним рівнем, а ось доставлянням даних між мережами опікується мережевий рівень, який і підтримує можливість правильного вибору маршруту передачі повідомлення навіть у тому разі, коли структура зв'язків між складовими мережами має характер, відмінний від прийнятого в протоколах канального рівня.

Мережі з'єднуються між собою спеціальними пристроями, які називають маршрутизаторами.

Щоб передати повідомлення від відправника, що перебуває в одній мережі, одержувачеві, що перебуває в іншій мережі, потрібно зробити деяку кількість транзитних передач між мережами, або хопів (від *hop* – стрибок), щоразу вибираючи відповідний маршрут. Таким чином, маршрут є послідовністю маршрутизаторів, через які проходить пакет.

Повідомлення мережного рівня називають пакетами (packets). При організації доставляння пакетів на мережному рівні використовується поняття «номер мережі». У цьому разі адреса одержувача складається зі старшої частини – номера мережі і молодшої – номера вузла в цій мережі. Усі вузли однієї мережі мають мати одну і ту саму старшу частину адреси, тому терміну «мережа» на мережному рівні можна дати й інше, формальніше визначення: мережа – це сукупність вузлів, мережні адреси яких містять один і той самий номер мережі [15].

Мережні протоколи (routed protocols) – реалізують просування пакетів через мережу. Саме ці протоколи зазвичай мають на увазі, коли говорять про протоколи мережного рівня;

На мережному рівні визначаються два види протоколів:

- **протоколи маршрутизації** (routing protocols) – протоколи обміну маршрутною інформацією. За допомогою цих протоколів маршрутизатори збирають інформацію про топологію міжмережєвих з'єднань;

- **протоколи дозволу адрес** (Address Resolution Protocol, ARP), які відповідають за відображення адреси вузла локальної мережі. Іноді їх

відносять не до мережного, а до каналного рівня, хоча тонкощі класифікації не змінюють їхнього призначення.

Протоколи мережного рівня реалізуються програмними модулями операційної системи, а також програмними й апаратними засобами маршрутизаторів. Прикладами протоколів мережного рівня є протокол міжмережевої взаємодії IP стека TCP/IP і протокол міжмережевого обміну пакетами IPX стека Novell.

Транспортний рівень (4). На шляху від відправника до одержувача пакети можуть бути спотворені або загублені. Хоча деякі додатки мають власні засоби обробки помилок, існують і такі, які вважають за краще відразу мати справу з надійним з'єднанням. Транспортний рівень забезпечує додаткам або верхнім рівням стека (прикладному і сеансовому) передачу даних із тим ступенем надійності, який їм потрібний. Модель OSI визначає п'ять класів сервісу, що надаються транспортним рівнем.

Ці види сервісу різняться якістю послуг, що надаються: терміновістю, можливістю відновлення перерваного зв'язку, наявністю засобів мультиплексування кількох з'єднань між різними прикладними протоколами через загальний транспортний протокол, а головне – здатністю до виявлення і виправлення помилок передачі, таких як спотворення, втрата і дублювання пакетів.

Сеансовий рівень (5). Сеансовий рівень забезпечує управління діалогом: фіксує, яка зі сторін є активною зараз, надає засоби синхронізації. Останні дають змогу вставляти контрольні точки в довгі передачі, щоб у разі відмови можна було повернутися назад до останньої контрольної точки, а не починати все спочатку. На практиці небагато додатків використовують сеансовий рівень, і він рідко реалізується у вигляді окремих протоколів, хоча функції цього рівня часто об'єднують із функціями прикладного рівня і реалізують в одному протоколі.

Представницький рівень (6). Представницький рівень має справу з формою подання інформації, що передається по мережі, не змінюючи при цьому її змісту. За рахунок рівня подання інформація, що передається прикладним рівнем однієї системи, завжди зрозуміла прикладному рівню іншої системи. За допомогою засобів даного рівня протоколи прикладних рівнів можуть подолати синтаксичні відмінності в поданні даних або ж відмінності в кодах символів, наприклад кодів ASCII і EBCDIC. На цьому рівні може виконуватися шифрування і дешифрування даних, завдяки чому секретність обміну даними забезпечується відразу для всіх прикладних служб. Прикладом такого протоколу є протокол Secure Socket Layer (SSL), який забезпечує секретний обмін повідомленнями для протоколів прикладного рівня стека TCP/IP.

Прикладний рівень (7). Прикладний рівень – це насправді просто набір різноманітних протоколів, за допомогою яких користувачі мережі дістають доступ до ресурсів, що розподіляються, таких як файли, принтери або гіпертекстові Web-сторінки, а також організовують свою спільну роботу, наприклад за допомогою протоколу електронної пошти. Одиниця

даних, якою оперує прикладний рівень, зазвичай називається **повідомленням (message)**.

Організація обміну даними в інформаційних мережах може здійснюватися двома різними способами: без встановлення логічного з'єднання між передаючим і приймаючим вузлами мережі і зі встановленням логічного з'єднання (зі встановленням сеансу зв'язку).

Спосіб зв'язку без встановлення логічного з'єднання характеризується наступним:

- він використовується в мережах з комутацією пакетів, причому кожен пакет розглядається як індивідуальний об'єкт, незалежна одиниця передачі інформації;
- пакети від відправника можна передавати в довільні моменти, одночасно множині адресатів по різних маршрутах;
- перед передачею даних крізь зв'язок між відправником і одержувачем наперед не встановлюється, не вимагається також синхронізації апаратури зв'язку на передаючому і приймальному пунктах;
- через зайнятість окремих ділянок маршруту може здійснюватися буферизація пакетів в проміжних вузлах зв'язку;
- передача сигналу від адресата до відправника, підтверджуючого отримання інформації, не здійснюється.

Це один з перших і простих способів обміну даними в комунікаційній технології. Він широко використовується в дейтаграмних мережах, в яких реалізуються дейтаграмні протоколи інформаційного обміну. Спосіб зв'язку (або режим зв'язку), орієнтований на логічне з'єднання, відноситься до пізнішої технології. Він забезпечує вищий рівень сервісу порівняно з дейтаграмним зв'язком.

Особливості організації обміну даними зі встановленням логічного з'єднання:

1. Перед передачею інформації між взаємодіючими абонентами (відправником і одержувачем) встановлюється логічний (віртуальний) канал, причому технологія створення (встановлення) каналу така: відправник посилає запит на з'єднання видаленому адресату через ряд проміжних вузлів зв'язку; адресат, одержавши цей запит, у разі «згоди» на встановлення логічного каналу посилає відправнику сигнал підтвердження; після отримання сигналу підтвердження відправником починається обмін даними з управлінням потоком, сегментацією і виправленням помилок.

2. Після завершення обміну даними адресат посилає пакет підтвердження цієї події відправнику (клієнту – ініціатору встановлення логічного каналу), який сприймається як сигнал для роз'єднання каналу. Отже, при використуванні цього способу зв'язку виділяються три етапи: встановлення каналу, обмін даними, роз'єднання каналу.

Зв'язок зі встановленням логічного каналу застосовується у віртуальних мережах, де використовуються протоколи інформаційного обміну типу віртуального з'єднання. До них відносяться протоколи:

управління передачею TCP, послідовних пакетів SPP, транзакції ATP і т. ін. Віртуальний зв'язок часто використовується в глобальних мережах [20].

При передачі по віртуальному каналу довгих повідомлень вони розбиваються на однакові частини (пакети), які відправляються в канал у порядку їх розміщення в повідомленні. Це позбавляє від необхідності забезпечувати кожен пакет службовою інформацією в повному обсязі, з тим щоб перетворити його на незалежну одиницю передачі інформації, як це має місце в дейтаграмних мережах. Крім того, передача пакетів в їх природній послідовності, визначеній порядком розміщення в повідомленні, істотно полегшує задачу формування первинного повідомлення з пакетів, що приймаються, на приймальному пункті.

Перший з розглянутих способів організації обміну даними в мережах відрізняється простотою в реалізації і порівняно невеликими накладними витратами. При малій завантаженості ліній зв'язку мережі він дозволяє істотно скоротити час на передачу довгого повідомлення. Крім того, він зручний при розсилці інформації за багатьма адресами.

У завантажених мережах реалізація такого способу може привести до значних затримок пакетів в проміжних вузлах зв'язку і навіть до втрати окремих пакетів, що негативно відображається на надійності доставки інформації адресатам.

Другий спосіб, навпаки, характеризується високими накладними витратами, проте він надає абонентам істотно великі зручності, забезпечує необхідну оперативність в обміні даними (в ідеальному випадку переповнювання з'єднань в проміжних вузлах зв'язку повністю виключається) і гарантовану надійність доставки інформації абонентам.

Таким чином, кожний з режимів зв'язку має свої особливості, а значить, і області застосування.

Режим «із з'єднанням» доцільно використовувати для тих застосувань, де взаємодія має довготривалий характер, конфігурація взаємодіючих об'єктів постійна, а потік даних не має великих пауз.

Режим «без з'єднання» більше підходить там, де взаємодія має короткочасний характер, при якому обсяг переданих даних невеликий, а інтервали між передачами значні (щодо швидкості передачі). Крім того, його доцільно використовувати в системах з підвищеними вимогами до надійності доставки даних адресату, оскільки ці вимоги можна задовольнити шляхом тиражування даних і передачі адресату по різних маршрутах.



Рис. 2.6. Структура системи управління процесами моделі ISO/OSI

Протоколи обміну даними, або протоколи верхнього рівня (вірніше, середнього, оскільки вони виконуються на 4-5 у рівнях моделі), служать, як говорить сама назва, для управління обміном даних. Незалежно від внутрішньої конструкції кожного конкретного протоколу верхнього рівня для них характерна наявність загальних функцій: ініціалізація зв'язку, передача і прийом даних, завершення обміну. Кожен протокол має засоби для ідентифікації будь-якої робочої станції мережі по імені, мережній адресі або по обох цих атрибутах. Активізація обміну інформацією між взаємодіючими вузлами починається після ідентифікації вузла адресата вузлом, що ініціює обмін даними.

Ініціююча станція встановлює один з методів організації обміну даними: метод дейтаграм або метод сеансів зв'язку. Протокол надає засоби для прийому/передачі повідомлень адресатом і джерелом. При цьому звичайно накладаються обмеження на довжину повідомлень.

Останніми роками все виразніше реалізується тенденція переходу на цифрові канали зв'язку. Обсяги і масштаби робіт в цьому напрямі безперервно збільшуються. Цифрові мережі інтегрального обслуговування (ISDN – Integrated Services Digital Network) розглядаються, як найближче майбутнє мереж загального користування.

Принципи адресації в інформаційних мережах. IP адреси. Ще одним завданням, яке потрібно враховувати при використанні інформаційно-комунікаційних мереж, є завдання адресації. На практиці зазвичай використовується відразу кілька схем адресації.

Найбільшого поширення набули три схеми адресації вузлів інформаційних мереж:

– **Апаратні адреси.** Ці адреси призначено для мережі невеликого або середнього розміру, тому вони не мають ієрархічної структури. Типовим представником адреси такого типу є адреса мережного адаптера локальної мережі. Така адреса зазвичай використовується тільки апаратурою, тому її намагаються зробити по змозі компактною і записують у вигляді двійкового або шістнадцяткового значення. У літературі такі адреси називають MAC-адресами.

– **Символьні адреси, або імена.** Ці адреси призначено для запам'ятовування користувачем і тому зазвичай мають смислове значення. Символьні адреси легко використовувати як у невеликих, так і у глобальних мережах. Для роботи у великих мережах символьне ім'я може мати складну ієрархічну структуру, наприклад `cisco.netacad.net`.

– **Числові складені адреси.** Символьні імена зручні для користувача, але через змінний формат і потенційно велику довжину їх передача по мережі не дуже економічно. Тому часто для роботи у великих мережах як адреси вузлів використовують числові складені адреси фіксованого і компактного форматів. Типовими представниками адрес цього типу є IP адреси. У них підтримується дворівнева ієрархія; адреса поділяється на старшу частину – номер мережі і молодшу – номер вузла.

Для того, щоб мережний рівень міг виконати своє завдання, йому необхідна власна система адресації, що не залежить від способів адресації вузлів в окремих підмережах. Така система адресації, що дала б змогу на мережному рівні в універсальний і однозначний спосіб ідентифікувати будь-який вузол складеної мережі. Природним способом формування мережної адреси є унікальна нумерація всіх підмереж основної мережі та нумерація всіх вузлів у межах кожної підмережі [19].

Таким чином, мережна адреса являє собою пару: номер мережі (підмережі) і номер вузла.

Номером вузла може бути або локальна адреса цього вузла, або деяке число, не пов'язане з локальною технологією, що однозначно ідентифікує вузол у межах даної підмережі.

У першому випадку мережна адреса стає залежною від локальних технологій і це обмежує її застосування.

Другий підхід більш універсальний. Але в обох випадках кожний вузол складеної мережі має, поряд зі своєю локальною адресою, ще одну універсальну мережну адресу.

Дані, які надходять на мережний рівень і які необхідно передати через основну мережу, забезпечуються заголовком мережного рівня. Дані разом із заголовком утворюють пакет. Заголовок пакета мережного рівня має уніфікований формат, що не залежить від форматів кадрів канального рівня тих мереж, які можуть входити в об'єднану мережу, і несе, поряд з іншою службовою інформацією, дані про номер тієї мережі, якій призначається цей пакет.

При передачі пакета з однієї підмережі в іншу пакет мережного рівня, інкапсульований у отриманий канальний кадр першої підмережі,

звільняється від заголовків цього кадру й оточується заголовками кадру каналного рівня наступної підмережі. Інформацією, на основі якої виконується ця заміна, є службові поля пакета мережного рівня.

Отже, мережний рівень використовує власну адресацію, що забезпечує кожному вузлу підмережі основної мережі свою універсальну мережну адресу, що складається з номера мережі й номера вузла. Завдяки такій системі адресації мережний рівень може пересилати інформацію до вузла одержувачеві, «не звертаючи уваги» на внутрішню структуру підмереж, а водночас для безпосереднього проходження пакетів до адресата цей рівень використовує технологію передачі даних конкретної підмережі, через яку йдуть ці пакети.

Основний тип адрес мережного рівня – IP адреса. IP адреса поділяється на дві частини: номер мережі та номер вузла.

IP адреса має довжину 4 байти, це дає в сукупності 32 біти доступної інформації. 32-бітова розрядність IP адреси приводить до того, що числа виходять більшими, навіть якщо їх подано в десятковій формі числення. IP адреса записується у вигляді чотирьох чисел, розділених крапками.

Для того щоб більш раціонально визначитися з розміром мережі й при цьому розмежувати частини IP адреси, що стосуються номера мережі та номера вузла, використовується система класів. Система класів використовує значення перших бітів адреси.

Значення перших бітів адреси є ознакою того, до якого класу належить та чи інша IP адреса (рис. 2.7). Якщо адреса починається з 0, то мережу відносять до *класу А*. Номер мережі класу А займає один байт, решта 3 байти виділяються для номерів вузла в цій мережі. Таким чином, мережі класу А мають номери в діапазоні від 1 до 122. (Номер 0 не використовується, а номер 127 зарезервовано для спеціальних цілей.). Якщо перші два біти адреси дорівнюють 10, то мережа належить *класу В* (тобто якщо перший октет IP адреси перебуває в діапазоні від 128 до 191).

Якщо адреса починається з послідовності 110, то це мережа *класу С* (тобто якщо значення першого октету в IP адресі перебуває в діапазоні від 192 до 223). У цьому разі під номер мережі виділяється 24 біти, а під номер вузла – 8 біт. Мережі класу С мають невелику (2^8 , тобто 256) кількість вузлів. Слід зазначити, що саме мережі класу С найпоширеніші.



Рис. 2.7. Класи IP адрес

Якщо адреса починається з послідовності 1110, то вона є адресою класу *D* і позначає особливу, групову адресу – multicast. Якщо в пакеті як адресу призначення зазначено адресу класу *D*, то такий пакет мають отримати всі вузли, яким присвоєно цю адресу.

Якщо адреса починається з послідовності 11110, то це означає, що ця адреса належить до класу *E*. Адреси цього класу зарезервовано для майбутніх застосувань.

Діапазони номерів мереж і максимальна кількість вузлів відповідають кожному класу мереж (табл. 2.1).

Таким чином, можна однозначно визначити, що більші мережі одержують адреси класу *A*, середні – класу *B*, а малі – класу *C*.

Таблиця 2.1

Клас мережі	Перші біти	Найменша адреса мережі	Найбільша адреса мережі	Максимальна кількість вузлів
A	0	1.0.0.0	126.0.0.0	2^{24}
B	10	128.0.0.0	191.255.0.0	2^{16}
C	110	192.0.1.0	223.255.255.0	2^8
D	1110	224.0.0.0	239.255.255.255	Multicast
E	11110	240.0.0.0	247.255.255.255	зарезервований

того, до якого класу (*A*, *B*, *C*) належить адреса мережі може бути подано першими 8,16 або 24, а номер хоста – останніми 24, 16 або 8 розрядами.

Діапазон значень першого байта для перших трьох класів мереж (табл. 2.2).

Таблиця 2.2

Клас мережі	Діапазон (десятковий) значень першого байта
A	1 до 126
B	128 до 191
C	192 до 254

2.3. Організація інформаційних систем передачі даних

Першими кроками проектування мережі мають бути мета й завдання, які залежно від конкретної організації або ситуації, що склалася, передбачено покласти на інформаційну мережу [26].

Основні вимоги для більшості мережних проектів:

- **Функціональність** – мережа має задовольняти робочі вимоги користувачів і забезпечувати зв'язок: користувач – користувач і користувач – прикладна програма з необхідною швидкістю і надійністю.

- **Масштабованість** – мережа має бути здатною до зростання. Початковий проект має розширюватися без будь-яких серйозних змін загального проекту.

- **Адаптованість** – мережа має розроблятися з урахуванням упровадження перспективних технологій. Мережа не повинна містити елементів, які можуть обмежувати реалізацію нових технологій.

- **Керованість** – проектована мережа не повинна ускладнювати розв'язання питань мережного моніторингу та управління.

При проектуванні високотехнологічних інформаційно-комунікаційних мереж доводиться розв'язувати такі базові питання:

- формування та розподіл інформаційних ресурсів мережі;
- топологія мережі;
- комунікаційне устаткування;
- функції та розміщення серверів;
- домени колізій;
- сегментація мережі;
- широкомовні домени тощо.

Сервери дозволяють мережним користувачам взаємодіяти і спільно використовувати файли, принтери та сервіси прикладних програм. Сервери зазвичай не використовують як робочі станції. На них запущено спеціалізовані операційні системи, наприклад NetWare, Windows NT, UNIX і Linux. Кожний сервер, як правило, реалізує одну функцію, наприклад електронну пошту або доступ до файлів.

Файл-сервер інформаційно-комунікаційної мережі – вузол мережі, що обслуговує та надає сервіс іншим вузлам (користувачам) за допомогою програмного забезпечення та комунікаційного устаткування на фоні розподілу спільно використовуваного інформаційного ресурсу.

Програмне забезпечення, яке дає змогу серверу надавати послуги іншим комп'ютерам, часто також називають сервером, з яким контактують програми-клієнти, установлені на цих комп'ютерах [19, 20, 104].

Програмне забезпечення, орієнтоване на роботу в мережі, перебуваючи на мережному файл-сервері, водночас доступне групі користувачів.

Клієнт-серверною інформаційною мережею називається мережа, що використовує один чи кілька центральних виділених серверів.

Серверне устаткування може виконувати свої функції в інтересах всієї інформаційно-комунікаційної мережі або окремих її сегментів чи робочих груп.

Сервер інформаційно-комунікаційної мережі підтримує всіх користувачів у межах цієї мережі, пропонуючи загальні сервіси, наприклад електронну пошту або розподіл адресації та контроль трафіку. Сервер робочої групи підтримує специфічний склад користувачів і реалізує, наприклад, текстову обробку та файлове розділення.

Якщо це можливо, трафік до серверів інформаційно-комунікаційної мережі має передаватися безпосередньо в MDF і не зачіпати інших мереж. Проте деякі мережі використовують маршрутизовану базову магістраль для серверів. У цих випадках руху трафіку через інші мережі зазвичай не можна запобігти.

В ідеалі сервери робочих груп мають установлюватися в додаткових серверних зонах (intermediate distribution facilities – IDF) ближче до користувачів, що мають доступ до прикладних програм на цих серверах.

Таке розміщення дає змогу трафіку рухатися тільки через мережну інфраструктуру додаткових серверних зон і не впливати на інших користувачів у цьому мережному сегменті. Мережні комутатори *рівня 2* моделі OSI інформаційно-комунікаційної мережі розміщено в центральній серверній зоні, при цьому сервери додаткових серверних зон мають працювати зі швидкостями 100 Мбіт/с або вищими.

Оскільки вузли Ethernet використовують протокол CSMA/CD, то кожний вузол мережі має «змагатися» з усіма іншими вузлами щодо отримання доступу до середовища передачі (домену колізій).

Якщо два вузли мережі починають одночасну передачу, відбувається колізія. При зіткненні кадрів переданий фрейм знищується, а в усі вузли сегмента посиляється відповідний сигнал. Вузли чекають довільний період часу, потім передають дані повторно.

Надмірна кількість зіткнень може знизити доступну ширину смуги частот мережного сегмента і відповідно зменшити продуктивність мережі до 35 або 40 %. Розв'язання цієї проблеми – сегментація.

Сегментація – поділ єдиного домену колізій на кілька дрібніших областей. У доменах меншого розміру кількість колізій менша, що дає змогу ефективніше використовувати ширину смуги частот.

Для сегментації домену колізій на *рівні 2* моделі OSI можуть використовуватися мости та комутатори. Сегментація на *рівні 3* досягається застосуванням маршрутизаторів.

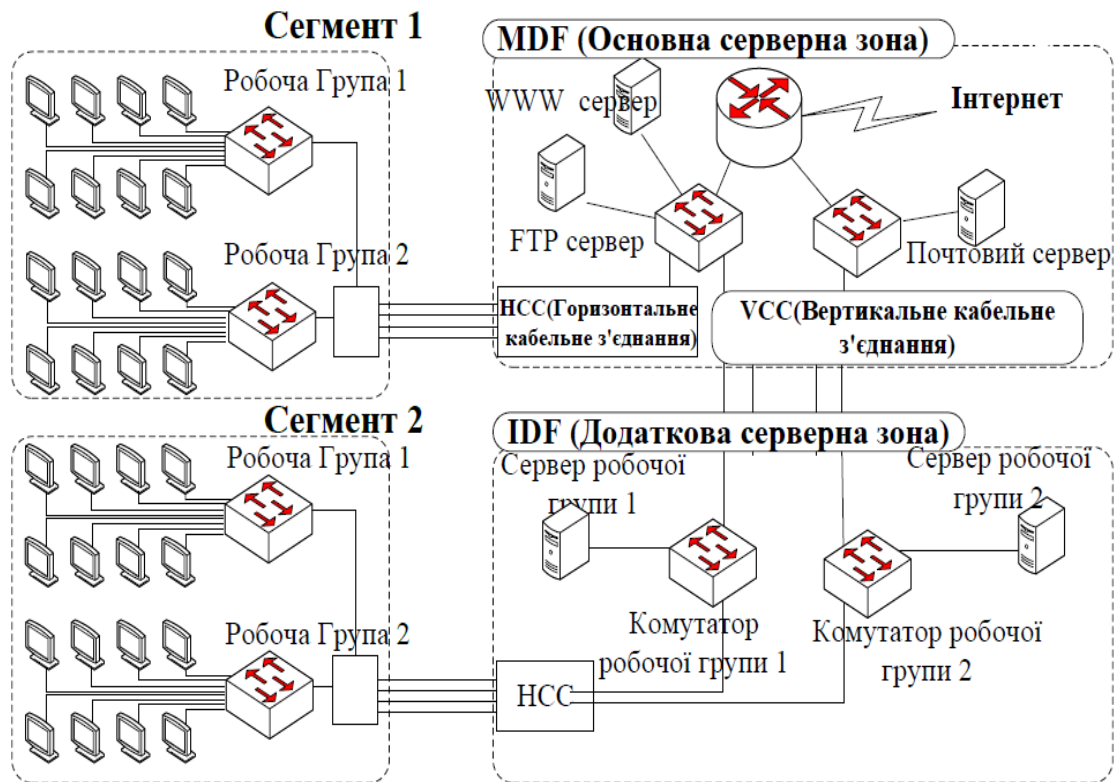


Рис. 2.8. Розміщення серверів і робочих груп інформаційно-комунікаційної мережі

Важливим при проектуванні є оцінювання доступності мережі. Через доступність оцінюється корисність мережі. На доступність впливають продуктивність, час відгуку та доступ до ресурсів. Фізична топологія мережі визначає, в який спосіб пов'язані між собою різні компоненти інформаційної мережі (рис. 2.9). Логічне проектування мережі стосується інформаційних потоків даних, а також імен і схем адресації, використаних у реалізації проектного рішення зазначеної мережі.

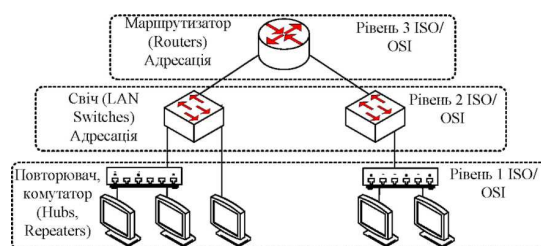


Рис. 2.9. Організація топології мережі по рівнях моделі OSI

Топологія мережі згідно з рівнями моделі OSI.

Топологія мережі рівня 1. Одним із найважливіших компонентів мережі є кабельне устаткування. Сьогодні з'єднання інформаційно-комунікаційної мережі найчастіше базується на технології Fast Ethernet. Fast Ethernet – це 10 Мбіт/с Ethernet, модернізований для швидкості 100 Мбіт/с і такий, що характеризується повнодуплексною функціональністю.

Він використовує стандартну Ethernet-орієнтовану логічну топологію шини для адреси канального рівня (MAC-адреса) (рис. 2.10).

Проектні питання для топології рівня 1 містять тип використаного для прокладання кабелю (зазвичай мідь або волоконно-оптичний) і загальну структуру кабельного устаткування.

Сильні і слабкі сторони топології мають бути ретельно проаналізовані, оскільки ефективність мережі повністю залежить від використовуваних кабелів.

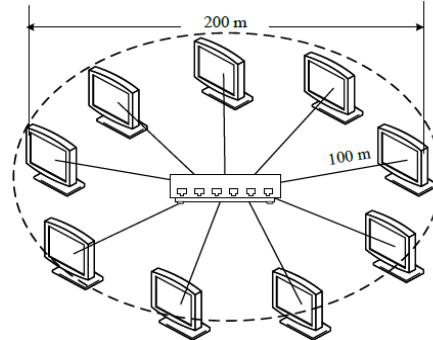


Рис. 2.10. Організація мережі за технологією Fast Ethernet

Для магістральних ліній (вертикального з'єднання) необхідно використовувати волоконно-оптичний кабель (рис. 2.11).

У великих мережах, де неможливо виконати обмеження на 100-метрову довжину кабелю для окремого сегмента (особливо для кількох додаткових серверних зон), може використовуватися кілька комутаційних панелей.

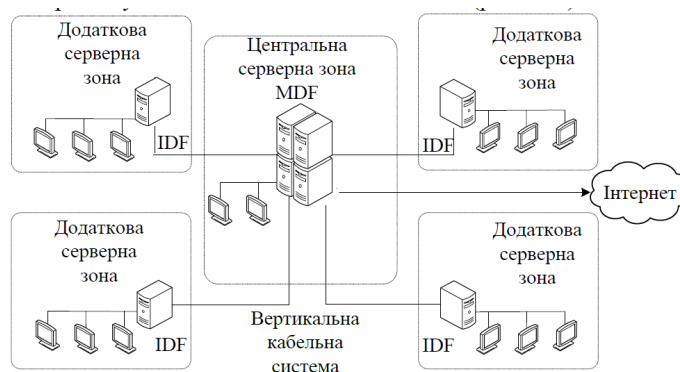


Рис. 2.11. Вертикальне з'єднання мережі

Схему з'єднання для такої топології наведено на рис. 2.12.

Сполучні кабелі (патч-кабелі) слугують для підключення горизонтальних мережних кабелів рівня 1 до портів мережного комутатора рівня 2. Вихідний порт комутатора рівня 2 з'єднується патч-кабелем з Ethernet-портом маршрутизатора рівня 3, чим забезпечується фізичне з'єднання окремої кінцевої хост-машини з маршрутизатором.

Для зв'язку різних додаткових серверних зон із центральним MDF використовуються крос-панелі для вертикальних кабелів (VCC). Тут необхідне застосування волоконно-оптичного кабелю, оскільки

вертикальні кабельні довжини перевищують стандартну 100-метрову межу.

Топологія мережі рівня 2. Призначення пристроїв **рівня 2** моделі OSI в мережі – переспрямування фреймів на основі інформації з MAC-адреси вузла-одержувача, виявлення помилок і зниження перевантажень у мережі. Найбільш поширені мережні пристрої **рівня 2** – це мости (bridges) і мережеві комутатори (switches). Пристрої рівня 2 обмежують розмір домену колізій.

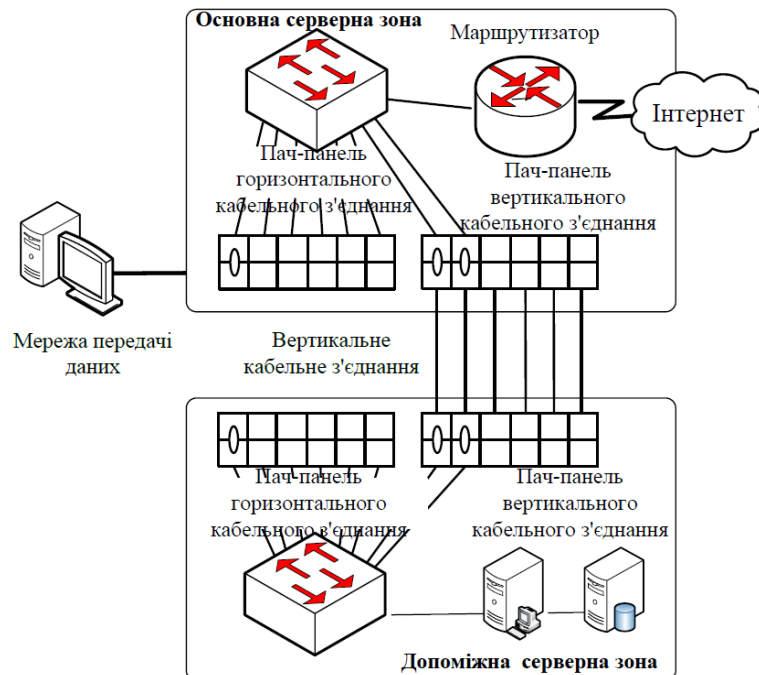


Рис. 2.12. Комутування основної та додаткової серверної зони на базі вертикальної та горизонтальної крос-панелі

Колізії та розмір домену колізій – два показники, які негативно впливають на продуктивність мережі. Розміри домену колізій і, відповідно, кількість колізій зменшуються шляхом мікросегментації мережі. Принцип мікросегментації ілюструє рис. 2.13.

Крім мікросегментації мережний комутатор підтримує так звану асиметричну комутацію, іншими словами, пересилання фреймів між каналами з різними швидкостями передачі.

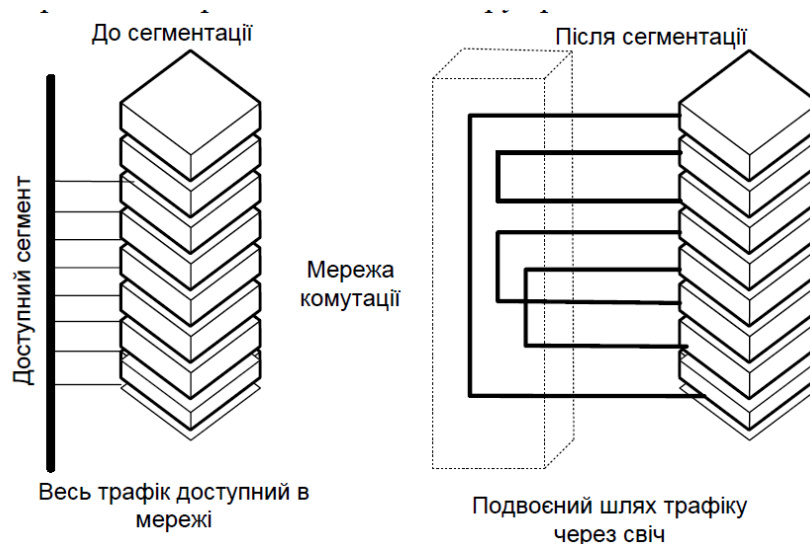


Рис. 2.13. Мікросегментація

Ця характеристика мережного комутатора важлива для узгодження трафіку між спільною для всієї компанії частиною мережі та елементами мережі в підрозділах компанії (рис. 2.14).

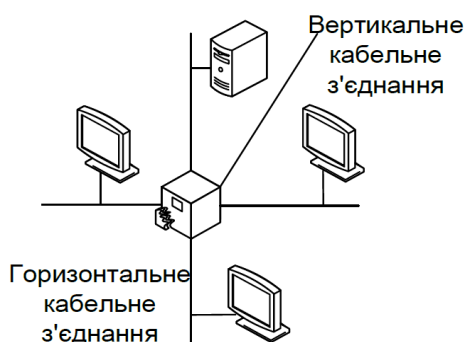


Рис. 2.14. Асиметрична комутація

Одне із завдань проектування мережі – визначення кількості 10-і 100-мегабітних портів для центральної та додаткової серверної зон. Це завдання виконується шляхом аналізу вимог користувачів щодо кількості горизонтальних кабельних з'єднань для кожної кімнати та сумарної кількості портів на всі кімнати компанії. Крім того, підраховується кількість вертикальних кабельних прогонів.

Розмір домену колізій визначається кількістю хостів, які фізично підключаються до окремого порту мережного комутатора. Цей розмір фактично визначає доступну для окремого користувача частину смуги пропускання кабелю.

В ідеальному випадку до окремого порту мережного комутатора має підключатися один користувач. Проте насправді до окремого порту комутатора через багатопортові повторювачі (Hubs) підключено кілька користувачів, що збільшує розміри домену колізій та кількість колізій, а отже, знижує ефективну продуктивність відповідного сегмента мережі та мережну продуктивність окремої хост-машини (рис. 2.15).

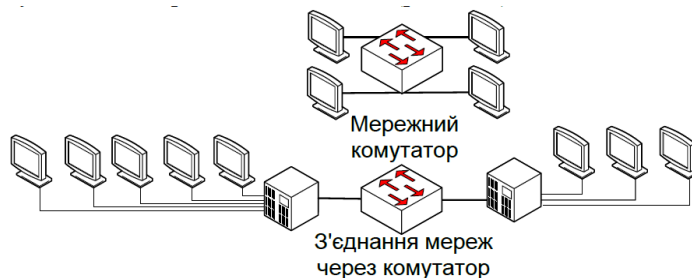


Рис. 2.15. Способи підключення до мережних комутаторів

У результаті проектування топології мережі рівня 2 визначають необхідну кількість мережних комутаторів, їхній тип, кількість портів з урахуванням резерву й можливого зростання мережі, а також типи й необхідну кількість багатопортівих повторювачів (Hubs).

Топології мережі рівня 3. Пристрої рівня 3 використовуються для створення унікальних сегментів. До таких пристроїв насамперед належить маршрутизатор. Пристрої забезпечують взаємодію між сегментами на основі адрес *рівня 3* моделі OSI, таких як IP-адреси. Використання пристроїв *рівня 3* реалізує поділ мереж на унікальні фізичні і логічні мережі. Маршрутизатори обслуговують вихід у глобальні мережі, наприклад, Інтернет.

Маршрутизація *рівня 3* визначає рух трафіку між унікальними фізичними мережними сегментами на основі спеціальної системи адресації. При цьому пересилаються пакети даних на основі адреси одержувача і не пересилається службова інформація мережі, наприклад запити ARP. Отже, інтерфейс маршрутизатора вважається входом і вихідною точкою домену ширококомовлення, що зупиняє ширококомовлення в інші сегменти інформаційно-комунікаційної мережі.

Маршрутизатори забезпечують масштабованість мережі, оскільки вони є завадою ширококомовленню і поділяють мережі на підмережі на основі адреси рівня 3 (рис. 2.16).

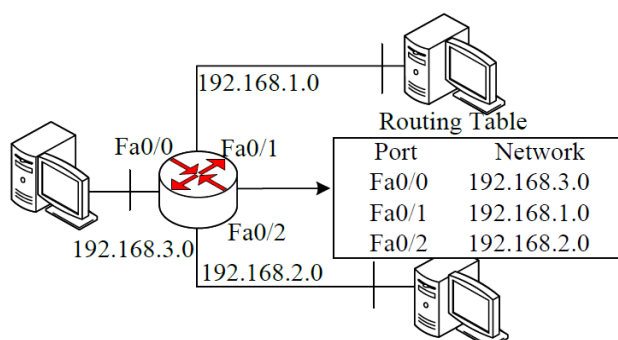


Рис. 2.16. Метод розподілу інформаційної мережі на підмережі на базі маршрутизаторів

Для ухвалення рішення про використання маршрутизаторів або комутаторів важливо докладно розглянути цю проблему. Якщо проблема зумовлюється протоколом, а не питаннями конкуренції, то переважають маршрутизатори. Маршрутизатори вирішують проблеми, що стосуються

широкомовлення, протоколів, які погано масштабуються, аспектів безпеки та адресації мережного рівня. Проте вони більше коштують і складніше конфігуруються. Приклад проекту, що містить кілька мереж, наведено на рис. 2.17. Увесь трафік із мережі 1 у мережу 2 має пройти через маршрутизатор. У цій реалізації є два широкомовні домени. Обидві мережі мають унікальну схему мережної адресації. За такою технологією може створюватися безліч фізичних мереж, якщо горизонтальні і вертикальні кабелі підключити до порту відповідного комутатора рівня 2. Підключення можна виконати патч-кабелями. Зазначена реалізація забезпечує належний рівень безпеки, оскільки інформаційний потік, що входить і виходить з локальної мережі, має пройти через маршрутизатор.

Концепція віртуальних інформаційно-комунікаційних мереж. Концепція віртуальних мереж (VLAN) припускає майже повну незалежність фізичної і логічної топологій. Адміністратори можуть використовувати засоби віртуальних мереж для групування робочих станцій навіть тоді, коли вони відокремлюються комутаторами і розміщені в інших сегментах інформаційно-комунікаційної мережі. Окрема віртуальна мережа припускає один домен колізій і один широкомовний домен [14-21].

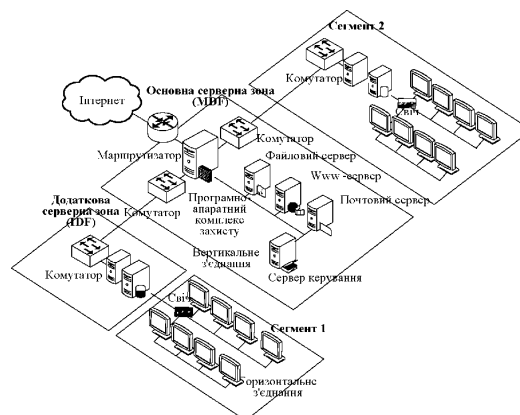


Рис. 2.17. Топологія розгалуженої інформаційної мережі із застосуванням сегментації, основних та додаткових серверних зон та базового комунікаційного устаткування

Особливості та переваги використання віртуальних інформаційно-комунікаційних мереж.

Віртуальна мережа полегшує адміністрування логічних груп станцій і серверів, які можуть взаємодіяти так, ніби вони перебувають у тому самому фізичному сегменті інформаційно-комунікаційної мережі.

Традиційна дротова мережа Віртуальна мережа

Віртуальні мережі спрощують адміністрування змін структури цих груп.

– Віртуальні мережі логічно сегментують комутовані мережі, спираючись на робочі функції, належність користувача до конкретного відділу або сегмента незалежно від фізичного розміщення користувачів або фізичного підключення до мережі.

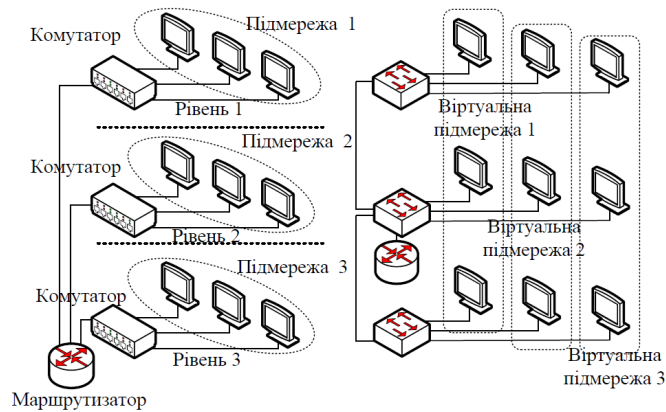


Рис. 2.18. Концепція побудови віртуальних мереж

– Усі робочі станції та сервери, використовувані конкретною робочою групою, належать одній віртуальній мережі незалежно від їх фізичного розміщення.

– Логічна група мережних станцій, сервісів і пристроїв не обмежена фізичним сегментом інформаційно-комунікаційної мережі (рис. 2.18).

– Конфігурація або деконфігурація віртуальних мереж реалізується через програмне забезпечення. Отже, конфігурація віртуальної мережі не потребує фізичного переміщення або перемикання мережного устаткування. Функціонування робочих станцій обмежується взаємодією з файловими серверами в тій самій віртуальній мережі.

VLAN логічно сегментують мережу в різні ширококомовні домени в такий спосіб, що пакети комутуються тільки між портами, призначеними тій самій віртуальній мережі.

Віртуальні мережі створюються для підтримки сервісів сегментації, що традиційно реалізуються маршрутизаторами. Маршрутизатори в топологіях віртуальних мереж реалізують ширококомовну фільтрацію, безпеку та управління трафіком.

Комутатори не забезпечують трафіку між різними віртуальними мережами, оскільки це порушує цілісність ширококомовного домену VLAN. Трафік між віртуальними мережами реалізує маршрутизатор.

Для визначення віртуальних мереж використовується фізичне призначення портів мережного комутатора. Зв'язок між двома чи більше віртуальними мережами (VLAN1 і VLAN2, рис. 2.19) може існувати тільки через маршрутизатор.

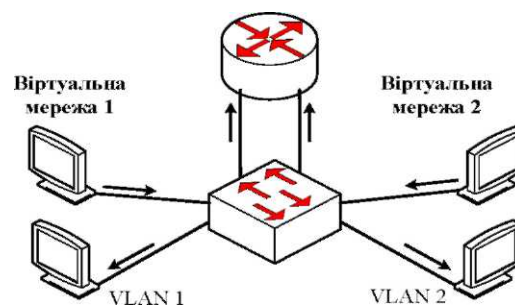


Рис. 2.19. Розподіл портів мережного комутатора.

Концепція віртуальних інформаційно-комунікаційних мереж об'єднує технології комутації *рівня 2* і маршрутизації *рівня 3* моделі OSI на обмеження розмірів доменів колізій і широкомовних доменів.

2.4. Ієрархічна технологія серверної взаємодії

Технологія «клієнт-сервер» є базовою для подальшого розвитку та інтеграції сучасних інформаційно-комунікаційних систем і мереж. Однак, достатньо великий клас задач, для яких вона була створена, поступово спрощуються з умов впровадження новітніх технологій і методів. Першочерговими, на даний час стають нові пріоритети та задачі, що потребують реорганізації принципів «клієнт-серверних» систем. Одна з таких технологій World Wide Web [73].

Фундаментальна архітектура «клієнт-сервер» (клієнт-комп'ютер, який використовує загальні ресурси, сервер-комп'ютер, який надає ті чи інші загальні ресурси, файлова система, база даних, принтерний сервіс, інші сервіси), основана на Web-технологіях, стала результатом розвитку та розробки великого числа стандартних та спеціалізованих додатків в сучасних мережних технологіях.

Використання технології гіпертекстових документів для побудови внутрішньої інформаційної інфраструктури компанії стимулювало бурхливий розвиток різних інформаційних систем. Спроба розрізнити та протиставити Web-технологію – архітектурі «клієнт-сервер» є помилковою. Web-технологія є результатом логічного розвитку та продовженням даної архітектури. Можна сказати, що система Web має «клієнт-серверну» архітектуру, тобто за допомогою одного клієнта можна підключитися до багатьох серверів [22].

Web-браузер, який забезпечує зручний інтерфейс з користувачем для доступу до інформації, це найважливіший рівень Web-серверної системи. Окрім інтерфейсу будь-яка інформаційна система повинна мати рівні обробки даних і їх зберігання. У розробників Intranet-мереж часто виникає проблема правильного узгодження роботи Web з іншими елементами системи, наприклад базами даних. Одним з перспективних способів вирішення цієї проблеми є багаторівнева архітектура серверної взаємодії, що впроваджується на основі використання та розвитку систем подібних архітектурі «клієнт-сервер».

Web-серверними моделями називають типові рішення організації інформаційного середовища на базі серверного розподілу інформаційних ресурсів та послуг інформаційно-комунікаційних систем та мереж.

Щоб зрозуміти її переваги, розглянемо докладніше звичайну клієнт-серверну систему.

Термін «клієнт-сервер», як архітектура, з'явилася на базі програмно-апаратних комплексів, в яких його функціональні частини взаємодіють за схемою «запит-відповідь».

Якщо розглянути дві взаємодіючі частини цього комплексу, то одна з них (клієнт) виконує активну функцію, тобто ініціює запити, а інша (сервер) пасивно на них відповідає (рис. 2.20):

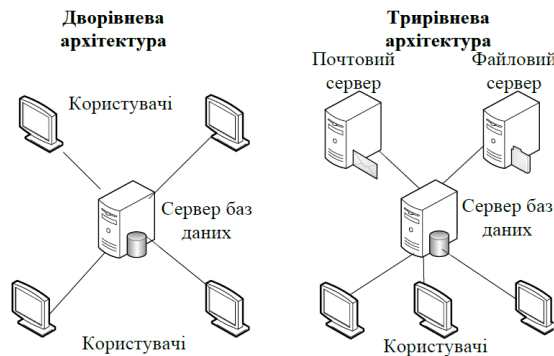


Рис. 2.20. Дво(три)рівнева архітектури

Згідно з встановленими задачами та функціональними особливостями ІКСМ, ролі клієнта та сервера можуть змінюватись, наприклад деякий програмний блок одночасно виконуватиме функції серверу по відношенню до одного блоку і клієнта по відношенню до іншого.

Будь-яка інформаційна система повинна мати мінімум три основні функціональні частини – модуль зберігання даних, модуль їх обробки і модуль інтерфейсу з користувачем. Кожна з цих частин може бути реалізована незалежно від двох інших. Наприклад, не змінюючи програм, що використовуються для зберігання і обробки даних, можна змінити інтерфейс з користувачем таким чином, що одні і ті ж дані відображатимуться у вигляді таблиць, графіків або гістограм. Не міняючи програм представлення даних і їх зберігання, можна змінити програми обробки, наприклад змінивши алгоритм повнотекстового пошуку.

Дворівнева архітектура клієнт-сервер. В класичній архітектурі клієнт-сервер (рис. 2.20) доводиться розподіляти на три основні частини застосування за двома фізичними модулями. Традиційно програмне забезпечення (ПЗ) зберігання даних, розташовується на сервері (наприклад, сервері бази даних), інтерфейс з користувачем – на стороні клієнта, а ось обробку даних доводиться розподіляти між клієнтською і серверною частинами. В цьому і полягає основний недолік дворівневої архітектури, з якого виходять декілька неприємних особливостей, сильно ускладнюючих розробку клієнт-серверних систем [22, 104].

Недоліки:

«Товстий клієнт»: складність адміністрування; ускладнюється оновлення ПО, оскільки його заміну потрібно проводити одночасно по всій системі; ускладнюється розподіл повноважень, оскільки розмежування доступу відбувається не по діях, а по таблицях; перевантажується мережа внаслідок передачі по ній необроблених даних; слабкий захист даних, оскільки складно правильно розподілити повноваження.

«Товстий сервер»: продуктивність програм, написаних на мовах типу PL/SQL, значно нижче, ніж створених на інших мовах, що має важливе

значення для складних систем; програми, написані на СУД-мовах, працюють недостатньо надійно; помилка в них може привести до виходу з ладу всього серверу баз даних; програми неможливо перенести на інші системи і платформи.

При розбитті алгоритмів обробки даних необхідно синхронізувати поведінку обох частин системи. Всі розробники повинні мати повну інформацію про останні зміни, внесені в систему, і розуміти ці зміни. Це створює великі складнощі при розробці клієнт-серверних систем, їх установці і супроводу, оскільки необхідно витратити значні зусилля на координацію дій різних груп фахівців. У діях розробників часто виникають суперечності, а це гальмує розвиток системи і змушує змінювати вже готові і перевірені елементи.

Щоб уникнути неузгодженості різних елементів архітектури, намагаються виконувати обробку даних на одній з двох фізичних частин – або на стороні клієнта («товстий клієнт»), або на сервері («тонкий клієнт»). Кожний підхід має свої недоліки. У першому випадку невинновдано перевантажується мережа, оскільки по ній передаються необроблені, а значить, надмірні дані. Крім того, ускладнюється підтримка системи і її зміна, оскільки заміна алгоритму обчислень або виправлення помилки вимагає одночасної повної заміни всіх інтерфейсних програм, а інакше можуть виникнути помилки або неузгодженість даних. Якщо ж вся обробка інформації виконується на сервері (коли таке взагалі можливо), то виникає проблема опису вбудованих процедур і їх відладки. Річ у тому, що мова опису вбудованих процедур звичайно є декларативною і, отже, у принципі не допускає покрокової відладки. Крім того, систему з обробкою інформації на сервері абсолютно неможливо перенести на іншу платформу, що є важливим недоліком.

Більшість сучасних засобів швидкої розробки додатків (RAD), які працюють з різними БД, реалізує першу стратегію, тобто «товстий клієнт» забезпечує інтерфейс з сервером бази даних через вбудований SQL. Такий варіант реалізації системи з «товстим клієнтом», окрім перерахованих вище недоліків, звичайно забезпечує неприпустимо низький рівень безпеки. Наприклад, у банківських системах доводиться всім операціоністам давати права на запис в основну таблицю облікової системи. Крім того, дану систему майже неможливо перекласти на Web-технологію, оскільки для доступу до серверу бази даних використовується спеціалізоване клієнтське ПО.

Багаторівнева архітектура клієнт-серверної взаємодії

Недоліки дворівневої клієнт-серверної архітектури усуваються шляхом введення третьої функціональної компоненти, на базі якої реалізовується сервер застосувань (рис. 2.20). Розвиток розглянутої архітектури, поява програм, які створюють проміжний рівень, привела до створення **«тонких клієнтів»**. Це дозволяє значно знизити вартість персонального комп'ютера, що реалізує технологію тонкого клієнта. Застосування «тонких клієнтів» пов'язано з тим, що значна частина задач,

які звичайний клієнт виконує в дворівневій архітектурі, перенесена на сервер застосувань. У клієнта залишилися задачі управління інтерфейсом користувача і зв'язку з сервером застосувань.

Багаторівнева архітектура дозволяє не тільки понизити вартість клієнтів, але і спрощує модернізацію процесу обробки даних, бо при цьому клієнти можуть залишатися без змін, а також дозволяє істотно спростити розподілені обчислення, роблячи їх не тільки більш надійними, але і більш доступними. Окрім цього, легко здійснюється масштабування засобів обробки даних. Для цього необхідно лише змінювати кількість серверів.

У результаті створюються всі передумови для створення складних розподілених інформаційних систем, які ефективно використовують всі переваги сучасних технологій.

Така архітектура більш розумно розподіляє модулі обробки даних, які у цьому випадку виконуються на одному або декількох окремих серверах. Ці програмні модулі виконують функції серверу для інтерфейсів з користувачами і клієнту – для серверів баз даних.

Крім того, різні сервери застосувань можуть взаємодіяти між собою для більш точного розділення системи на функціональні блоки, виконуючи певні ролі. Наприклад, можна виділити сервер управління персоналом, який виконуватиме всі необхідні для управління персоналом функції. Пов'язавши з ним окрему базу даних, можна приховати від користувачів всі деталі реалізації цього серверу, дозволивши їм звертатися тільки до його загальнодоступних функцій. Крім того, таку систему дуже просто адаптувати до Web, оскільки простіше розробити html-форми для доступу користувачів до певних функцій бази даних, ніж до всіх даних.

У трьохрівневій архітектурі «тонкий клієнт» не переобтяжений функціями обробки даних, а виконує свою основну роль системи представлення інформації, що поступає з серверу застосувань. Це зменшує обсяг даних, які передаються між клієнтом і сервером застосувань, що дозволяє підключати клієнтські комп'ютери навіть по повільних лініях типу телефонних каналів. Крім того, клієнтська частина може бути настільки проста, що у більшості випадків її реалізують за допомогою універсального браузерa. Але, якщо зміни обов'язкові, то цю процедуру можна здійснити швидко і безболісно.

Трьохрівнева архітектура клієнт-сервер дозволяє більш точно призначати повноваження користувачів, оскільки вони одержують права доступу не до самої бази даних, а до певних функцій серверу застосувань. Це підвищує захищеність системи (порівняно із звичайною архітектурою) не тільки від умисного нападу, але і від помилкових дій персоналу.

Для прикладу розглянемо систему, різні частини якої працюють на декількох віддалених, один від одного серверах. Припустимо, що від розробника поступила нова версія системи, для установки якої в дворівневій архітектурі необхідно одночасно поміняти всі системні модулі. Якщо ж цього не зробити, то взаємодія старих клієнтів з новими серверами

може привести до непередбачуваних наслідків, оскільки розробники звичайно не розраховують на таке використання системи.

В трьохрівневій архітектурі ситуація спрощується. Помінявши сервер застосувань і сервер зберігання даних (це легко зробити одночасно, оскільки обидва вони звичайно знаходяться поряд), відразу змінюємо набір доступних сервісів. Таким чином, вірогідність помилки через невідповідність версій серверної і клієнтської частин різко скорочується. Якщо в новій версії який-небудь сервіс зник, то елементи інтерфейсу, що обслуговували його в старій системі, просто не працюватимуть. Якщо ж змінився алгоритм роботи сервісу, то він коректно працюватиме навіть із старим інтерфейсом.

Слід зазначити і той факт, що в трьохрівневій системі каналами зв'язку між сервером застосувань і базою даних передається достатньо багато інформації. Проте це не уповільнює обчислень, оскільки для зв'язку вказаних елементів можна використовувати більш швидкісні лінії. Це потребує мінімальних витрат, оскільки обидва сервери звичайно знаходяться в одному приміщенні. Таким чином збільшується сумарна продуктивність системи – над однією задачею тепер працюють два різні сервери, а зв'язок між ними можна здійснювати по найшвидкісніших лініях з мінімальними витратами засобів. Правда, виникає проблема узгодженості сумісних обчислень, яку покликані вирішувати менеджери транзакцій – нові елементи багаторівневих систем.

Менеджери транзакцій

Особливістю багаторівневої архітектури є використання менеджерів транзакцій, які дозволяють одному серверу застосувань одночасно обмінюватися даними з декількома серверами баз даних. Якщо, користувач береже частину інформації в БД Oracle, частину – в БД Informix, а частину – в текстових файлах, то без менеджера транзакцій не обійтися [91].

Менеджер транзакцій (MT) – це програмне забезпечення або комплекс програмного забезпечення, за допомогою якого можна погоджувати роботу різних компонентів інформаційної системи.

MT використовується для управління розподіленими різнорідними операціями і узгодження дій різних компонентів інформаційної системи. Слід зазначити, що практично будь-яке складне ПО вимагає використання MT. Наприклад, банківські системи повинні здійснювати різні перетворення представлень документів, тобто працювати одночасно з даними, що зберігаються як в базах даних, так і в звичайних файлах, – саме ці функції і допомагає виконувати MT [76].

Логічно MT ділиться на декілька частин:

- **комунікаційний менеджер (Communication Manager)** – контролює обмін повідомленнями між компонентами інформаційної системи;
- **менеджер авторизації (Authorisation Manager)** – забезпечує аутентифікацію користувачів і перевірку їх прав доступу;
- **менеджер транзакцій (Transaction Manager)** – управляє розподіленими операціями;

– **менеджер ведення журнальних записів (Log Manager)** – стежить за відновленням і супроводом розподілених операцій;

– **менеджер блокувань (Lock Manager)** – забезпечує правильний доступ до даних, що спільно використовуються.

Звичайно комунікаційний менеджер з'єднаний з авторизацією, а менеджер транзакцій працює спільно з менеджерами блокувань і системних записів. Причому, такий менеджер рідко входить в комплект поставки ПО, оскільки його функції (ведення записів, розподіл ресурсів і контроль операцій), як правило, виконує сама база даних. Перші менеджери транзакцій з'явилися на початку 70-х рр. (наприклад, CICS); з тих пір вони трохи змінилися ідеологічно, але вельми істотно – технологічно. Найбільші ідеологічні зміни відбулися в комунікаційному менеджері, оскільки в цій області з'явилися нові об'єктно-орієнтовані технології (CORBA, DCOM і т.д.). Через бурхливий розвиток комунікаційних засобів в майбутньому слід чекати широкого використання різних типів менеджерів транзакцій.

Багаторівневі клієнт-серверні системи достатньо легко можна перекласти на Web-технологію, для цього достатньо замінити клієнтську частину універсальним або спеціалізованим браузером, а сервер застосувань – Web-сервером і невеликими програмами виклику процедур серверу. Для розробки цих програм можна використовувати, як Common Gateway Interface (CGI), так і більш сучасну технологію Java, детальніше про них йтиметься далі.

Структура та основні принципи функціонування Web-серверних систем

За Web-технологією на сервері розміщуються так звані Web-документи, які візуалізуються і інтерпретуються програмою навігації, яка функціонує на робочій станції (рис. 2.21). Програму навігації називають Web-навігатором або Web-браузером.

Складові Web-сервера:

1. Компонент представлення – реалізує інтерфейс з користувачем.
2. Прикладний компонент – забезпечує виконання прикладних функцій.
3. Менеджер ресурсів – виконує накопичення інформації та управління даними.

В якості компоненти представлення використовується Web-документ.

Web-документ являє собою: текстовий файл спеціального формату, який об'єднує певні Web-сторінки. Кожна з таких сторінок може мати в своєму складі посилання на інші об'єкти, що знаходяться в будь-якому вузлі мережі.

Web-документ являє собою: текстовий файл спеціального формату, який об'єднує певні Web-сторінки.

Кожна з таких сторінок може мати в своєму складі посилання на інші об'єкти, що знаходяться в будь-якому вузлі мережі. Безпосередньо, Web-документ повинен мати тільки одну Web-сторінку. З метою оптимізації

роботи вузлів мережі, доцільно об'єднувати будь-яку кількість таких сторінок різних Web-документів.

Система гіперпосилань, реалізована у Web-документі, основана на тому, що деякі виділенні ділянки одного документа, котрими можуть бути частини тексту і рисунки, виступають в якості посилань на інші логічно пов'язані з ними об'єкти: іншу частину Web-документа, інший Web-документ чи документ іншого формату (наприклад, документ Word чи Excel). Зазначений Web-документ, може розміщатися на будь-якому комп'ютері мережі у вигляді:

- мультимедійного об'єкта (малюнок, звук, відео, тощо);
- програм, які при переході на них по посиланнях, будуть виконуватися на сервері;
- програм, які при переході на них по посиланнях, будуть передані з сервера на робочу станцію для інтерпретації чи запуску на виконання навігатором;
- будь-який інший сервіс (електронна пошта, копіювання файлів з іншого комп'ютера мережі, пошук інформації та ін.).

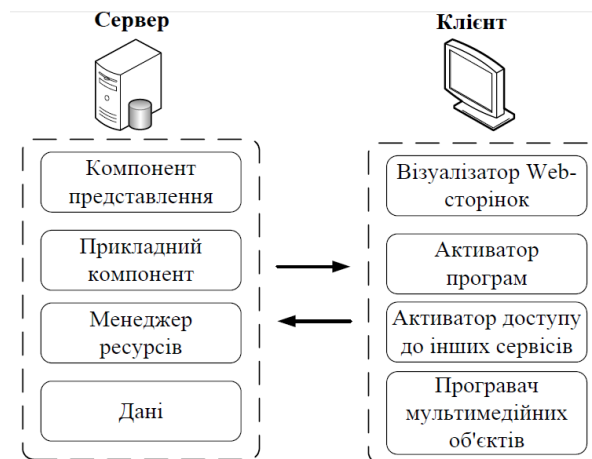


Рис. 2.21. Архітектура «клієнт-сервер» заснована на Web-технології

Із розкритого поняття Web-документа зрозуміло, що програма навігації, виконувана на робочій станції, може не тільки візуалізувати Web-сторінки і виконувати переходи до інших об'єктів, але й активізувати програми на сервері. Дана програма навігації також може інтерпретувати і запускати на виконання програми, які відносяться до Web-документа, для виконання на робочій станції. До Web-навігаторів відносяться такі відомі продукти, як: Netscape Navigator компанії Netscape або Internet Explorer від Microsoft.

Клієнтський комп'ютер, на якому повинна виконуватися програма навігації, може бути повністю стандартизований. У такий комп'ютер, крім процесора, основної пам'яті і монітора, достатньо включити невелику ділянку зовнішньої пам'яті, необхідної для зберігання і роботи програми навігації, а також пристрій контакту з лінією зв'язку. Крім того, програму навігації можна взагалі реалізувати апаратно в спеціалізованому процесорі.

Можна виділити такі особливості архітектури «клієнт-сервер» що основана на Web-технології:

- сервері зароджується кінцева інформація, що потрібна для представлення користувачу програмою навігації; усі інформаційні ресурси, а також прикладна система сконцентровані на сервері;
- я обміну даними між клієнтами і сервером використовуються протоколи відкритого стандарту TCP/IP, які використовуються в Internet;
- легшене централізоване управління не тільки сервером, але й комп'ютерами-клієнтами, так як вони стандартизовані з точки зору програмного забезпечення (на кожній робочій станції достатньо присутності тільки стандартної програми навігації);
- робочих станціях, крім своїх програм можуть виконуватися програми з других комп'ютерів мережі.

2.5 Організація взаємодії Web-навігаторів

Обмін інформацією за Web-технологією не відрізняється від стандартного інформаційного обміну, який реалізується за принципом «клієнт-сервер», коли програма-сервер виконує обробку запитів, що поступають від програми-клієнта.

Передачу, із сервера на робочу станцію, документів й інших об'єктів по запитах, які надходять від навігатора, забезпечує функціонуюча на сервері програма, яка має назву Web-сервер. Коли Web-навігатору необхідно отримати документи чи інші об'єкти від Web-сервера, він відправляє серверу запит. При достатніх правах доступу між сервером і навігатором встановлюється логічний зв'язок. Далі сервер оброблює запит та передає Web-навігатору результати обробки, наприклад певний Web-документ та розриває встановлений зв'язок.

Web-сервер виступає в ролі базового концентратора інформаційних потоків. У даному випадку він забезпечує передачу інформації з різних джерел, а потім однорідним чином надає її користувачу.

Програми Web-навігації виступають, як клієнтські програми, що розташовуються на робочих станціях мережі, або як службові Web-додатки. Web-навігатори використовуються для безпосередньої візуалізації і інтерпретації Web-документів, що зберігаються на сервері, а також для доступу до інших окремих сервісів (рис. 2.22):

- сервісу копіювання файлів з сервера (FTP-сервісу);
- сервісу управління сервером (Telnet-сервісу);
- сервісу багаторівневих меню по доступу до інформаційних ресурсів системи (Gopher-сервісу).

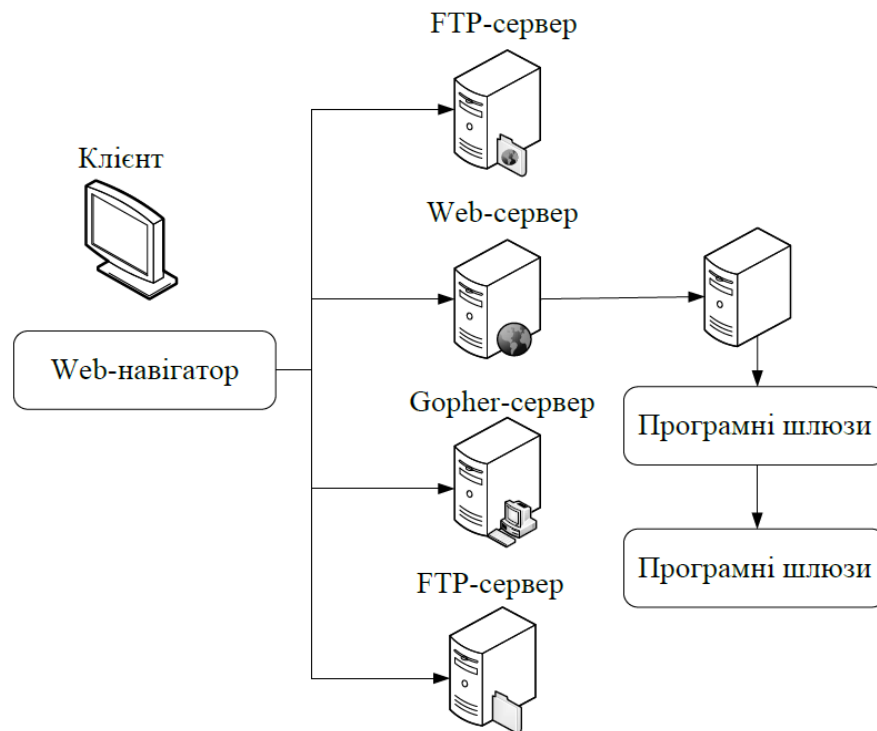


Рис. 2.22. Узагальнена схема взаємодії Web-навігатора з сервером

При використанні Web-технології базовою програмою є програма, що забезпечує функціонування базового Web-сервера з умов обробки запитів від Web-клієнтів. Взаємодія між Web-клієнтом і Web-сервером здійснюється відповідно до протоколу HTTP (Hyper Text Transfer Protocol – протокол передачі гіпертексту). В стані активного функціонування, Web-сервер контролює логічний порт (порт № 80), та за замовченням вважає, що будь-які повідомлення, прислані до цього порту, призначені для Web-сервера [87].

При отриманні запиту від Web-клієнта, Web-сервер встановлює зв'язок по протоколу TCP/IP і обмінюється інформацією відповідно до протоколу HTTP. У разі запиту захищеної інформації Web-сервер може зажадати від користувача введення ідентифікатора і пароля. Захищені Web-документи надаються тільки за наявності у користувачів відповідних прав доступу.

Для доступу до тієї інформації, яка не може оброблятися Web-сервером безпосередньо, наприклад для доступу до баз даних, використовується система програмних шлюзів. Програмний шлюз, одержавши запит від Web-сервера, обробляє його сам або виступає, як посередник між Web-сервером і яким-небудь іншим сервером, наприклад, сервером СУБД (рис. 2.21). Програмні шлюзи розробляються відповідно до певних стандартів, що визначають способи виклику Web-сервером прикладних програм або функцій динамічних бібліотек, а також способи обміну інформацією з цими програмними об'єктами. Одним з найбільш поширених стандартів даного типу є інтерфейс CGI (Common Gateway Interface – загальний інтерфейс шлюзів).

Розглянемо повну послідовність кроків, що реалізовується Web-сервером при обробці запиту, що поступив від Web-клієнта.

1. Web-навігатор або інший Web-клієнт посилає Web-серверу запит на отримання від нього якого-небудь інформаційного ресурсу. Запит передається у форматі HTTP, а адреса ресурсу вказується у форматі URL.

2. Після отримання запиту, Web-сервер визначає наявність запрошуваного ресурсу серед локальних ресурсів, тобто серед ресурсів, якими даний сервер управляє.

3. Якщо запрошуваний ресурс є в наявності, то Web-сервер перевіряє права доступу до цього ресурсу і, якщо права не порушені, то повертає зміст ресурсу Web-клієнту.

4. Якщо запит Web-клієнта порушує права доступу до ресурсу, то Web-сервер відхиляє запит і повертає відповідне попередження клієнту.

5. У випадку, якщо запрошуваний ресурс не відноситься до локальних ресурсів Web-сервера, сервер визначає наявність в його файлах настройки інформації про переміщення ресурсу в мережі. Якщо, ресурс був розміщений на сервері, але в даний момент переміщений в інше місце, то сервер повідомляє про це клієнту (рис. 2.23).

6. Якщо Web-сервер підтримує віртуальне дерево іншого Web-сервера, то запит буде переспрямований на потрібний ресурс по аналогії з попереднім кроком (рис. 2.23).

7. Якщо Web-сервер використовується, як сервер-посередник (проху-сервера), то він виступає з одного боку, як Web-сервер для клієнта, що послав запит, а з іншого боку – як Web-клієнт, який посилає запит до іншого Web-сервера (рис. 2.24).

8. Після повернення інформації клієнту, сервер розриває з'єднання з ним.

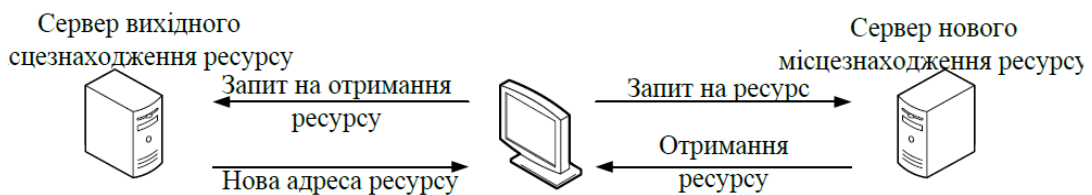


Рис. 2.23. Загальна схема організації запитів

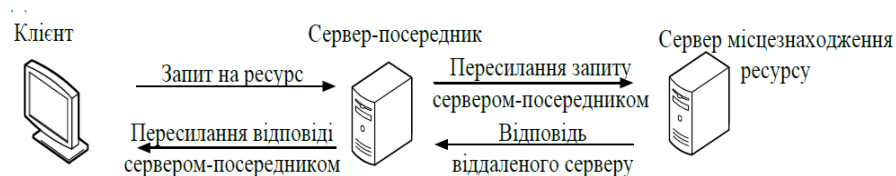


Рис. 2.24. Використання Web-сервера як сервера-посередника

2.6. Розподілена обробка інформації на основі мігруючих програм

Однією з головних особливостей Web-архітектури є розподілена обробка інформації на основі мігруючих програм. Функціонуюча програма навігації робочої станції може не тільки візуалізувати Web-сторінки і виконувати переходи до інших ресурсів, але і активізувати інші стандартні, або спеціалізовані серверні програми. Зазначені програми навігації ідентифікують і активізують програмне забезпечення Web-документа з умов їх попередньої передачі разом з цими чи іншими документами сервера. Такий вид розподіленої обробки інформації дозволяє сконцентрувати всю прикладну систему безпосередньо на сервері [19].

Існує три основні види програм, які можуть бути пов'язані з Web-документом і передаватися на робочу станцію для виконання:

- Java-аплети, підготовлені і використовувані за технологією Java;
- програми, написані на мові сценаріїв JavaScript, VBScript (Visual Basic Scripting);
- програмні компоненти ActiveX Controls, відповідні технології ActiveX.

Наявність декількох різновидів мігруючих програм пояснюється їх різними можливостями, а також конкуренцією між провідними корпораціями у області програмних і мережових технологій – корпораціями Sun Microsystems, Netscape, Microsoft та ін.

Java-технологія

Технологія Java була розроблена компанією Sun Microsystems на початку 90-х років у зв'язку з виникненням гострої необхідності в комп'ютерних програмах, орієнтованих на використання в мережевому середовищі та спрямованих на інтеграцію з Web-сервісом. До таких програм спочатку були пред'явлені вимоги по мобільності, що припускають незалежність від апаратних і операційних платформ, а також безпека і надійність обробки інформації [111].

У результаті була розроблена мова програмування Java, а також цілісна технологія створення і використання мобільних програм, що одержала назву Java-технології.

Реалізований в мові модульний принцип побудови програм і простота мови, дають можливість не тільки швидко розробляти нові програми, але і застосовувати елементи вже написаних і перевірених програм, а також ефективно модернізувати старі. Крім того, в стандарт мови входить безліч корисних бібліотек, на основі яких можна будувати обчислювальні системи будь-якої складності. Цей стандартний набір постійно поповнюється новими важливими функціями.

Незалежність від апаратно-операційних платформ, а також безпека і надійність обробки інформації були досягнуті розробкою віртуального Java-процесора, призначеного для виконання Java-програм шляхом їх інтерпретації. При цьому будь-яка Java-програма повинна відповідати специфікації цього абстрактного процесора, яка повністю визначає його машинно-незалежну систему команд, типи оброблюваних даних, а також

реєстри. Тому для можливості виконання Java-програми віртуальним Java-процесором її початкові тексти повинні бути відтрансльовані у високорівневі машинно-незалежні коди цього абстрактного процесора, так звані коди байта Java-програми, що були відтрансльовані, призначені для виконання на робочій станції в середовищі Web-навігатора; їх називають Java-аплетами або просто аплетами. За своєю структурою кожен аplet є невеликою програмкою, в якій повинно бути визначено декілька обов'язкових функцій. Аplet, завантажується по мережі з сервера і виконується в середовищі Web-навігатора (рис. 2.25).

Посилання на аплети розташовуються у Web-документах, але безпосередньо до складу Web-документів аплети не входять. Вони зберігаються в окремих файлах на сервері. Для високої надійності і безпеки передбачені дві важливі функції:

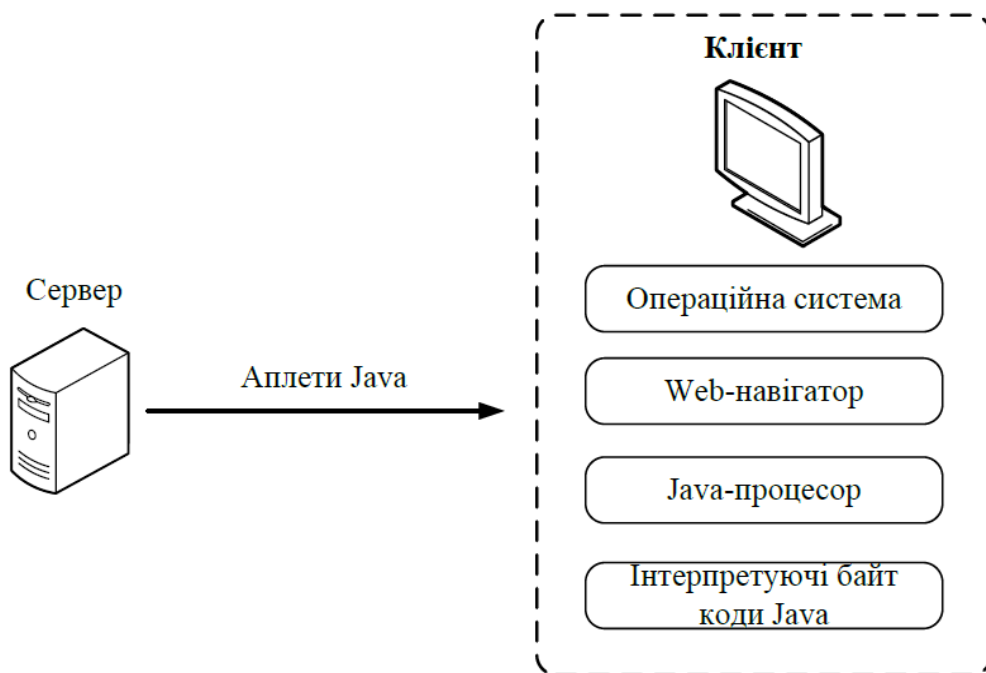


Рис. 2.25. Схема передачі і виконання машинно-незалежних Java-програм

- перевірка *кодів байта* перед їх виконанням на цілісність і правильність інструкцій;
- контроль і блокування небезпечних дій в процесі інтерпретації *кодів байта*.

З урахуванням запуску програми, першу функцію реалізує завантажувач кодів байта, а другу – диспетчер безпеки віртуального Java-процесора. Диспетчер безпеки забороняє аплетам здійснювати доступ до файлів і периферійних пристроїв, а також виконувати системні функції такі, як розподіл пам'яті тощо. Слід зазначити, що на мові Java можуть створюватися не тільки аплети, що є мігруючими програмами, але і стаціонарні програмні застосування. Проте для високої швидкодії початковий текст таких програм слід компілювати не в коди байта, а в

машинно-залежні коди, що забезпечують високу швидкість виконання. Паралельно з Java-технологією з'явилися технології створення і застосування мігруючих програм, засновані на використанні мов сценаріїв. Найбільш важливою відмінністю таких технологій від Java-технології є покомандна інтерпретація початкових текстів програм, що виключає необхідність їх компіляції перед виконанням. Однак, ще раз зауважимо, що в Java-технології мобільна Java-програма для можливості виконання повинна відкомпілюватися в коди байта. Функція інтерпретації мобільних програм, написаних на мові сценаріїв, покладена на Web-навігатора.

Технології, засновані на використанні мов сценаріїв

Мови сценаріїв часто називають ще мовами скриптів (script – сценарій) або макромовами, їхні функціональні можливості спрощують відлагодження і створення складених на них програм. До основних представників мов сценаріїв, призначених для написання мігруючих програм, відносяться:

- мова JavaScript, розроблена спільно компаніями Netscape і Sun Microsystems, а також подібна їй мова VBScript (Visual Basic Scripting) від Microsoft;

- мова VRML (Virtual Reality Modeling Language – мова моделювання віртуальної реальності), розроблена компанією Silicon Graphics.

Java Script зовсім не є похідною від Java. Хоча ці мови мають деякі загальні атрибути, але достатньо різняться (табл. 2.3).

Java Script є спрощеною мовою з базовими об'єктно-орієнтованими функціями. Властивість простоти пояснюється відсутністю жорсткої архітектури і семантики. Об'єктно-орієнтована орієнтація виявляється в можливостях роботи з вікнами, рядком стану й іншими елементами інтерфейсу Web-навігатора і мережевого оточення, як з об'єктами, до яких можна звертатися по імені згідно зі встановленою ієрархією.

Java Script бідніша за мову Java, але набагато зручніша і ефективніша для ряду завдань, пов'язаних з обробкою Web-документів і взаємодією з користувачем.

Команди Java Script вбудовуються безпосередньо в Web-сторінку і виконуються Web-навігатором під час завантаження цієї сторінки або під час певних дій, вироблюваних користувачем при роботі з нею. Наприклад: при клацанні мишею на одному з об'єктів сторінки, при позиціюванні покажчика в місце розташування посилання або при введенні інформації в поля HTML-форми.

Порівняльні характеристики мов Java і JavaScript

Java	JavaScript
☐ Програма для можливості виконання на стороні клієнта повинна відкомпілюватися в коди. ☐ Об'єктно-орієнтовані. ☐ Аплети утворюють об'єктні класи із спадкоємством. ☐ Аплети викликаються з Web-сторінок, але зберігаються відособлено від Web-документів в окремих файлах на сервері. ☐ Типи даних і змінні повинні бути заздалегідь оголошені. ☐ Статичне скріплення. Об'єктні зсипання повинні існувати на етапі компіляції. ☐ Не може здійснювати запис в дискову пам'ять і виконувати системні функції.	☐ Програма інтерпретується на стороні клієнта в початковому вигляді. ☐ Об'єктно-базовані. ☐ Відсутні класи і механізм спадкоємства. ☐ Програми викликаються з Web-сторінок і вбудовані безпосередньо в Web-документи. ☐ Типи даних і змінні не оголошуються, а вводяться. ☐ Динамічне скріплення. Об'єктні посилання перевіряються під час виконання. ☐ Не може здійснювати запис в дискову пам'ять і виконувати системні функції.

Як і для будь-якої іншої технології або мови, використовуваних в ІКСМ мережі, забезпечення безпеки обробки інформації є першочерговим завданням. Java Script не реалізує деякі можливості функцій безпеки, оскільки при виконанні стандартних функцій побічно роблять захист більш уразливим. Java Script не може, також, безпосередньо відкрити порт TCP/IP, а здатна тільки забезпечити завантаження об'єкта за заданою адресою і забезпечити формування даних, що передаються Web-серверам. Сучасні Web-навігатори дозволяють встановлювати рівні безпеки і управляти ними так, що програма на JavaScript може звернутися тільки до обмеженого кола інформації й даних. Швидкість створення програм, невеликі розміри програмних модулів, зручний доступ до всіх внутрішніх функцій Web-навігатора, а також безпека JavaScript-технології, привели до високої популярності мови JavaScript.

До недоліків технології Java Script слід віднести: невисоку швидкодію Java Script-програм. Мова сценаріїв VBS cript (Visual Basic Scripting) від Microsoft багато в чому подібна Java Script. Вона є підмножиною мови Visual Basic і також призначена для програмування сторінок Web. З її допомогою можна примусити взаємодіяти різні об'єкти на Web-сторінці, включаючи програмні компоненти іншого типу, наприклад: аплети Java і програмні компоненти ActiveX Controls.

На відміну від макромов JavaScript і VBScript, мова VRML розроблена корпорацією Silicon Graphics спеціально для створення програм, що моделюють тривимірні віртуальні простори. Інтерпретатори VRML підключаються до Web-навігаторів найчастіше у вигляді окремих

програмних модулів (plugins). Початкові тексти програм на мові VRML оформляються у вигляді окремого VRML-файлу і викликаються за посиланням з Web-документа при його перегляді Web-навігатором [2]. Клацання мишею по такому посиланню приводить до відкриття окремого вікна, що дозволяє пройти по розташованому в ньому фрагменту тривимірної реальності.

Технології ActiveX. Під ActiveX розуміється набір технологій від Microsoft, направлених на доповнення, інтеграцію і уніфікацію існуючих методів управління і обробки інформації в ІКСМ, побудованих за Web-архітектурою. Основна ідея ActiveX-технологій полягає у використанні однакового способу доступу до всіх інформаційних ресурсів мережі (рис. 2.26). Основою такого уніфікованого способу доступу є Web-технологія.

ActiveX підтримує такі типи мобільних програм, які можуть бути пов'язані з Web-документом і передаватися на робочу станцію для виконання:

- програмні компоненти ActiveX Controls;
- аплети Java;
- програми, написані на мовах сценаріїв Java Script, VBS script (Visual Basic Scripting) і VRML.

Програмні компоненти ActiveX Controls є звичайними виконуваними програмами, які можуть завантажуватися з сервера для виконання на робочій станції. Як і при використанні Java-аплетів, посилання на ці програми розташовуються у Web-документах. Безпосередньо до складу Web-документів програмні компоненти ActiveX Controls не входять. Вони зберігаються в окремих файлах на сервері.



Рис. 2.26. Інтеграція методів доступу до інформаційних ресурсів мережі

Програмні компоненти ActiveX Controls, а також програми, написані на макромовах Java Script і VBS script, можуть включати виклики функцій API ActiveX за поданням ряду сервісів, такі як:

- створення високоякісних мультимедійних ефектів;
- відкриття і редагування електронних документів шляхом звернення до додатків, що підтримують стандарт OLE (Object Linking and Embedding – скріплення і вбудовування об'єктів), наприклад, до додатків Microsoft Office;
- звернення до операційної системи для оптимальної настройки параметрів виконання одержаних з сервера програм.

Порівняно з технологією Java, технологія ActiveX Controls має як недоліки, так і переваги. Недоліки пов'язані перш за все з нижчим рівнем безпеки розподіленої обробки інформації. Програмні компоненти ActiveX Controls, завантажені на клієнтську систему, можуть звертатися до будь-якої її частини подібно до звичайного додатку.

Разом з тим, програмні компоненти ActiveX Controls, на відміну від Java-апплетів, дозволяють реалізувати функції, властиві повномасштабним програмним застосуванням. Ця особливість для корпоративної мережі є істотною перевагою за умови вживання відповідних заходів безпеки, наприклад: при дозволі завантаження програм ActiveX Controls вона працює тільки з серверів корпорації.

Що ж до продуктивності, то оскільки Java є мовою, що інтерпретується, апплети Java виконуються на віртуальній машині клієнтської системи з меншою швидкістю, ніж скомпільовані елементи ActiveX Controls.

Але з іншого боку, апплети Java дуже компактні, тому завантажуються швидко. Для завантаження ж програм ActiveX Controls потрібен більший час. Слід також врахувати, що завантажені програми ActiveX Controls залишаються в клієнтській системі, тоді як апплети Java необхідно кожного разу завантажувати заново. Ця особливість з погляду безпеки є недоліком, оскільки порушується централізація прикладної системи. Але з погляду продуктивності досягається перевага перед використанням Java-апплетів.

2.7. Організація системи доступу до баз даних

Взаємодія Web-навігатора з сервером системи управління базами даних (сервером СУБД) може здійснюватися двома основними способами:

- доступ до сервера СУБД через Web-сервер;
- доступ до сервера СУБД безпосередньо.

Доступ до сервера СУБД через Web-сервер

Для доступу Web-навігатора до сервера СУБД через Web-сервер використовується система програмних шлюзів. Програмний шлюз, одержавши запит від Web-сервера, виступає, як посередник між сервером Web і сервером СУБД. Одними з найбільш поширених стандартів даного типу є інтерфейс CGI (Common Gateway Interface – загальний інтерфейс шлюзів), а також його вдосконалена специфікація названа, як FastCGI (прискорений CGI).

Для доступу Web-навігатора до сервера СУБД через Web-сервер за стандартом CGI, необхідна відповідна CGI-програма, що виконує роль програмного шлюзу між Web-сервером і сервером СУБД (рис. 2.27).

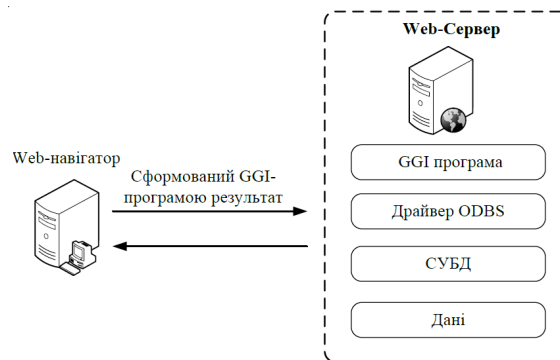


Рис. 2.27. Схема доступу до СУБД через CGI-програму

CGI-додатки працюють незалежно від Web-сервера, а їх запуск здійснюється по виклику з Web-документа при його обробці Web-навігатором. CGI-програма взаємодіє з Web-сервером за допомогою двостороннього обміну через стандартні канали вводу/виводу даного додатку.

Оскільки CGI-програми працюють незалежно від Web-сервера і мають простий загальний інтерфейс, розробники Web-документів мають можливість створювати свої CGI-програми на будь-якій мові, що підтримує стандартні файлові операції вводу/виводу. Крім того, при незалежній розробці можна створювати такі додатки, які легко переносяться з одного на інший Web-сервер. Існують і стандартні CGI-програми, спеціально розроблені для взаємодії Web-серверів з різними СУБД, наприклад: програма Web DBC.

Інтерфейс між Web-навігатором і сервером СУБД у складі Web-документів застосовують HTML-форми, які дозволяють формувати запити до бази даних. CGI-програма одержує інформацію від Web-сервера або через стандартне введення. Все залежить від методу доступу, який використовується при обміні даними між Web-навігатором і Web-сервером. Далі CGI-програма через драйвер ODBC (Open DataBase Connectivity) звертається до серверу СУБД і повертає Web-серверу відповідь на запит через стандартний вивід.

Драйвер ODBC забезпечує уніфікований спосіб доступу до різних СУБД за допомогою стандартної мови запитів SQL. Завдяки стандарту ODBC, прикладні програми можуть використовувати єдиний діалект SQL і взаємодіяти з різними СУБД. Можна обійтися і без драйвера ODBC, але у цьому випадку CGI-програма повинна бути написана з орієнтацією на конкретну СУБД, що функціонує на даному сервері.

Стандарт CGI має й певні недоліки – зниження швидкості обробки запитів при збільшенні інтенсивності їх надходження. При кожному виклику CGI-програми її доводиться завантажувати з диска (тобто, запускати новий процес). Після закінчення роботи програми потрібно звільнити ресурси, що використалися нею. Такі операції створюють помітне додаткове навантаження на сервер, що позначається на його продуктивності. До того ж запуск нового процесу при кожному запиті знижує ефективність постійних процесів і доступність даних. Інформацію,

яка згенерувала в ході обробки одного запиту, неможливо використовувати при обробці іншого.

Для того, щоб обійти проблеми, пов'язані з швидкодією CGI, багато постачальників Web-серверів, включаючи Microsoft і Netscape, розробили відповідні інтерфейси прикладного програмування (API). Корпорацією Microsoft був розроблений інтерфейс ISAPI (Internet Server API), а корпорацією Netscape – інтерфейс NSAPI (Netscape Server API). Ці інтерфейси тісно інтегровані з Web-сервером, дозволяючи зберігати доступність постійно використовуваних процесів і даних. Програми з інтерфейсом ISAPI компілюються у файли бібліотек DLL, що динамічно підключаються до середовища. Вони завантажуються в пам'ять під час першого звернення до них і тому для повторного виклику цих програм не потрібно породжувати новий процес. Функції інтерфейсу NSAPI завантажуються в серверний простір процесів. Відповідно при виклику цих функцій також не породжуються додаткові процеси. Завдяки API-інтерфейсу програма, що його використовує, може залишати з'єднання з СУБД відкритим, так що наступному запиту до бази даних не доведеться витрачати час на відкриття і закриття з'єднання. Проте API-інтерфейси Web-серверів – хоч і непогане, але нестандартне рішення. Більшість додатків не можна переносити з одним API на інший, і дуже рідко вдається переносити додатки на інші платформи. Крім того, більшість додатків для Web-серверів все ще створюються для інтерфейсу CGI, тому перехід до додатків на базі API не представляється економічно виправданим. Поступово з'являються способи побудови деякого проміжного варіанту, який, з одного боку, задовольняв би вимогам мобільності, незалежності і простоти програмування, а з іншого боку – був би достатньо ефективним. Одним з таких рішень є специфікація Fast CGI. Ідея цієї специфікації в тому, що прикладна програма використовує спосіб передачі параметрів і даних, який застосовується в CGI, але при цьому не віддаляється з пам'яті, а залишається резидентною, обробляючи запити, що поступають.

Таким чином, додатки на базі Fast CGI, подібно до CGI-програм, працюють незалежно від Web-сервера і запускаються через стандартні посилання в Web-документах. Однак, як і програми на базі API, програми для Fast CGI є такими, що постійно діють в процесі роботи сервера. Коли програма закінчує обробку чергового запиту, її процес залишається відкритим в очікуванні нового запиту. При доступі Web-навігатора до бази даних через інтерфейс Fast CGI виходить схема, в якій фактично використовуються три сервери: Web-сервер, Fast CGI-програма і сервер бази даних. Web-сервер приймає запит Web-навігатора і передає його Fast CGI-програмі, яка в свою чергу звертається до сервера баз даних. Результат повертається по зворотному ланцюжку.

Організація безпосереднього доступу до сервера СУБД.

Для доступу Web-навігатора до сервера СУБД безпосередньо можуть використовуватися як Java-аплети (рис. 2.28) і програмні компоненти

ActiveX Controls (рис. 2.29), так і спеціалізовані програмні модулі, що підключаються до навігатора (plugins).

Для використання Java-апплетів для доступу до різних серверів СУБД розроблений стандартний інтерфейс JDBC (Java DataBase Connectivity). Даний інтерфейс орієнтований на забезпечення взаємодії з сервером СУБД не тільки Java-апплетів, що виконуються на клієнтських станціях, але і Java-програм, що запускаються на сервері.

Доступ Web-навігатора до сервера СУБД за допомогою програмних компонентів ActiveX Controls припускає, як і у разі Java-апплетів, запит і передачу відповідної програми на робочу станцію, а також її подальше виконання на робочій станції. У цьому випадку взаємодія з сервером СУБД повинна виконуватися через інтерфейс ODBC.

Використання для доступу Web-навігатора до сервера СУБД спеціалізованих програмних модулів (plugins), що підключаються до навігатора, вимагає попередньої установки відповідного програмного доповнення на робочій станції. Після цього взаємодія з сервером СУБД здійснюватиме встановлений програмний засіб, що одержує управління від Web-навігатора при обробці відповідного виклику у Web-документі.

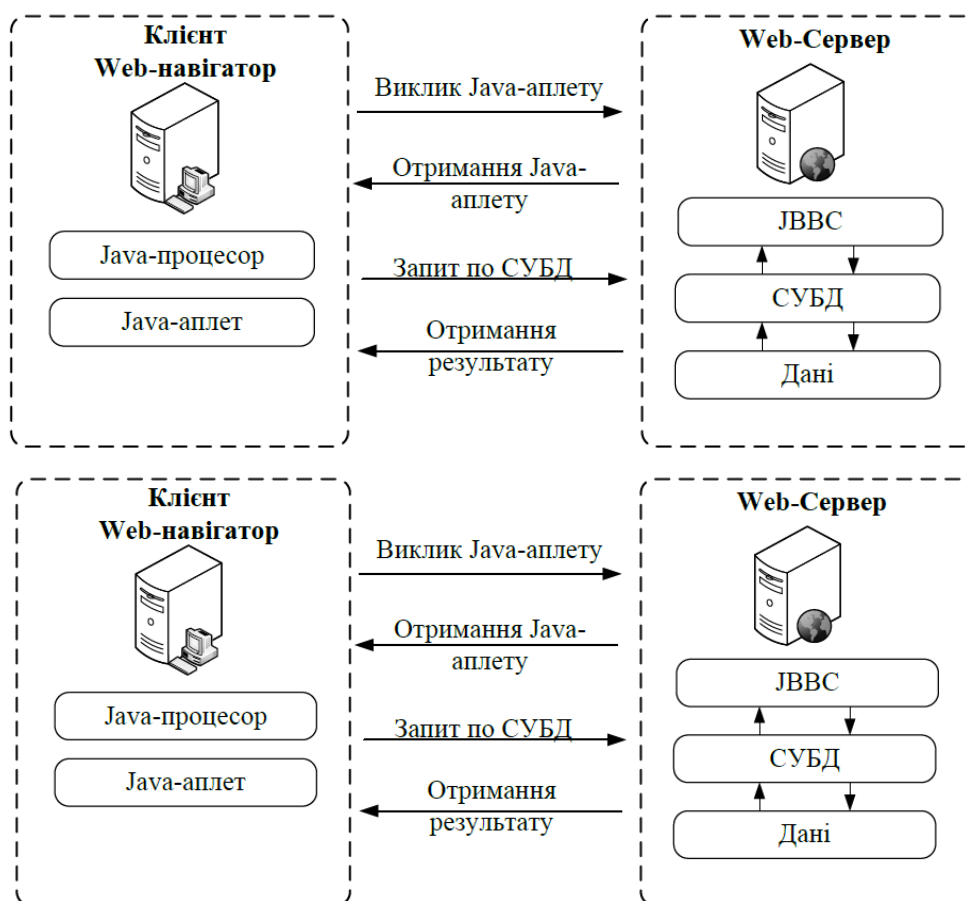


Рис. 2.28. Доступ до СУБД за допомогою Java-апплета

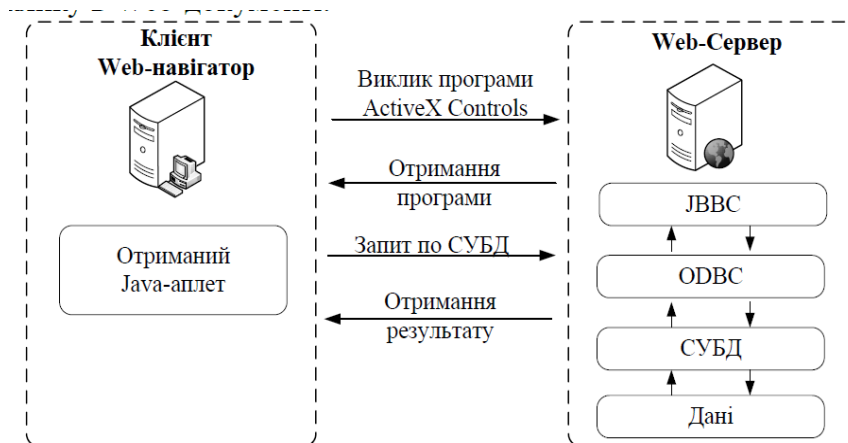


Рис. 2.29. Схема доступу до СУБД за допомогою програмного компонента ActiveX Controls

Для уникнення несумісності взаємодія підключених програмних модулів з сервером СУБД, як і у разі програмних компонентів ActiveX Controls, повинно виконуватися через інтерфейс ODBC.

2.8. Сучасні систем серверної взаємодії

Технологія Hyper-Tier. Більшість сучасних інформаційних систем працюють з трьохрівневою моделлю, але сучасний етап розвитку ІКСМ все частіше впроваджує нові серверні архітектури [24]. Архітектура Hyper-Tier – нова серверна архітектура побудови ІКСМ, що пропонує простий спосіб переходу до обробки даних на новому рівні. Прикладом зазначеної архітектури є побудована гібридна система Intranet/Internet, відома так само, як Extranet. Сутність цієї архітектури полягає в чіткому розділенні рівнів:

- інтерфейс-браузер або інтерфейс комп'ютера користувача;
- рівень координації, включаючи Web-сервер, засоби забезпечення безпеки, засоби пошуку і служби каталогів;
- рівень ресурсів, який визначається існуючими даними, логікою застосування і бізнес-правилами.

Використовуючи концепцію Hyper-Tier, спочатку потрібно створити Web-сервер і набір клієнтських модулів. Це дасть користувачам можливість отримати стандартний інтерфейс і доступ до корпоративних інформаційних систем.

Дана архітектура потребує від групи професійних аналітиків і адміністраторів стандартизувати всі структури даних в масштабах організації. Концепція Hyper-Tier також вимагає від розробника провести аналіз логіки застосування. Логіка, як і раніше, може залишатися частиною складної програми в системі клієнт-сервер, але було б розумніше виділити її в окремий програмний модуль. Програмісти створюють застосування, виходячи з того, що код повинен бути якомога більш компактним і ефективним. Тим часом, ніщо не заважає використовувати компактні проміжні програмні модулі для обробки транзакцій, забезпечення безпеки і обслуговування каталогів. Перевага цього підходу полягає в тому, що не

потрібно викидати існуючу систему і починати все з нуля. Спочатку користувачам надають новий інтерфейс, а вже потім, не перериваючи роботи системи, застарілі компоненти замінюють на нові, і відбувається перехід до модульної структури [81]. Головне ж в концепції Nurer-Tier – гнучкість. Звичайно, нова архітектура не стане рішенням всіх проблем. Але, принаймні, вона дійсно внесе істотні зміни в справжній стан речей.

Інформаційні системи на базі ASP.NET технологій

Сьогодні в області розробки ПО можна спостерігати чергову хвилю активності по перекладу наявних клієнт-серверних автоматизованих систем в середовище Web за допомогою технології Microsoft ASP.Net [21]. ASP.Net виявляє собою спробу наблизити Web-архітектуру до традиційної моделі «event-driven». Середовище приховує розділення клієнта і серверу, надаючи універсальну модель для обробки подій. Події, що виникають на клієнті, можна обробити в коді, виконуваному на сервері. Технологія отримала назву Web Forms. Елемент управління в WebForms існує в двох площинах – як повноцінний об'єкт на сервері і як DHTML – представлення елемента управління на клієнті. Архітектура серверної сторони практично відповідає моделі «event-driven». Web-сторінка (форма) ASP.Net компілюється і є програмою, генерованою HTML. Ця програма запускається кожного разу, коли Web-сторінка запрошується браузером. Для розробника сторінка ASP.Net може бути фізично розділена на два файли.

Перший файл містить наповнення сторінки, тут розміщуються спеціальні HTML-теги, маркуючи серверні елементи управління і клієнтські скрипти.

Другий файл містить серверний код, що відповідає за генерацію сторінки і обробку подій. За рядком клієнтського наповнення сторінки слідує рядок, що виконується на сервері. Важливо, що серверний код можна писати на мові, що строго типізується. Все це спрощує відладку, підвищує читабельність програми і, як наслідок, зменшує час розробки. Web Forms, підтримує декілька типів серверних елементів управління.

Розглянемо найважливіші з них. Найпростіші – HTML-серверні, тобто HTML-елементи, доступні і програмовані на сервері. Кожний такий елемент управління надає програмісту інтерфейс, дуже схожий на HTML-елемент, який він і генерує. Головна відмінність в тому, що події HTML-серверного елемента можуть бути оброблені як на клієнті (в звичайному DHTML), так і на сервері.

Більш витонченими є Web-серверні елементи управління – головна «родзинка» ASP.Net. Web-серверний елемент не має однозначного HTML-уявлення. Цей об'єкт генерує якийсь DHTML, який реалізує потрібну функціональність. Для різних браузерів можуть генеруватися різні DHTML. В комплект поставки Visual Studio.NET входять елементи управління для створення основних примітивів графічного інтерфейсу. Якщо їх не вистачає, можна розробити власні або розширити стандартні.

Web-серверні елементи можуть бути прив'язані до даних (data-binding). Такі елементи, як «список» або «таблиця», можна заповнити значеннями з джерела даних, яким є результат запиту до БД або просто масив об'єктів. Ще одна новина – шаблони елементів, що описують, як саме з елементів джерела даних формуватиметься той, що вимагається HTML. Трохи абстрагуємося від «списку» й отримаємо елемент управління «повторювач», який бере шаблон і повторює його для кожного елемента джерела даних. Шаблоном може бути довільний набір HTML-тегів або інших елементів управління. Web-серверні елементи підтримують тільки серверні події. Серверна подія виникає на клієнті, але обробляється на сервері. У момент його виникнення (як події DHTML) інформація про нього запам'ятовується, HTML-форма пересилається на сервер, запускаються обробники, форма переформується і пересилається клієнту. Такий процес іменується round-trip. Вся механіка реалізується в середовищі ASP.Net. Технологія адаптована до підходу, коли більшість подій обробляється на сервері.

У загальному випадку Web-серверні елементи управління володіють більшою потужністю, ніж HTML-серверні. Якщо немає необхідності в клієнтській обробці подій, це кращий вибір. Недоліками Web-серверних елементів є:

- необхідність обігу на сервер для обробки подій;
- менший контроль над одержуваням DHTML.

Переваги Web-орієнтованих систем, що базуються на клієнт-серверній архітектурі:

- мінімум витрат на обслуговування бізнес-процесів та максимальна оперативність при обробці даних;
- зручність в обслуговуванні, більшість операцій може виконуватись автоматично;
- один працівник може легко обслуговувати декілька процесів одночасно без особливих зусиль;
- мінімум витрат на комунікації між підрозділами компанії;
- Web-сервер, СУБД і програмні модулі, що забезпечують функціонування бізнес логіки, як правило розміщуються на одному комп'ютері;
- працівнику для взаємодії з системою потрібен звичайний браузер;
- працювати з системою можна з майже всіх комп'ютерів, що підключені до Інтернету.

2.9. Комп'ютерної мережі моніторингу режимів систем електропостачання залізниць

Підвищення рівня безпеки руху залізничного транспорту можливо шляхом організації високої надійності і якості функціонування тягових електричних мереж і силового електричного обладнання в процесі передачі й споживання електроенергії залізницями на тягу [30-33, 80]. В

сучасних умовах, коли функціонує ринок електроенергії, до електротехнічної галузі додатково висувається ряд підвищених вимог як при виробництві і передачі електроенергії, так і в режимі споживання її, а також дуже актуальним стає питання забезпечення надійності і якості функціонування силових електричних мереж. Показовим у цьому плані представляється господарство електропостачання залізниць, високий рівень надійності якого тісно пов'язаний з організацією безпеки руху залізничного транспорту. У зв'язку з цим дуже важливою є проблема розробки методів і мережевих технологій організації ефективного функціонування систем електропостачання залізничного транспорту, забезпечення високого рівня їх надійності і якості роботи, а також пошук нових шляхів економії електричної енергії в процесі споживання її на тягу, оскільки зростання її частки збільшує собівартість продукції яка досить висока на енергоємних технологічних виробництвах. Розглядаючи через призму фізичного та морального старіння електротехнічного обладнання, що знаходиться в експлуатації, можна також виявити додаткові негативні впливи не тільки на економічність режимів і збільшення собівартості електроенергії, а в деяких випадках і на надійність функціонування енергосистеми, що значно збільшує аварійність та суттєво зменшує рівень безпеки руху. У той же час процес реабілітації і оновлення технічного стану електричного господарства залізниць вимагає істотного фінансування та багаторічної роботи. У зв'язку з цим проблема забезпечення надійності та якості функціонування існуючих тягових мереж залізничного транспорту, при незначних інвестиціях, може бути розв'язана «практично безальтернативно» шляхом комп'ютеризації технологічних процесів постачання електричної енергії на тягу. Досвід застосування комп'ютерних засобів для комерційного керування електричними мережами стимулював проведення наукових досліджень в області розробки нових принципів організації систем управління, а також математичних моделей, методів і комп'ютерно-орієнтованих алгоритмів.

Система електропостачання залізниць тісно пов'язана з єдиною енергосистемою та застосовується для живлення районних і не тягових споживачів. До особливостей систем електропостачання залізничного транспорту можна віднести велику нерівномірність навантажень, труднощі захисту від короткого замикання, несинусоїдальність і несиметрія струму, істотний вплив на лінії передачі інформації, труднощі, пов'язані із забезпеченням процесу повернення енергії при рекуперативному гальмуванні локомотивів. При такому стані електричних мереж, розвиток системних аварій у зв'язку з ненадійністю устаткування й помилок персоналу, як показує досвід багатьох країн, може призвести до багатомільйонних економічних втрат. У зв'язку з цим, природним є рішення проблеми забезпечення надійності й ефективності функціонування електричного виробництва безпосередньо шляхом забезпечення інформатизації й інтелектуалізації процесів керування.

Проблема контролю стану тягових електричних мереж і керування ними тісно пов'язана з необхідністю моделювання комплексу задач, пов'язаних з реєстрацією значень параметрів режимів і подання отриманої первинної інформації. Рішення сукупності задач керування електричним господарством сприяло появі великої кількості підходів, способів, прийомів, технічних засобів, а надалі комп'ютерних компонентів і мережних технологій. Найважливішими задачами, які необхідно вирішувати при формуванні сучасних інформаційних технологій керування та оптимізації функціонування силових електричних мереж, є визначення вектора Hd , доаварійних параметрів штатних режимів мережі, вектора Ya комплексу аварійних сигналів у випадку виникнення аварійного режиму, вектора Sp післяаварійних параметрів і вектора V_3 набору параметрів визначальне функціонування системи релейного й мікропроцесорного захисту, що функціонує синхронно за часом t . Цей процес може бути представлений

$$Hd = F(Id, Ud, Z, f, Td, t)$$

$$Ya = F(Ia, Ua, Z, f, Td, t)$$

$$Sp = F(Ip, Up, Z, f, Tp, t)$$

$$V_3 = F(Ia, Ua, Z, f, T, t)$$

де Td, Ta, Tp – тривалість часу відповідно доаварійного, аварійного і післяаварійного режимів функціонування електричної мережі;

$T = Td + Ta + Tp$. Визначення векторів Hd, Ya, Sp, V_3 може бути реалізоване на основі сучасних комп'ютерних методів або їхніх модифікацій. Оскільки компоненти векторів Hd, Ya, Sp, V_3 , що відображають стан електричної мережі, можуть бути аналоговими й дискретними, то відповідно в обчислювальному середовищі синтезується блок аналогових вимірювальних перетворювачів, де сигнали перетворюються в цифрову форму, зручну для обробки за допомогою комп'ютерних засобів. Дискретні сигнали, що надходять із вільних контактів засобів релейного захисту, автоматики, логічних елементів та інших датчиків, перетворюються і кодуються у вигляді цифрового еквівалента для подальшої обробки. Моніторинг технічного стану силових електричних мереж на основі первинних даних $f(t)$, які знімаються з об'єкта і представляються у вигляді необхідної сукупності ординат $f_i(t_i)$, може бути реалізовано за допомогою математичного апарату диференціальних тейлорівських перетворень шляхом формування зображення $X(K)$ вихідних функцій $X(t)$ у вигляді T -спектру згідно з таким виразом

$$X(k) = \frac{H^k}{K!} \left[\frac{d^k X(t)}{dt^k} \right]_{t=0} \quad \mp \quad X(t) = \sum_{k=0}^{\infty} \left(\frac{t}{H} \right)^k X(k)$$

де $X(t)$ – оригінал, що є функцією аргументу t ; $X(K)$ – диференціальне зображення оригіналу $X(t)$, $K = 0, 1, 2, \dots$; H – масштабна

постійна, що має ту ж розмірність, що й аргумент t ; $\overline{\quad}$ – символ відповідності між оригіналом $X(t)$ і диференціальним зображенням $X(K)$. Оскільки функція $X_j(t)$, $j=\overline{1,m}$ отримана в процесі проведення моніторингу, представляється в реальному часі сукупністю ординат $X_j(t_j)$ в моменти часу $t_i (i=\overline{1,n})$ на інтервалі $(0,H)$, то для одержання її зображення, тобто, значень T -дискрет $X_j(0), X_j(1), \dots, X_j(k)$ первинної функції $X_j(t_j)$ для уникнення операції диференціювання, скористаємося зворотним перетворенням за виразом (2) і враховуючи, що $X_j(t_0) = X_j(0)$ записаного як

$$X_j(t_j) = \sum_{k=0}^{k=\infty} \left(\frac{t_j}{H} \right)^k X_j(k).$$

Підставивши значення ординат $X_j(t_j)$ у вираз (3), одержимо n лінійних алгебраїчних рівнянь із n невідомими T -дискретами $X_j(0), X_j(1), \dots, X_j(k)$ виду

$$\begin{aligned} \frac{t_1}{H} X_j(1) + \left(\frac{t_1}{H} \right)^2 X_j(2) + \dots + \left(\frac{t_1}{H} \right)^n X_j(n) &= x_j(t_1) - X_j(0) \\ \frac{t_2}{H} X_j(1) + \left(\frac{t_2}{H} \right)^2 X_j(2) + \dots + \left(\frac{t_2}{H} \right)^n X_j(n) &= x_j(t_2) - X_j(0) \\ \frac{t_n}{H} X_j(1) + \left(\frac{t_n}{H} \right)^2 X_j(2) + \dots + \left(\frac{t_n}{H} \right)^n X_j(n) &= x_j(t_n) - X_j(0). \end{aligned}$$

При рішенні системи лінійних алгебраїчних рівнянь (4) одержимо n невідомих T -дискрет $X_j(0), X_j(1), \dots, X_j(k)$, що відображають $x_j(t)$ на інтервалі $(0,H)$. T -дискрети $X_j(0), X_j(1), \dots, X_j(k)$ можуть використовуватися для подальших обчислень в T -області з наступним переходом в область оригіналів. Таким чином, у результаті проведення моніторингу, отримуємо перинні дані параметрів режимів електричних мереж у вигляді сукупності ординат $X_j(t_j)$ вихідних функцій $x_j(t)$ і набору у вигляді T -дискрет $X_j(0), X_j(1), \dots, X_j(k)$, що відображають $x_j(t)$ на деякому інтервалі. Цей факт дозволяє організувати обчислювальний процес як на основі первинних даних $x_j(t_j)$, $i=\overline{1,n}$ шляхом обробки математичних залежностей, $\varphi(x_j(t), Y_j(t))=0$, де оператор φ визначає математичний зв'язок між вектором $Y_j(t)$ заданих і $x_j(t_j)$ невідомих величин, так і в області диференціальних зображень, шляхом представлення залежності $\varphi(x_j(t), Y_j(t))=0$ у вигляді $\varphi(X_j(k), Y_j(k))=0$.

Високий рівень складності електричних об'єктів і мереж, різноманіття компонентів і можливість їхнього функціонування в широкому спектрі частот, а також зміни станів сприяли появі великої кількості підходів, способів, прийомів, технічних засобів, а надалі комп'ютерних компонентів і мережних технологій рішення сукупності задач керування тяговими електричними мережами залізниць. На рівні тягових підстанцій вирішується набір задач, пов'язаних з технологією керування

електропостачанням, як правило, в автоматичному режимі. Ці задачі пов'язані з реєстрацією первинних даних одним із розглянутих способів, а також організація обробки первинної інформації та передачі і представлення її в реальному часі у відповідній формі необхідним споживачам. Фактично на рівні тягових підстанцій реалізується моніторинг параметрів електричних мереж, включаючи силове устаткування для визначення їхнього стану, реалізації прогнозу і, відповідно, режиму функціонування. На основі первинних даних, визначається відстань L до місця аварії. Обчислення L може бути реалізовано безпосередньо на основі зареєстрованих даних $x_j(t_j)$, $i=\overline{1,n}$, або в області T -зображень, що може бути записано відповідно

$$a = F(I^{K3}, U^{K3}, R_o, Z_\phi, Z_{m\phi}, I_3),$$

$$a(k) = F(I^{K3}(k), U^{K3}(k), R_o(k), Z_\phi(k), Z_{m\phi}(k), I_3(k))$$

де $I^{K3}, U^{K3}, R_o, Z_\phi, Z_{m\phi}, I_3$, – параметри режиму тягової мережі в момент аварії.

Також первинна інформація використовується для визначення залишкового Q_3 ресурс високовольтного обладнання, наприклад, повітряних вимикачів, що може бути реалізовано згідно з виразом

$$Q_3^{\max} = Q - \sum_{i=1}^k I_{\max}^k \tau_k, \quad \text{де } Q - \text{початковий ресурс повітряного}$$

високовольтного вимикача.

На рівні тягових підстанцій також дуже важливим є реалізація моніторингу діелектричних параметрів і стану ізоляції високовольтних тягових трансформаторів, що реалізується шляхом автоматичного контролю стану основної ізоляції по параметрах: зміна тангенса кута діелектричних втрат $\Delta \text{tg} \delta$, ємності $\Delta C/C$ і зміна модуля повної провідності $\Delta Y/Y$. Аналогічно на рівні тягових підстанцій може бути реалізовано комерційний облік електроенергії по тарифах диференційованих за часом доби і т. ін.

Наведені підходи є основою розробки комп'ютерно-орієнтованих методів і мережних комп'ютерних компонентів спеціального призначення для рішення в автоматичному режимі комплексу задач управління технологічним процесом постачання електроенергії на тягу. На основі розроблених комп'ютерних сегментів, кожний із яких виконує моделювання однієї або декілька задач, виникає можливість формування локальної мережі керування тяговою підстанцією і створення на її базі відповідних мережових технологій.

В основу організації корпоративних систем управління електричними мережами залізниць і, відповідно, локальних мереж управління системами електропостачання на рівні тягових підстанцій шляхом організації безперервного контролю параметрів режимів, будемо базуватися на дослідженні спільних властивостей математичних моделей, методів, алгоритмів, особливостей об'єктів функціонування, а також

обчислювальних архітектур і мережних технологій, включаючи вплив зовнішнього середовища. Оскільки спектр задач керування на рівні тягових підстанцій досить широкий, то основну увагу виділимо проблемі, пов'язаній з технологією оперативно-диспетчерського керування тяговими енергетичними системами. Задачі такого типу розв'язуються, в основному, в автоматичному режимі. Комп'ютеризація цих процесів потребує повноти інформації, а в деяких випадках певної її надлишковості. При проведенні безперервного моніторингу параметрів режимів тягових електричних мереж використовується принцип синхронності і єдності вимірювання первинної інформації як основи вибору процедур оперативного керування і забезпечення функціонування розподілених баз даних. Ядром інформатизації процесу оперативно-диспетчерського керування є інтегроване середовище первинних даних, сформоване з єдиних загальносистемних інформаційних позицій у взаємозв'язку з методами обробки даних. Тягові підстанції ЕЧЕ кожної залізниці можуть бути опорними, транзитними або тупиковими і представляють нижній рівень системи електропостачання залізничного транспорту. Цей рівень є домінуючим з точки зору формування первинної інформації, яка відображає параметри режимів електропостачання, захисту інформації, діагностики, контролю та прогнозу технічного стану електричного обладнання. Завдяки тому, що на нижньому рівні формування первинної інформації реалізується з єдиних загальносистемних позицій, то цей підхід закладено в основу для її інтелектуальної обробки і формування на базі результатів обчислень управлінських процедур. Необхідно зазначити, що первинна інформація архівується і згідно з нормативними документами зберігається в необробленому вигляді необхідний термін. Оскільки проблема комп'ютеризації технологічних процесів на рівні тягових підстанцій пов'язана з організацією комерційного обліку електроенергії, розподілом споживання її (залізницями в основному на тягу), транспортуванням електроенергії іншим споживачам, а у деяких випадках і з генерацією електроенергії, то для забезпечення надійності роботи електричного обладнання необхідно реалізувати не тільки постійний моніторинг, а також діагностику, прогноз технічного стану й ідентифікацію аномальних режимів силового електричного обладнання і електричних мереж тягових підстанцій. Комп'ютеризація швидкоплинних технологічних процесів нижнього рівня дозволяє вирішувати автоматично комплекс задач, пов'язаних з реєстрацією і відповідним чином формуванням інтегрованого середовища первинної інформації для організації керуючих впливів і передачі її для подальшого користування на наступних рівнях управління (Рис. 2.30).

Моделювання сукупності задач керування, які необхідно вирішувати на рівні тягової підстанції, може бути реалізовано на основі синтезу локальної комп'ютерної мережі спеціального призначення, схемна реалізація якої наведена на рис. 2.30. В основу логічної структури локальної мережі тягової підстанції використана фізична топологія

«зірка». В якості мережних вузлів використовується сервер локальної мережі, на який покладено комплекс функцій управління роботою компонентів і сегментів мережі, а також формування єдиного інтегрованого середовища первинної інформації, включаючи ряд процедур ведення бази аварійних і комерційних даних.

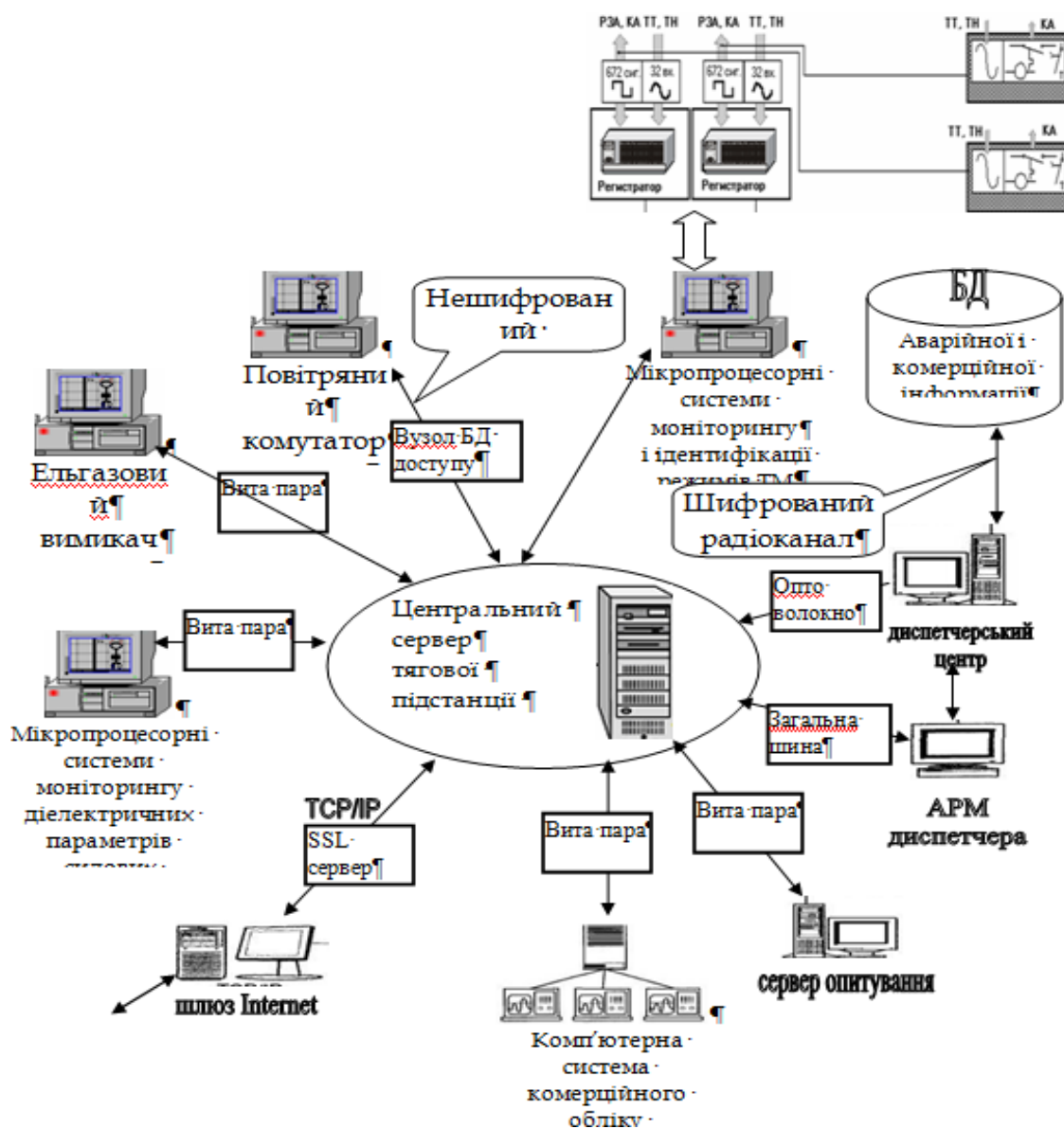


Рис. 2.30. Локальна мережа тягової підстанції залізниць

У зв'язку з тим, що на нижньому рівні комп'ютеризації технологічних процесів, що протікають в електроенергетичних системах в процесі їх моніторингу, можуть накопичуватися великі обсяги первинної інформації, то сервер має бути захищений комплексом апаратно-програмних засобів від несанкціонованого доступу. Крім того, для своєчасної передачі інформації на більш високі рівні керування, сервер локальної мережі має працювати через маршрутизатор віддаленого офісу, який з'єднує локальну мережу з мережею дистанції електропостачання або з корпоративною мережею залізниці. Такі маршрутизатори орієнтовані на масового

споживача, підтримують інтерфейси локальних мереж і низько-швидкісні протоколи. Загальна продуктивність таких маршрутизаторів складає декілька десятків тисяч протоколів в секунду. В локальній мережі тягової підстанції спеціального призначення в якості мережних вузлів використовується: мікропроцесорна система моніторингу і ідентифікації режимів силового електричного обладнання тягових мереж; система моніторингу і визначення запасу ресурсу високовольтних комутаторів струму; мікропроцесорна структура моніторингу діелектричних параметрів високовольтних силових трансформаторів; мікропроцесорний комплекс моніторингу і визначення запасу ресурсу сучасних високовольтних елегазових вимикачів. Для організації роботи локальної мережі тягової підстанції та оперативного обміну первинною інформацією використовується сервер опитування і шлюз Internet, що дозволяє дублювати обмін інформацією між сегментами корпоративної мережі. З метою оперативного керування, в якості мережного термінального вузла включається АРМ диспетчера. При необхідності може бути також АРМ технолога, АРМ організації звітних документів та ін. При достатньо повній комп'ютеризації технологічних процесів на тягових підстанціях в локальну мережу управління включається, в якості мережного сегменту, комп'ютерна система комерційного обліку електроенергії по тарифах диференційованих за зонами доби, як по окремих фідерах, так і по тяговій підстанції в цілому, а при необхідності виконується технологічний облік. Для розвантаження локальної мережі від трафіку передачі інформації можна використовувати мікросегментацію, що реалізується шляхом об'єднання однорідних термінальних вузлів, наприклад, автоматизованих робочих місць у локальній мережі нижнього рівня з топологією «спільна шина». Типи каналів передачі даних вибираються за умовою необхідної швидкості обміну даними, умовної пропускної спроможності, вартості, надійності і зручності експлуатації. Для локальних мереж, у яких реєструються і оброблюються великі обсяги інформації, доцільно використовувати високошвидкісні оптоволоконні лінії, а для вузлів, які не потребують високої швидкості передачі даних, пропонується виту пару або коксиал. Має бути також організований поточний контроль достовірності, цілісності і конфіденційності інформації при її передачі. Відзначимо, що логічна топологія локальної мережі тягової підстанції може гнучко змінюватись залежно від того, який клас задач необхідно розв'язувати в кожний момент часу, що залежить від стану мережі, а також обсягу трафіку, який циркулює в ній. Широкі можливості в плані зміни логічної топології мережі без зміни фізичної з'являються завдяки застосуванню магістральних маршрутизаторів або програмних комутаторів. На цьому рівні виконується також організація первинної інформації із загальносистемних позицій, на базі якої за необхідністю, формується експрес і повної аварійної та комерційної інформації, а також реалізується можливість передачі первинних даних на всі рівні керування.

Запитання для самоконтролю

1. Розкрийте поняття інформаційно-комунікаційної системи.
2. Назвіть основні топології та технології проектування інформаційно-комунікаційних мереж.
3. Сутність випадкового методу доступу до ресурсів системи.
4. У чому полягає відмінність між фізичною і логічною структуризацією мережі?
5. Які основні типи протоколів використовуються в моделі ISO/OSI?
6. Перерахуйте основні функції рівнів моделі ISO/OSI.
7. Дайте визначення поняттю «IP адреса»?
8. Назвіть основні вимоги для проектування більшості мережних проектів.
9. Розкрийте поняття «сегментація» мережі.
10. У яких випадках проектування топології мережі використовується вертикальне чи горизонтальне з'єднання?
11. Назвіть основні особливості та переваги використання віртуальних інформаційно-комунікаційних мереж.
12. Розкрийте концепцію віртуальних інформаційно-комунікаційних мереж.
13. Що являє собою технологія «клієнт-сервер»?
14. Що розуміється під Web-серверними моделями?
15. Назвіть основні види технології «клієнт-сервер».
16. Поясніть поняття «менеджер транзакцій».
17. Для чого використовуються Web-навігатори?
18. Принципи взаємодії Web- навігаторів.
19. Охарактеризуйте повну послідовність кроків, що реалізовується Web-сервером при обробці запиту, що поступив від Web-клієнта?
20. Розкрийте поняття «Java-технологія».
21. Яка різниця між програмами Java Script і Java?
22. Перерахуйте основні способи взаємодії Web-навігатора з сервером СУБД.
23. Як організовуються системи доступу до баз даних?
24. Які перспективи розвитку систем серверної взаємодії?
25. Поясніть схему одноманітного доступу до інформаційних ресурсів мережі.
26. Поняття технології ActiveX.
27. Інформаційні системи на базі ASP.NET технологій.
28. Розкрийте переваги Web-орієнтованих систем, що базуються на клієнт-серверній архітектурі.

Розділ 3. ЗАХИСТ ДАНИХ У БЕЗДРотовИХ СИСТЕМАХ ПЕРЕДАЧІ

3.1. Особливості передачі інформації в бездротових мережах

Інтенсивне збільшення кількості мобільних користувачів інформаційних систем та їх ресурсів ставить перед сучасними технологіями гостру необхідність в оперативному створенні бездротових комунікацій з метою швидкого та якісного обміну даними з територіально рознесеними інформаційними системами та об'єктами.

Бездротові з'єднання між користувачами та бездротова система доступу до глобальних інформаційних ресурсів є показником абсолютного домінування та розвитку інформаційних технологій у всіх сферах життєдіяльності суспільства.

Завдяки активному підключенню користувачів до інформаційно-комунікаційної мережі з довільної точки інтегрованого офісного комплексу або територіально рознесених інформаційних об'єктів (без необхідності комутативного (дротового) з'єднання), робить структуру інформаційної мережі більш гнучкою та мобільною.

Зазначені переваги стосуються оптимальності побудови топології мережі, ефективності використання трафіку, мережного обладнання, організації та впровадження захисту інформаційних ресурсів, тощо.

WI-FI технологія («*Wireless Fidelity*» – «**висока точність безпроводної передачі даних**») – це сучасна бездротова технологія з'єднання мобільних користувачів з інтегрованими глобальними (або локальними) інформаційними мережами та їх ресурсами і послугами.

Сучасний етап розвитку інформаційного суспільства передбачає розвиток цілої системи технічних стандартів *Wi-Fi-технологій*, що вводяться з метою якісної передачі цифрових потоків даних по радіоканалах.

Поширення бездротових мереж, розвиток інфраструктури інформаційно-комунікаційних мереж, поява мобільних технологій із вбудованим бездротовим рішенням (*Intel Centrino*), приводять до глобального поширення використання таких систем. Такі рішення розглядаються насамперед, як засіб розгортання мобільних і стаціонарних бездротових локальних мереж із забезпеченням можливості оперативного доступу до глобальних інформаційних ресурсів.

Особливої актуальності, відносно бездротових мереж, набуває так звані *WLAN-мережі* (*Wireless Local Area Network*). Впровадження таких мереж рекомендовано там, де розгортання кабельної системи неможливе або економічно недоцільно.

Використання бездротових технологій для побудови інформаційних мереж має ряд переваг перед звичайними комутативними технологіями:

– швидкість розгортання мережі та впровадження інформаційно-комунікаційного устаткування;

- мобільність користувачів мережі, користувачі мобільних пристроїв при підключенні до локальних бездротових мереж можуть легко переміщатися в рамках зони радіопокриття;

- відносно висока швидкість обміну даними, що дозволяє використовувати їх для вирішення широкого спектру завдань;

- можливість об'єднання просторово рознесених підмереж в одну спільну мережу там, де комутативне з'єднання підмереж неможливе або недоцільне;

- можливість бездротового підключення до мережних провайдерів та їх послуг;

- бездротова мережа може виявитися єдиним підходом до розв'язання задач проектування та впровадження інформаційної мережі у рамках зазначеної території (географічний регіон, будівля, офіс, спеціалізовані інформаційні задачі тощо).

Однак, необхідно пам'ятати про технічні обмеження, що стосуються технологій побудови безпроводних мереж.

Обмеження, що стосуються процесів проектування бездротових мереж:

- менша швидкість передачі даних порівняно з сучасними комутативними каналами зв'язку;

- необхідність використання підсистеми канального завадостійкого кодування з метою забезпечення вірогідної передачі даних (високий рівень впливу мультиплікативних завад на інформаційні сигнали бездротових мереж);

- застосування спеціальних засобів захисту інформаційних потоків та ресурсів з умов використання системи бездротової передачі.

Технічні пристрої, що входять до складу каналу зв'язку, призначені для того, щоб повідомлення дійшли до споживача найкращим чином – для цього сигнали обробляють та перетворюють згідно з визначеними алгоритмами. Такими перетвореннями сигналу є, наприклад: модуляція і перетворення безперервних сигналів в дискретні. Відповідно до типу сигналів канали поділяють на безперервні та дискретні.

Канал зв'язку є сукупністю технічних методів та засобів, що використовуються з умов організації процесу передачі даних між джерелом повідомлення і споживачем.

Перетворення дискретного повідомлення в інформаційний сигнал каналу зв'язку здійснюється у вигляді операцій – форматування, кодування і модуляції. Кодування є перетворенням повідомлень в послідовність кодових символів, а модуляція – перетворенням цих символів в сигнали, придатні для передачі по інформаційному каналу.

При кодуванні відбувається процес перетворення елементів повідомлень у відповідні їм числа (кодові символи). Кожному елементу повідомлення присвоюється визначена сукупність кодових символів, яка називається *кодовою комбінацією*. Сукупність кодових комбінацій утворює код. Основні показники якості дискретних систем наведені на рис. 3.1.



Рис. 3.1. Основні показники якості дискретних систем зв'язку

У результаті перетворень безперервного сигналу, які називають *дискретизацією* і *квантуванням*, отримують сигнали, що розглядаються, як числа в тій або іншій системі числення, що є дискретними сигналами. Ці числа перетворюють в кодові комбінації електричних сигналів, які і передають по лініях зв'язку, як неперервні. При використанні носієм інформації постійного струму отримують послідовність відео імпульсів. При необхідності цю послідовність модулюють гармонічним коливанням і отримують послідовність радіоімпульсів.

У загальному вигляді модель системи передавання даних представлена на рис. 3.2. Хоча ця модель і містить основні елементи, властиві будь-якій системі передачі інформації, вона може служити лише простою ілюстрацією до опису *інформаційної системи передачі даних*, оскільки практично не відображає тих дій, які повинні (або можуть) виконуватися над інформацією в процесі її передачі від джерела до споживача [100].

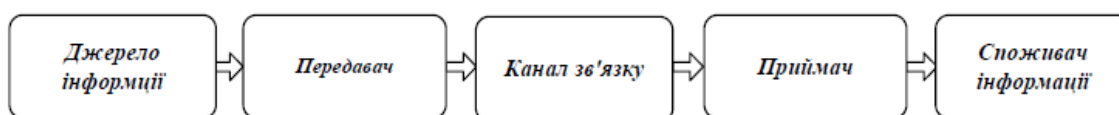


Рис. 3.2. Узагальнена схема передачі даних

Значно повнішою в цьому сенсі є модель системи передачі (і зберігання) інформації, приведена на рис. 3.3. Потрібно відзначити, що насправді проблеми, що виникають при передачі (причому не тільки з використанням радіохвиль) і зберіганні інформації (на оптичних дисках, магнітних носіях і в пам'яті комп'ютерів) схожі, тому методи їх вирішення і структура технічних пристроїв також багато в чому ідентичні.

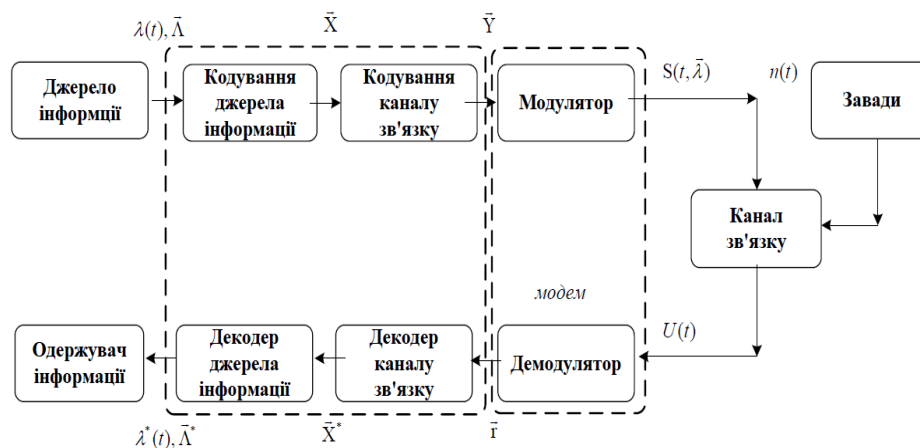


Рис. 3.3. Структурна схема системи передачі інформації

Стисло охарактеризуємо призначення і функції елементів цієї моделі.

1. Джерело інформації або повідомлення – це фізичний об’єкт, система або явище, що формують повідомлення для його передачі від джерела повідомлення до споживача інформації.

Повідомлення – це значення або зміна деякої фізичної величини, що відображає стан об’єкта (системи або явища). Як правило, первинні повідомлення – мова, музика, зображення, вимірювання параметрів навколишнього середовища і т. д. – є функціями часу неелектричної природи. З метою передачі по каналу зв’язку ці повідомлення перетворюються в електричний сигнал, зміни якого в часі (t) відображає повідомлення, що передається. Значна частина таких повідомлень, за своєю природою не є сигналами – це масиви чисел, текстові або інші файли і т. п. Повідомлення такого типу можна подати у вигляді деяких векторів $\bar{L}$.

2. Кодування джерела інформації. Переважна частина інформаційних повідомлень містять в собі надлишкову інформативність та мають повільно змінну частоту, що в загальному випадку погано пристосована для її ефективної передачі по каналах зв’язку. Тому повідомлення ($\lambda(t)$ або $\bar{L}$), як правило, піддаються кодуванню. Процедура кодування включає попередньо дискретизацію безперервного повідомлення $\lambda(t)$, тобто його перетворення в послідовність елементарних дискретних повідомлень $\{\lambda\}$.

Кодування джерела інформації може переслідувати різні цілі: скорочення обсягу переданих даних (стискання даних), збільшення кількості переданої за одиницю часу інформації, підвищення достовірності передачі, забезпечення секретності при передачі і т. д.

Таким чином, на виході кодера джерела по переданому повідомленню $\lambda(t)$ або $\bar{L}$ формується послідовність кодових символів $\bar{X}$, яка називається інформаційною послідовністю, що допускає точне або наближене відновлення початкового інформаційного повідомлення.

3. Кодування в каналах зв'язку. При передачі інформації по каналу зв'язку із завадами в прийнятих даних можуть виникати помилки. Якщо такі помилки невеликі або виникають достатньо рідко, інформація може бути використана споживачем. Якщо отримана інформація містить велику кількість помилок, її не можливо використовувати.

Кодування в каналі, або завадостійке кодування, це спосіб обробки переданих даних, що забезпечує зменшення кількості помилок, які виникають у процесі передачі по каналу з завадами. Існує багато різних методів завадостійкого кодування інформації, але всі вони базуються на наступному: при завадостійкому кодуванні до переданих повідомлень вноситься спеціальним чином організована надлишковість (у послідовності коду, що передається, вводяться надлишкові символи), що дозволяє приймаючій стороні виявляти і виправляти виникаючі помилки. Таким чином, якщо при кодуванні джерела проводиться усунення природної надлишковості, що має місце в повідомленні, то при кодуванні в каналі надлишковість до переданого повідомлення свідомо вноситься. На виході кодера каналу в результаті формується послідовність кодових символів $Y(X)$, яка називається кодовою послідовністю каналу зв'язку.

Потрібно відзначити, що як завадостійке кодування, так і стискання даних не є обов'язковими операціями при передачі інформації. Ці процедури (і відповідні блоки в структурній схемі системи передачі інформації) можуть бути відсутніми. Проте це може призвести до істотних втрат в завадостійкості системи, зменшенню швидкості передачі і зниженню якості передачі інформації. Тому всі сучасні системи включають ефективно та завадостійке кодування даних.

4. Модулятор. Функції модулятора в інформаційних системах передачі даних – це узгодження повідомлення джерела або кодових послідовностей, що виробляються кодером, з властивостями каналу зв'язку і забезпечення можливості одночасної передачі великого числа повідомлень по загальному інформаційному каналу зв'язку.

Дійсно, більшість безперервних $\lambda(t)$ і дискретних $\bar{\lambda}$ повідомлень, що підлягають передачі, а також результати їх кодування – послідовності кодових символів $\bar{X}$ і $\bar{Y}$ – є порівняно низькочастотними сигналами з широкою смугою ($\Delta F < 1 \text{ МГц}$, $\Delta F \sim f_0$). У той же час ефективна передача з використанням електромагнітних коливань (радіохвиль) можлива лише для достатньо високочастотних сигналів ($f_0 > 1 \dots 1000 \text{ МГц}$) з відносно вузько смуговими спектрами ($\Delta F \ll f_0$). Тому модулятор повинен перетворити повідомлення джерела (t) або X відповідні їм кодові послідовності $\bar{X}$ і $\bar{Y}$ в сигнали $S(t, X(t))$, $S(t, Y(A(t)))$ (накласти повідомлення на сигнали), властивості яких забезпечували б її можливість ефективної передачі по радіоканалу (або іншим існуючим каналам зв'язку – телефонним, оптичним і т. д.).

Існує значна кількість методів модуляції сигналів, що забезпечують ефективну та якісну передачу інформації. Найпростішими з них є амплітудна, частотна і фазова модуляції безперервних сигналів.

5. Канал зв'язку – це система передачі інформації, що використовує як носій від джерела до споживача електромагнітні хвилі або радіохвилі, а як середовище розповсюдження – навколишній простір або радіоканал.

Розглянемо інформаційний канал зв'язку у вигляді ланки радіотехнічної системи передачі інформації, на вхід якого поступає сигнал передавача $S(t, \lambda(t))$, а на виході виходить сигнал, який зазвичай називають прийнятим коливанням.

Існує багато моделей інформаційних каналів більшої або меншої складності, проте в загальному випадку сигнал $S(t, Y(\lambda(t)))$, проходячи по каналу зв'язку, піддається ослабленню, набуває деякої часової затримки (або фазове зрушення) і зашумлюється. Коливання $U(t)$, що приймається, в цьому випадку матиме вигляд

$$U(t) = \epsilon S(t - T, Y(\lambda(t))) + n(t), \quad (3.1)$$

де ϵ – згасання, T – часове запізнювання, $n(t)$ – завади в каналі зв'язку.

6. Одержувач інформації. Функції одержувача системи передачі інформації – з максимально можливою точністю по прийнятому коливанню $U(t)$ відтворити на своєму виході передане повідомлення $\lambda(t)$ або $\bar{\lambda}$ з метою подальшого використання для прийняття якісних рішень.

Прийняте (відтворене) повідомлення через завади в загальному випадку відрізняється від переданого. Прийняте повідомлення називатимемо оцінкою (мається на увазі оцінкою повідомлення) і позначатимемо тим же символом, що і відправлене повідомлення, але із знаком: $\lambda^*(t)$ або $\bar{\lambda}$.

7. Демодулятор. Для відтворення оцінки повідомлення $\lambda^*(t)X(t)$ приймач системи повинен по прийнятому коливанню $U(t)$ і з урахуванням відомостей про використані при передачі види сигналу і способи модуляції отримати оцінку кодової послідовності $Y(\lambda^*(t))$, яка називається прийнятою послідовністю $\bar{r}$. Ця процедура називається демодуляцією, детектуванням або прийомом сигналу. При цьому демодуляція повинна виконуватися так, щоб прийнята послідовність $\bar{r}$ в мінімальному ступені відрізнялася від переданої кодової послідовності $\bar{Y}$. Завдання демодуляції прийнятого коливання $U(t)$ співпадає з різними варіантами завдання оптимального прийому сигналу на фоні завад (оптимальне виявлення, оптимальне розрізнення двох або декількох сигналів і т. д.).

8. Декодер каналу зв'язку. Прийняті послідовності $\bar{r}$ в загальному випадку можуть відрізнитися від переданих кодових слів $\bar{Y}$, тобто містити помилки. Кількість таких помилок залежить від рівня завад в каналі зв'язку, швидкості передачі, вибраного для передачі сигналу і способу модуляції, а також від способу прийому (демодуляції) коливання $U(t)$.

Функція декодера каналу зв'язку – виявити і, по можливості, виправити помилки, що виникли при впливі завад та відтворити з максимальним наближенням переданий сигнал від джерела інформації до

споживача. Процедура відтворення повідомлення, виявлення і виправлення помилок в прийнятій послідовності $\bar{r}$ називається декодуванням каналу.

Результатом декодування $\bar{r}$ є оцінка інформаційної послідовності $\bar{X}$. Вибір завадостійкого коду, способу кодування, а також методу декодування повинні проводитися так, щоб на виході декодера каналу залишилося якомога менше не виправлених помилок.

Питанням завадостійкого кодування/декодування в системах передачі (і зберігання) інформації приділяється велика увага, оскільки цей прийом дозволяє істотно підвищити якість її передачі. У багатьох випадках, коли вимоги до достовірності інформації, що приймається, високі (у комп'ютерних мережах передачі даних, в дистанційних системах управління і т. п.), передача без завадостійкого кодування взагалі неможлива.

9. Декодер джерела інформації. Оскільки інформація джерела $(\lambda(t), \bar{L})$ в процесі передачі піддавалася кодуванню з метою її компактнішого (або зручнішого) представлення (стискання даних, економне кодування, кодування джерела), необхідно відновити її до результативного (або початкового вигляду) за прийнятою послідовністю $\bar{X}$. Процедура відновлення $\bar{L}$ по $\bar{X}$ називається декодуванням джерела і може бути зворотною операцією кодування (неруйнівне кодування/декодування), або відновлювати наближене значення $\bar{L}$, що більшою чи меншою мірою відрізняється від $\bar{L}$ (руйнуюче кодування/декодування). До операції відновлення $\bar{L}$ по $\bar{X}$ відноситимемо також відновлення, якщо в цьому є необхідність, безперервної функції $\lambda^*(t)$ за набором дискретних значень оцінок $\bar{L}$.

Таким чином, коротко розкривши загальну структуру інформаційної системи передачі даних, перейдемо до детальнішого вивчення її основних елементів.

3.2. Завадостійкі способи кодування в каналах бездротового зв'язку

У системах та мережах бездротового зв'язку найпоширенішим методом завадостійкого кодування є використання кодів згортання, при яких вхідна послідовність інформаційних бітів перетворюється в спеціальному кодері згортання таким чином, щоб кожному вхідному біту відповідало більш, як один вихідний. Тобто, кодер згортання додає певну надлишкову інформацію до вихідної послідовності з умов забезпечення цілісності і достовірності інформаційного повідомлення [40].

Будь-який кодер згортання будується на основі кількох послідовно зв'язаних комірок з пам'яттю та логічних елементах, що зв'язують ці комірки між собою. Кількістю комірок визначається кількість можливих станів кодера.

Річ у тому, що у разі надлишковості кодування навіть при виникненні помилок прийому, вихідну послідовність бітів можна безпомилково відновити. Для відновлення вихідної послідовності бітів на стороні приймача застосовується декодер Вітербі.

Існує три найбільш поширених методи боротьби з помилками в процесі передачі даних в бездротових мережах:

- коди виявлення помилок;
- коди з корекцією помилок, які називають також схемами прямої корекції помилок (Forward Error Correction – FEC);
- протоколи з автоматичним запитом повторної передачі (Automatic Repeat Request – ARQ).

Код виявлення помилок дозволяє досить легко встановити наявність помилки. Як правило, подібні коди використовуються спільно з певними протоколами канального або транспортного рівнів, що мають схему ARQ. Схеми FEC часто використовуються в бездротовій передачі, де повторна передача не ефективна, а рівень помилок досить високий.

Технології виявлення помилок. Технології виявлення помилок засновані на передачі в складі блоку даних надлишкової службової інформації, за якою можна судити з деякою мірою вірогідності про достовірність прийнятих даних.

Контроль по паритету є найбільш допустимим методом контролю даних. У той же час це найменш потужний алгоритм контролю, оскільки з його допомогою можна виявити лише одиночні помилки в даних, що перевіряються. Метод полягає в підсумовуванні по модулю 2 всіх бітів контрольованої інформації. Таким чином можна відмітити, що для інформації, що складається з непарного числа одиниць, контрольна сума завжди дорівнює 1, а при парному числі одиниць – 0. Наприклад, для даних 100101011 результатом контрольного підсумовування буде значення 1. Зрозуміло, що результатом підсумку є додатковий біт даних, який пересилається разом з контрольованою інформацією. При спотворенні в процесі пересилки будь-якого біта вихідних даних (або контрольного розряду) результат підсумовування відрізнятиметься від прийнятого контрольного розряду, що говорить про помилку відновлення кодової конструкції. Проте подвійна помилка, наприклад 110101010, буде невірно прийнята за коректні дані. Тому контроль по паритету застосовується до невеликих порцій даних, як правило, до кожного байта, що дає коефіцієнт надмірності для цього методу 1/8. Метод рідко застосовується в комп'ютерних мережах через значну надмірність і невисокі діагностичні здібності.

Вертикальний і горизонтальний контроль по паритету є модифікацією описаного вище методу. Його різниця полягає в тому, що вихідні дані розглядаються у вигляді матриці, рядки якої складають байти даних. Контрольний розряд підраховується окремо для кожного рядка і для стовпця матриці. Цей метод виявляє значну частину подвійних помилок, проте володіє ще більшою надмірністю.

Циклічний надлишковий контроль (Cyclic Redundancy Check – CRC)

– на даний час, найбільш популярний метод контролю в обчислювальних мережах (і не лише в мережах; даний метод широко використовується у технологіях стискування інформації при її збереженні на жорстких дисках). Метод заснований на обробці вихідних даних у вигляді одного багаторозрядного двійкового числа. Наприклад, кадр стандарту Ethernet, що складається з 1024 байт, розглядатиметься, як одне число, що складається з 8192 біт. Контрольною інформацією вважається залишок від ділення цього числа на заздалегідь відомого дільника R . Зазвичай, як дільник вибирається сімнадцяти або тридцятитрьох розрядне число, щоб залишок від ділення мав довжину 16 розрядів (2 байт) або 32 розряди (4 байт). При відновленні кадру даних, знову обчислюється залишок від ділення на зазначене число R , але при цьому до даних кадру додається і контрольна сума, що міститься в ньому. Якщо залишок від ділення на R дорівнює нулю, то робимо висновок про відсутність помилок в отриманому кадрі, інакше кадр вважається спотвореним.

Визначений метод має найвищу обчислювальну складність, але його діагностичні можливості набагато ширші, ніж в методі контролю по паритету. Метод CRC виявляє всі одиночні помилки, подвійні помилки і помилки в непарному числі бітів. Метод також має невисоку міру надмірності. Наприклад, для кадру Ethernet розміром 1024 байти контрольна інформація завдовжки 4 байти складає лише 0,4 %.

Методи корекції помилок.

Методом прямої корекції помилок (Forward Error Correction – FEC) називається техніка завадостійкого каналного кодування, яка дозволяє приймачу ідентифікувати помилки в інформаційному потоці даних, а також надає можливість провести корекцію й їх виправлення. Коди, що забезпечують пряму корекцію помилок, вимагають введення більшої надлишковості в інформаційний потік даних, ніж коди, які лише виявляють помилки.

При використанні будь-якої надлишковості не всі комбінації коду є дозволеними. Наприклад, контроль по паритету робить дозволеними лише половину кодів. Якщо ми контролюємо три інформаційних біта, то дозволеними 4-битніми кодами з доповненням до непарної кількості одиниць будуть: 000 1, 001 0, 010 0, 011 1, 100 0, 101 1, 110 1, 111 0, тобто всього 8 біт з 16 можливих. Для того, щоб оцінити кількість додаткових бітів, необхідних для виправлення помилок, потрібно знати, так звану відстань Хеммінга між дозволеними комбінаціями кодів.

Відстанню Хеммінга називається мінімальне число бітових розрядів, якими відрізняється будь-яка пара дозволених кодів. Для схем контролю по паритету відстань Хеммінга дорівнює 2 [99-111].

Можна довести, якщо надлишковий код з відстанню Хеммінга рівною n , то такий код буде в здатен розпізнавати $(n-1)$ кратні помилки і виправляти $(n-1)/2$ – кратні помилки. Оскільки коди з контролем по

паритету мають відстань Хеммінга рівну 2, вони можуть лише виявляти однократні помилки і не можуть їх виправляти.

Коди Хеммінга ефективно виявляють і виправляють ізольовані помилки, тобто окремі спотворені біти, які розділені великою кількістю коректних бітів. Проте при появі довгої послідовності спотворених бітів (пульсації помилок) коди Хеммінга не працюють.

Найчастіше в сучасних системах зв'язку застосовується тип кодування, що реалізовується кодуючим пристроєм згортання (Convolutional coder), бо таке кодування неважко реалізувати апаратно з використанням ліній затримки (delay) і суматорів. Коди згортання відносяться до кодів з пам'яттю (Finite memory code); це означає, що вихідна послідовність кодера є функцією не лише поточного вхідного сигналу, але також декількох бітів з числа останніх чи попередніх кодових слів. Довжина кодового обмеження (Constraint length of a code) показує, як багато вихідних елементів виходить з системи в перерахунку на один вхідний. Коди часто характеризуються їх ефективним ступенем (або коефіцієнтом) кодування (Code rate). Коефіцієнт кодування (наприклад, 1/2) вказує, що на кожен вхідний біт приходить два вихідних.

У бездротових системах з блоковими кодами широко використовується метод чергування блоків. Перевага чергування полягає у тому, що приймач розподіляє пакет помилок, що спотворив деяку послідовність бітів, по числу блоків. Чергування виконується за допомогою читання і запису даних в різному порядку, завдяки чому стає можливим виправлення помилок. Якщо під час передачі на пакет впливають перешкоди, то всі ці біти виявляються рознесеними по різних блоках. Отже, будь-яка контрольна послідовність може виправити лише невелику частину від загальної кількості інвертованих бітів.

Методи автоматичного запиту повторної передачі. В простому випадку захист від помилок полягає лише в їх виявленні. Система повинна попередити передавач про виявлення помилки, а також при необхідності повторної передачі. Такі процедури захисту від помилок відомі, як методи автоматичного запиту повторної передачі (Automatic Repeat Request – ARQ). В безпроводних локальних мережах застосовується процедура «запиту ARQ із зупинками» (stop-and-wait ARQ).

У даному випадку джерело інформації (повідомлення) чекає підтвердження (Acknowledgement – ACK), або, як ще його називають, квитанції, від приймача і лише після цього посилає наступний кадр. Якщо ж підтвердження не приходить протягом певного часу, то кадр вважається загубленим і його передача повторюється. На рис. 3.4 видно, що у цьому випадку продуктивність обміну даними нижче потенційно можливої; хоча передавач міг би послати наступний кадр відразу ж після відправки попереднього, він зобов'язаний чека ти отримання підтвердження.

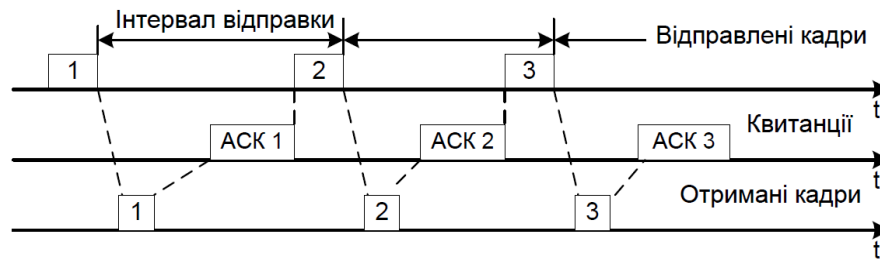


Рис. 3.4. Процедура запитів ARQ із зупинками

3.3. Організація мереж бездротового зв'язку

Основні елементи мережі. Для побудови бездротових мереж використовуються мережні адаптери, комутаційне обладнання та точки доступу.

Мережним адаптером є пристрій, який підключається через порт розширення PCI, PCMCIA, Compact Flash. Існують також адаптери з підключенням через порт USB 2.0. Бездротовий Wi-Fi адаптер виконує таку ж саму функцію, що і мережна карта в дротовій мережі. Він застосовується для підключення комп'ютера користувача до бездротової мережі. Завдяки платформі: Centrino, усі сучасні ноутбуки мають вбудовані адаптери Wi-Fi, що сумісні з багатьма сучасними стандартами. Wi-Fi адаптерами, як правило, забезпечені і КПК (кишенькові персональні комп'ютери), що також дозволяє підключати їх до бездротових мереж.

З умов організації системи доступу до бездротової мережі, адаптер може встановлювати зв'язок безпосередньо з іншими адаптерами мережі. Така мережа називається бездротовою одноранговою мережею або Ad Hoc мережею. Адаптер також може встановлювати зв'язок через спеціальний пристрій – точку доступу. Такий режим називається інфраструктурою. Для вибору варіанту підключення адаптер має бути налаштований на використання або Ad Hoc, або інфраструктурного режиму (детально дана технологія розглянута нижче).

Точка доступу є автономним модулем з вбудованим мікрокомп'ютером і приймально-передавальним пристроєм.

Через точку доступу здійснюється взаємодія й обмін інформацією між бездротовими адаптерами, а також зв'язок з комутативними сегментами мережі. Таким чином, точка доступу відіграє роль загального комутатора мережі.

Точка доступу повинна мати мережевий інтерфейс (uplink port), за допомогою якого вона може бути підключена до звичайної комутативної (комп'ютерної) мережі. Через цей же інтерфейс здійснюється налаштування точки доступу на визначені для неї функції і сервіси.

Точка доступу може використовуватися, як для підключення до неї клієнтів (базовий режим точки доступу), так і для взаємодії з іншими точками доступу з метою побудови розподіленої мережі (Wireless Distributed System – WDS). Цей режим носить назву бездротового мосту «точка – точка» і «точка – багато точок».

Доступ до мережі забезпечується шляхом передачі широкомовних сигналів через ефір. Приймаюча станція може отримувати сигнали в діапазоні роботи декількох передавальних станцій. Станція-приймач використовує ідентифікатор зони обслуговування (Service Set Identifier – SSID) для фільтрації отримуваних сигналів і виділення безпосередньо потрібних.

Зоною обслуговування (Service Set – SS) називаються логічно згруповані пристрої, що забезпечують підключення до бездротової мережі.

Базова зона обслуговування (Basic Service Set – BSS) – це група станцій, які пов'язані одна з одною на основі технологій бездротового зв'язку. Технологія BSS передбачає наявність особливої станції, яка називається точкою доступу (access point).

Станція інформаційної мережі бездротового зв'язку – це комп'ютер або інший периферійний пристрій, мережне устаткування, підключене до бездротової мережі через внутрішній або зовнішній бездротовий адаптер мережного інтерфейсу.

Маршрутизатори (Routers). Бездротові маршрутизатори працюють, як «ворота», між зовнішньою глобальною мережею та внутрішніми локальними чи корпоративними мережами. Вони розподіляють трафік між певною комутативною мережею і глобальною. Більшість із них мають вбудований адаптер, що автоматично призначає IP-адресу кожному комп'ютеру всередині визначеної мережі. Окремий мережний вхід з'єднує маршрутизатор із зовнішньою мережею, даючи змогу користувачам розділяти з'єднання з глобальною мережею. Більшість маршрутизаторів має вбудовану апаратно-програмну систему захисту інформації (firewall) та інші спеціальні функції для підвищення безпеки бездротової мережі [24, 106].

Комутатори бездротової мережі (Switches and hubs). Ethernet-технологія – це основа кожної інформаційної мережі. При підключенні додаткових елементів мережі використовуються звичайні Ethernet-комутатори. Практично кожний сучасний комп'ютер має вбудований Ethernet-адаптер. Відповідно, більшість бездротових маршрутизаторів мають вбудовані три або чотири Ethernet-порти. Switches і hubs можуть підтримувати безліч з них без значного зменшення швидкості зв'язку для кожного. Багато точок доступу й більшість бездротових мережних адаптерів мають вбудовані всебічноспрямовані антени. У більшості ситуацій, ці вбудовані антени слугують для здійснення процесу передачі та прийому інформаційного потоку даних між точкою доступу й найближчим користувачем (рис. 3.5).

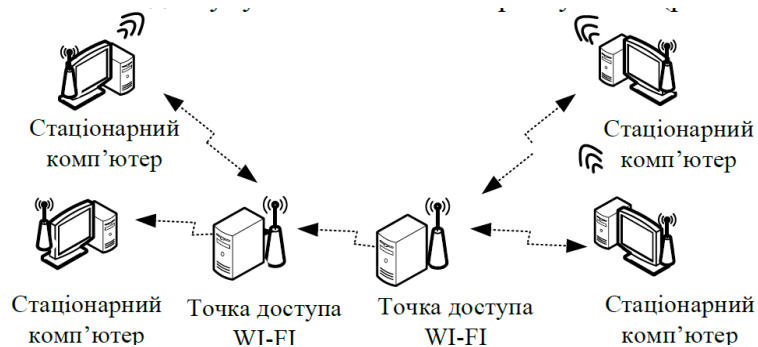


Рис. 3.5. Методика обміну даними через точку доступу

Під час зв'язку між базовою станцією та бездротовим мережним адаптером беруть участь дві антени – по одній на кожному кінці. На кожному з них антена з високим коефіцієнтом підсилення впливає на якість сигналу, тому ефективною може бути заміна стандартної антени на спрямовану в точці доступу або на мережному інтерфейсі. Спрямовані антени можуть забезпечити значне поліпшення якості сигналу у вузькій зоні покриття. Крім того, вони здатні зменшити вплив завад від бічних зон за межами пелюстка спрямованості антени.

Бездротові мережі Wi-Fi підтримують декілька різних режимів роботи, що реалізуються для конкретних цілей. Рівень доступу до середовища передачі даних називають MAC-рівнем (або підрівнем – Media Access Control) каналного рівня. Саме на MAC-рівні встановлюються правила спільного використання середовища передачі даних одночасно кількома вузлами бездротової мережі.

MAC-рівень визначає два основні типи архітектури та режими роботи бездротових мереж:

- локальні бездротові Ad-Нос-мережі;
- інфраструктурні мережі (Infrastructure Mode).

Локальною бездротовою мережею (Ad-Нос) називається мережа, яка являє собою автономну групу станцій, що працює без підключення до глобальних мереж передачі даних. Вона містить дві або більше бездротових станцій без використання точок доступу. Ad-Нос-мережі також називаються одноранговими й незалежними базовими наборами служб. У режимі Ad-Нос (рис. 3.6), який називають також незалежним базовим обслуговуванням (Independent Basic Service Set-IBSS), або режимом типу «точка-точка» (Point to Point), станції взаємодіють безпосередньо.

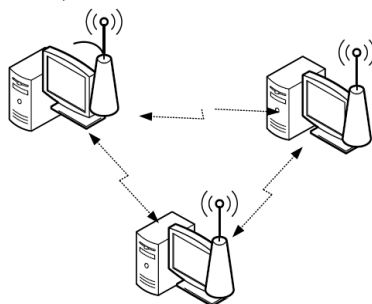


Рис. 3.6. Локальна бездротова мережа з Ad-Нос режимом

Ad-Нос-режим: однорангова взаємодія типу «точка – точка». Користувачі (комп'ютери) здійснюють обмін інформаційними повідомленнями без застосування точок доступу.

У режимі Ad-Нос клієнти встановлюють зв'язок безпосередньо один із одним. Встановлюється однорангова взаємодія за типом «точка-точка», і користувачі взаємодіють безпосередньо без використання точок доступу. При цьому створюється одна зона обслуговування, що не має інтерфейсу для підключення до локальної мережі.

Для цього режиму потрібен мінімум устаткування: кожна станція має бути оснащена бездротовим адаптером. За такої конфігурації немає потреби створювати мережеву інфраструктуру. Основними недоліками режиму Ad-Нос є обмежений діапазон можливостей цієї мережі та неможливість підключення до зовнішньої мережі (наприклад, до Інтернету). Основна перевага даного режиму – простота організації: він не вимагає додаткового устаткування (точки доступу). Режим може застосовуватися для створення тимчасових локальних мереж передачі даних.

Необхідно мати на увазі, що режим Ad-Нос дозволяє встановлювати з'єднання на швидкості не більше 11 Мбіт/с, незалежно від використовуваного устаткування. Реальна швидкість обміну даними буде нижча і складе не більш $11/N$ Мбіт/с, де N – число пристроїв в мережі. Дальність зв'язку складає не більше ста метрів, а швидкість передачі даних швидко падає із збільшенням відстані.

Режим Infrastructure Mode. Інфраструктурною бездротовою мережею називається мережа, яка являє собою групу станцій, що працює з підключенням до глобальних мереж передачі даних та інформаційних ресурсів з використанням однієї або більше точок доступу.

Кожна бездротова станція обмінюється повідомленнями та даними з точкою доступу, що передає їх на інші вузли у комутативній мережі. Будь-яка мережа, що вимагає комутативного підключення через точку доступу до периферійного устаткування, файлового сервера або інтернет-шлюзу, є *інфраструктурною*. Інфраструктурну мережу зображено на рис. 3.7.

Базовим набором служб називається інфраструктурна мережа, що використовує тільки одну базову станцію для забезпечення прийому та передачі інформаційних потоків даних.

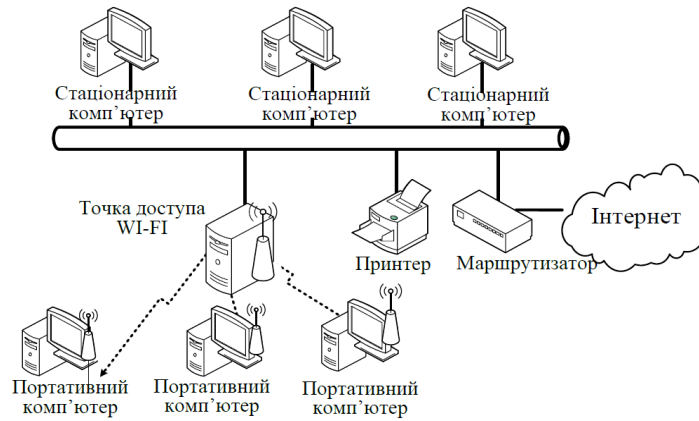


Рис. 3.7. Інфраструктурна бездротова мережа з комутацією через точку доступу до стандартної мережі

Розширеним набором служб називається інфраструктурна бездротова мережа, що використовує дві або більше точок доступу для забезпечення прийому та передачі інформаційних потоків даних.

Крім двох різних режимів функціонування бездротових мереж на каналному рівні ISO/OSI визначаються правила колективного доступу до середовища передачі даних. Необхідність існування таких регламентуючих правил цілком очевидна при організації системи передачі даних, одночасно кожному вузлу бездротової мережі. У результаті інтерференції кількох таких сигналів, базові вузли не можуть одержати та ідентифікувати адресу переданих даних. Саме тому необхідне існування твердих регламентуючих правил, які визначали б колективний доступ до середовища передачі даних.

На рівні каналу визначаються два типи колективного доступу до середовища передачі даних:

- функція розподіленої координації (Distributed Coordination Function – DCF);
- – функція централізованої координації (Point Coordination function – PCF).

Функція розподіленої координації (DCF) – метод, що дає змогу знизити ймовірність виникнення колізій та одночасно гарантує всім вузлам мережі рівноправний доступ до середовища передачі даних.

Зазначені методи координації ґрунтуються на організації колективного доступу до інформаційних ресурсів з виявленням частоти носія інформаційного сигналу з умов використання алгоритму запобігання колізіям (Carrier Sense Multiple Access/Collision Avoidance, CSMA/CA). За такої організації кожен вузол перш ніж почати передачу, «прослуховує» середовище, намагаючись виявити наявність сигналу, і тільки за умови, що середовище вільне, починає передачу даних.

Однак, у цьому разі велика ймовірність виникнення колізій: коли два або більше вузлів мережі одночасно (або майже одночасно) виявлять, що середовище вільне і почнуть передавати інформаційні повідомлення. Для

зниження ймовірності виникнення таких ситуацій використовується механізм запобігання колізіям (Collision Avoidance – CA).

Суть цього механізму полягає у тому, що кожний вузол мережі, переконавшись, що середовище вільне, перш ніж почати передачу, очікує дозволу протягом певного проміжку часу. Цей проміжок є випадковим і складається з двох складових: обов'язкового проміжку (DCF Interframe Space) і вибраного у випадковий спосіб проміжку зворотного відліку. У результаті кожний вузол мережі перед початком передачі очікує протягом випадкового проміжку часу отримання дозволу на саму передачу. Зазначена затримка у роботі значно знижує ймовірність виникнення колізій, оскільки ймовірність того, що два вузли мережі будуть очікувати протягом того самого проміжку часу, надзвичайно мала.

Для того, щоб гарантувати всім вузлам мережі рівноправний доступ до середовища передачі даних, необхідно відповідним чином визначити алгоритм вибору тривалості проміжку зворотного відліку (backoff time). Проміжок зворотного відліку хоч і є випадковим, але визначається на підставі деяких дискретних проміжків часу, тобто дорівнює цілому числу – кількості елементарних часових проміжків, названих тайм-слотами (Time Slot). Для вибору проміжку зворотного відліку кожний вузол мережі формує так зване *вікно конкурентного доступу* (Contention Window – CW), що використовується для визначення кількості тайм-слотів, протягом яких станція очікувала перед початком передачі. Фактично вікно CW – це діапазон для вибору кількості тайм-слотів, причому мінімальний розмір вікна визначається в 31 тайм-слот, а максимальний розмір – в 1023 тайм-слоти. Проміжок зворотного відліку визначається, як кількість тайм-слотів, залежна від розміру вікна CW:

$$\text{Back off time } [CW_{\min}, CW_{\max}] \times \text{Slot time.}$$

Коли вузол мережі намагається одержати доступ до середовища передачі даних, то після неодмінного проміжку очікування запускається процедура зворотного відліку. Тобто, включається зворотний відлік лічильника тайм-слотів, починаючи від вибраного значення вікна CW. Якщо протягом усього проміжку очікування середовище залишається вільним (лічильник зворотного відліку дорівнює нулю), то вузол починає передачу.

Після успішної передачі вікно CW формується знову. Якщо за час очікування передачу почав інший вузол мережі, то зворотний відлік лічильника припиняється, а передача даних відкладається. Тільки після того, як середовище стане вільним, цей вузол знову почне процедуру зворотного відліку, але вже з меншим розміром вікна CW. Зрозуміло, що даний розмір вікна затримки визначається попереднім значенням лічильника зворотного відліку і, відповідно встановлюється меншим за значенням часу очікування.

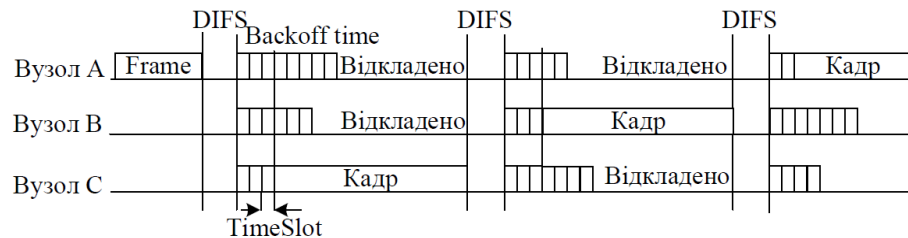


Рис. 3.8. Реалізація рівноправного доступу до середовища передачі даних у методі DCF

При цьому очевидно, що чим більшу кількість разів вузол відкладає передачу через зайнятість середовища, тим вища ймовірність того, що наступного разу він одержить доступ до середовища передачі даних (рис. 3.8). Розглянутий алгоритм реалізації колективного доступу до середовища передачі даних гарантує рівноправний доступ усіх вузлів мережі до середовища. Однак, за такого підходу, ймовірність виникнення колізій хоча й мала, але однак існує. Зрозуміло, що знизити ймовірність виникнення колізій можна, збільшивши максимальний розмір формованого вікна CW. Проте у цьому разі збільшується час затримок при передачі й тим самим знижується продуктивність бездротової мережі.

Інтеграція бездротового сегмента. Бездротова інформаційна мережа потребує специфічного набору компонентів комунікаційного обладнання на відміну від стандартної дротової мережі. Найбільш істотна відмінність полягає у відсутності комутативного з'єднання між сервером мережі, комп'ютерами бездротових клієнтів та інших пристроїв, що формують загальну інфраструктуру мережі. Інтерфейс бездротової мережі між дротовою та бездротовою частинами має використовувати радіопередавачі й приймачі для забезпечення проходження інформаційних потоків даних.

Питання вибору конфігурації. Для вибору конфігурації бездротової мережі передусім необхідно виміряти рівень сигналу на певній території та з огляду на вже наявну мережну інфраструктуру скласти проект майбутньої мережі. За наявності стандартної комутаційної мережі з виходом до глобальних інформаційних ресурсів та функціонуванням серверів, робочих станцій, мережних принтерів й т. ін., рекомендовано зберегти відповідну інфраструктуру, лише доповнивши її бездротовими можливостями. У такому разі застосовується одна або кілька точок доступу, що працюють у режимі інфраструктурної бездротової мережі (Infrastructure Mode). Дане устаткування повинно використовуватись для об'єднання всіх бездротових пристроїв з утворенням прозорого мосту між бездротовим і дротовими сегментами мережі. При цьому кожна точка має підключатися до порту дротового комутатора/маршрутизатора.

Якщо використовуються декілька не пов'язаних між собою і розташованих на різних територіях сегментів дротової мережі, їх можна зв'язати за допомогою додаткових точок доступу, які працюють у режимі *мультиплексного мосту «Wireless/Multiple Bridge»* (рис. 3.9), призначеному для об'єднання двох і більше сегментів дротових мереж.

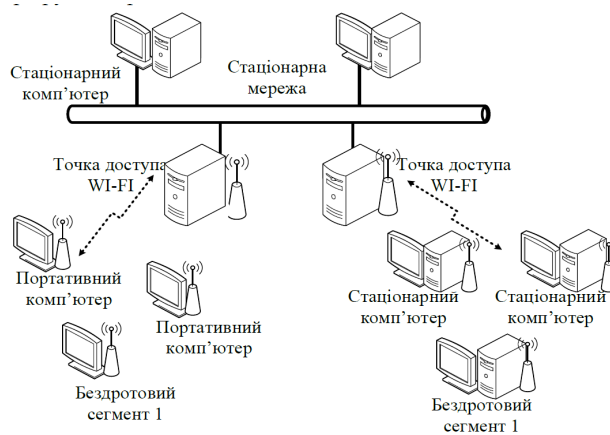


Рис. 3.9. Режим мультиплексорного мосту для об'єднання двох і більше сегментів дротових мереж

Для поліпшення якості сигналу можна скористатися зовнішніми додатковими антенами: вузько-спрямованою для з'єднання в зоні прямого бачення (коли необхідно, щоб сигнал поширювався в одному напрямі) та всебічно-спрямованою (коли необхідно збільшити зону покриття у приміщенні).

Більшість бездротових мережних інтерфейсних адаптерів виконують тільки одну функцію: вони здійснюють обмін даними між комп'ютером і мережею.

Бездротовий доступ до дротової мережі. Будь-яка точка доступу може виступати, як базова станція, поповнюючи наявну дротову мережу бездротовим зв'язком (рис. 3.10) [40, 63]. Точка доступу забезпечує такий самий зовнішній вигляд іншої частини мережі, як і додатковий комутатор (хаб або світч), що з'єднує дротові вузли. У такому різновиді інтегрованої мережі кожний пристрій може здійснювати обмін даними з будь-яким іншим мережним вузлом, незалежно від способу підключення. При цьому не має значення в який спосіб, за допомогою дротового чи радіозв'язку, підключено конкретне комунікаційне устаткування до мережі.

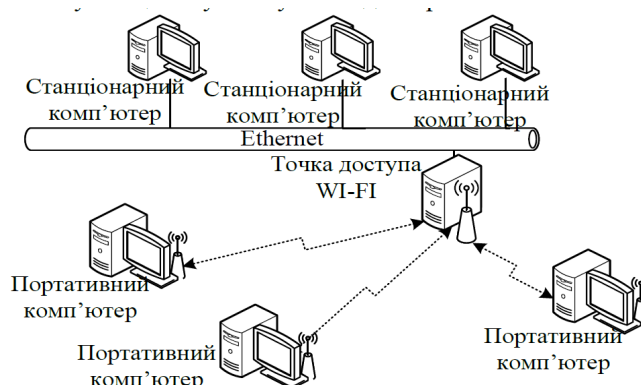


Рис. 3.10. Інтеграція бездротових сегментів до стандартної мережі

У комбінованій структурі мережі, що містить як дротові підключення, так і бездротові зв'язки, найкращим способом функціонування системи може стати використання окремих пристроїв, що поєднують функції

бездротової точки доступу із дротовим хабом або світчем (рис. 3.11). Такий тип точки доступу іноді описується, як *широкосмуговий маршрутизатор*. Головними перевагами комбінування точки доступу та хаба є зручність їх використання для малих локальних бездротових мереж. Комбінована одиниця може також стати найшвидшим способом розширення наявної мережі з додаванням як дротових так і бездротових вузлів у віддаленому місці розташування.

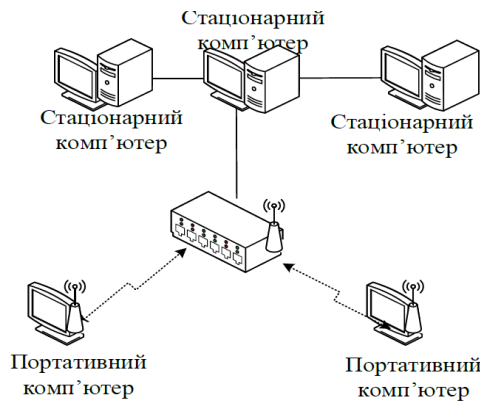


Рис. 3.11. Використання типу точки доступу, як широкосмугового маршрутизатора

Широкосмуговий шлюз являє собою точку доступу, яка містить та використовує порт для безпосереднього підключення до DSL-передавача або кабельного модему, що підтримує високошвидкісний доступ до глобальної мережі (рис. 3.12).

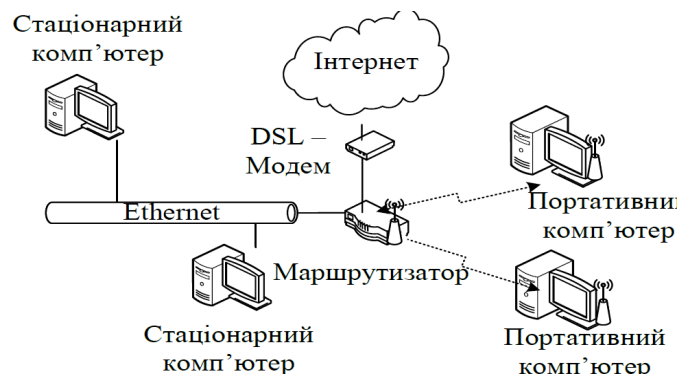


Рис. 3.12. Режим – широкосмуговий шлюз для змішаної мережі

Деякі шлюзові пристрої містять кілька Ethernet-портів для комутаційних підключень до локальних комп'ютерів. Такий підхід особливо ефективний для найбільш розгалуженої комбінованої інформаційної мережі.

Режими WDS і WDS WITH AP. Термін WDS (Wireless Distribution System) розшифровується як «розподілена бездротова система». У цьому режимі точки доступу з'єднуються лише між собою, утворюючи мостове з'єднання. При цьому кожна точка може з'єднуватися з декількома іншими точками. Всі точки у цьому режимі повинні використовувати один і той же

канал, тому кількість точок, що беруть участь в утворенні моста, не повинна бути надмірно великим. Підключення клієнтів здійснюється лише по дротовій мережі через uplink-порти точок (рис. 3.13).

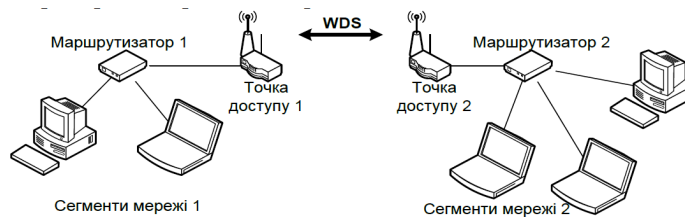


Рис. 3.13. Складний мостовий режим

Режим бездротового моста, аналогічний дротовим мостам, призначений для об'єднання підмереж в спільну мережу. За допомогою бездротових мостів можна об'єднувати проводові LAN, що знаходяться як в сусідніх будівлях, так і на відстані до декількох кілометрів. Це дозволяє об'єднати в мережу філії і центральний офіс, а також підключати клієнтів до мережі провайдерів Internet (рис. 3.14).

Бездротовий міст може використовуватися там, де прокладання кабелю між будівлями неможливе. Дана реалізація дозволяє досягти значної економії засобів і забезпечує простоту налаштування і гнучкість конфігурації при переміщенні офісів.

До точки доступу, що працює в режимі моста, підключення бездротових клієнтів неможливе. Бездротовий зв'язок здійснюється лише між парою точок, що реалізують міст.

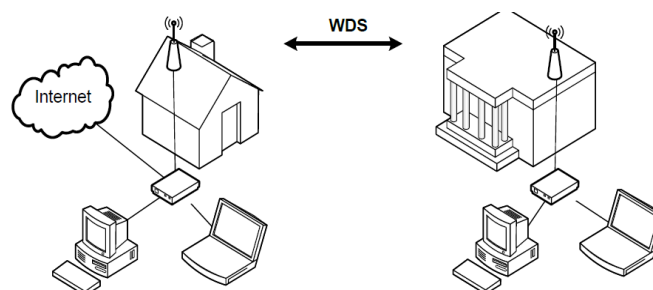


Рис. 3.14. Мостовий режим між будівлями WDS Internet

Термін WDS with AP (WDS with Access Point) означає «розподілена бездротова система, що включає точку доступу», тобто за допомогою цього режиму можна не лише організувати мостовий зв'язок між точками доступу, але і одночасно підключити клієнтські комп'ютери (рис. 3.15). Даний підхід дозволяє досягти істотної економії устаткування і спростити топологію мережі. Зазначена технологія підтримується більшістю сучасних точок доступу. Проте необхідно пам'ятати, що всі пристрої у складі однієї WDS with AP працюють на одній частоті і створюють взаємні перешкоди, що обмежує кількість клієнтів до 15-20 вузлів. Для збільшення кількості клієнтів, що підключаються, можна використовувати декілька

WDS-мереж, налаштованих на різні канали і поєднаних кабелем через uplink-порти [106].

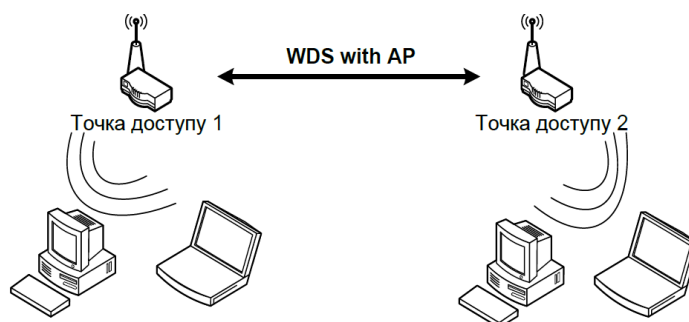


Рис. 3.15. Режим WDS with AP

Топологія організації безпроводних мереж в режимі WDS аналогічна звичайним дротовим топологіям.

Режим повторювача. При роботі точки доступу з клієнтами може виникнути ситуація коли виявляється неможливо з'єднати точку доступу з дротовою інфраструктурою, або присутні деякі перешкоди, що безпосередньо утрудняють здійснення зв'язку точки доступу з місцем розташування бездротових станцій клієнтів. У такій ситуації можна використовувати точку доступу в режимі повторювача (Repeater) (рис. 3.16).

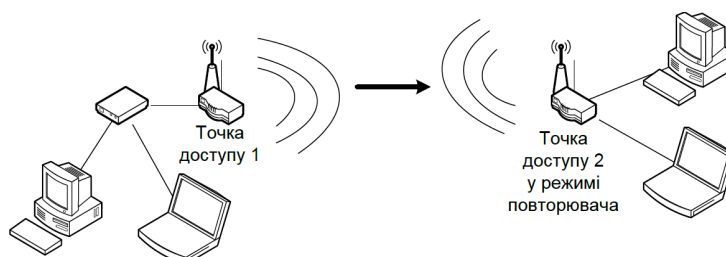


Рис. 3.16. Режим повторювача

Аналогічно дротовому повторювачу, бездротовий повторювач просто ретранслює всі пакети інформаційного потоку. Ця ретрансляція здійснюється через той же канал, через який вони були отримані.

При використанні точки доступу в режимі повторювача (ретранслятора) слід пам'ятати, що накладення широкомовних доменів може привести до скорочення пропускної спроможності каналу удвічі, бо початкова точка доступу також приймає сигнал, що ретранслюється.

Режим повторювача не включений в стандарт 802.11, тому для його реалізації рекомендується використовувати однотипне устаткування одного виробника. З появою WDS даний режим втратив свою актуальність.

Режим клієнта. При переході від комутаційної архітектури до бездротової інколи можна виявити, що наявні мережні пристрої підтримують дротяну мережу Ethernet, але не мають стандартних інтерфейсних роз'ємів комутаційного устаткування для бездротових

мережних адаптерів. Для підключення таких пристроїв до бездротової мережі можна використовувати точку доступу «клієнт» (рис. 3.17). За допомогою точки доступу, що функціонує в режимі клієнта, до бездротової мережі підключається лише один пристрій. Цей режим не включений в стандарт 802.11 і підтримується не всіма виробниками.

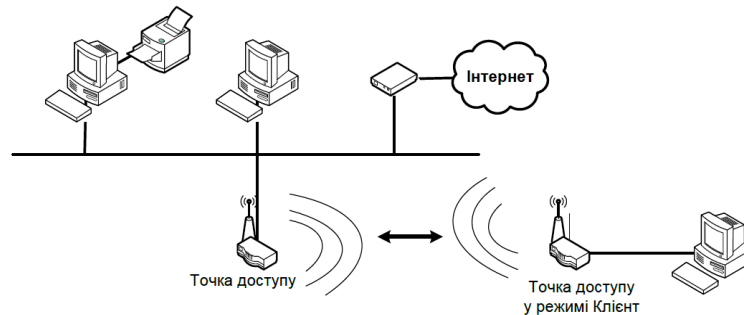


Рис. 3.17. Режим клієнта

Топологія бездротової мережі – «шина». Топологія типу «шина» безпосередньо своєю структурою передбачає ідентичність мережного устаткування комп'ютерів, а також рівні можливості та права всіх абонентів (рис. 3.18).

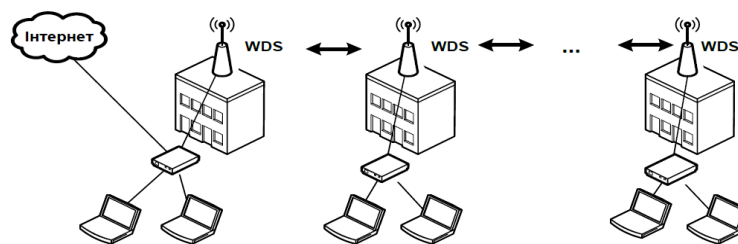


Рис. 3.18. Топологія типу «шина»

В даній інформаційній системі відсутній центральний абонент, через якого передається вся інформація. Зазначений метод підключення збільшує надійність всієї системи, адже при відмові будь-якого центру перестає функціонувати вся керована цим центром система. Розширення самої мережі з умов додавання нових абонентів при визначеній топології досить просте: введення параметрів нової точки доступу приводить до короткочасного перезавантаження параметрів системи.

Відмова у роботі окремих точок, учасниць топології типу «шина», не впливає на роботу абонентів, що залишилися, оскільки вся структура має рівні і незалежні права для кожного користувача.

Топологія побудови мережі «кільце». «Кільце» – це топологія, в якій кожна точка доступу сполучена лише з двома іншими (рис. 3.19) елементами. Виділеного центру у даному випадку немає, всі точки можуть бути рівноправними.

Розширення топології та підключення нових абонентів в «кільце» здійснюється за умови обов'язкової зупинки роботи двох крайніх точок, що знаходяться на безпосередній відстані від підключеної нової станції.

У той же час основна перевага кільця полягає у тому, що ретрансляція сигналів кожним абонентом дозволяє істотно збільшити розміри всієї мережі в цілому (до десятків кілометрів). Кільце у цьому відношенні істотно перевищує ефективність процесу організації роботи будь-якої іншої топології.

Топологія зв'язків між точками в цьому режимі відповідає ациклічному графу – типу «дерево» (рис. 3.19).

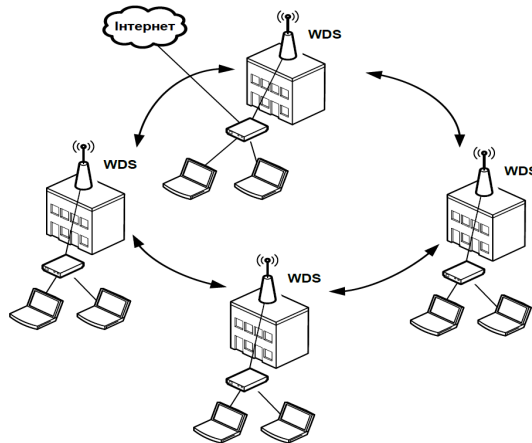


Рис. 3.19. Топологія типу «кільце»

Для усунення зайвих зв'язків, здатних приводити до появи надлишкових циклів в графі, реалізується алгоритм Spanning tree. Впровадження цього алгоритму дозволяє виявити і блокувати зайві зв'язки. При зміні топології мережі – наприклад, через відключення деяких точок або неможливості роботи каналів – алгоритм Spanning tree запускається знову, і раніше заблоковані зайві зв'язки можуть використовуватися замість тих, що вийшли з процесу обміну даними.

Топологія побудови мережі «зірка». «Зірка» – це топологія з явно виділеним центром, до якого підключаються всі абоненти бездротової мережі (рис. 3.20). Обмін інформацією йде виключно через центральну точку доступу, на яку в результаті лягає дуже велике навантаження з урахування кількості запитів, кількості інформаційних потоків та їх обсягів.

Функціонування зазначеної топології достатньо стійке до відмов роботи різних точок мережі: вихід з роботи звичайної точки доступу ніяк не відбивається на функціонуванні частини мережі. Однак, будь-яка відмова центральної точки робить мережу повністю непридатною.

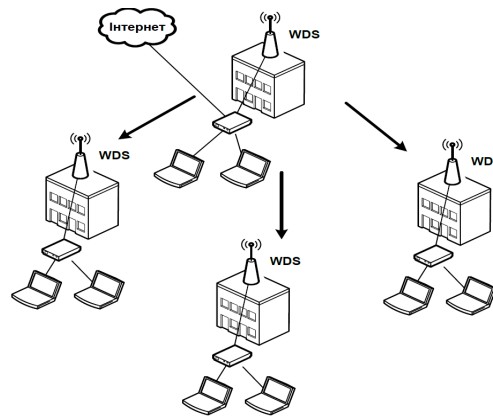


Рис. 3.20. Топологія типу «зірка»

Недоліки топології «зірка» полягають в жорсткому обмеженні кількості абонентів. Оскільки всі точки використовують один і той же канал, зазвичай центральний абонент не може обслуговувати більше 10 периферійних абонентів через велике падіння швидкості та появу колізій. У більшості випадків, наприклад, для об'єднання декількох районів в місті використовують комбіновані топології.

3.4. Супутникові інформаційні системи

Системи супутникового зв'язку (ССЗ) використовуються для передачі різного типу інформаційних потоків та даних на значні відстані. З моменту своєї появи супутниковий зв'язок стрімко розвивався, і з нагромадженням досвіду, удосконаленням апаратури, розвитком методів передачі сигналів відбувався перехід від окремих ліній супутникового зв'язку до локальних і глобальних систем [39].

Такі темпи розвитку супутникових систем зв'язку пояснюються низкою переваг, якими вони характеризуються. До них, зокрема, належать більша пропускна здатність каналів, необмежене перекриття простору, висока якість і надійність каналів. Завдяки перевагам, які визначають широкі можливості супутникового зв'язку, він стає унікальним та ефективним засобом інформаційного обміну даними. Супутниковий зв'язок у цей час є основним видом міжнародної та національної системи передачі даних на великі та середні відстані.

Усі системи можна поділити на системи двох видів: супутники, що працюють на негеостаціонарних і на геостаціонарних орбітах. Негеостаціонарні супутники використовуються в основному для військових, наукових і метеорологічних досліджень. Їхня головна особливість – неможливість підтримки цілодобового зв'язку між супутником та базовими станціями. Однак, переміщуючись по заданій орбіті відносно поверхні Землі, вони можуть збирати дані з великої площі земної поверхні.

Геостаціонарні супутники виводяться на таку орбіту в площині екватору, при якій їхня кутова швидкість збігається зі швидкістю обертання Землі навколо своєї осі. Висота над поверхнею Землі, де

виконуються умови сталості швидкостей і рівності відцентрової та гравітаційної сил, становить 36 тис. км. Теоретично один розташований у такий спосіб супутник може забезпечити високоякісний зв'язок для третини земної поверхні. Насправді обслуговуються істотно менші території. Особливістю супутників на геостаціонарних орбітах є значна часова затримка (близько 240 мс) у супутниковому каналі, викликана необхідністю двічі долати відстань у 36 тис. км від наземної станції до супутника.

Далі розглянемо системи, де застосовуються супутники зв'язку, що обертаються на орбітах синхронно з обертанням Землі. Це дає змогу істотно спростити систему зв'язку. У такому разі кожна земна станція працює безперервно з одним і тим самим супутником. Раніше при використанні несинхронних супутників існувала необхідність періодичного перемикання антеною системи кожної земної станції з одного супутника на інший, що викликало перерви при передачі інформаційних потоків. До того ж значну частину вартості супутникових систем зв'язку становила не дуже надійна апаратура спостереження. Використання стаціонарних супутників забезпечує безперебійний зв'язок, але потребує додаткового запасу робочого ресурсу часу для проведення багаторазових корекцій орбіти супутника. Вважається, що цей додатковий запас робочого ресурсу часу для корекції орбіти є порівняно невеликою платою за простоту експлуатації системи та відсутність перерв зв'язку. Земні станції при використанні стаціонарних супутників спрощуються за рахунок відмови від складної та дорогої системи спостереження.

Супутникові системи зв'язку можуть різнитися також і типом сигналу, який передається, і що може бути цифровим або аналоговим. Передача інформації в цифровій формі має низку переваг порівняно з іншими методами передачі.

Переваги систем цифрового супутникового зв'язку:

- простота й ефективність об'єднання багатьох незалежних сигналів і перетворення цифрових повідомлень у «пакети» для зручності комутації;
- менші енерговитрати порівняно з передачею аналогового сигналу;
- відносна несприятливість цифрових каналів до ефекту нагромадження спотворень при ретрансляціях, що звичайно становить серйозну проблему в аналогових системах зв'язку;
- потенційна можливість одержання дуже малих ймовірностей помилок передачі та досягнення високої точності відтворення переданих даних шляхом виявлення та виправлення помилок;
- конфіденційність зв'язку;
- гнучкість реалізації цифрової апаратури, що припускає використання мікропроцесорів, цифрову комутацію та застосування мікросхем із більшим ступенем інтеграції компонентів.

Сегменти систем супутникового зв'язку. Більшість систем супутникового зв'язку складається з кількох сегментів.

Космічний сегмент. Космічний сегмент систем супутникового зв'язку складається з геостаціонарних супутників, що перебувають на висоті до 35,600 км. Геостаціонарні супутники обертаються навколо Землі з тією самою швидкістю, що й сама Земля, тому здаються нам нерухомими. Зв'язок із такими супутниками набагато стійкіший, ніж із супутниками на інших орбітах, оскільки:

- протягом усього сеансу зв'язку між користувачем та геостаціонарним супутником встановлюється постійний канал обміну даними. Упродовж усього сеансу користувач не змінює джерела інформації;
- сеанс зв'язку між користувачем та геостаціонарним супутником може підтримуватись протягом необмеженого інтервалу часу;
- геостаціонарний супутник має стаціонарне місце на орбіті, що забезпечує достовірний та високоякісний зв'язок.

Система супутникового зв'язку може складатися з трьох чи більшої кількості основних та кількох запасних супутників, що перебувають на орбіті. Основні супутники отримують свої назви відповідно до територій, над якими вони розташовуються. Трьох геостаціонарних супутників, розташованих рівномірно по всій довжині екватора, достатньо для покриття 98 % поверхні Землі їхніми глобальними променями. Поза зоною обслуговування залишаються тільки приполярні області.

Анени супутників окрім глобальних променів діаграм спрямованості формують зональні (локальні) промені, у напрямі яких концентрується випромінювана потужність систем передачі інформації. На карті зони обслуговування глобальний промінь кожного супутника зображають у вигляді овалу, центр якого збігається з даним супутником, а зональні промені – у вигляді кіл (рис. 3.21).

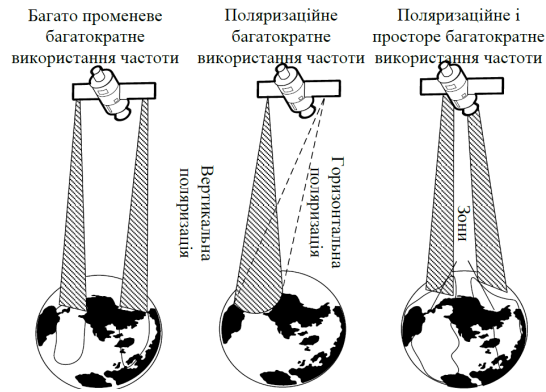


Рис. 3.21. Зональні промені діаграм спрямованості при різних методах поляризації та типах антен

Технологія зональних променів дає змогу значно зменшити масу та габаритні розміри призначених для користувача супутникових терміналів, не погіршуючи при цьому якості їх роботи. Зональними променями покривається вся суша та основні морські шляхи. Супутник може перерозподіляти енергію між своїми зональними променями, збільшуючи пропускну здатність одного з них за рахунок її зменшення в іншому промені. У такий спосіб супутник динамічно змінює навантаження відповідно до інтенсивності супутникового трафіку, що надходить із певного регіону.

Наземний сегмент. Наземний сегмент систем супутникового зв'язку складається з таких компонентів:

- супутникового центру управління (SCC – Satellite Control Center);
- мережі берегових та наземних станцій (LES – Land Earth Station);
- мережних координуючих станцій (NCS – Network Coordination Station);
- мережного операційного центру (NOC – Network Operation Center).

До завдань супутникового центру управління належать підтримка супутників у заданих позиціях над екватором і безперервне спостереження за справністю всіх бортових систем. Дані про стан супутників надходять із чотирьох станцій спостереження, телеметрії та контролю. Супутник приймає сигнали від призначених для користувача супутникових телефонів і передає їх на берегову станцію, яка слугує шлюзом між космічним сегментом і наземними мережами. Усі інформаційні канали контролюються мережним операційним центром, який, у свою чергу, спирається на мережні координуючі станції.

Призначений для користувача сегмент – це устаткування супутникового зв'язку, сервери, телефони й термінали, якими безпосередньо користується абонент. Сучасні супутникові телефони мають достатньо широкі можливості і водночас прості в експлуатації. До супутникового комутаційного обладнання користувача можна легко підключити комп'ютер, факсимільний апарат, відео-термінал або інші пристрої – залежно від завдань.

Станції супутникового зв'язку. Станція супутникового зв'язку використовується з метою обміну інформацією між наземними інформаційними об'єктами, а також у системах збору й розподілу даних. Супутникова станція із мережею земних станцій забезпечує систему телекомунікаційного зв'язку та передачі інформаційних потоків даних (зокрема, цифрової низькочастотної мовної інформації). При передачі телекомунікаційного трафіку супутникові системи утворюють групові тракти.

Групові тракти станцій супутникового зв'язку – сукупність програмно-апаратних та технічних методів і засобів, що забезпечують проходження групового сигналу на фоні організації кількох телекомунікаційних підканалів, що поєднуються в один супутниковий канал передачі даних.

Групові канали передачі станцій супутникового зв'язку – сукупність програмно-апаратних та технічних методів і засобів, що забезпечують передачу інформаційних сигналів з однієї точки простору в іншу. Канали й групові тракти супутникових систем широко використовуються на ділянках магістральних і внутрішньозональних телекомунікаційних мереж. Зокрема, на місцевих лініях зв'язку супутникові системи дають змогу:

- організовувати прямі закріплені канали й тракти між будь-якими пунктами зв'язку в зоні обслуговування супутника;
- працювати в режимі незакріплених каналів, при якому супутникові канали й тракти можуть оперативно перемикатися з одних напрямів на інші при зміні потреб трафіку мережі;
- використання найбільш ефективних методів обробки інформаційних потоків (пакетна обробка).

Крім систем з постійно закріпленим за ними каналом, ефективних при постійній передачі інформації на високих швидкостях (10 кбіт/с і вищих), існують системи, що використовують часове, частотне, кодове або комбіноване розділення каналу між багатьма абонентськими станціями супутника.

Ще однією характеристикою, що дає змогу класифікувати супутникові системи, є використання протоколу. В перших супутникових системах протоколи не застосовувались, тобто, канал був прозорим для кожного користувача. Недоліком таких систем була, наприклад, передача інформації користувача, як правило, без підтвердження приймаючою стороною її доставляння. Інакше кажучи, у таких системах немає застережень щодо правила діалогу між учасниками обміну інформацією. У цьому разі якість переданої інформації визначається якістю супутникового каналу. При типових значеннях імовірності помилки на символ у межах $10^{-6} \dots 10^{-7}$ передача більших обсягів інформації через супутникові системи, навіть із використанням різних завадостійких кодів, дуже ускладнюється, і навіть унеможливорюється. Сучасні супутникові системи використовують протокол, що підвищує надійність зв'язку зі збереженням високої швидкості обміну інформацією між абонентами.

Складові та технічні характеристики супутникових систем.

Супутникова станція за конструктивною ознакою складається з таких компонентів:

- – високочастотного модуля (ODU);
- – низькочастотного модуля (IDU).

Високочастотний модуль складається з антени та приймача-передавача, в якому встановлено низькочастотні модулі, які, у свою чергу, складаються з модему та мультиплексора (устаткування, яке створює канал).

Стандартний варіант комплектації передбачає наявність параболічної антени невеликого діаметра та приймача-передавача. Залежно від місця розташування супутникової станції відносно центра зони висвітлення супутника та швидкості передачі в каналі використовуються потужніші передавачі або антени більшого діаметра. На наземному сегменті встановлюється модем і мультиплексор.

Високочастотні та низькочастотні модулі з'єднані між собою радіочастотними (RF) кабелями комутації. По них надходить сигнал проміжної частоти (IF).

За функціональним призначенням наземний сегмент поділяється на базовий комплект, що забезпечує передачу самого каналу, та на додаткове устаткування, що забезпечує спрямовану передачу цього каналу.

Одностороння антена звичайно виконується за схемою офсет (зі зміщеним центром). Схема офсет дає змогу знизити рівень бічних пелюсток, що йдуть паралельно, створюючи максимальні завади. Ця схема дає також змогу уникнути нагромадження атмосферних опадів на поверхні рефлектора.

Супутниковий модем – радіотехнічний засіб підсистеми модулятора, призначений для кодування переданого цифрового потоку, що надходить з мультиплексора.

Супутниковий мультиплексор – радіотехнічний засіб, призначений для забезпечення спрямованої передачі низькочастотної телекомунікаційної інформації та інших інформаційних потоків даних. Супутниковий мультиплексор дає змогу скомбінувати телекомунікаційні повідомлення із синхронною та асинхронною передачею даних по одному каналу локальної наземної або супутникової мережі зв'язку. Це дає змогу знизити телекомунікаційні витрати шляхом збільшення можливостей передачі важливої інформації та одночасного зменшення пропускної здатності каналу.

Супутниковий шлюз – радіотехнічний програмно-апаратний засіб, що забезпечує вихід на інформаційно-комунікаційні мережі наземних телекомунікацій. Шлюз може забезпечувати:

- вихід на телекомунікаційні мережі;
- послуги міжміського зв'язку з виходом на інформаційні мережі загального користування;
- послуги міжнародного телекомунікаційного зв'язку;

- вихід на спеціальні телекомунікаційні мережі;
- вихід на глобальні інформаційно-комунікаційні мережі передачі даних (ROCHET, INTERNET, RELCOM і т. ін.).

Ресурс системи супутникового зв'язку. *Ресурс зв'язку* (Ccommunications Resource – CR) – це час (тривалість сеансу зв'язку) і ширина смуги частот, доступних для передачі корисного сигналу в певну інформаційно-комунікаційну систему.

Для створення ефективної системи зв'язку необхідно спланувати розподіл ресурсу між користувачами системи, щоб співвідношення час/частота було оптимальним. Результат такого планування – рівноправний доступ користувачів до ресурсу.

Із проблемою спільного використання ресурсу зв'язку пов'язані терміни «ущільнення» і «множинний доступ». При використанні терміна «ущільнення» вимоги користувача до спільного використання ресурсу зв'язку постійні або (найчастіше) зазнають незначних змін. Розподіл ресурсу виконується апіорно, а спільне використання ресурсу зазвичай прив'язане до локального пристрою.

Застосування множинного доступу, як правило, потребує віддаленого спільного використання ресурсу, як, скажімо, у разі супутникового зв'язку. За динамічної схеми множинного доступу контролер системи має враховувати потреби кожного користувача ресурсу зв'язку. Час, необхідний для передачі відповідної керуючої інформації, установлює верхню межу ефективного використання ресурсу зв'язку.

Існують три основні способи збільшення пропускну здатності (загальної швидкості передачі даних) ресурсу зв'язку:

- збільшення ефективної ізотропно-випромінюваної потужності (effective isotropic radiated power – EIRP) передавача або зниження витрат системи, що в кожному разі приведе до збільшення відношення сигнал/шум (E/N);
- збільшення ширини смуги каналу передачі даних;
- підвищення ефективності розподілу ресурсу зв'язку на базі множинного доступу.

Основні способи розділення ресурсу зв'язку такі:

1. **Частотне розділення** (frequency division – FD). Розділяються певні піддіапазони смуги частоти, що використовується у даному випадку.

2. **Часове розділення** (time division – TD). Користувачам виділяються періодичні часові інтервали. У деяких системах їм надається обмежений час для зв'язку. В інших випадках час доступу користувачів до ресурсу визначається динамічно.

3. **Кодове розділення** (code division – CD). Виділяються певні елементи набору ортогонально (або майже ортогонально) розділених спектральних кодів, кожний з яких використовує весь діапазон частот.

4. **Просторове розділення** (space division – SD), або багатопроменеве багаторазове використання частоти. За допомогою точкових променевих

антен радіосигнали розділяються й спрямовуються в різні боки. Цей метод припускає багаторазове використання одного частотного діапазону.

5. Поляризаційне розділення (polarization division – PD), або подвійне поляризаційне багаторазове використання частоти. Для розділення сигналів застосовується ортогональна поляризація, що дає змогу використовувати один частотний діапазон.

Методи та принципи, що використовуються при побудові інтегрованих інформаційно-комунікаційних систем супутникового зв'язку, наведено на рис. 3.22.

Ключовим моментом усіх схем ущільнення та множинного доступу є те, що при використанні ресурсу різними сигналами інтерференція не надає некерованих взаємних завад, які роблять неможливим процес детектування. Інтерференція припустима доти, доки сигнали одного каналу збільшують імовірність появи помилок в іншому каналі. Уникнути взаємних завад між різними користувачами дає змогу застосування в різних каналах ортогональних сигналів [99].

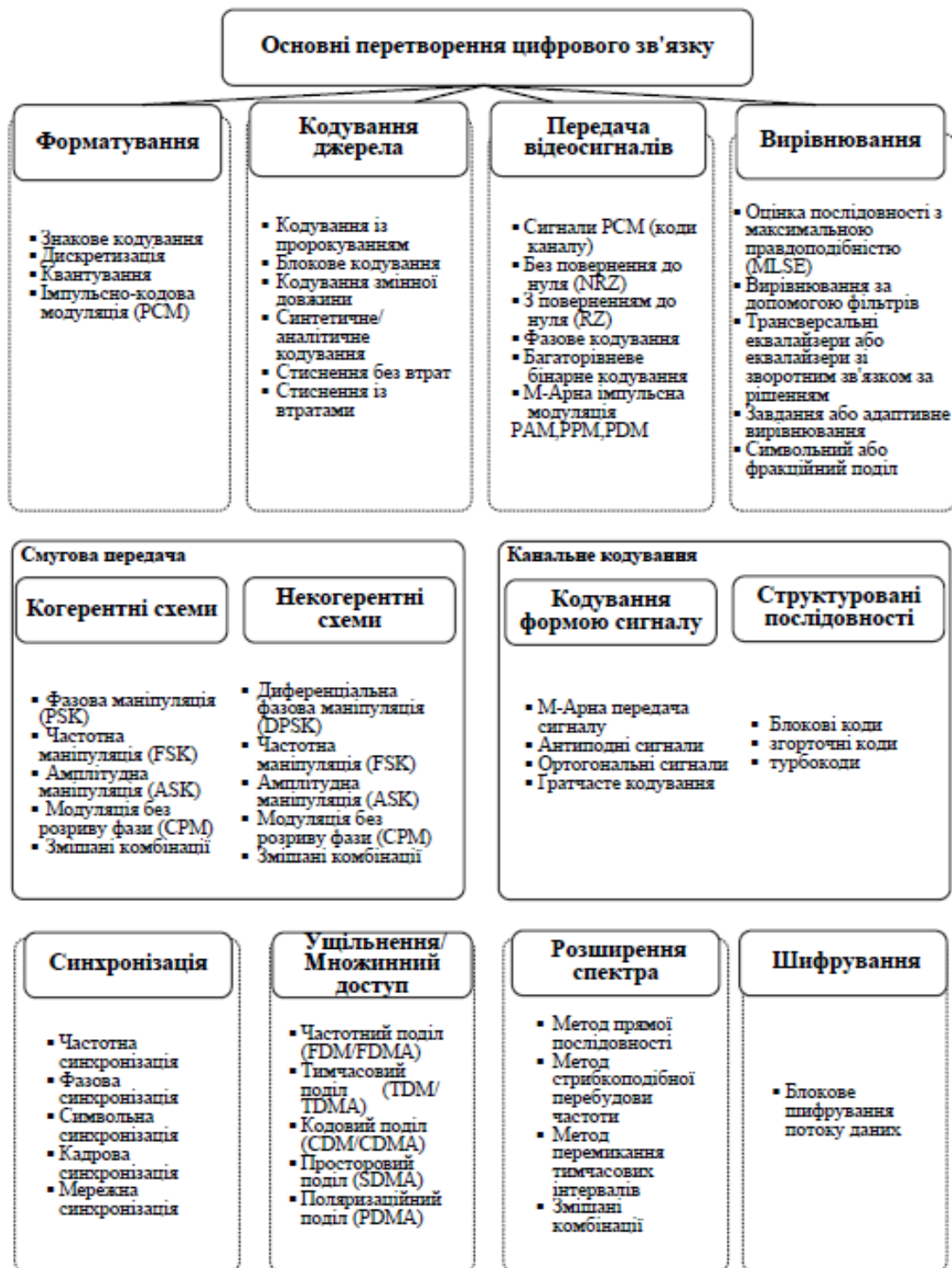


Рис. 3.22. Класифікація методів та засобів побудови інтегрованих інформаційно-комунікаційних систем супутникового зв'язку

Методи кодування в системах супутникового зв'язку. Оскільки канали й тракти супутникових ліній входять у національні та міжнародні мережі загального користування, до їхніх якісних показників висуваються доволі жорсткі вимоги. Тому при передачі цифрових сигналів у супутникових системах застосовують завадостійке кодування, яке називають також *прямим виправленням помилок* (FEC в англійській мові)

літературі). Сьогодні широко застосовуються добре розроблені коди з прямим виправленням помилок двох основних класів.

Блокові коди. Послідовність даних поділяється на блоки з n символів (звичайно від 1 до 7); кожному блоку ставиться у відповідність кодова комбінація з символів, що передається каналом зв'язку.

Кодування згортання. Застосування кодування згортання дає змогу не тільки підвищити ймовірність переданої інформації, але й отримати енергетичну вигоду, що дорівнює зменшенню потужності передавача. Результатом даного процесу є розширення смуги частот, яку займає радіосигнал, з огляду на необхідність передачі надлишкових перевіірочних символів. Величина вигоди залежить від кодової швидкості засобу кодування й алгоритму декодування. Для декодування використовують алгоритм, запропонований Вітербі. Декодування здійснюється у зворотному порядку: спочатку декодують внутрішній код, а далі символи декодованого сигналу переставляють на початкові позиції, у результаті чого пакети помилок «розбивають» на одинарні помилки (які легше виправити) і потім декодують зовнішній код.

3.5. Організація множинного доступу до інформаційних ресурсів

Більшість супутників зв'язку перебувають на геостаціонарній геосинхронній орбіті. Це означає, що супутник перебуває на круговій орбіті, що лежить у площині земного екватора. При цьому супутник перебуває на такій висоті над рівнем моря (приблизно 35 830 км), на якій період його обертання навколо Землі дорівнює періоду обертання самої Землі навколо Сонця. Оскільки при спостереженні із Землі такі об'єкти здаються нерухомими, то три супутники, розташовані через 120° один від одного, дають змогу охопити територію всієї земної кулі (окрім полярних областей). Більшість супутникових систем зв'язку використовують нерегенеративні ретранслятори або транспондери. Нерегенеративний означає, що сигнали «Земля – супутник» підсилюються, зсуваються за частотою та ретранслюються на Землю без обробки сигналу, демодуляції або повторної модуляції.

Найбільш використовуваним діапазоном у комерційних системах супутникового зв'язку є так звана *смуга* (C-band). У цьому діапазоні для передачі сигналу «Земля – супутник» застосовуються несуча частота 6 ГГц і частота 4 ГГц передачі сигналу «супутник – Земля». Відповідно до міжнародних угод для систем передачі у смузі дозволено використовувати будь-який супутник, що працює в спектральному діапазоні шириною в 500 МГц. Здебільшого такий супутник має 12 транспондерів із шириною смуги 36 МГц кожний. Найбільш поширені транспондери працюють у режимі FDM/FM/FDMA (ущільнення із частотним розподіленням, частотна модуляція, множинний доступ із частотним розподіленням).

Розглянемо складові зазначених режимів.

1. **FDM** – сигнали, подібні до телекомунікаційних, що мають поодинокую бічну смугу шириною 4 кГц і обробляються з використанням

частотного розподілення каналів, у результаті чого формується багатоканальний сигнал.

2. **FM** – складений сигнал модулює несучу на базі методу частотної модуляції та передається на супутник.

3. **FDMA** – піддіапазони смуги транспондера (36 МГц) можуть розподілятися між різними користувачами. Кожному користувачеві виділяється певна смуга, на якій він одержує доступ до транспондера.

Таким чином, складені канали з частотним розподіленням модулюються методом фазової модуляції, після чого інформація, розділена за різними смугами відповідно до системи FDMA, передається на супутник. Основною перевагою технології FDMA порівняно з TDMA є простота. Канали FDMA не вимагають синхронізації або централізованого розділення часу. Кожний із каналів незалежний від інших [39].

Ця технологія еквівалентна методам розділення частотних каналів для систем безпроводного зв'язку.

Ущільнення – множинний доступ із часовим розподіленням.

На рис. 3.23 наведено випадок, коли ресурс зв'язку розділено шляхом надання кожному з M сигналів (або користувачів) усього спектру протягом невеликого відрізка часу, який називається *часовим інтервалом* (time slot). Проміжки часу, що розділяють використовувані інтервали, називаються *захисними інтервалами* (guard time). Захисний інтервал створює деяку часову невизначеність між сусідніми сигналами, відіграючи роль буфера й знижуючи тим самим інтерференцію.

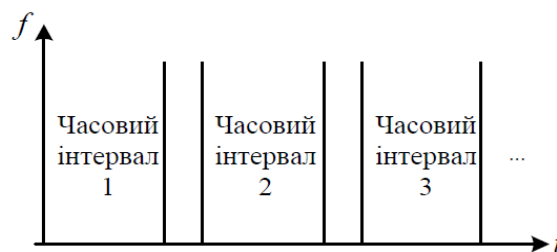


Рис. 3.23. Ущільнення з часовим розділенням

Приклад використання технології TDMA в супутниковому зв'язку наведено на рис. 3.24.

Час розбивається на інтервали, які називають *кадрами* (frame). Кожний кадр поділяється на часові інтервали, які можна розподілити між користувачами. Загальна структура кадрів періодично повторюється, так що передача даних за схемою TDMA – це один або більше часових інтервалів, які періодично повторюються протягом кожного кадру.



Рис. 3.24. Типова конфігурація TDMA

Кожна наземна передавальна станція транслює інформацію у вигляді пакетів у такий спосіб, щоб вони надходили на супутник згідно з установленим розкладом. Після прийняття транспондером такі пакети ретранслюються на Землю разом з інформацією від інших передавальних станцій. Приймальна станція детектує та розушлює ущільнені дані відповідного пакета, після чого інформація надходить до відповідних користувачів.

Найпростішою з-поміж схем TDM/TDMA є схема з фіксованим розділенням. При використанні такої схеми M часових інтервалів, що утворюють кадр, заздалегідь розподілені між джерелами сигналу на доволі тривалий проміжок часу. Роботу такої системи унаочнює схема, зображена на рис. 3.25.

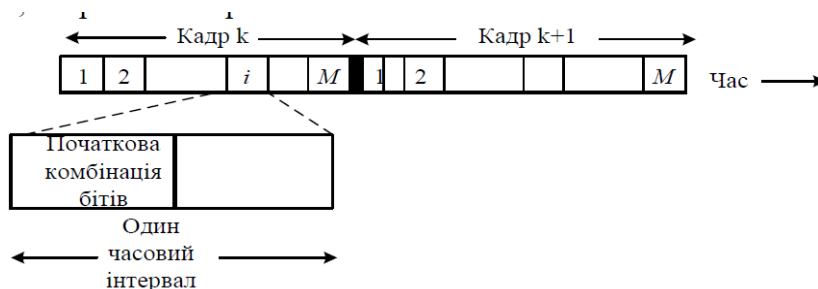


Рис. 3.25. TDM з фіксацією ущільнення

Операція ущільнення полягає в наданні кожному джерелу можливості використовувати один або більше інтервалів. Розушлювання – це розпізнавання інтервалів із подальшим розподілом даних між відповідними користувачами. Два комутуючі ключі на рис. 3.26 мають бути синхронізовані таким чином, щоб повідомлення, яке відповідає джерелу I , потрапляло на вихід каналу I , і т.д.

Саме повідомлення в загальному випадку складається з початкової комбінації бітів (preamble) і власне інформаційної частини. Початкова комбінація зазвичай складається з елементів, які відповідають за синхронізацію, адресацію та захист від помилок.

Схема TDM/TDMA із фіксованим розподіленням надзвичайно ефективна, коли вимоги користувача можна передбачити, а потік даних значний (тобто часові інтервали практично завжди заповнені). Проте в разі

пульсуючого або випадкового потоку даних зазначений метод себе не виправдовує.

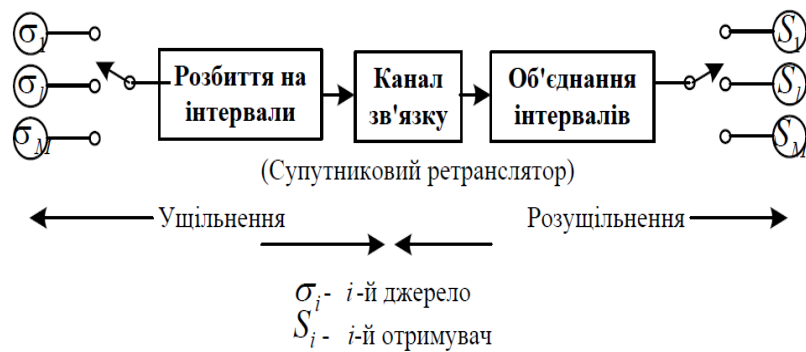


Рис. 3.26. TDM з фіксацією ущільнення

Розглянемо простий приклад (рис. 3.27). Тут кадр утворюють чотири інтервали, кожний з яких закріплено за користувачами *A*, *B*, *C* і *D*. Схеми активності чотирьох користувачів наведено на рис. 3.27,а.

Протягом першого інтервалу передачі кадру користувач *A* не відправляє даних, користувач *B* не передає даних протягом другого інтервалу, а користувач *C* – протягом третього.

У разі використання TDMA з фіксованим розділенням усі інтервали кадру розподілені заздалегідь. Якщо «власник» інтервалу не передає даних протягом зазначеного проміжку часу, цей інтервал не використовується. На рис. 3.27,б зображено потік даних і невикористані інтервали. Якщо вимоги користувачів не передбачені, як у наведеному прикладі, то мають застосовуватися більш ефективні методи із застосуванням динамічного розділення інтервалів. Саме про такі методи йдеться при застосуванні систем із комутацією пакетів, статистичних мультиплексорів або концентраторів. Відповідні системи дають змогу досягти результату, зображеного на рис. 3.27,в, де пропускна здатність системи залишається постійною завдяки використанню всіх доступних часових інтервалів.

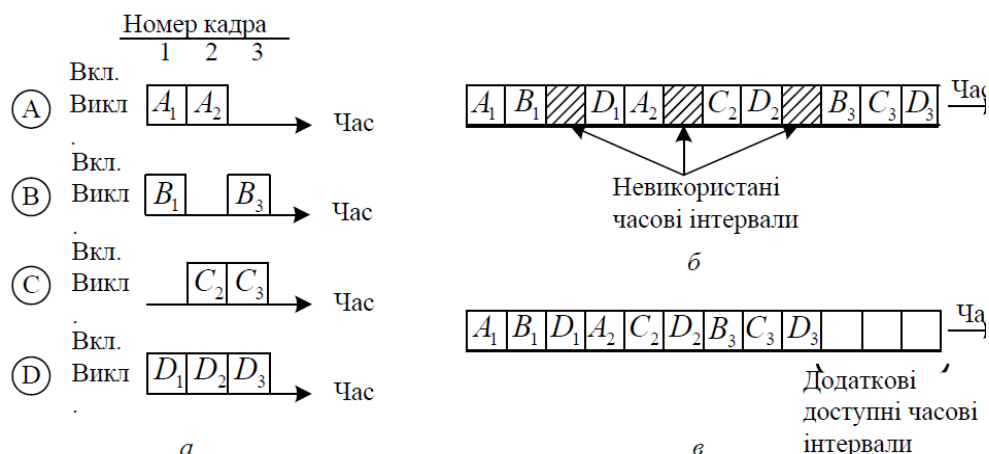


Рис. 3.27. TDM з фіксованим розподілом і система з комутацією пакетів:

- а) схема активності користувачів;
- б) TDM з фіксованим розподілом;
- в) комутація пакетів з часовим розподілом (концентрація)

Багатоканальний розподіл ресурсу зв'язку. Загальний спосіб керування ресурсом зв'язку, що дає змогу розділяти частотні діапазони на заздалегідь визначений період часу.

Для визначення розподілу частотних діапазонів розглянемо випадок рівномірного пропорційного розподілу смуги шириною W між групами M (або класами) користувачів. Відповідно вважатимемо, що частотний діапазон розбито на смуги шириною W/M Гц, які будуть постійно доступні відповідним групам. Аналогічно для призначення розподілу часових інтервалів вісь часу розбивається на інтервали тривалістю T . У свою чергу, кожний із кадрів розбивається N на інтервалів тривалістю T/N кожний. Припустимо, що активність користувачів синхронізована в часі, а розподілені інтервали періодично розташовані в кадрах. Кожний користувач може передавати дані, коли починається його інтервал часу, причому протягом цього інтервалу користувач може використовувати виділену смугу частот. Часовий інтервал однозначно задається як m -й інтервал кадру n .

Множинний доступ з кодовим розділенням. У разі FDMA площа ресурсу зв'язку була розділена на горизонтальні відрізки, що відповідають частотним діапазонам. Ту саму площину було розбито по вертикалях на часові інтервали TDMA. Ці два підходи є найпоширенішими в застосуванні множинного доступу. Метод множинного доступу є результатом поєднання FDMA і TDMA, як показано на рис. 3.28.

Цей метод називається **множинним доступом з кодовим розділенням** (code-division multiple access – CDMA).

Множинний доступ із кодовим розділенням є практичним втіленням методів розширення спектра (spread-spectrum – SS), які можна поділити на дві основні категорії:

- розширення спектра методом прямої послідовності (direct sequence – DSSS);
- розширення спектру методом стрибкоподібної перебудови частоти (frequency hopping – FHSS).

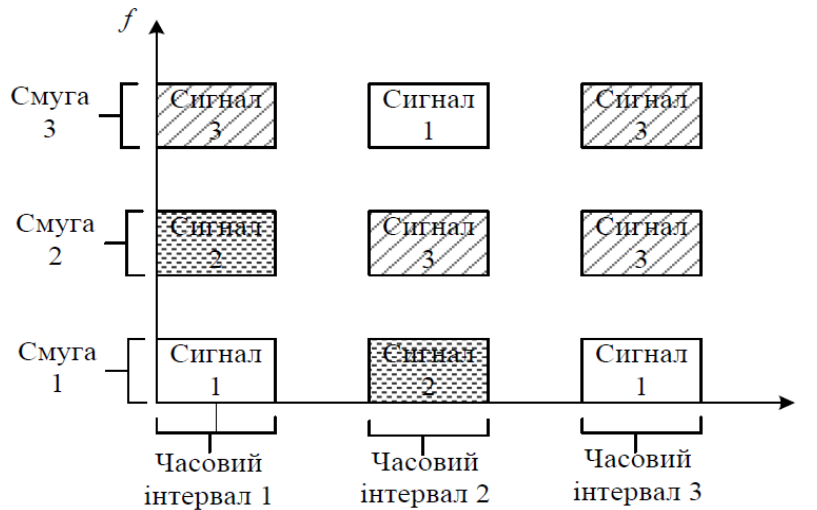


Рис. 3.28. Ущільнення з кодовим розподілом

Ці методи розділення каналів на базі розширення спектру переданого сигналу цілком ідентичні щодо організації різних режимів роботи бездротових мереж та докладно розглянуті в попередньому розділі.

Процес модуляції з використанням перебудови частоти приведений на рис. 3.29.

Під час кожної зміни частоти генератор псевдошумової послідовності спрямовує кодову послідовність на пристрій стрибкоподібної перебудови частоти. Цей пристрій видає одну із припустимих для стрибка частоту. Вважатимемо, що використовується Марна частотна маніпуляція (Mary frequency shift keying – MFSK). У разі звичайної системи MSFK дані модулюють несучу хвилю з фіксованою частотою. У разі MFSK із перебудовою частоти (FH – MFSK) частота несучої зміщується по всьому діапазону частот передачі. FH-модуляцію (див. рис. 3.29) можна подати як процес, що складається з модуляції даних і модуляції перестроювання частоти.

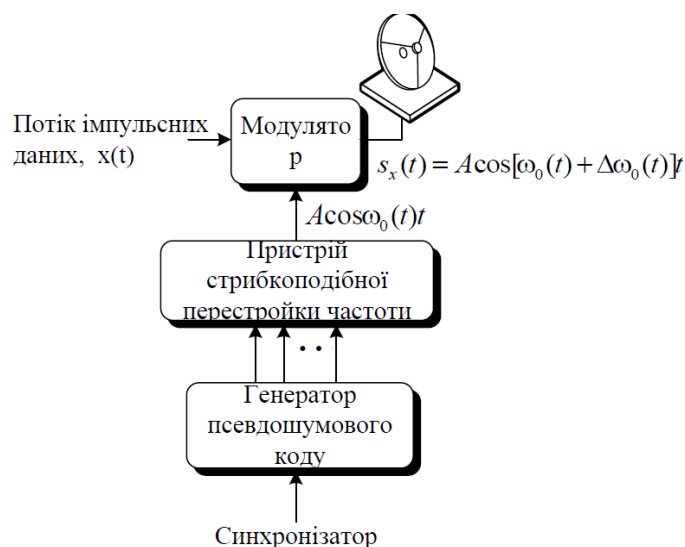


Рис. 3.29. Процес модуляції схеми FH – CDMA

Зазначені дії можна поєднати. Тоді модулятор на основі псевдошумового коду та власне даних генеруватиме тони передачі.

Конфіденційність передачі інформаційних потоків даних у разі використання мішаного методу CDMA є основною та унікальною перевагою цього методу множинного доступу.

Якщо код групи користувачів відомий лише дозволеним членам цієї групи, CDMA забезпечує конфіденційність зв'язку, оскільки несанкціоновані особи, котрі не мають коду, не можуть отримати доступу до переданої інформації.

Канали із завмираннями. Для певної частини використовуваного спектра характерні завмирання, сигнали в цій частині діапазону будуть ослабленими. У разі застосування схеми FDMA користувач частини спектра може зазнавати постійних труднощів зі зв'язком. Згідно зі схемою FH – CDMA користувач зазнаватиме аналогічних труднощів тільки при зміщенні частоти у відповідну частину спектра. Таким чином, можливі проблеми зі зв'язком рівномірно розподіляються між всіма користувачами.

Інформаційний потік у системах множинного доступу. На рис. 3.30 представлена блок-схема потоку даних щодо реалізації алгоритму множинного доступу (multiple access algorithm – MAA), між контролером і наземною станцією зв'язку.

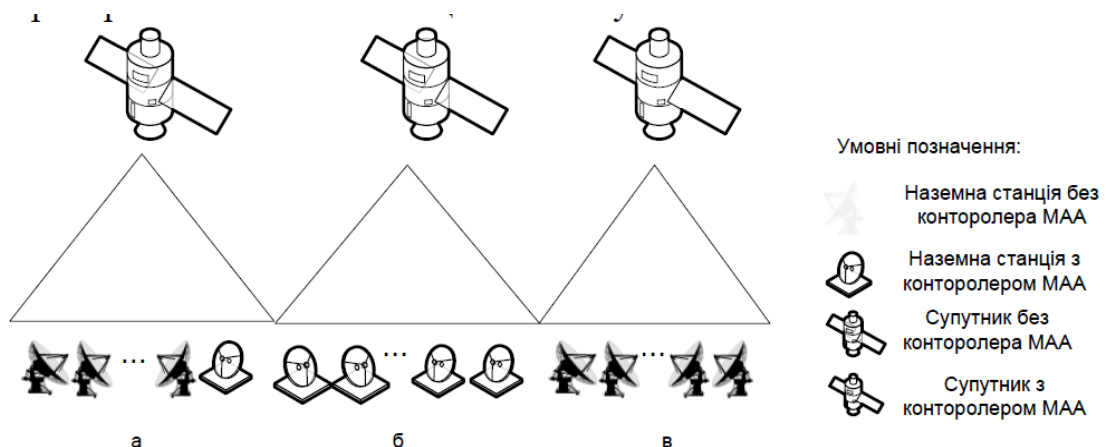


Рис. 3.30. Блок-схема потоку даних

Спрямовувати та керувати інформаційними потоками може безпосередньо супутник або одна наземна базова станція. Керування може бути розподілене також між усіма наземними станціями. Порядок передачі даних наведено на рис. 3.31.

Розподіл інформаційного потоку по каналах – розподіл інформаційних ресурсів та даних, здійснюваний при обміні інформацією між супутником та користувачем (наприклад, канали N може бути надано користувачеві X, а канали N+1=M – користувачеві Y).

Розподіл інформаційного потоку по каналах – розподіл інформаційних ресурсів та даних, здійснюваний при обміні інформацією між супутником та користувачем (наприклад, канали може бути надано користувачеві).

Ця інформація змінюється рідко й може поширюватися між наземними станціями без використання системи зв'язку, наприклад, за допомогою інформаційного бюлетеня розподілу.

Стан мережі (*network state – NS*) – це стан ресурсу зв'язку, тобто час і ширина смуги частот, доступних для передачі інформаційного сигналу в певну інформаційно-комунікаційну систему.

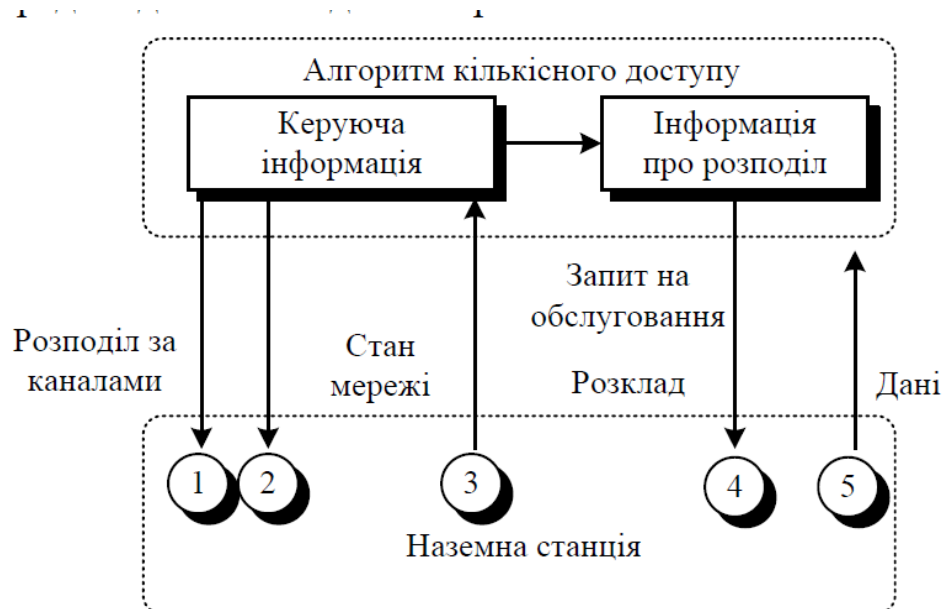


Рис. 3.31. Інформаційний потік у системах кількісного доступу

Наземна станція одержує вказівки щодо доступності ресурсу зв'язку, а також про те, як варто використовувати час, частоту, кодові позиції ресурсу для передачі запиту на обслуговування.

Запитом на обслуговування називається передане станцією кодове повідомлення (запит) на виділення ресурсу зв'язку для передачі т сегментів інформаційного сигналу.

Після одержання запиту (запитів) на обслуговування контролер передає станції розклад, відповідно до якого дані мають розподілятися в ресурсі зв'язку.

Станція передає дані відповідно до зазначеного розкладу.

Множинний доступ із наданням каналів на вимогу. Супутниковими системами з фіксованим розподілом називаються системи множинного доступу, що дають змогу передавальній станції періодично одержувати доступ до інформаційного каналу незалежно від реальних потреб користувача або системи.

Супутниковими системами з наданням каналів на вимогу (*demand-assignment multiple access – DAMA*) називаються системи множинного доступу з динамічним розподілом, які надають доступ до інформаційного каналу тільки на відповідний запит передавальної станції.

Якщо передача даних станцією зв'язку ведеться нерегулярно або стрибкоподібно, схема DAMA може бути значно ефективнішою за схему фіксованого розподілу. Корисність схеми DAMA пояснюється тим, що

фактична потреба в ресурсах рідко збігається з максимальним попитом. Якщо пропускна здатність системи дорівнює загальному максимальному попиту, а обмін даними відбувається нерегулярно, більшу частину часу можливості системи будуть використовуватися не повністю.

Проте система з більш низькою пропускною здатністю, що використовує буферизацію та схему DAMA, може успішно підтримувати стрибкоподібний процес обміну даними, хоча в цьому разі все-таки можливі деякі затримки передачі даних. На рис. 3.32 узагальнюються основні розбіжності між системою з фіксованим розподілом, пропускна здатність якої дорівнює сумі вимог усіх користувачів, та динамічною системою, пропускна здатність якої визначається середніми вимогами користувачів.

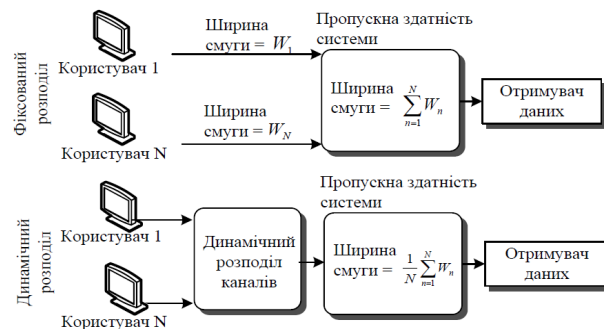


Рис. 3.32. Зменшення ширини смуги для систем з динамічним розподілом каналів

Використання методів супутникової комутації інформаційних потоків. Сучасні супутники зв'язку звичайно використовують кілька променів, які забезпечують покриття в певному регіоні. Прикладом є супутник, що перебуває над Атлантичним океаном, окремі промені спрямовуються в Північну Америку, Європу, Південну Америку і Африку. Для взаємозв'язку станцій різних регіонів використовуються комутатори.

Супутникова комутація (satellite-switched TDMA – SS/TDMA) – це процес забезпечення ефективного циклічного взаємозв'язку обміну інформаційними потоками та даними (із часовим розділенням доступу до інформаційних ресурсів) із зонами перекриття діаграм спрямованості променів різних супутників.

Основою системи є розміщена на супутнику мікрохвильова матриця комутації, програмована за допомогою наземного управління на циклічну зміну станів. Таким чином, у кожний момент комутації зв'язуються роздільні промені каналів Земля – супутник. Наземна станція може зв'язатися зі станціями, що використовують інший промінь, посиляючи пакети TDMA під час відповідних виділених інтервалів часу. Схема комутації станів обирається так, щоб максимально збільшити пропускну здатність системи з урахуванням наявних обмежень на обмін даними. Для досягнення повного взаємозв'язку N променів потрібно N! різних станів, або режимів, супутника. Шість режимів, необхідних для повного взаємозв'язку трипроменевої системи, наведено в табл. 3.1

Вхід	Вихід					
	Режим 1	Режим 2	Режим 3	Режим 4	Режим 5	Режим 6
<i>A</i>	<i>A</i>	<i>A</i>	<i>B</i>	<i>B</i>	<i>C</i>	<i>C</i>
<i>B</i>	<i>B</i>	<i>C</i>	<i>A</i>	<i>C</i>	<i>A</i>	<i>B</i>
<i>C</i>	<i>C</i>	<i>B</i>	<i>C</i>	<i>A</i>	<i>B</i>	<i>A</i>

У режимі 1 приймачі супутника на променях А, В і С з'єднано з передавачами для променів А, В і С. Наземна станція, яка використовує один із цих променів, може зв'язатися з іншою станцією, яка використовує той самий промінь. Такий промінь називають самоорієнтованим.

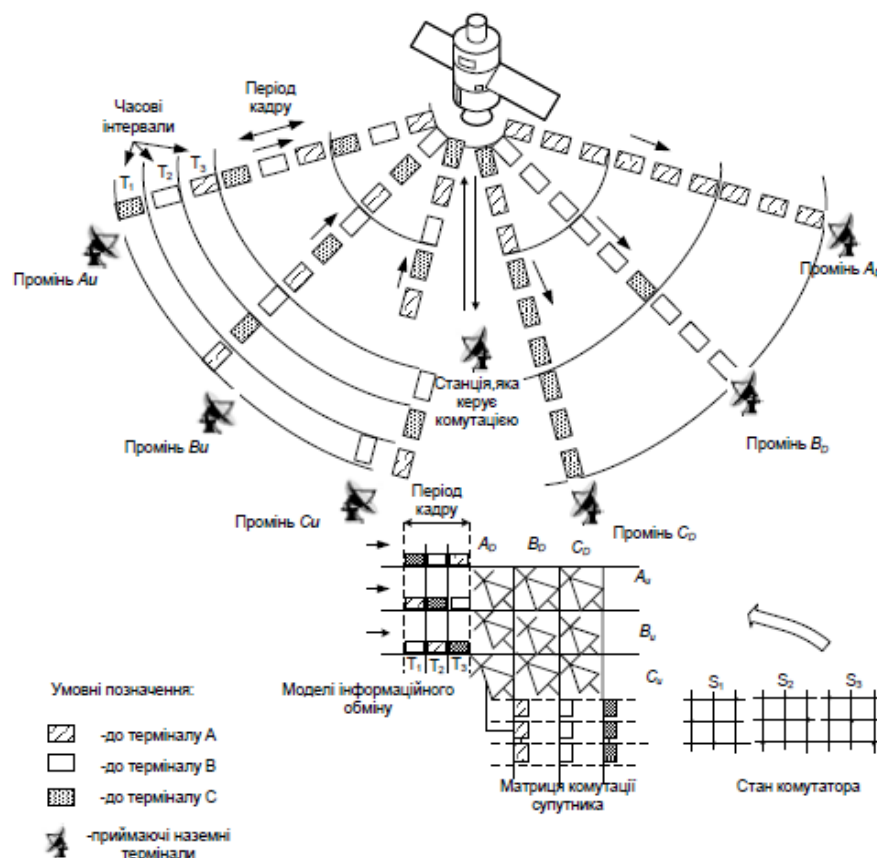


Рис. 3.33. TDMA із супутниковою комутацією (satellite switched TDMA-SS/TDMA)

Приклад трипроменевої (промені А, В і С) системи SS/TDMA наведено на рис. 3.33. Мікрохвильова матриця комутації для даного супутника є координатною. Таку матрицю можна подати як набір поздовжніх і поперечних ліній. При активізації ліній (однієї поздовжньої та однієї поперечної) виникає контакт на їх перетині. Координатний комутатор дає змогу одночасно встановлювати зв'язок тільки між двома компонентами матриці – одним поздовжнім і одним поперечним. Якщо канал станції A_{ij} пов'язаний із каналом B_D станції жодний із цих каналів не може бути одночасно пов'язаний з будь-яким іншим каналом. Три схеми процедури обміну даними протягом інтервалів часу T_1 , T_2 , T_3 при

існуванні трьох станів комутації S_1, S_2, S_3 зображено на рис. 3.33. Протягом інтервалу T_1 маємо режим S_1 промені самоорієнтовані. Протягом інтервалу T_2 режим S_2 дає змогу передавати сигнали зі станцій A_u, B_u, C_u на станції A_D, B_D, C_D . Протягом інтервалу T_3 режим S_3 , канали передачі так само зв'язуються з каналами прийому, забезпечуючи доставку даних необхідному адресатові.

Схеми процедури обміну даними, а також їхня тривалість вибираються з метою оптимізації пропускної здатності супутника та максимально ефективного обслуговування користувачів. Для обліку змін в інформаційному потоці циклічна схема в разі потреби може змінюватися наземною станцією.

Матриця інформаційного обміну. Матрицю, що характеризує обмін даними між областями, які обслуговуються сфокусованим променем, наведено на рис. 3.34.

Якщо обміном даними системи SS/TDMA керує комутатор, що не блокує (дозволяє передачу всіх повідомлень без видачі будь-якого аналогу сигналу «зайнято»), кожному каналу в кадрі TDMA призначається часовий інтервал тривалістю k секунд. Для ефективного використання ресурсу зв'язку повний інформаційний обмін на рис. 3.34 має відбутися протягом часу кадру який має бути щонайменшим.

		Адресат						Передана інформація (проміжна сума)
		1	2	...	j	...	N	
Джерело	1	t_{11}	t_{12}		t_{1j}		t_{1N}	S_1
	2	t_{21}	t_{22}		t_{2j}		t_{2N}	S_2
	$\vdots$							
	i	t_{i1}	t_{i2}		t_{ij}		t_{iN}	S_i
	$\vdots$							
Отримана інформація (проміжна сума)	N	t_{N1}	t_{N2}		t_{Nj}		t_{NN}	S_N
		R_1	R_2		R_j		R_N	Сума

Рис. 3.34. Матриця інформаційного обміну

Системи зв'язку множинного доступу та їхня архітектура. Інформація про використання часу, частоти й кодових функцій, необхідна користувачам для спілкування між собою за допомогою супутника, міститься в протоколі або алгоритмі множинного доступу (multiple access algorithm – МАА).

Система множинного доступу – це система, що об'єднує апаратне та апаратно-програмне забезпечення, яке підтримує алгоритм множинного доступу (протокол доступу) з метою своєчасного впорядкування і ефективної передачі інформаційних потоків та даних між станцією супутникового зв'язку і користувачем [100].

Основні структури супутникових систем зв'язку множинного доступу наведено на рис. 3.35. В умовних позначеннях подано символи, використовувані для наземних станцій, які мають або не мають контролера

алгоритму доступу. На цій станції розміщують сервер, що реагує на запити щодо обслуговування, які надходять від усіх інших користувачів. Запит спричиняє передачу даних від контролера до супутника й назад. Реакція контролера приводить до іншої передачі за допомогою супутника. Таким чином, кожна послуга потребує двох сеансів передачі даних із Землі на супутник і назад. Випадок розподілу керування згідно з алгоритмом доступу між усіма наземними станціями (виділеного контролера не існує). Усі наземні станції використовують однаковий алгоритм і мають у своєму розпорядженні ідентичні знання про запит щодо доступу та алгоритму розподілу доступу. Отже, кожна послуга в цьому разі потребує одного циклу зв'язку «станція – супутник – станція». Контролер алгоритму доступу, що перебуває безпосередньо на супутнику. Запит користувача надходить на супутник, що може негайно надіслати відповідний сигнал. Таким чином, у цій системі для надання послуги зв'язку достатньо одного циклу зв'язку.

Система наземних станцій – SCPC-система (рис. 3.35)

Більшість мереж наземних станцій працюють згідно з принципом стандартного варіанта зв'язку, де використовується зв'язок за схемою «point-to-point» («точка–точка») – дві наземні станції, з'єднані супутниковим каналом і розташовані безпосередньо у користувачів. За наявності такого каналу користувачі можуть встановлювати зв'язок один з одним у будь-який момент. Частіше доводиться мати справу з конфігурацією мережі типу «зірка» (принцип «центр із кожним»). У разі використання цієї схеми можлива організація потоків цифрової інформації зі швидкістю від 32 кбіт/с до 8 Мбіт/с і забезпечення телефонного, телефаксного зв'язку між центром і периферією. Така система має одну з основних переваг – передачу більших обсягів інформації з високою швидкістю. Завдяки використанню супутникових цифрових каналів вона є не критичною щодо дальності та достатньо захищена.

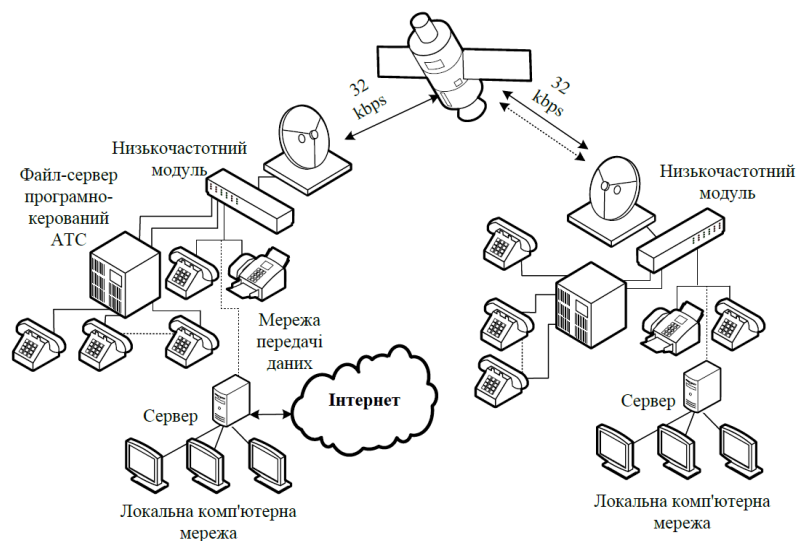


Рис. 3.35. Схема роботи SCPC – системи

Наземна системи повного доступу (Telecommunications Earth Station – TES) призначена для обміну телекомунікаційною та цифровою інформацією в інформаційних мережах супутникового зв'язку, побудованих за принципом «кожний із кожним» («mesh») або в мережах із повним доступом (рис. 3.36).

Ця система дає змогу встановлювати телекомунікаційний зв'язок між будь-якими двома абонентами мережі. Окрім того, абонентам забезпечується вихід у міжнародні глобальні інформаційно-комунікаційні мережі загального користування через **телепорт** (Gateway). У найпростішій конфігурації забезпечується зв'язок по одному телефонному або факсимільному каналу.

Абонентів надається додаткова можливість організації передачі цифрової інформації між двома станціями, що входять до мережі. Мережа працює за принципом, згідно з яким абонент не має жорстко закріпленого за ним супутникового каналу (DAMA), а цей канал надається йому на першу вимогу (запит), причому з високою (понад 99 %) імовірністю комутації.

Цей спосіб дає змогу зменшити кількість задіяних супутникових каналів. Загалом використання саме TES-системи є найбільш оперативним і дієвим способом доступу в міжнародні телекомунікаційні мережі, а також оптимальним засобом зв'язку з тими територіальними областями, які мають нерозвинену інфраструктуру зв'язку або взагалі не мають її.

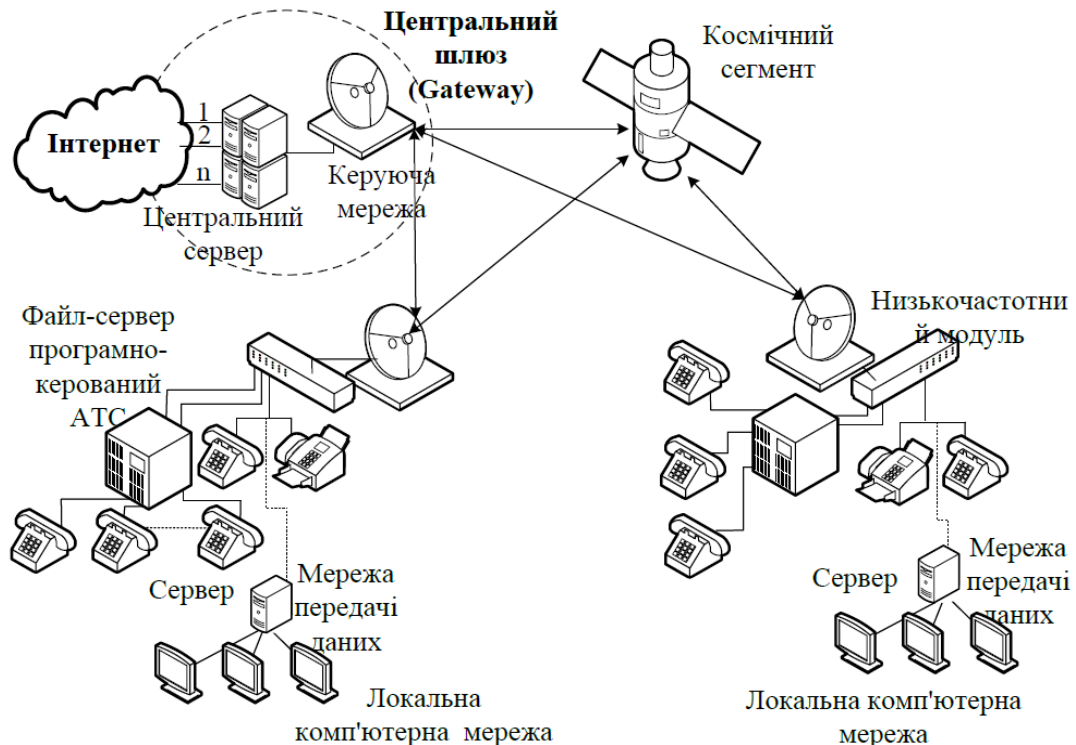


Рис. 3.36. Схема роботи TES – системи

Система персональних наземних станцій (PES)

Наземна система має у своєму складі центральну станцію (HUB station) із багатьма периферійними (PES) або remote. Ефективність випромінювання, велика потужність і висока якість прийому центральної станції уможливорює застосування на периферійних станціях малих антен діаметром 0,5...1,8 м і малопотужних (0,5...2 Вт) передавачів. Це значно знижує вартість абонентської системи зв'язку. На відміну від інших згаданих щойно систем, у цій системі передача інформації завжди відбувається через HUB-станцію. З погляду енергетики системи та її вартості (відповідно й вартості пропонованих послуг) оптимальним є розташування центральної базової стації в центрі зони висвітлення супутника.

Система персональних наземних станцій (Personal Earth Station-PES) – супутникова діалогова пакетно-комутована мережа, призначена для обміну телекомунікаційною та цифровою інформацією в рамках системи супутникового зв'язку з топологією типу «зірка» з можливістю повного дуплексу (рис. 3.37).

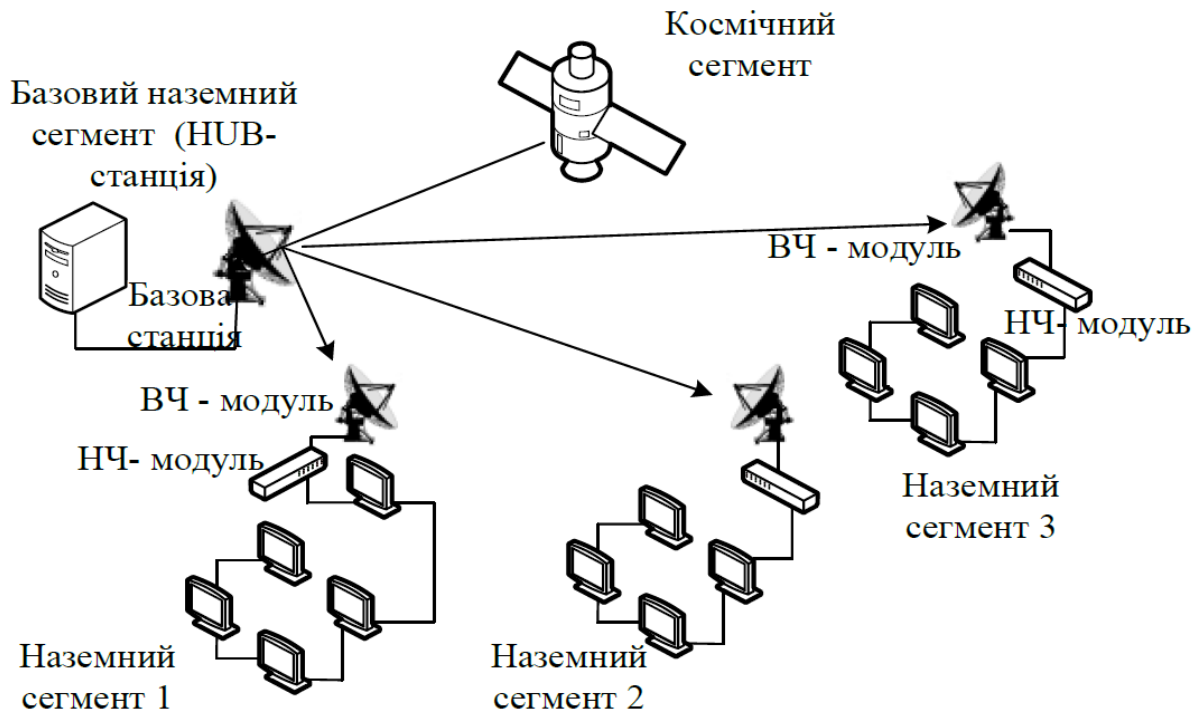


Рис. 3.37. Структура PES – системи

Запитання для самоконтролю:

1. Назвіть основні переваги застосування бездротових локальних мереж та їх особливості.
2. Наведіть теоретичні основи передачі даних в бездротових мережах.
3. У чому полягає технологія частотного розширення спектра?
4. Які ви можете назвати робочі режими систем та мереж бездротового зв'язку?
5. Назвіть основні елементи бездротової мережі.
6. Що називають локальною безпроводною мережею з (Ad-Hoc) режимом?
7. Яку функцію виконують бездротові інтерфейсні адаптери?
8. Назвіть види модуляції в системах бездротового зв'язку.
9. Яка різниця між фазовою і частотною модуляцією, принципи використання у БСМ?
10. Охарактеризуйте технологію розширення спектру бездротових мереж.
11. Розкрийте технологію FHSS.
12. Яке призначення широкосмугового шлюзу?
13. Принципи використання точки доступу, як широкосмугового маршрутизатора.
14. Поясніть поняття «базовий та розширений набір служб».
15. Поясніть режим клієнта в БСМ.
16. Наведіть структурні схеми побудови БСМ з умови її з'єднання з комутативною стандартною мережею.
17. Поясніть функції та задачі роботи БСМ в режимі повторювача.
18. Наведіть структурні схеми побудови БСМ з топологією – кільце, зірка, тощо.
19. Поясніть функції та задачі роботи БСМ в режимі «складний мостовий режим».
20. Поясніть функції та задачі роботи БСМ в режимі Infrastructure Mode.
21. Дайте визначення поняття «системи супутникового зв'язку».
22. Назвіть основні переваги систем цифрового супутникового зв'язку.
23. Назвіть складові наземного сегмента систем супутникового зв'язку.
24. Основні методи кодування в системах супутникового зв'язку.
25. Наведіть особливості множинного доступу у супутникових системах.
26. Порівняйте продуктивність FDMA і TDMA.
27. Назвіть особливості розподілу інформаційного потоку по каналах зв'язку.
28. Розкрийте зміст методів супутникової комутації інформаційних потоків.

29. Назвіть основні характеристики системи зв'язку множинного доступу та її архітектури.
30. Охарактеризуйте канали із завмираннями.
31. Що таке супутникова комутація? Які існують її методи?
32. Розкрийте поняття «матриця інформаційного обміну».
33. Охарактеризуйте систему множинного доступу.
34. Опишіть схему роботи SCPC-системи.
35. Розкрийте суть поняття системи повного доступу (TES-система).

Розділ 4. ОРГАНІЗАЦІЯ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

4.1. Основи криптографічного захисту

«Криптографія» – грецьке слово, що походить від слів *kryptos* (таємний, схований) та *graphy* (запис) і містить методи та засоби забезпечення перетворення даних з метою маскування (шифрування) змісту інформації для гарантування конфіденційності та цілісності, а «криптоаналіз» орієнтований на зламування шифротекстів (шифрів). Шифротекст – це дані, які представлені у зашифрованій формі та мають прихований семантичний зміст, який утворюється після шифрування (криптографічного перетворення) відкритого тексту (з неприхованим семантичним змістом).

Зародження криптографії почалося з глибокої давнини, з якої до нас дійшов ряд систем шифрування, які швидше за все з'явилися одночасно з писемністю у 4 тис. до н. е. Методи секретного переписування були винайдені незалежно в багатьох стародавніх суспільствах (Єгипет, Шумер, Китай).

За свідченням Геродота у Стародавньому Єгипті роль шифру зазвичай відігравала спеціально створена жрецькими мова. Там паралельно існували три алфавіти: письмовий, священний і таємний, останній з яких застосовувався пророками для приховування змісту повідомлень.

В епоху розквіту Риму шифрований зв'язок для його органів влади став життєво необхідним. У цей час застосовувався відомий шифр заміни, пов'язаний з ім'ям Юлія Цезаря, про якого Гай Светоній повідомляє: «Існують і його листи до Цицерона і листи до близьких про домашні справи: в них, якщо потрібно було повідомити про що-небудь негласно, він користувався тайнописом, тобто змінював букви так, щоб з них не складалося жодного слова. Щоб розібрати і прочитати їх, потрібно кожного разу читати четверту букву замість першої, наприклад, D замість A і так далі». Наприклад, відповідно до цього шифру послання сенату VENI VIDI VICI (ПРИЙШОВ ПОБАЧИВ ПЕРЕМІГ), зроблене Цезарем після односторонньої війни з понтийським царем Фарнаком, представлялося б шифротекстом SBKF SFAF SFZF.

Відомий принципово інший шифр, пов'язаний з перестановкою букв повідомлення за певним (відомим відправнику і одержувачу) правилом. Стародавні помітили, що якщо смужку пергаменту намотати спіраллю на паличку і написати на ній вздовж палички текст повідомлення то, після зняття смужки букви будуть розташовані хаотично. Це те ж саме, ніби букви писати не підряд, а через домовлене число по кільцю доти, доки весь текст не буде вичерпаний. Так відкритий текст ДЕРЖВНИЙ при діаметрі палички в 3 букви дасть шифротекст ДАЙЕВРНЖИ, для розшифрування якого слід знати систему засекречування і мати ключ у вигляді палички, прийнятого діаметру (рис. 4.1). Цей шифр іменувався скитала (сцитала) за назвою стержня, на який намотувалися свитки папірусу.

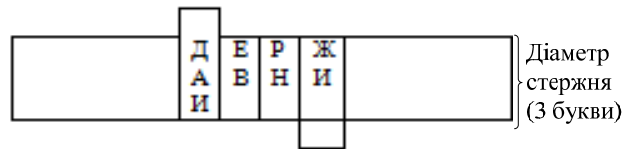


Рис. 4.1. Приклад шифрування за допомогою шифра скитала

Варто зазначити, що грецький письменник і історик Полібій винайшов так званий полібіанський квадрат (II ст. до н. е.) розміром 5×5, заповнений алфавітом у випадковому порядку. Для шифрування на квадраті знаходили букву тексту і вставляли в шифротекст нижню від неї у тій самій колонці. Якщо буква була в нижньому рядку, то брали, верхню з тієї самої колонки.

Наведемо спрощений приклад такого квадрату (рис. 4.2), для якого відкритому тексту ДЕРЖАВНИЙ буде відповідати шифротекст РГНКЖИЙГБ.

А	З	І	Й	Є
Ж	В	П	Б	Л
К	И	Е	Д	С
М	Т	Г	Р	Ц
О	Х	Ф	Н	І

Рис. 4.2. Приклад зашифрованого тексту полібіанським квадратом

Паралельно з методами шифрування створювалися і засоби їх реалізації. Так, наприклад, винахідливі римляни застосовували два шифруючих диски (IV ст. до н. е.), які були розміщені на спільну вісь. Кожен з них містив на ободі алфавіт у випадковій послідовності. Знайшовши на одному диску букву тексту, з іншого диска зчитували відповідну їй букву шифру. Такі пристрої використовувалися аж до епохи Відродження. Але з моменту падіння Римської імперії багато досягнень криптографії були втрачені і лише в кінці Середньовіччя її застосування починає відроджуватися.

В ручних шифрах того часу часто використовуються таблиці, що дають прості шифрувальні процедури перестановки букв у повідомленні. Тут ключем служать розмір таблиці, фраза, що задає перестановку, або спеціальна особливість таблиць. Проста перестановка без ключа – один з найпростіших методів шифрування, споріднений шифру скитала. Наприклад, повідомлення ДЕРЖАВНИЙ ЕКОНОМІКО ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ записується в таблицю в рядки. Для таблиці з 5 рядків і 11 колонок це виглядає так, як показано на рис. 4.3:

Д	Е	Р	Ж	А	В	Н	И	Й	Е	К
О	Н	О	М	І	К	О	Т	Е	Х	Н
О	Л	О	Г	І	Ч	Н	И	Й	У	Н
І	В	Е	Р	С	И	Т	Е	Т	Т	Р
А	Н	С	П	О	Р	Т	У			

Рис. 4.3. Приклад шифрування за допомогою таблиць

Після того, як відкритий текст записали рядками, для утворення шифротексту він зчитується колонками. Якщо його записувати групами по 3 букви, то вийде: ДООІА ЕНЛВН РООЕС ЖМГРП АПСО ВКЧИР НОНТТ ИТИЕУ ЙЕЙТ ЕХУТ КННР. Для використання цього шифру відправнику й одержувачу необхідно домовитися про загальний ключ як розмір таблиці. Групування букв не входить у ключ шифру і використовується лише для зручності запису беззмістовного тексту.

Середньовічні вчені часто використовували магічний квадрат у вигляді рівносторонньої таблиці з вписаними в їх комірки послідовними натуральними числами від 1, що дають у сумі в кожній колонці, кожному рядку і кожній діагоналі те саме число. В такі квадрати вписувався відкритий текст відповідно до наведеної в них нумерації. Якщо потім виписати вміст таблиці колонками, то виходить шифротекст утворений перестановкою букв. Вважалося, що такі створені шифротексти охороняє не тільки ключ, але і магічна сила. На рис. 4.4 наведено приклад магічного квадрата і його шифротексту.

16	3	2	13	Ї	Х	А	А
5	10	11	8	С	О	Р	Н
9	6	7	12	Ф	Т	І	М
4	15	14	1	И	І	Ц	З

Рис. 4.4. Приклад шифрування за допомогою магічного квадрата

Отриманий з відкритого тексту ЗАХИСТ ІНФОРМАЦІЇ, шифротекст ЇСФИХОТІАРІЦАНМЗ має досить вагомий вигляд. На перший погляд здається, начебто магічних квадратів дуже мало, але їх число дуже швидко зростає зі збільшенням розміру квадрату. Так, існує лише один магічний квадрат розміром 3×3 (не враховуючи його повороти), квадратів 4×4 уже 880, а 5×5 близько 250000, тому їх великі розміри стали вагомою основою для надійної системи шифрування того часу, оскільки ручний перебір всіх варіантів ключа для цього шифру був немислимий.

Одна з відомих фігур ренесансної архітектури пов'язана з ім'ям Леона Батисту Альберта, який винайшов шифр поліалфавітної заміни, що є стійким до розкриття і докладно описав пристрої з коліс, що прокручуються, для його реалізації. Цей шифр можна описати спеціальною таблицею шифрування (рис. 4.5), яку іноді називають таблицею (квадратом) Віженера, названу ім'ям дипломата Блеза Віженера, який у XVI ст. розвивав і удосконалював криптографічні системи.

	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я	–
А	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я	–
Б	–	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я
В	я	–	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю
Г	ю	я	–	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь
Д	ь	ю	я	–	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ
Е	ш	щ	ь	ю	я	–	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч
Є	ч	ш	щ	ь	ю	я	–	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц
Ж	ц	ч	ш	щ	ь	ю	я	–	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х
З	х	ц	ч	ш	щ	ь	ю	я	–	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф
И	ф	х	ц	ч	ш	щ	ь	ю	я	–	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й	К	Л	М	Н	О	П	Р	С	Т	У
І	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	–	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й	К	Л	М	Н	О	П	Р	С
Й	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	–	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й	К	Л	М	Н	О	П	Р
К	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	–	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й	К	Л	М	Н	О	П
Л	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	–	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й	К	Л	М	Н	О
М	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	–	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й	К	Л	М
Н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	–	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й	К	Л	М	Н
О	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	–	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й	К	Л
П	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	–	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й	К
Р	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	–	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й
С	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	–	А	Б	В	Г	Д	Е	Є	Ж	З	И	І
Т	і	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	–	А	Б	В	Г	Д	Е	Є	Ж	З	И
У	і	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	–	А	Б	В	Г	Д	Е	Є	Ж	З	И
Ф	и	і	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	–	А	Б	В	Г	Д	Е	Є	Ж	З
Х	з	и	і	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	–	А	Б	В	Г	Д	Е	Є	Ж
Ц	ж	з	и	і	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	–	А	Б	В	Г	Д	Е	Є
Ч	є	ж	з	и	і	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	–	А	Б	В	Г	Д	Е
Ш	є	ж	з	и	і	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	–	А	Б	В	Г	Д	Е
Щ	д	є	ж	з	и	і	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	–	А	Б	В	Г	Д
Ь	г	д	є	ж	з	и	і	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	–	А	Б	В	Г
Ю	г	д	є	ж	з	и	і	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	–	А	Б	В	Г
Я	в	г	д	є	ж	з	и	і	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	–	А	Б	В
–	б	в	г	д	є	ж	з	и	і	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	–	А	Б

Рис. 4.5. Приклад квадрату Віженера

Кожен рядок у цій таблиці відповідає одному типовому шифру Цезаря для алфавіту з проміжком. Повідомлення, що шифрується, виписують у рядок, а під ним розміщують ключ. Якщо він виявився коротший за відкритий текст, то його циклічно повторюють. Шифротекст формується шляхом знаходження символу у колонці таблиці за буквою тексту і рядка, що відповідає букві ключа. Наприклад, використовуючи ключ НАУ для відкритого тексту АВІАЦІЙНИЙ сформується шифротекст, який наведений на рис. 4.6:

повідомлення	А	В	І	А	Ц	І	Й	Н	И	Й
ключ	Н	А	У	Н	А	У	Н	А	У	Н
шифротекст	Н	В	Т	Н	Ц	Т	Ь	Н	С	Ь

Рис. 4.6. Приклад шифрування квадратом Віженера

Цей розповсюджений підхід дожив і до наших днів. Практично таку операцію можна реалізувати додаванням кодів ASCII символів відкритого тексту і ключа за деяким модулем.

Крім своїх архітектурних шедеврів, Альберт ще ввів у практику криптографії багатоалфавітні (поліалфавітні) шифри заміни. Його книга «Трактат про шифр» (1466 р.) була першою у світі науковою працею з криптографії (не враховуючи арабських рукописів, які у Європі мало знали).

Історики вважають Йогана Тритемія другим батьком сучасної криптографії, який у роботі «Стеганографія» першим систематично описав застосування таблиць шифрування, які заповнені алфавітом у випадковому порядку, а також зазначив, що можна шифрувати дві букви за один раз. Такі шифри, на відміну від раніше описаних (монограмних), були названі біграмними підстановочними шифрами і різко підсилили їхню стійкість до

розкриття. Найбільш відомий шифр біграмами називається Play-fair (Чесна гра), винайдений у 1854 р. Він застосовувався Великобританією в Першу світову війну. Опишемо його на прикладі магічного квадрата (рис. 4.4):

Відкритий текст розбивався на пари букв (біграми) і шифротекст складався з нього за такими двома дуже простими правилами:

1. Якщо обидві букви біграми початкового тексту належали одній колонці таблиці, то буквами шифру вважалися ті, що знаходились під ними. Так біграма ЗИ давала текст ВТ. Якщо буква відкритого тексту знаходилася в нижньому рядку, то для шифру бралася відповідна буква з верхнього ряду і біграма СІ давала шифр ЦЄ. (Біграма з однієї букви чи пари однакових букв теж підпорядковувалася цьому правилу і текст ЗЗ давав шифротекст ВВ).

2. Якщо обидві букви біграми початкового тексту належали одному рядку таблиці, то буквами шифру вважаються букви, які знаходились праворуч від них. Так біграма ИД давала шифротекст ЄС. Якщо буква відкритого тексту знаходилася у правій колонці, то для шифру бралася відповідна буква з лівої колонки і біграма СЕ давала шифр КД. Якщо обидві букви біграми відкритого тексту лежали в різних рядах і колонках, то замість них бралися такі дві букви, щоб уся четвірка їх представляла прямокутник. При цьому послідовність букв у шифрі була дзеркальною початковій парі. Наприклад, ВР шифрувалося як БТ, а ДХ як ИН.

Шифрований текст слова АВІАЦІЙНИЙ за біграмами показано на рис. 4.7 в нижньому рядку.

А	В	І	А	Ц	І	Й	Н	І	Й
З	Ж	О	Є	М	О	Б	Й	Е	З

Рис. 4.7. Шифротекст за біграмами

З'являються професійні і навіть потомственні криптографи, типу сімейства Ардженті, який служив у папи Римського.

Починаючи з тих часів, багато видатних математиків стали залучатися до криптографічної служби, наприклад, у Росії Леонард Ейлер, якому історики приписують знаменитий гороскоп Івана VI, а у Франції таким математиком був Франсуа Бієт.

У XVII ст. в Англії математик Джон Валліс очолював криптографічну службу і одержав популярність за рідкісні успіхи в розшифруванні, а в Німеччині того часу кращим криптографом був Лейбніц.

Роджер Бекон, будучи лордом-канцлером при королі Якові I, добре знав потреби держави в надійних шифрах і у 1580 р. написав роботу з криптографії, яка одержала успішний практичний розвиток, наприклад, він вперше запропонував двійкове кодування букв латинського алфавіту, що використовується зараз у комп'ютерах.

У XIX ст. почалася автоматизація процесу шифрування, наприклад, держсекретар Томас Джефферсон (згодом президент США) у 1790 р.

винайшов шифруюче колесо, що реалізує поліалфавітну заміну тексту повідомлення за ключем, довжина періоду якого визначалася найменшим загальним кратним періодів обертів шифруючих коліс, наприклад, чотирьом колесам з періодом обертів 13, 15, 17 і 19 відповідала довжина періоду ключа 62985. Відомі також циліндр Базери (запропонований Етьеном Базери в 1891 р.), криптографічна машина (1917 р.) Жильбера Вернама та роторна машина Едварда Хеберна (1917 р.), яку згодом назвали Енігмою. У 1942 р. Аланом Тьюрингом була створена швидкодіюча ЕОМ під назвою «Колосс», спеціалізована для злому шифрів Енігми.

Завершує історію цього етапу криптографії математик Клод Елвуд Шеннон, який під час Другої світової війни, досліджуючи математичними методами надійність шифрування, включив криптологію в загальну теорію інформації.

4.2. Криптографічні методи

Суть криптографії – у забезпеченні конфіденційності даних (відкритого тексту, секретного ключа) шляхом їх шифрування.

Крім забезпечення конфіденційності, криптографія застосовується для розв’язання таких задач, як:

- перевірка справжності (ідентифікація). Одержувач може встановити відправника, а зловмисник не може під нього маскуватися;
- цілісність. Отримувач може перевірити несанкціоновану модифікацію в тексті, а зловмисник не може видати підроблений текст за справжній;
- не заперечення авторства. Відправник не може в подальшому заперечувати відсилку даних.

Початкове повідомлення називають відкритим текстом P (plaintext), а процес приховування його семантичного змісту називають шифруванням і позначають E (encipher). У результаті шифрування утворюється шифротекст C (ciphertext), а одержання початкового відкритого тексту здійснюється в процесі розшифрування D (decipher) шифротексту (криптограми). Ця послідовність показана на рис. 4.8. В математичній формі функція шифрування і розшифрування відповідно записується як $E(P)=C$ і $D(C)=P$, а оскільки $D(C)$ є відновлення P , то справедливо $D(E(P))=P$.

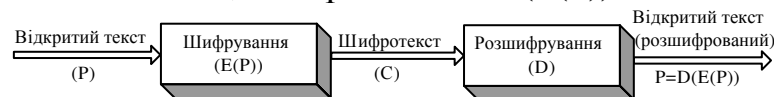


Рис. 4.8. Шифрування і розшифрування

Сучасна криптографія містить у собі чотири базові розділи:

- симетричні криптосистеми (системи з секретним ключем або одноключові);
- асиметричні криптографічні системи (системи з відкритим ключем або двоключові);
- криптографічні протоколи;
- керування ключами.

Криптографічний алгоритм, також названий **шифром** – це математична функція, яка використовується для шифрування і дешифрування.

Якщо безпека алгоритму заснована на збереженні самого алгоритму в таємниці, то це **обмежений алгоритм**. Обмежені алгоритми представляють тільки історичний інтерес, оскільки не відповідають сьогоднішнім стандартам і не допускають можливості якісного контролю чи стандартизації. Крім того, у кожній групі користувачів повинен бути свій унікальний алгоритм і такі групи не можуть використовувати відкриті апаратні чи програмні продукти, оскільки зломисник може купити такий самий продукт і розкрити алгоритм.

Сучасна криптографія вирішує ці проблеми за допомогою **ключа** K (key), що використовується в функціях E і D , може приймати будь-яке значення і бути обраним з великої множини, яку називають **простором ключів**. Ключовий простір розглядаються як потужність множини ключів, які використовують для даного шифру. Тоді відносно K функції E і D приймають вигляд $A_k(P)=C$, $D_k(C)=P$, при цьому справедлива рівність $D_k(E_k(P))=P$ (рис. 4.9).

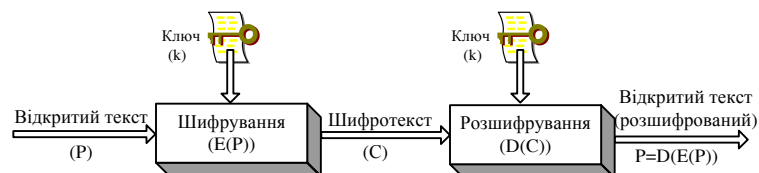


Рис. 4.9. Шифрування і розшифрування за допомогою ключа

Для деяких алгоритмів при шифруванні і розшифруванні використовуються різні ключі K_1 – для шифрування, K_2 – для розшифрування, то у цьому випадку $A_{k_1}(P) = C$, $D_{k_2}(C)=P$, $D_{k_2}(E_{k_1}(P))=P$ (рис. 4.10).

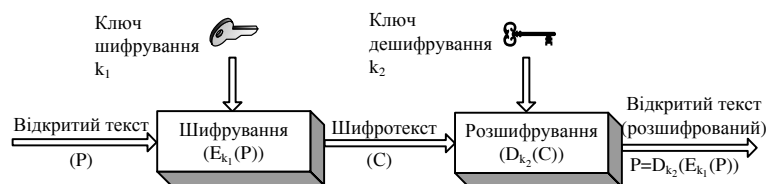


Рис. 4.10. Шифрування і розшифрування за допомогою двох різних ключів

Безпека цих алгоритмів цілком заснована на ключах, а не на деталях алгоритмів. Це значить, що алгоритм може бути опублікований і проаналізований. Продукти, що використовують цей алгоритм, можуть широко тиражуватися. Не має значення, що зломиснику відомий алгоритм, якщо йому не відомий конкретний ключ, то він не зможе прочитати шифротекст.

У криптографії існують дві базові методології з використанням ключів – **симетрична** (рис. 4.9) і **асиметрична** (рис. 4.10) і які відповідно називають із секретним ключем і з відкритим ключем. Кожна методологія використовує свої власні процедури, свої способи розподілу ключів, їх типи, алгоритми шифрування і розшифрування ключів.

Для сучасних криптографічних систем захисту інформації **існують загальні вимоги**, до яких відносяться:

- шифротекст (C) повинен піддаватися читанню тільки при наявності ключа (k);
- число операцій, необхідних для визначення ключа (k) шифрування, за фрагментом шифротексту (C) і відповідного йому відкритого тексту (P), повинно бути не менше загального числа можливих ключів (k);
- число операцій, необхідних для розшифровування (D(C)) шляхом перебору всіх можливих k (лобова атака), повинно мати строгую нижню оцінку і виходити за межі можливостей сучасних та перспективних комп'ютерних систем та мереж;
- знання алгоритму шифрування не повинно впливати на надійність криптографічного захисту;
- незначна зміна ключа (k) повинна приводити до істотної зміни шифротексту (C);
- структурні елементи алгоритму шифрування повинні бути незмінними;
- довжина шифрованого тексту (C) повинна бути близькою довжині відкритого тексту (P);
- не повинно бути простих і легко встановлюваних залежностей між ключами, що використовуються в процесі шифрування (D(C));
- алгоритм повинен допускати як програмну, так і апаратну реалізацію, при цьому зміна довжини ключа (k) не повинна вести до якісного погіршення алгоритму шифрування.

Спроба криптоаналізу називається **розкриттям** (зламуванням шифру), за допомогою якого можна отримати P, не маючи k. Успішно проведений криптоаналіз може визначити P чи k, а також знайти слабкі місця в криптосистемах, що зрештою приведе до визначення відкритого тексту чи ключа.

Основне припущення криптоаналізу, вперше сформульоване у XIX ст. Датчманом А. Керкгофом (Dutchman A. Kerckhoffs) – безпека повинна цілком визначатися ключем, а криптоаналітик має повний опис алгоритму і його реалізації.

Покажемо відомі типи розкриття, які засновуються на припущенні, що криптоаналітик має всю повноту знання про використовуваний алгоритм шифрування.

1. Розкриття на основі тільки шифротексту. У криптоаналітика є шифротексти ($C_1, C_2, \dots, C_i$) декількох відкритих текстів ($P_1, P_2, \dots, P_i$), зашифрованих одним алгоритмом. Криптоаналітик розкриває як можна більшу кількість криптограм (визначення P), або ключів

шифрування з метою розкриття інших шифротекстів, зашифрованих тим самим ключем (ключами). Іншими словами, маючи

$$C_1=E_k(P_1), C_2=E_k(P_2), \dots, C_i=E_k(P_i),$$

можна визначити $P_1, P_2, \dots, P_i$ та k або алгоритм відновлення

$$P_{i+1} \text{ із } C_{i+1}=E_k(P_{i+1}).$$

2. **Розкриття на основі відкритого тексту.** У криптоаналітика є доступ до шифротекстів ($C_1, C_2, \dots, C_i$) і їх відкритих текстів ($P_1, P_2, \dots, P_i$). Він розкриває ключ (ключі) з метою розшифрування інших шифротекстів, зашифрованих тим же ключем (ключами). Іншими словами, маючи

$$P_1, C_1=E_k(P_1), P_2, C_2=E_k(P_2), \dots, P_i, C_i=E_k(P_i)$$

можна визначити k або алгоритм відновлення

$$P_{i+1} \text{ із } C_{i+1}=E_k(P_{i+1}).$$

3. **Розкриття на основі підбраного відкритого тексту.** У криптоаналітика є шифровані і відкриті тексти декількох повідомлень, а також можливість підібрати відкритий текст для шифрування. Це надає більше варіантів, ніж розкриття на основі відкритого тексту, оскільки криптоаналітик здійснює вибір блоків відкритого тексту, що підлягають шифруванню і це може дати більше інформації про ключ. Криптоаналітик одержує ключ (ключі), шифрування чи алгоритм, що дозволяє розкрити нові повідомлення, зашифровані тим же ключем (ключами). Іншими словами, маючи

$$P_1, C_1=E_k(P_1), P_2, C_2=E_k(P_2), \dots, P_i, C_i=E_k(P_i)$$

та можливість вибирати $P_1, P_2, \dots, P_i$ визначається k або алгоритм знаходження

$$P_{i+1} \text{ із } C_{i+1}=E_k(P_{i+1}).$$

4. **Розкриття на основі адаптивно підбраного відкритого тексту.** Криптоаналітик може вибирати відкритий текст, що підлягає шифруванню, також уточнювати наступний вибір на базі раніше отриманих результатів шифрування. При розкритті з використанням підбраного відкритого тексту криптоаналітик бере для шифрування тільки один великий блок відкритого тексту, а при адаптивному вибирається менший блок і потім наступний, використовуючи результати першого вибору і т. д.

5. **Розкриття з використанням підбраного шифротексту.** Криптоаналітик для розкриття може вибирати різні шифротексти і має доступ до розшифрованих відкритих текстів. Наприклад, маючи «чорний ящик», що реалізує автоматичне розшифрування, необхідно одержати ключ. Іншими словами, маючи

$$C_1, P_1=D_k(C_1), C_2, P_2=D_k(C_2), \dots, C_i, P_i=D_k(C_i),$$

визначаємо k . Таке розкриття зазвичай застосовується до систем з відкритим ключем, але іноді буває ефективним і для симетричних алгоритмів. (Часто розкриття третього і п'ятого типу разом називають розкриттям на основі підбраного тексту.)

6. **Розкриття на основі підбраного ключа.** Криптоаналітик має деяку інформацію про зв'язок між різними ключами. Цей тип розкриття

часто буває дуже практичний і відрізняється від усіх раніше розглянутих. Криптоаналітик вибирає зв'язок між парою невідомих ключів, за допомогою яких зашифровані дані. У варіанті з відомим відкритим текстом є відкритий і шифрований двома ключами текст, а у варіанті з підібраним ключем – криптоаналітик вибирає відкритий текст для шифрування двома ключами.

7. **Бандитський криптоаналіз.** Криптоаналітик загрожує, використовує тортури чи шантажує кого-небудь, поки не знайде ключ. Хабарництво іноді називається **розкриттям з купівлею ключа**, часто є дуже вагомим способом зламування шифрів.

Базові шифри. Підстановочні і перестановочні шифри. До появи комп'ютерів криптографія складалася з алгоритмів на символній основі, які або заміняли одні символи іншими, або реалізовували їх перестановку. Кращі алгоритми робили і заміни (підстановки) і перестановки (перемішування) з циклічними повторами.

Сучасні зміни полягають у тому, що алгоритми стали працювати з бітами, а не символами, що важливо хоча б з погляду розміру алфавіту (перехід з 26 елементів до двох). Більшість криптографічних алгоритмів комбінують підстановки і перестановки.

Підстановочним називають такий **шифр**, у якому кожний символ відкритого тексту в шифротексту замінюється іншим символом. Одержувач інвертує підстановку шифротексту, відновлюючи відкритий текст. У криптографії використовують чотири типи підстановочних шифрів (рис. 4.11).

Знаменитий **шифр Цезаря** є простим підстановочним шифром і дійсно дуже простим, тому, що алфавіт шифротексту є зміщеним, а не випадково розподіленим.

Прості підстановочні шифри легко розкриваються, оскільки шифр не ховає частоти використання різних символів у відкритому тексті і для відновлення, наприклад, англійського шифротексту, криптоаналітику необхідні тільки частоти використання 26 англійських символів.

Однозвучні підстановочні шифри використовувалися вже у 1401 р. в герцогстві Мантуа. Вони більш складні для розкриття, хоча і не ховають усіх статистичних властивостей мови відкритого тексту. На основі розкриття з відомим відкритим текстом ці шифри зламуються елементарно, а на основі тільки шифротексту – складніше, але використовуючи комп'ютер, це займе декілька секунд.



Рис. 4.11. Класифікація підстановочних шифрів

Поліграмні підстановочні шифри кодують відразу групи символів. Частинним випадком поліграмного шифру є біграмний Play-fair.

Поліалфавітні підстановочні шифри були винайдені Ліном Баттістой (Leon Battista) у 1568 р. Вони використовувалися армією Сполучених Штатів у ході Громадянської війни в Америці. Шифр (квадрат) Віженера (Vigenere), який вперше опублікований у 1586 р. і шифр Бофора (Beaufort) також є прикладами поліалфавітних підстановочних шифрів.

У поліалфавітних підстановочних шифрах використовується множина однолітерних ключів для шифрування тільки одного символу відкритого тексту. Першим ключем шифрується перший символ відкритого тексту, другим – другий символ, і так далі. Після використання усіх ключів вони повторюються циклічно. Якщо застосовується 20 однолітерних ключів, то кожна двадцята літера шифрується тим же ключем. Цей параметр називається періодом шифру. Шифри з довгим періодом складніше розкрити, чим з коротким, але використання обчислювальної техніки значно спростило цю задачу.

Шифр зі змінним ключем (іноді названий книжковим шифром), що використовує один текст для шифрування іншого тексту і хоча період ключа дорівнює довжині тексту, він також може бути легко зламаний.

У **перестановочному шифрі** міняється не відкритий текст, а порядок символів. У **простому колонковому перестановочному шифрі** відкритий текст пишеться горизонтально на розграфленому листі фіксованої ширини, а шифротекст зчитується вертикально. Дешифрування є записом шифротексту вертикально на розграфленому листі фіксованої ширини і потім зчитування відкритого тексту горизонтально. Символи шифротексту ті ж самі, що й у відкритому тексті, і мають приблизно ті самі частотні характеристики, що і звичайно.

Відповідно до базових методологій використання ключів є два відповідних базових типів алгоритмів: **симетричні і асиметричні**.

Симетричні алгоритми, іноді називаються умовними алгоритмами, у яких ключ шифрування може бути розрахований за ключем дешифрування і навпаки. У більшості симетричних алгоритмів ключі шифрування і дешифрування ті самі (рис. 4.9). Ці алгоритми також називають алгоритмами із секретним ключем (передається секретним каналом) чи алгоритмами з одним ключем, вони вимагають, щоб відправник і одержувач погодили використовуваний ключ перед початком безпечної передачі повідомлень. Безпека симетричного алгоритму визначається ключем, знання якого дозволяє розшифрувати повідомлення. Тому, поки повідомлення є секретними, ключ повинен триматись у таємниці.

Симетричні алгоритми поділяються на дві категорії.

1) Алгоритми, що обробляють відкритий текст побітово (іноді побайтово) називаються **потокowymi чи алгоритмами з потокowymi шифрами**.

2) Алгоритми, що працюють з групами бітів, які складають блоки (наприклад, 64 біт) називаються **блоковими чи алгоритмами з блоковими шифрами**. До появи комп'ютерів алгоритми зазвичай обробляли відкритий текст посимвольно, що може розглядатися як потокове шифрування символів.

Алгоритми з відкритим ключем (асиметричні алгоритми) розроблені таким чином, що ключ, використовуваний для шифрування, відрізняється від ключа дешифрування (рис. 4.11). Більше того, ключ дешифрування не може бути (принаймні протягом певного інтервалу часу) розрахований за ключем шифрування. Алгоритми називаються «з **відкритим ключем**» тому, що ключ шифрування може бути відкритим і хто завгодно може використовувати його (отримуючи не секретним каналом) для шифрування відкритого тексту, але тільки власник відповідного ключа дешифрування може розшифрувати повідомлення. У цих системах ключ шифрування часто називається **відкритим**, а розшифрування – **закритим**.

Безпека алгоритмів. Різні алгоритми надають різні ступені безпеки залежно від того, наскільки важко зламати алгоритм. Якщо вартість злому алгоритму вище, ніж вартість зашифрованих даних, то ці дані швидше за все у безпеці. Якщо час злому алгоритму більше, ніж час, протягом якого зашифровані дані повинні зберігатися в секреті, то також швидше за все інформація у безпеці. Якщо обсяг даних, зашифрований одним ключем, менше, ніж обсяг даних, необхідний для злому алгоритму, і тоді, швидше за все, інформація у безпеці.

Криптографія більше цікавиться криптосистемами, які важко зламати обчислювальним способом.

Криптосистема це алгоритм плюс усі можливі відкриті тексти, шифротексти і ключі. Алгоритм вважається **обчислювально безпечним** (чи, як іноді називають, криптостійкими), якщо він не може бути зламаний з використанням доступних ресурсів зараз чи у майбутньому. Термін

«доступні ресурси» є досить розпливчастим. Складність розкриття можна визначити різними способами (рис. 4.12).

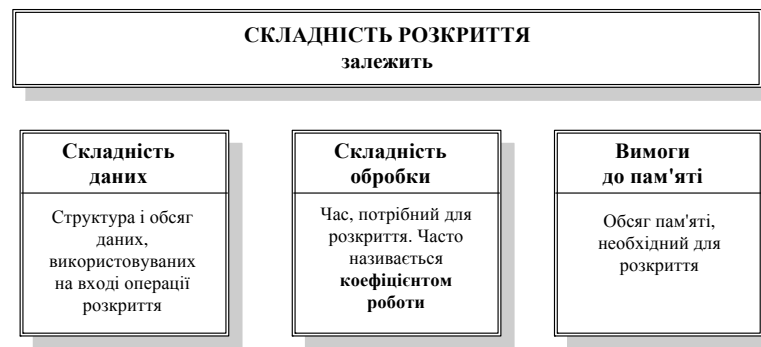


Рис. 4.12. Характеристики складності розкриття даних

Як емпіричний метод складність розкриття визначається за максимальним з цих трьох коефіцієнтів. Ряд операцій розкриття припускають взаємозв'язок коефіцієнтів, наприклад, більш швидке розкриття можливе за рахунок збільшення вимог до пам'яті.

Складність виражається порядком величини. Якщо складність обробки для даного алгоритму складає 2^{128} , то 2^{128} операцій потрібно для розкриття алгоритму (ці операції можуть бути складними і тривалими). Так, якщо передбачається, що обчислювальні потужності здатні виконувати мільйон операцій у секунду, і для рішення задачі використовується мільйон паралельних процесорів, одержання ключа займе у понад 10^{19} років, що в мільярд раз перевищує час існування всесвіту. У той час, як складність розкриття залишається постійною (поки будь-який криптоаналітик не придумає кращого способу розкриття), потужність комп'ютерів зростає. За останні піввіку обчислювальні потужності феноменально виросли і немає ніяких причин підозрювати, що ця тенденція не буде продовжена. Багато криптографічних зломів придатні для паралельних комп'ютерів. Задача розбивається на мільярди маленьких шматочків, рішення яких не вимагає міжпроцесорної взаємодії. Оголошення алгоритму безпечним просто тому, що його нелегко зламати, використовуючи сучасну техніку, у кращому випадку ненадійно. Якісні криптосистеми проектуються стійкими до злому з урахуванням розвитку обчислювальних засобів на багато років вперед.

Криптографічні протоколи. Криптографія вирішує проблеми секретності, перевірки дійсності, цілісності і людської нечесності. Можна вивчити все про криптографічні алгоритми і методи, але вони представляють тільки академічний інтерес, якщо не використовуються для вирішення будь-якої проблеми. Саме тому протоколи являються невід'ємною частиною криптографічних систем.

Протокол – це порядок дій, що починаються двома чи більше сторонами, призначений для вирішення певної задачі. «Порядок дій» означає, що протокол виконується у певній послідовності від початку до кінця, а кожна дія має свою чергу і ініціюється після закінчення

попередньої. «Починаються двома чи більш сторонами» означає, що для реалізації протоколу потрібно принаймні дві особи, тому, що одна особа не зможе реалізувати протокол. Окрема особа може виконати деякі дії, вирішуючи певну задачу (наприклад, запису на диск), але це не протокол. Нарешті, «призначений для вирішення певної задачі» означає, що протокол повинен приводити до якогось результату. У протоколів є також й інші характеристики (рис. 4.13).

Виконання протоколу реалізуються діями, лінійно, поки не буде команди перейти до наступної дії, кожна з яких за меншою мірою містить в собі:

- обчислення, що виконуються однією чи декількома сторонами;
- або повідомлення, якими обмінюються сторони.

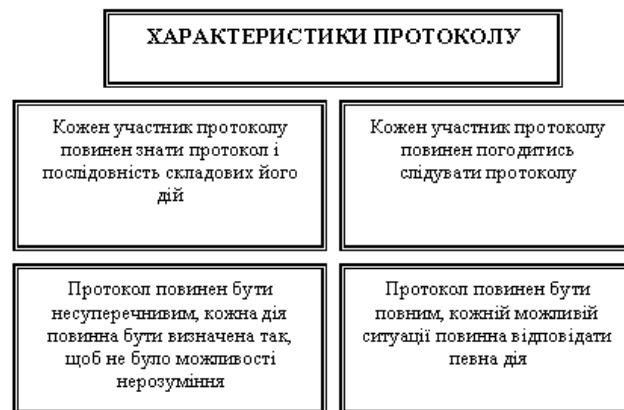


Рис. 4.13. Характеристики протоколу

Передача інформації з використанням симетричної криптографії.

У якісній криптосистемі безпека цілком залежить від знання ключа й абсолютно не залежить від знання алгоритму і тому керування ключами так важливо в криптографії. Ключ повинен залишатися в секреті перед, після і протягом роботи протоколу – доти, поки повинен залишатися в таємниці переданий шифротекст, у противному випадку він відразу буде розкритий.

Симетричні криптосистеми мають такі недоліки:

Розподіл ключів повинен проводитися в секреті. Ключі настільки ж важливі, як і всі шифротексти, зашифровані цими ключами, тому що знання ключа дозволяє розкрити криптограми. Розподіл ключів є дуже важливою задачею і часто кур'єри особисто доставляють ключі за призначенням.

Якщо ключ скомпрометований (украдений, розгаданий, випитаний, отриманий за хабар і т. ін.), то можна розшифрувати всі криптограми, зашифровані цим ключем.

Якщо кожна пара користувачів мережі використовує окремий ключ, то загальна їх кількість швидко росте із зростанням числа користувачів. Розв'язання цієї проблеми можливе шляхом зменшення кількості користувачів, але це не завжди можливо.

Поняття **односпрямованої функції** є центральним у криптографії з відкритими ключами. Односпрямовані функції відносно легко обчислюються, але інвертуються досить складно. Хорошим прикладом такої функції може бути розбита на тисячу малих шматочків ваза, яку нелегко знову скласти з цих шматочків.

Строгого математичного доказу існування односпрямованих функцій немає, як немає і реальних свідчень можливості їхньої побудови. Незважаючи на це, багато функцій виглядають у точності як односпрямовані і їх можна розрахувати, але досі, не має простого способу інвертувати їх. Наприклад, в обмеженій області легко обчислити x^2 , але набагато складніше $x^{\sqrt{2}}$.

Односпрямована функція з секретом (функція-пастка) – це особливий тип односпрямованої функції із секретним люком. Її легко обчислити в одному напрямку і важко – у зворотному. Але якщо вам відомий секрет, ви можете легко розрахувати і зворотну функцію. Тобто, легко обчислити $f(x)$ за відомим x , але важко за відомою $f(x)$ обчислити x . Однак, існує невелика секретна інформація y , що дозволяє, при знанні $f(x)$ і y , легко обчислити x .

Вагомим прикладом односпрямованої функції з секретом може бути годинник, який легко розібрати на сотні маленьких деталей і важко знову зібрати. Але, із секретною інформацією (інструкцією збирання) набагато легше вирішити цю задачу.

У односпрямованої хеш-функції може бути низка імен: функція стискання, функція згортання, дайджест повідомлення, цифровий відбиток, характерна ознака, криптографічна контрольна сума, код цілісності повідомлення, код виявлення маніпуляцій та ін. Але як би не називалась ця функція, вона є центральною в сучасній криптографії і особливо важливе значення має при реалізації багатьох протоколів.

Хеш-функції, які довгий час використовувалися в комп'ютерних науках, є математичними чи іншими функціями, які одержують на вході рядок змінної довжини (**прообраз**) і перетворюють його в рядок фіксованої, зазвичай меншої, довжини (значення хеш-функції, згортка). Приклад такого згортання може бути реалізований за допомогою бінарної функції XOR шляхом одержання прообразу і повертання байта, утвореного виконанням операції побітового складання за модулем 2 ($\oplus$) всіх бітів вхідних байтів, де

$$0 \oplus 0 = 0, 0 \oplus 1 = 1, 1 \oplus 0 = 1, 1 \oplus 1 = 0.$$

Суть хеш-функції полягає в одержанні цифрового відбитку прообразу, тобто утворення значення, за яким можна встановити ідентичність отриманого прообразу і дійсного. Оскільки хеш-функція є співвідношенням «багато до одного», то неможливо з усією визначеністю сказати, що два цифрові відбитки різних документів не збігаються, але хеш-функцію можна використовувати для оцінки з прийнятною точністю.

Односпрямована хеш-функція – це хеш-функція, що працює тільки в одному напрямку, тобто легко обчислити її значення за прообразом, але

важко створити прообраз, значення хеш-функції якого дорівнює заданій величині. Зазначимо, що якісні односпрямовані хеш-функції – це хеш-функція **без колізій (зіткнень)**, тобто достатньо важко створити два прообрази з однаковим значенням хеш-функції.

Хеш-функція є відкритою і секрету її розрахунку не існує. Безпека односпрямованої хеш-функції полягає саме в її односпрямованості. Зміна одного біта прообразу приводить до зміни, у середньому, половини бітів значення хеш-функції. Обчислювально неможливо знайти прообраз, що відповідає заданому значенню хеш-функції.

Код перевірки дійсності повідомлення (message authentication code, MAC), відомий також як код перевірки дійсності даних (data authentication code, DAG), є односпрямованою хеш-функцією з додаванням секретного ключа. Тоді значення хеш-функції залежить від і прообразу, і ключа. У цьому випадку теорія залишається тією самою, що і для хеш-функцій, але тільки той, хто знає ключ, може перевірити значення функції.

Організація зв'язку з використанням асиметричної криптографії.

У 1976 р. Уїтфілд Діффі і Мартін Хеллман змінили парадигму криптографії (яка засновувалась на одноключових системах), описавши асиметричну **криптографію**, що базується на двох різних ключах – відкритому і закритому. Визначення закритого ключа за відкритим вимагає величезних обчислювальних ресурсів. Хто завгодно, використовуючи відкритий ключ, може зашифрувати повідомлення, але не розшифрувати його. Розшифрувати шифротекст може тільки власник закритого ключа. Це схоже на поштову скриньку, де процес шифрування з відкритим ключем можна порівняти з опусканням у її проріз листа, що може зробити кожний. Розшифрування закритим ключем нагадує витягування листа з поштової скриньки, що набагато складніше і може знадобитися зварювальний агрегат, але якщо знати секрет (код замка від поштової скриньки), можна легко дістати лист.

Математичною основою процесу є односпрямовані хеш-функції з секретом, за допомогою яких легко реалізується шифрування в прямому напрямку, а дешифрування – в зворотному і воно настільки важке, що, не знаючи секрету, навіть на комп'ютерах Cray за тисячі (і мільйони) років неможливо розшифрувати криптограму. Секретом (люком) служить закритий ключ, який робить розшифрування таке ж простим, як і шифрування.

Слід зазначити, що криптографія з відкритими ключами усуває проблему розподілу ключів, властиву симетричним криптосистемам.

Зазвичай ціла мережа користувачів приймає для використання певну асиметричну криптосистему. У кожного з них є відкритий і закритий ключ, при цьому відкриті ключі містяться в загальнодоступній базі даних. Ось як на основі цієї криптографії відправник може переправити повідомлення одержувачу:

1. Відправник і одержувач домовляються використовувати асиметричну криптосистему.

2. Одержувач посилає відправнику свій відкритий ключ.
3. Відправник шифрує своє повідомлення, використовуючи відкритий ключ одержувача і відсилає його.
4. Одержувач приймає і розшифровує повідомлення своїм секретним ключем.

Змішані (гібридні) криптосистеми. Алгоритми з відкритими ключами не замінюють симетричні алгоритми і використовуються не для шифрування повідомлень, а для шифрування ключів за такими двома причинами:

1. *Алгоритми з відкритими ключами працюють повільно.* Симетричні алгоритми принаймні в 1000 разів швидше, ніж алгоритми з відкритими ключами. Так, комп'ютери стають усе швидше і швидше, і років через 15 криптографія з відкритими ключами досягне швидкостей, порівнянних із сьогодишньою швидкістю симетричної криптографії. Але вимоги до обсягу переданої інформації також зростають, і завжди буде вимагатися шифрувати дані швидше, ніж це зможе зробити криптографія з відкритими ключами.

2. *Криптосистеми з відкритими ключами уразливі стосовно розкриття на основі підбраного відкритого тексту.* Криптоаналітик не зможе розкрити k , але зможе визначити P .

Розкриття на основі підбраного відкритого тексту може бути особливо ефективним, якщо число можливих шифротекстів відносно мале. Наприклад, якщо P – це грошова сума в доларах, менша ніж \$1000000, то таке розкриття спрацює, криптоаналітик перебере весь мільйон значень. Навіть якщо P не так добре визначене, таке розкриття може бути дуже ефективним. Корисним може бути також просте знання того, що шифротекст не відповідає конкретному відкритому тексту. Симетричні криптосистеми не чутливі до розкриттів такого типу, тому що криптоаналітик не може виконати тестових розшифрувань з невідомим ключем.

У більшості реалізацій криптографія з відкритими ключами використовується для засекречування і розповсюдження сеансових ключів, що використовуються симетричними алгоритмами для закриття потоку повідомлень. Іноді такі реалізації називаються змішаними (гібридними) криптосистемами.

Використання криптографії з відкритим ключем для розподілу секретних ключів вирішує дуже важливу проблему їх розподілу.

4.3. Шифрування інформації в каналах зв'язку з використанням ключів

Як відомо, інформаційні мережі характеризуються їх поділом на сім рівнів моделі ISO/OSI, кожний з яких відповідає за дотримання певних умов і виконання функцій. Це має фундаментальне значення для створення стандартних інформаційно-комунікаційних мереж та забезпечення шифрування даних на певних рівнях цієї моделі (зазвичай це найнижчі або

найвищі рівні). Якщо шифрування здійснюється на нижніх рівнях, то воно називається *канальним*, а на верхніх – *наскрізним*.

При **канальному шифруванні** (рис. 4.14) здійснюється перетворення абсолютно всіх даних, що проходять через кожний канал зв'язку (відкритий текст, інформація про його маршрут трансляції, використовуваний комунікаційний протокол тощо). На мережевих вузлах здійснюється розшифрування вхідного потоку даних для відповідної її обробки і подальшого зашифрування для передачі на інший вузол мережі.

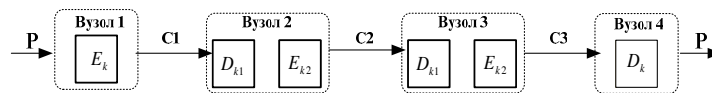


Рис. 4.14. Канальне шифрування

Такий підхід є ефективним засобом захисту інформації, оскільки шифруються всі дані, що рухаються від вузла до вузла мережі і у криптоаналітика немає ніякої додаткової інформації про джерело переданих даних, для кого вони призначені, яка їх структура тощо. А якщо період простою замінити передачею випадкових бітів, то важко навіть визначити, де починається і де закінчується текст певного повідомлення.

Рівнозначними ключами зазвичай забезпечуються тільки два сусідні вузли мережі і вони після використання змінюються незалежно від інших пар вузлів.

Основний недолік канального шифрування в тому, що дані потрібно шифрувати при передачі кожним фізичним каналом і у результаті вартість реалізації для великих мереж може стати достатньо високою.

Також може виникнути необхідність додатково захищати кожний вузол, через який проходять передані мережею даних.

При **наскрізному шифруванні** (рис. 4.15) криптографічні перетворення здійснюються на одному з верхніх рівнів моделі OSI, а шифруванню підлягає тільки змістовна частина повідомлення. Після зашифрування до нього додається службова інформація, необхідна для маршрутизації повідомлення, і далі здійснюється відправлення адресатові. При такому підході немає необхідності розшифровувати й зашифровувати повідомлення при його проходженні проміжними вузлами. Таким чином, текст залишається зашифрованим на всьому шляху від відправника до одержувача.

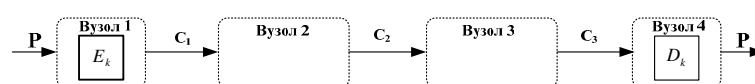


Рис. 4.15. Наскрізне шифрування

Недоліком наскрізного шифрування є те, що службова інформація, яка використовується для маршрутизації повідомлень, передається мережею у відкритому вигляді. У цьому випадку криптоаналітик може отримати

важливу інформацію стосовно джерела і приймача повідомлення, часу сеансів, комунікацій тощо.

До того ж, оскільки криптографічний алгоритм реалізується на верхніх рівнях моделі OSI, доводиться також мати справу з багатьма істотними розбіжностями в комунікаційних протоколах та інтерфейсах залежно від типів комп'ютерних мереж і підключених до них комп'ютерів. Усе це ускладнює практичне застосування наскрізного шифрування.

Комбіноване шифрування включає каналне і наскрізне шифрування та обходиться воно значно дорожче, ніж одне окремо взите. Проте саме такий підхід дає змогу якнайкраще захистити дані, що передаються мережею. Шифрування в кожному каналі зв'язку не дозволяє неавторизованій стороні аналізувати службову інформацію, використовувану для маршрутизації, а наскрізне – зменшує ймовірність доступу до незашифрованих даних у мережевих вузлах.

При комбінованому шифруванні робота з ключами відбувається роздільно: адміністратори мережі відповідають за ключі, які використовуються при каналному шифруванні, а про ключі, що застосовуються при наскрізному шифруванні, знаходяться в зоні користувачів.

Апаратне шифрування реалізується шляхом використання спеціалізованих апаратних засобів, які вбудовуються в лінію зв'язку й здійснюють шифрування всієї переданої інформації. Перевага апаратного шифрування над програмним пов'язано з тим, що воно має більшу швидкість. Криптографічні алгоритми складаються з величезної кількості складних операцій, що виконуються над бітами відкритого тексту. Сучасні універсальні комп'ютери погано пристосовані для ефективного виконання цих операцій. Спеціалізоване устаткування дає змогу виконувати їх набагато швидше. Крім того, апаратуру легше фізично захистити від проникнення ззовні. Програма, що виконується на персональному комп'ютері, практично беззахисна. За допомогою настроявача, неавторизована сторона може модифікувати програму, щоб знизити стійкість використовуваного криптографічного алгоритму. Що стосується апаратури, то вона звичайно розміщується в спеціальних контейнерах, які роблять неможливою зміну схеми її функціонування. Чіп, як правило, покривається спеціальним хімічним складом, і в результаті будь-яка спроба перебороти захисний шар цього чипу приводить до самознищення його внутрішньої логічної структури. Крім того, екранування чипів захистить інформацію від витоку через канали побічного електромагнітного випромінювання і наведення.

Програмне шифрування. Здійснюється шляхом використання певного криптографічного алгоритму, реалізованого у відповідній програмі. Переваги такої реалізації пов'язані з тим, що програмні засоби шифрування легко копіюються, вони прості у використанні, їх неважко модифікувати відповідно до конкретних потреб.

У всіх поширених операційних системах є вбудовані засоби шифрування, зазвичай їх призначено для шифрування окремих файлів, а роботу з ключами покладено на користувача. Слід пам'ятати, що не можна зберігати ключі разом із зашифрованими за їх допомогою файлами, а незашифровані копії файлів необхідно вилучати відразу ж після шифрування.

Шифрування і стиснення. Методи стиснення даних доцільно використовувати з криптографічними алгоритмами, оскільки при розкритті шифротексту криптоаналітик в основному покладається на властивості надлишковості відкритих текстів, а застосування процедур стиснення дає можливість позбутися цієї надлишковості. Крім того, стиснення зменшує довжину відкритого тексту, що дозволяє скоротити час його шифрування. Якщо такий текст спробувати стиснути після його обробки за допомогою високоякісного криптографічного алгоритму, то це практично не вдасться, оскільки характеристики шифротексту будуть близькими до характеристик зовсім випадкового набору символів. До речі, стиснення може служити своєрідним тестом для перевірки якості криптографічного алгоритму. Якщо шифротекст піддається стисненню, то варто використати більш якісний алгоритм.

4.4. Алгоритми організації цифрового підпису

Існує безліч алгоритмів цифрового підпису, які базуються на системах з відкритими ключами. Закритий ключ призначений для підпису документів, а відкритий – для перевірки підпису. Іноді процес підпису називають **шифруванням із закритим ключем**, а процес перевірки підпису – **розшифруванням з відкритим ключем**. За таким принципом працює алгоритм RSA, а в інших – інші реалізації. Наприклад, використання односпрямованих хеш-функції і міток часу іноді приводить до появи додаткових етапів під час підписання і перевірки підпису. Багато алгоритмів можна використовувати для цифрового підпису, але не можна для шифрування.

Рядок бітів, приєднаний до документа після його підписання (у попередньому прикладі, значення односпрямованої хеш-функції документа, зашифроване закритим ключем), будемо називати **цифровим підписом** чи просто **підписом**. Весь протокол, за допомогою якого одержувач повідомлення перевіряє особистість про відправника і цілісність повідомлення, називається посвідченням дійсності.

Використання цифрових підписів. Одним із найбільш ранніх запропонованих застосувань цифрових підписів було спрощення перевірки дотримання договорів про ядерні випробування. Сполучені Штати і Радянський Союз дозволили один одному розмістити на чужій території сейсмографи для спостереження за ядерними випробуваннями. Проблема була в тому, що кожна зі сторін повинна бути упевненою, що інша сторона не підробила дані цих сейсмографів. Одночасно, інша сторона повинна

була бути упевнена, що ці датчики посилають тільки ту інформацію, що потрібна для спостереження за ядерними випробуваннями.

Метод умовного посвідчення дійсності може вирішити першу проблему, але тільки цифрові підписи можуть вирішити обидві проблеми. Сторона, на території якої стоїть сейсмограф, може прочитати, але не змінити дані сейсмографа, а сторона, що стежить, знає, що дані не були підроблені.

Підпис документа за допомогою симетричних криптосистем і посередника. Ці протоколи працюють, але вони вимагають від посередника чималих витрат часу. Він повинен цілими днями розшифровувати і шифрувати повідомлення, виступаючи посередником між кожною парою людей, що хочуть обмінюватися підписаними документами. Посередник зберігає повідомлення в базі даних (хоча цього можна уникнути, посилаючи одержувачу копію шифрованого повідомлення відправника). Він буде вузьким місцем будь-якої системи зв'язку, навіть якщо він проста комп'ютерна програма.

Такого посередника, якому будуть довіряти всі кореспонденти, важко знайти і важко зберегти. Він повинен бути безгрішний, якщо він зробить хоча б одну помилку на мільйон підписів, то назавжди втратить довіру. Посередник повинний бути абсолютно безпечний. Якщо його база даних із секретними ключами коли-небудь розкриється, чи хто-небудь зможе перепрограмувати його, усі підписи стануть марними. Така схема теоретично може працювати, але вона недостатньо підходить для практичного застосування.

Дерева цифрових підписів. Ральф Меркл запропонував систему цифрових підписів, засновану на криптографії із секретним ключем, що створює нескінченну кількість одноразових підписів, використовуючи деревоподібну структуру. Основною ідеєю цієї схеми є розміщення коренів дерева в деякому відкритому файлі, таким чином засвідчуючи його. Корінь підписує одне повідомлення і засвідчує підвузли дерева. Кожний з цих вузлів підписує одне повідомлення і засвідчує свої підвузли й т.д.

Підпис документа за допомогою криптографії з відкритими ключами.

Існують алгоритми з відкритими ключами, які можна використовувати для цифрових підписів. У деяких алгоритмах, наприклад RSA, для шифрування може бути використаний чи відкритий, чи закритий ключ. Зашифруйте документ своїм закритим ключем, і ви одержите надійний цифровий підпис. В інших випадках – прикладом є DSA – для цифрових підписів використовується окремий алгоритм, що неможливо використовувати для шифрування. Ця ідея вперше була винайдена Діффі і Хеллманом. Цей протокол набагато краще попереднього. Посередник не потрібний ні для підпису документів, ні для її перевірки. Такий підпис відповідає усім вимогам:

1. Цей підпис достовірний.

2. Цей підпис не підроблений.

3. Цей підпис не можна використовувати повторно. Підпис є функцією документа і не може бути перенесений в інший документ.

4. Підписаний документ не можна змінити. Після будь-якої зміни документа підпис не зможе більше підтверджуватися відкритим ключем відправника.

5. Від підпису неможливо відмовитися. Одержувачу не потрібна допомога відправника при перевірці підпису.

Підпис документа і мітки часу. В цифрові підписи часто включають мітки часу. Дата і час підписання документа додаються до документа і підписуються разом із усім змістом повідомлення. Банк зберігає цю мітку часу в базі даних. Тепер, якщо одержувач спробує одержати готівку за чеком відправника в другий раз, банк перевірить мітку часу у своїй базі даних.

Підпис документа за допомогою криптографії з відкритими ключами й односпрямованими хеш-функціями. На практиці алгоритми з відкритими ключами часто недостатньо ефективні для підпису великих документів. Для економії часу протоколи цифрового підпису нерідко використовують разом з односпрямованими хеш-функціями. Відправник підписує не документ, а значення хеш-функції для даного документа. У цьому протоколі односпрямована хеш-функція й алгоритм цифрового підпису узгоджуються заздалегідь.

Швидкість помітно зростає, а ймовірність одержати для двох різних документів однакове 160-бітне значення хеш-функції складає тільки один шанс із 2^{160} . Зазначимо, що повинна використовуватися тільки односпрямована хеш-функція, інакше створити різні документи з тим самим значенням хеш-функції неважко, і підпис одного документа приведе до помилкового підпису відразу багатьох документів.

У протоколі є й інші вигоди. Підпис може бути відділений від документа. Значно зменшуються вимоги до обсягу пам'яті одержувача, у якому зберігаються документи і підписи. Архівна система може використовувати цей протокол для підтвердження існування документів, не зберігаючи зміст. У центральній базі даних можуть зберігатися лише значення хеш-функції для файлів. Зовсім не потрібно переглядати файли, користувачі поміщають свої значення хеш-функції в базу даних, а база даних зберігає ці значення, позначаючи їх часом одержання документа. Якщо в майбутньому виникне яка-небудь розбіжність із приводу автора і часу створення документа, база даних зможе дозволити його за допомогою значення хеш-функції, що зберігається в ній. Подібна система має велике значення при збереженні секретної інформації.

Алгоритм цифрового підпису. Електронний цифровий підпис забезпечує цілісність повідомлень (документів), переданих незахищеними телекомунікаційними каналами загального користування в системах обробки інформації різного призначення, з гарантованою ідентифікацією її автора (особи, що підписала документ).

При практичній реалізації цифрового електронного підпису (особливо великих документів) використовуються односпрямовані дайджести, що шифруються секретним ключем відправника і таким чином розшифровується не все повідомлення, а лише його дайджест, що захищає послання від несанкціонованої зміни. Процедура ефективної генерації електронного підпису проілюстрована на рис. 4.16,а.

Перевірка ефективно згенерованого електронного підпису може бути реалізована способом, зображеним на рис. 4.16,б.

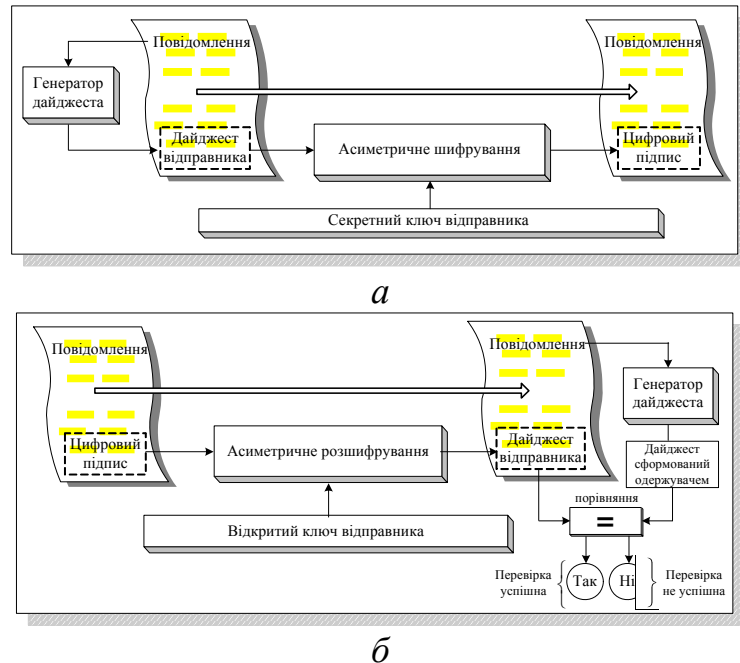


Рис. 4.16. Електронний підпис: а – генерація; б – перевірка.

Після того, як відправник згенерував дайджест повідомлення і зашифрував його своїм секретним ключем (утворивши таким чином цифровий підпис), одержувач шифрує код дайджесту відкритим ключем відправника і за відкритим текстом відомим алгоритмом генерує дайджест прийнятого повідомлення. Якщо дайджести сформовані відправником і одержувачем співпадають, то вважається, що процедура перевірки цілісності й аутентифікації відправника пройшла успішно.

Одна з основних вимог до методів цифрового підпису – неможливість перебування двох або більше документів під одним підписом. Для цього використовується процедура хешування, у результаті якої до кожного документа ставиться відповідне велике і непередбачене число, що власне і підписується.

4.5. Алгоритми з використанням ключів

Алгоритми блокового шифрування. Характерною рисою блокових криптоалгоритмів є той факт, що в ході своєї роботи вони роблять перетворення блоку вхідної інформації фіксованої довжини й одержують результуючий блок того ж обсягу, але недоступний для прочитання стороннім особам, які не володіють ключем. Таким чином, схему роботи блокового шифру можна описати функціями $C=E(P,K)$ і $P=D(C,K)$.

Ключ K – параметр блокового криптоалгоритму і є деяким блоком двійкової інформації фіксованого розміру. Початковий (P) і зашифрований

(С) блоки даних також мають фіксовану розрядність, рівну між собою, але необов'язково рівну довжині ключа.

Блокові шифри є основою, на якій реалізовані практично всі криптосистеми. Методика створення ланцюжків із зашифрованих блоковими алгоритмами байтів дозволяє шифрувати ними пакети інформації необмеженої довжини. Така властивість блокових шифрів, як швидкість роботи, використовується асиметричними криптоалгоритмами, повільними за своєю природою. Відсутність статистичної кореляції між бітами вихідного потоку блокового шифру використовується для обчислення контрольних сум пакетів даних і в хешуванні паролів.

Криптоалгоритм іменується ідеально стійким, якщо прочитати зашифрований блок даних можна, перебравши всі можливі ключі, доти, поки повідомлення не виявиться осмисленим. Тому що за теорією ймовірності шуканий ключ буде знайдений з імовірністю $1/2$ після перебору половини всіх ключів, то на злом ідеально стійкого криптоалгоритму з ключем довжини N буде потрібно в середньому 2^{N-1} перевірок. Таким чином, у загальному випадку стійкість блокового шифру залежить тільки від довжини ключа і зростає експоненційно з її зростанням. Навіть припустивши, що перебір ключів здійснюється на спеціально створеній багатопроесорній системі, у якій завдяки діагональному паралелізму на перевірку 1 ключа іде тільки 1 такт, то на злом 128-бітного ключа сучасній техніці буде потрібно не менше 10^{21} років.

Крім цієї умови до ідеально стійких криптоалгоритмів застосовується ще одна дуже важлива вимога, якій вони повинні обов'язково відповідати. При відомих початковому і зашифрованому значеннях блоку ключ, яким зроблене це перетворення, можна визначити також тільки повним перебором. Ситуації, в яких сторонньому спостерігачу відома частина вихідного тексту, зустрічаються повсюдно. Це можуть бути стандартні написи в електронних бланках, фіксовані заголовки форматів файлів, що досить часто зустрічаються в тексті, довгі слова чи послідовності байт. У світлі цієї проблеми описана вище вимога не є нічим надмірним і також строго виконується стійкими криптоалгоритмами, як і перше.

Таким чином, на функцію стійкого блокового шифру $C=E(P,K)$ накладаються такі умови:

- функція E повинна бути оберненою;
- не повинно існувати інших методів прочитання повідомлення P за відомим блоком C , крім як повним перебором K ;
- не повинно існувати інших методів визначення, яким K було зроблене перетворення P у шифротекст C , крім як повним перебором ключів.

Розглянемо методи, за допомогою яких розроблювачі блокових криптоалгоритмів домагаються одночасного виконання цих трьох умов з дуже великою часткою вірогідності.

Усі дії, вироблені над даними блоковим криптоалгоритмом, засновані на тому факті, що перетворений блок може бути представлений у вигляді цілого не негативного числа з діапазону, що відповідає його розрядності. Так, наприклад, 32-бітний блок даних можна інтерпретувати як число з діапазону 0..4'294'967'295. Крім того, блок, розрядність якого звичайно є «степенем двійки», можна трактувати як кілька незалежних не негативних чисел з меншого діапазону (розглянутий вище 32-бітний блок можна також представити у вигляді двох незалежних чисел з діапазону 0..65535 чи у вигляді чотирьох незалежних чисел з діапазону 0..255).

Над цими числами в блокових криптоалгоритмах і здійснюються за визначеною схемою (табл. 4.1) наступні дії (ліворуч дані умовні позначки цих операцій на багатьох графічних схемах алгоритмів):

За параметр V для кожного з цих перетворень може використовуватися:

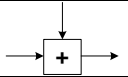
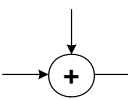
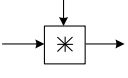
- фіксоване число (наприклад, $P'=P+125$);
- число, одержуване з ключа (наприклад, $P'=P+F(K)$);
- число, одержуване з незалежної частини блоку (наприклад, $P_2'=P_2+F(P_1)$).

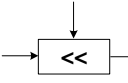
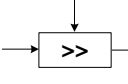
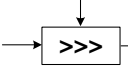
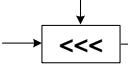
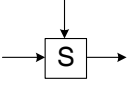
Останній варіант використовується в схемі, названої за іменем її творця – мережею Фейстеля (нім. Feistel).

Послідовність виконуваних над блоком операцій, комбінації перерахованих вище варіантів V і самі функції F складають «ноу-хау» кожного конкретного блокового криптоалгоритму.

Характерною ознакою блокових алгоритмів є багаторазове і непряме використання матеріалу ключа. Це диктується в першу чергу вимогою неможливості зворотного декодування у відношенні ключа при відомих вихідному і зашифрованому текстах. Для рішення цієї задачі в приведених вище перетвореннях найчастіше використовується не саме значення ключа чи його частини, а деяка, іноді необоротна функція від матеріалу ключа. Більш того, у подібних перетвореннях той самий блок чи елемент ключа використовується багаторазово. Це дозволяє при виконанні умови оборотності функції щодо величини P зробити функцію необоротної щодо ключа K .

Таблиця 4.1

Біективні математичні функції		
	Додавання	$P'=P+V$
	Складання за модулем 2 (виключаюче АБО)	$P'=P \text{ XOR } V$
	Множення за модулем 2^N	$P'=(P*V) \bmod (2^N)$

Бітові зсуви		
	Арифметичний зсув ліворуч	$P' = P \text{ SHL } V$
	Арифметичний зсув праворуч	$P' = P \text{ SHR } V$
	Циклічний зсув ліворуч	$P' = P \text{ ROL } V$
	Циклічний зсув праворуч	$P' = P \text{ ROR } V$
Табличні підстановки		
	S-box (англ. substitute)	$P' = \text{Table}[P, V]$

Оскільки операція шифрування чи розшифрування окремого блоку в процесі кодування пакета інформації виконується багаторазово (іноді до сотень тисяч разів), а значення ключа i , отже, функцій $V_i(K)$ залишається незмінним, то іноді стає доцільно заздалегідь однократно обчислити дані значення і зберігати їх в оперативній пам'яті разом із ключем. Оскільки ці значення залежать тільки від ключа, то вони в криптографії називаються *матеріалом ключа*. Необхідно відзначити, що дана операція ніяким чином не змінює ні довжину ключа, ні криптостійкість алгоритму в цілому. Тут відбувається лише оптимізація швидкості обчислень шляхом *хешування* проміжних результатів. Описані дії зустрічаються практично в багатьох блокових криптоалгоритмах і називаються *розширенням ключа*.

Варіантом практичного застосування блокових алгоритмів є використання їх для забезпечення імітозахисту переданої каналами зв'язку інформації.

Імітозахистом повідомлення називається процес введення додаткового блока (імітовставки) у кінець розбитого на блоки інформаційного повідомлення. Для впровадження імітовставки застосовуються алгоритми блокового шифрування в режимі гамування із самовідновленням або шифрування зі зчепленням блоків.

Специфіка організації різних типів захищених каналів зв'язку зумовила появу алгоритмів блокового шифрування (рис. 4.17).



Рис. 4.17. Класифікація блокових алгоритмів

Усе розмаїття симетричних криптосистем ґрунтується на описаних далі базових методах:

- метод багатоалфавітного підставлення;
- метод простої заміни, або режим електронної кодової книги (Electronic Codebook Mode – ECB);
- метод гамування, або режим за модулем, що дорівнює потужності алфавіту;
- метод гамування із самовідновленням, або гамування зі зворотним зв'язком (Cipher-Feedback mode – CFB);
- метод гамування зі зворотним зв'язком на виході (Output-Feedback mode – OFB);
- метод шифрування зі зчепленням блоків (Cipher Block Chaining mode – CBC).

Метод багатоалфавітного підставлення – це найпростіший вид перетворень, що полягає в заміні символів вихідного тексту на інші (того самого алфавіту) за більш-менш складним правилом. У разі багатоалфавітних підставлень кожний символ вихідного тексту за певним законом перетворюється в символ шифрованого тексту. При цьому закон перетворення змінюється від символу до символу.

Для забезпечення високої криптостійкості системи потрібне використання ключів великого розміру. До цього класу належать криптосистеми з одноразовим ключем, що мають абсолютну теоретичну стійкість.

Метод переставлення – метод криптографічного перетворення, що полягає в переставленні символів вихідного тексту за деяким правилом. Шифри переставлень не використовуються в чистому вигляді, оскільки їхня криптостійкість недостатня.

Метод гамування – це перетворення вихідного тексту, при якому його символи додаються (за модулем, що дорівнює потужності алфавіту) до символів псевдовипадкової послідовності, згенерованої за деяким правилом.

Гамування не можна цілком виділити в окремий клас криптографічних перетворень, оскільки зазначена псевдовипадкова послідовність може генеруватися, наприклад, за допомогою блокового

шифру. У разі коли послідовність випадкова (наприклад, знята з фізичного датчика) і кожний її фрагмент використовується тільки один раз, дістаємо криптосистему з одноразовим ключем.

Метод простої заміни. У цьому режимі блоки відкритого тексту шифруються незалежно від інших блоків на одному ключі. Цей режим названо *режимом електронної кодової книги*, оскільки теоретично існує можливість створити книгу, в якій кожному блоку відкритого тексту відповідатиме блок зашифрованого тексту.

Проте в разі коли довжина блока дорівнює 64 бітам, то книга містить 2^{64} записів, і кожна книга відповідатиме одному ключеві.

Зашифрування може бути описано залежністю: $C_i = F(P_i)$ для $i = 1, \dots, N$, де C_i і P_i – блоки відповідно зашифрованого та відкритого тексту, а F – криптографічне перетворення, реалізоване алгоритмом блокового шифрування.

Ідентичні блоки відкритого тексту на тому самому ключі будуть зашифровані однаково. З погляду криптоаналізу цей режим є найбільш «слабким» (оскільки існує велика кількість криптографічних атак).

Метод ускладненого гамування. У цьому режимі алгоритм блокового шифрування використовується для ускладнення попередньої гама, виробленої одноканальною лінією затримки. Помилка під час передачі всього повідомлення призводить до спотворення при розшифруванні тільки одного блока. Таким чином, у разі використання цієї методики стає неможливим поширення помилки за рахунок розсинхронізації вузлів обчислення попередньої гама на передавальному і приймальному боках.

Для запобігання цьому небажаному явищу на практиці застосовуються пристрої синхронізації роботи шифраторів, якщо шифратор реалізується апаратно. Початковий стан вузла створення вихідної гама задається ініціалізуючим вектором (синхропосилка), що передається відкритими каналами зв'язку в зашифрованому або відкритому вигляді. Гама, отримана вузлом генерації попередньої гама, обробляється згідно з алгоритмом блокового шифрування, після чого результуюча гама підсумовується за модулем із блоком відкритого тексту.

Зашифрування можна подати у такому вигляді:

$$C_i = P_i \oplus F(Y_i), i = 1, \dots, N,$$

де Y_i – створена гама;

Y_i – синхропосилка.

Метод гамування із самовідновленням. Цей режим характеризується тим, що шифратор у цьому разі має властивість самосинхронізації.

Початкове заповнення нагромаджувача, що на практиці звичайно реалізується у вигляді регістра зсуву, є синхропосилкою Y_i , яка передається по відкритому каналу передачі даних. Математичне подання шифрування має такий вигляд:

$$C_1 = P_1 \oplus F(Y),$$

$$C_i = P_i \oplus F(Y_{i-1}).$$

Відповідно розшифрування має вигляд:

$$P_1 = C_1 \oplus F(Y),$$

$$P_i = C_i \oplus F(C_{i-1}).$$

Симетричні алгоритми. Як відомо, симетричні алгоритми шифрування (криптографія із секретними ключами) засновані на тому, що відправник і одержувач інформації використовують той самий ключ, який повинен зберігатися в таємниці і передаватися секретним каналом (способом, що виключає його перехоплення).

Обмін інформацією здійснюється в 3 етапи:

1) відправник передає одержувачеві ключ (використовується секретний канал).

2) відправник, використовуючи ключ, зашифровує повідомлення, що посилає одержувачеві.

3) одержувач приймає повідомлення і розшифровує його.

На рис. 4.18,а проілюстровано використання симетричного шифрування.

Потокові симетричні методи шифрування реалізуються на основі генератора псевдовипадкових чисел (ПВЧ)), а блокові на перестановках (Р – блоки), підстановках (S – блоки) і зсувах.

Першими відомими симетричними алгоритмами шифрування даних є:

– Lucifer – алгоритм фірми IBM, США;

– DES (Data Encryption Standart) – стандарт шифрування даних) – симетричний 64-бітовий блоковий алгоритм шифрування фейстелевського типу (розроблений у 1977 р., США), який використовується для захисту комерційної інформації;

– В-Срут – алгоритм компанії Telecom, Великобританія;

– IDEA – швейцарський міжнародний алгоритм;

– ГОСТ – радянський стандарт шифрування даних.

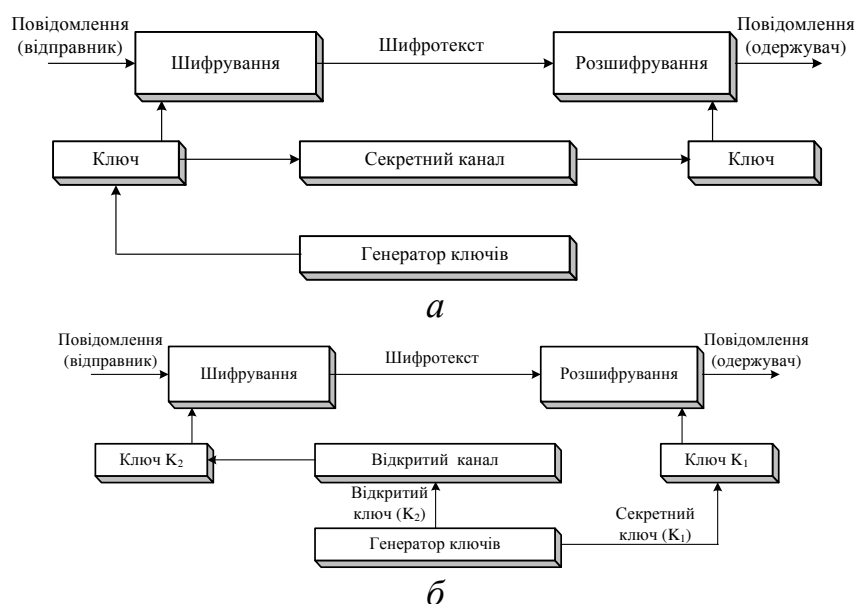


Рис. 4.18. Шифрування: а – симетричне; б – асиметричне.

Алгоритми симетричного шифрування використовують ключі не дуже великої довжини і можуть швидко шифрувати великі обсяги даних. Основним недоліком симетричного шифрування є те, що секретний ключ повинен бути відомий і відправникові, і одержувачеві. З одного боку це ставить нову проблему розсилання ключів, а з іншого, одержувач на підставі наявності шифрованого і розшифрованого повідомлення не може довести, що одержав це повідомлення від конкретного відправника, оскільки таке ж повідомлення він міг згенерувати і сам.

Асиметричні алгоритми шифрування.

Криптосистема з відкритим ключем визначається трьома етапами реалізації алгоритмів: генерація ключів, шифрування та розшифрування.

Як відомо, в асиметричних алгоритмах шифрування для зашифровування інформації використовують один ключ (відкритий), а для розшифровування – інший (секретний). Ці ключі різні і не можуть бути отримані один з іншого. Алгоритм генерації ключів відкритий, будь-який користувач може подати йому на вхід випадковий рядок r належної довжини й одержати пару ключів (k_1, k_2) . Один із ключів (наприклад, k_1) публікується (відкритий ключ), а другий – зберігається в таємниці (секретний ключ).

Схема обміну інформацією така:

- 1) одержувач обчислює відкритий і секретний ключі, секретний ключ зберігає в таємниці, відкритий же робить доступним (повідомляє, публікує).
- 2) відправник, використовуючи відкритий ключ одержувача, шифрує і пересилає йому повідомлення.
- 3) одержувач приймає повідомлення і розшифровує його, використовуючи свій секретний ключ.

Алгоритми шифрування E_{k_1} та розшифрування D_{k_2} такі, що для будь-якого відкритого тексту

$$m \ D_{k_2}(E_{k_1}(m)) = m.$$

Розглянемо тепер гіпотетичну атаку зломисника на цю систему. Супротивникові відомий відкритий ключ k_1 , але невідомий відповідний секретний ключ k_2 . Супротивник перехопив криптограму d і намагається знайти повідомлення m , де $d = E_{k_1}(m)$. Оскільки алгоритм шифрування відкритий, супротивник може просто послідовно перебрати всі можливі повідомлення довжини n , обчислити для кожного такого повідомлення m_i криптограму $d_i = E_{k_1}(m_i)$ та зрівняти d_i із d . Те повідомлення, для якого $d_i = d$, і буде відкритим текстом.

Якщо система має такі технічні можливості, то відкритий текст буде знайдено досить швидко. А в гіршому випадку перебір буде виконано за час порядку $2^n(n)$, де $T(n)$ – час, необхідний для шифрування повідомлення довжини n . Якщо повідомлення мають довжину порядку 1000 біт, то такий

перебір нездійснений на практиці на жодному з найпотужніших комп'ютерів.

Ми розглянули лише один із можливих способів атаки на криптосистему та найпростіший алгоритм пошуку відкритого тексту, названий алгоритмом *повного перебору*. Використовується також інша назва: *метод грубої сили*. Інший найпростіший алгоритм пошуку відкритого тексту – вгадування. Цей очевидний алгоритм вимагає невеликих обчислень, але спрацьовує з дуже малою ймовірністю (при великих довжинах текстів). Насправді супротивник може намагатися атакувати криптосистему різними способами, використовуючи різні, більш витончені алгоритми пошуку відкритого тексту.

Крім того, зломисник може спробувати відновити секретний ключ, використовуючи знання (у загальному випадку несекретні) про математичну залежність між відкритим і секретним ключами. Природно вважати криптосистему стійкою, якщо будь-який такий алгоритм потребує практично нездійсненого обсягу обчислень або спрацьовує з дуже малою ймовірністю. (При цьому супротивник може використати не тільки детерміновані, але й імовірнісні алгоритми). Це і є теоретично складний підхід до визначення стійкості.

Використання асиметричного методу шифрування проілюстроване на рис. 4.18,б.

Першими найбільш відомими асиметричними алгоритмами є:

- RSA – його стійкість залежить від складності факторизації великих цілих чисел;

- ECC (криптосистема на основі еліптичних кривих) – є конкурентом стосовно інших асиметричних алгоритмів шифрування, тому що при еквівалентній стійкості використовує ключі меншої довжини і має велику продуктивність;

- ElGamal – криптостійкість заснована на обчислювальній складності задачі логарифмування цілих чисел у кінцевих полях.

Істотним недоліком асиметричних методів є низька швидкодія (на 3-4 порядки повільніше одноключових), тому їх сполучають із симетричними. Для розсилання ключів повідомлення шифрують секретним ключем, який потім шифрують відкритим асиметричним ключем одержувача і після цього зашифрований текст і ключ відправляють йому мережею.

На рис. 4.19,а. відображене ефективне шифрування, реалізоване шляхом сполучення симетричного й асиметричного методів, а розшифрування ефективно зашифрованого повідомлення ілюструє рис.4.19,б.

Алгоритм DES. Найбільш відомим представником перших симетричних алгоритмів став DES (Data Encryption Standard), розроблений фірмою IBM. DES став стандартом шифрування для урядових закладів США із 70-х років і фактично є блоковим шифром, що використовує підстановки, перестановки, зсуви і додавання за модулем 2. Довжина блоку шифрування в початковому варіанті DES була 64 біта, а ключ мав розмір

56 біт. З підвищенням обчислювальної потужності комп'ютерної техніки, а також з появою спеціалізованих мікросхем для злому DES-шифрограм, довжина ключа була збільшена до 256 біт.

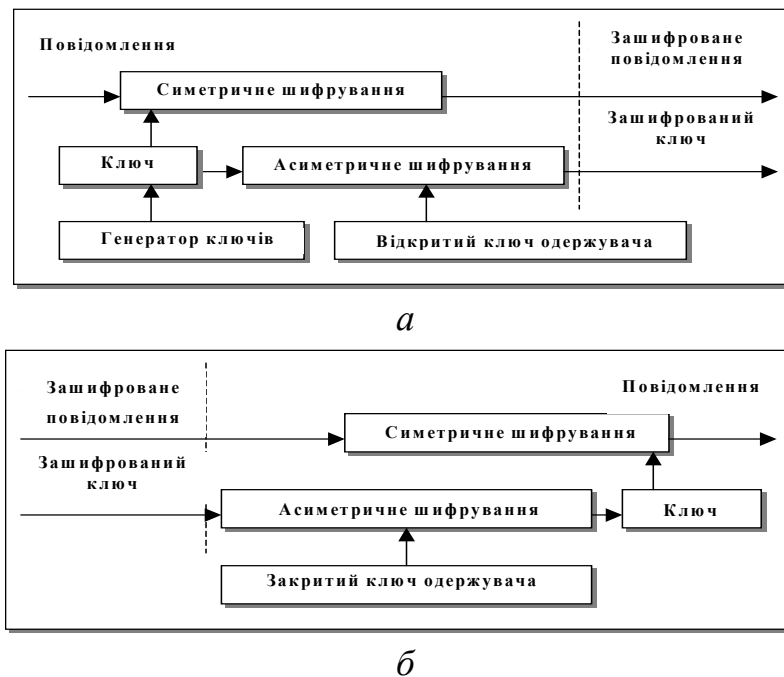


Рис. 4.19. Криптографічне перетворення:

а – шифрування повідомлення; *б* – розшифрування повідомлення.

Підстановки і перестановки, використовувані в алгоритмі, фіксовані і не залежать від ключа шифрування. Розширений ключ, що задає вибір відповідного підключу в кожному з 16 циклів шифрування, визначається наступним алгоритмом (рис. 4.20):

- секретний 56-бітний ключ (X) ділиться на два 28 бітові напівблоки A і B ;
- напівблоки A та B циклічно зсуваються на K_i біт ліворуч щодо попереднього свого положення (i – номер циклу, K_i – набір заздалегідь визначених чисел);
- 48-бітний підключ KEY_i виходить на кожній ітерації в результаті зчеплення за визначеним правилом частин підблоків A_i і B_i .

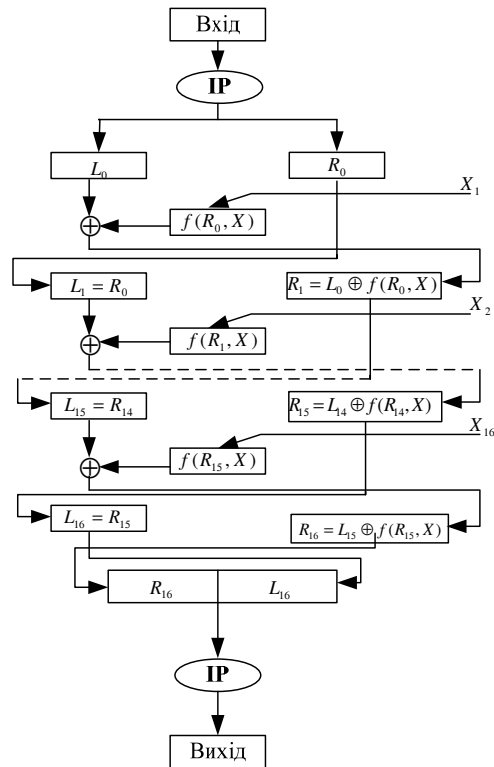


Рис. 4.20. Структурна схема алгоритму DES

Основні етапи алгоритму шифрування DES полягають у наступному:

До 64-бітного блоку початкового тексту застосовується фіксована перестановка IP. На кожному ітеративному кроці виконується операція шифрування, при якій:

- 64-бітний блок тексту P, що шифрується, розбивається на ліву (L) і праву (R) 32-х бітові половини P_1 і P_2 ;
- права половина P розбивається на 8 бітових тетрад, кожна з яких за циклічним законом доповнюється крайніми бітами із сусідніх тетрад до 6-бітного слова;
- отриманий 48-бітний блок (8 слів по 6 біт кожне) складається за модулем 2 з 48 бітами підключа. Отриманий результат розбивається на 8 блоків по 6 біт;
- кожний з отриманих на попередньому кроці блоків надходить на вхід функції фіксованого S-блоку, що виконує нелінійну заміну наборів 6-бітних блоків тетрадами;
- отримані 32 біта піддаються фіксованій перестановці, результатом якої є одержання блоку $F_i(P_2)$;
- компоненти правого 32-бітного зашифрованого напівблоку $F_i(P_2)$ підсумовуються за модулем 2 з компонентами лівого напівблоку P_1 і міняються місцями.

До блоку тексту, отриманому після 16 циклів, застосовується зворотна фіксована перестановка, у результаті чого виходить підсумковий 64-бітний шифротекст.

При розшифровці кодованого DES-блоку порядок операції буде зворотний.

Шифр Ель-Гамаля.

Система ґрунтується на властивостях дискретного логарифмування у скінченному простому полі, що є складною задачею з обчислювального погляду і потребує значних обчислювальних ресурсів.

Нехай сторона, що здійснює діяльність секретного зв'язку, генерує два числа: просте число N і ціле число Q (системні ключі).

1. Сторона A вибирає секретне число X ($1 \leq X \leq N$), обчислює число $Y = (Q^X) \bmod N$ і повідомляє його всім учасникам обміну (X, Y – персональні ключі).

2. Сторона B вибирає випадкове секретне число K (сеансовий ключ) таке, що $K < N$. Для шифрування числа M (повідомлення) отримуємо два числа: $a = Q^K \bmod N$ і $b = (Y^K M) \bmod N$. Числа a і b повідомляються стороні A .

3. Сторона A розшифровує повідомлення a, b шляхом обчислення в цілих числах рівняння $(M \cdot a^x) \bmod N = b$.

Розглянемо роботу шифру на конкретному прикладі. Припустимо, що $N=11$, $Q=2$, $X=8$, $K=9$, а шифроване повідомлення $M=4$.

1. Нехай $P=11$ та $Q=2$ (системні ключі).

2. Якщо $X=8$ то $Y=2^8 \bmod 11=3$ ($X=8$, $Y=3$ система персональних ключів сторони A).

3. Далі, якщо сторона B хоче передати стороні A секретне повідомлення $M=4$, вона генерує сеансовий ключ $K=9$ і тоді обчислює два числа $a=2^9 \bmod 11=6$, $b=(3^9 * 4) \bmod 11=5$.

4. Сторона A , отримавши секретне повідомлення $a=6$, $b=5$ і розв'язавши діфантове рівняння $(M * 6^9) \bmod 11=5$, отримує $M=4$.

Шифр Ривеста-Шамира-Адлемана (RSA)

Найбільш відомою асиметричною криптосистемою став алгоритм RSA, що є першою практичною реалізацією на основі поняття односпрямованої функції з секретом запропонованою Діффі і Хелманом. Покажемо процес формування ключа шифрування і розшифрування за допомогою RSA.

Формування ключа. Для того щоб сформувати ключ, одержувачу необхідно виконати такі операції.

1. Вибрати два випадкових простих числа p і q , що задовольняють умові $|p| \approx |q|$.

2. Обчислити $N = pq$.

3. Обчислити $\phi(N) = (p-1)(q-1)$.

4. Вибрати випадкове ціле число $e < \phi(N)$, що задовольняє умові $\gcd(e, \phi(N)) = 1$, і знайти ціле число d таке, що $ed \equiv 1 \pmod{\phi(N)}$.

(Оскільки $\gcd(e, \phi(N)) = 1$, це рівняння має рішення d , яке можна знайти за допомогою розширеного алгоритму Евкліда.)

5. Використати пару (N, e) як параметри відкритого ключа, ретельно знищити числа p, q і $\phi(N)$ і запам'ятати число d як закритий ключ.

Шифрування. Для того щоб переслати одержувачу секретне повідомлення, що має довжину $m < N$, відправник створює шифротекст c .
$$c \leftarrow m^e \pmod{N} .$$

З погляду відправника, простір початкових повідомлень є множина усіх позитивних чисел, що менше числа N .

Розшифрування. Для того щоб розшифрувати шифротекст c , одержувач обчислює формулу

$$m \leftarrow c^d \pmod{N} .$$

Розглянемо роботу RSA на конкретному прикладі. Припустимо, що одержувач вибрав числа $N=7 \times 13=91$ і $e=5$. Тоді $\phi(N)=6 \times 12=72$. Застосовуючи алгоритм Евкліда до пари $(a, b) = (72, 5)$, одержувач отримує наступне число.

$$72 \times (-2) + 5 \times 29 = 1$$

Інакше кажучи, $5 \times 29 = 1 \pmod{72}$. Отже, секретним показником степеня, який був використаний одержувачем при шифруванні, є число 29. Одержувач встановлює пару $(N, e)=(91, 5)$ як параметри відкритого ключа криптосистеми RSA.

Припустимо, що відправник шифрує вихідне повідомлення $m = 3$, використовуючи формулу

$$c = 3^5 = 243 = 61 \pmod{91}.$$

Зашифроване повідомлення є число 61.

Для того щоб розшифрувати повідомлення 61, Одержувач обчислює значення $61^{29} = 3 \pmod{91}$.

Час шифрування, розшифрування за алгоритмом RSA у 1000 разів перевищує алгоритм блокового шифрування DES. Але застосування даного алгоритму додає нову функціональність у секретне переписування. Після опублікування ключів будь-який абонент може зашифрувати конфіденційну інформацію загальновідомим алгоритмом і відіслати абоненту, що опублікував ключі. При цьому прочитати цю інформацію зможе тільки власник секретного ключа.

За кількістю застосувань підпис Ель-Гамала лідирує за розміром самого підпису, який може бути в кілька разів менше, ніж у системі RSA, що дуже істотно для завантажених телекомунікаційних мереж.

При виборі підпису для практичного застосування у відкритих системах доцільно орієнтуватися на експлуатаційні характеристики підписів і їх відповідність технічним можливостям системи. Цілком розумним може виявитися використання різних підписів. Залежно від розподілу обчислювальних потужностей у відкритій системі і потоку повідомлень іноді має сенс задіяти одночасно обидва види підпису, щоб забезпечити рівномірне навантаження мережі і підвищити її пропускну здатність.

Криптосистеми на еліптичних кривих. Система Ель-Гамала базується на тому, що операція логарифмування в скінченному простому полі є складним технічним завданням, але скінченні поля не єдині алгебраїчні структури, в яких можна поставити завдання обчислення

дискретного логарифма. У 1985 році Кобліц і Міллер незалежно один від одного запропонували використовувати для побудови криптосистем алгебраїчні структури, визначені на множині точок на еліптичних кривих. Розглянемо випадки визначення еліптичних кривих над простими скінченними полями довільної характеристики та над полями Галуа характеристики 2.

Нехай $p > 3$ – просте число; $a, b \in GF(p)$, такі що $4a^2 + 27b^2 \neq 0$. Еліптичною кривою (рис. 4.21) E над полем $GF(p)$ (еліптичною кривою у формі Веєрштрасса) називається множина розв'язків (x, y) рівняння над полем $GF(p)$ разом із додатковою точкою ∞ , яку називають нескінченно віддаленою точкою.

$$y^2 = x^3 + ax + b$$

Позначимо кількість точок на еліптичній кривій E через $\#E$. Верхня та нижня межі для $\#E$ визначаються теоремою Хассе:

$$p + 1 - 2\sqrt{p} \leq \#E \leq p + 1 + 2\sqrt{p}.$$

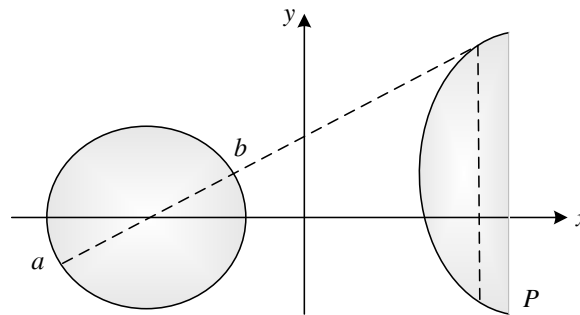


Рис. 4.21. Еліптична крива

Задамо бінарну операцію на E (в адитивному записі) такими правилами:

1. $\infty + \infty = \infty$;
2. $\forall (x, y) \in E, (x, y) + \infty = (x, y)$;
3. $\forall (x, y) \in E, (x, y) + (x, -y) = \infty$;
4. $\forall (x_1, y_1) \in E, (x_2, y_2) \in E, x_1 \neq x_2, (x_1, y_1) + (x_2, y_2) = (x_3, y_3)$, де $x_3 = \lambda^2 - x_1 - x_2$,
 $y_3 = \lambda(x_1 - x_3) - y_1$ і $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$.
5. $\forall (x_1, y_1) \in E, y_1 \neq 0, (x_1, y_1) + (x_1, y_1) = (x_2, y_2)$,
де $x_2 = \lambda^2 - 2x_1$, $y_2 = \lambda(x_1 - x_3) - y_1$ і $\lambda = \frac{3x_1^2 + a}{2y_1}$.

Множина точок еліптичної кривої E із заданої в такий спосіб операцією утворює абелеву групу.

Якщо $\#E = p + 1$, то крива E називається *суперсингулярною*.

Еліптична крива, яка не є суперсингулярною кривою E над полем $GF(2^m)$ характеристики 2, задається у такий спосіб.

Нехай $m > 3$ – ціле число та $a, b \in GF(2^m)$, $b \neq 0$. Еліптичною кривою E над полем $GF(2^m)$ називається множина розв'язків (x, y) рівняння

$y^2 + xy = x^3 + ax + b$ над полем $GF(2^m)$ разом із нескінченно віддаленою точкою.

У цьому разі множина точок еліптичної кривої E із заданої в такий спосіб операцією також утворює абелеву групу.

Користуючись операцією додавання точок на кривій, можна визначити операцію множення точки $P \in E$ на довільне ціле число n : $nP = P + P + \dots + P$, де операція додавання виконується n раз.

Тепер побудуємо однобічну функцію, на основі якої можна буде створити криптографічну систему.

Нехай E – еліптична крива, $P \in E$ – точка на цій кривій. Виберемо ціле число $n < \#E$. Тоді як пряму функцію виберемо добуток nP . Для його обчислення за оптимальним алгоритмом знадобиться не більше як $2\log_2 n$ операцій додавання. Обернену задачу сформулюємо в такий спосіб: за заданою еліптичною кривою E , точкою $P \in E$ і добутком nP знайти n . Відомі алгоритми розв’язування цієї задачі потребують експонентного часу.

Тепер ми можемо описати криптографічний протокол, аналогічний відомому протоколу Діффі–Хеллмана. Для встановлення захищеного зв’язку двоє користувачів A і B спільно вибирають еліптичну криву E і точку P на ній. Далі кожний із користувачів вибирає своє секретне ціле число – відповідно α і β . Користувач A обчислює добуток αP а користувач B – добуток βP . Далі вони обмінюються обчисленими значеннями. При цьому параметри самої кривої, координати точки на ній і значення добутків є відкритими й можуть передаватися незахищеними каналами зв’язку. Потім користувачі A та B відповідно множать здобуте значення на α та β . Згідно з властивостями операції множення на число виконується рівність $\alpha \cdot \beta P = \beta \cdot \alpha P$. Таким чином, обидва користувачі одержать спільне секретне значення (координати точки $\alpha\beta P$), яке зможуть використовувати для одержання ключа шифрування.

Зауважимо, що неавторизованій стороні для відновлення ключа доведеться розв’язати складну з обчислювального погляду задачу визначення α і β за відомими E , P , αP і βP .

Приклад. Алгоритм генерації ключової пари для цифрового підпису і його перевірки:

При генерації ключів ми будемо використовувати такі параметри: E – еліптична крива, P , Q і O – точки поля $E(GF(p))$ цієї кривої, n – порядок точок кривої, d – секретний ключ. Алгоритм генерації ключів складається з 5 кроків.

Крок 1. Вибираємо еліптичну криву E , визначену на скінченному полі (Z_p) . Нехай $a=b=1$, $p=23$. Тоді крива має вид: $y^2 = x^3 + x + 1 \pmod{23}$. Обчислимо точку $P(1)$: нехай $x=0$, тоді $y^2=0+0+1=1$. Точка $P(1)$ має координати $(0,1)$. Використовуючи формули для додавання точок на еліптичній кривій, знайдемо всі точки поля $E(GF(p))$.

Далі $Y=2^9 \bmod 11=3$, $P(2)=P+Q$, $x_1=0$, $y_1=1$, $x_2=0$, $y_2=1$, а так як $P=Q$, то для знаходження λ і координат точки використовуємо:

$$\lambda = \frac{3x_1^2 + a}{2y_1} \bmod 23 = \frac{3 \cdot 0^2 + 1}{2 \cdot 1} \bmod 23 = 12;$$

$$x_3 = \lambda^2 - x_1 - x_2 = (12^2 - 0 - 0) \bmod 23 = (144 - 0 - 0) \bmod 23 = 6;$$

$$y_3 = \lambda(x_1 - x_3) - y_1 = (12(0 - 6) - 1) \bmod 23 = 19.$$

Таким чином знайдена точка $P(2)$, яка має координати $(6,19)$.

Аналогічно знаходимо інші точки множини $E(GF(p))$. У випадку, коли координата $y=0$, отримуємо нескінченно віддалену точку O . Множина $E(GF(p))$ складається з точок, значення яких наведено нижче у таблиці, а також нескінченно віддаленої точки O .

Таблиця 4.2

Таблиця значень точок множини $E(GF(p))$					
P(1)	(0,1)	P(10)	(12,4)	P(19)	(19,5)
P(2)	(6,19)	P(11)	(1,16)	P(20)	(5,4)
P(3)	(3,13)	P(12)	(17,20)	P(21)	(11,20)
P(4)	(13,16)	P(13)	(9,16)	P(22)	(7,12)
P(5)	(18,3)	P(14)	(4,0)	P(23)	(18,20)
P(6)	(7,11)	P(15)	(9,7)	P(24)	(13,7)
P(7)	(11,3)	P(16)	(17,3)	P(25)	(3,10)
P(8)	(5,19)	P(17)	(1,7)	P(26)	(6,4)
P(9)	(9,18)	P(18)	(12,19)	P(27)	(0,22)

Крок 2. Вибираємо точку $P \in E(Z_p)$. Нехай така точка буде $P=(12,19)$.

Крок 3. Знайдемо порядок цієї точки n , який буде 14, оскільки при $n=14$ виконується умова: $nP = O$.

Крок 4. Візьмемо випадкове число $d \in [1, n-1]$. Так як d не повинне перевищувати 14, то вибираємо його рівним $d=6$.

Крок 5. Обчислюємо точку Q за формулою:

$$Q = dP = 6P.$$

Для знаходження Q використовуємо операції додавання точок. У результаті виконання обчислень знайдені координати точки $Q(13,7)$.

Крок 6. Секретним ключем оголошуємо $d=6$, а відкритим – (E, P, n, Q) , що відповідає: $([x, y, a, b, y], [P_x, P_y], [n], [Q_x, Q_y])$, який записується у такому вигляді:

$$[y^2 = x^3 + x + 1, (p = 23), P(12,19), n = 14, Q(13,7)].$$

Алгоритм формування підпису

При формуванні цифрового підпису повідомлення використовуються такі параметри: $\tilde{P}$ – повідомлення, для якого формується підпис; $h(\tilde{P})$ – хеш функція цього повідомлення; r і s – параметри, з яких складається підпис повідомлення; ξ , C і k – коефіцієнти, що використовуються для знаходження значень r і s .

Крок 1. Вибираємо випадкове число $k \in [1, n-1]$. Наприклад $k=5$.

Крок 2. Обчислюємо коефіцієнт цифрового підпису C за формулою:

$$C = kP = (x_1, y_1),$$

$$C = 5P.$$

Для знаходження C використовуємо операції додавання точок. У результаті обчислень отримали значення $C = (7, 11)$. Звідси випливає, що $x_1 = 7, y_1 = 11$.

Крок 3. Обчислюємо перший параметр цифрового підпису r :

$$r = x_1 \bmod n,$$

$$r = 7 \bmod 14 = 7.$$

Крок 4. Обчислюємо коефіцієнт цифрового підпису ξ , використовуючи для його знаходження рівняння Діофанта:

$$\xi = k^{-1} \bmod n,$$

$$\xi = 5^{-1} \bmod 14 = 3.$$

Крок 5. Обчислюємо хеш-функцію $h(\tilde{p})$ повідомлення $\tilde{p}$. У нашому прикладі візьмемо, що $h(\tilde{p}) = 9$.

Крок 6. Обчислюємо другий параметр цифрового підпису s :

$$s = \xi(h(\tilde{p}) + dr) \bmod n,$$

$$s = 3 \cdot (9 + 6 \cdot 7) \bmod 14 = 13.$$

Крок 7. Підписом повідомлення $\tilde{p}$ є пара цілих чисел r та s . У нашому прикладі $r = 7, s = 13$.

Алгоритм перевірки підпису

При перевірці підпису використовуються такі параметри: підпис повідомлення $\tilde{p} = (r, s)$; w, u_1, u_2, f, g – проміжні коефіцієнти; v – параметр для перевірки підпису.

Крок 1. Якщо r і s – цілі числа, що належать до інтервалу $[1, n-1]$, переходимо до кроку 2, в противному випадку результат перевірки негативний (підпис відхиляється). В даному прикладі параметри r, s належать до інтервалу $[1, n-1]$.

Крок 2. Обчислюємо проміжний коефіцієнт w :

$$w = s^{-1} \bmod n,$$

$$w = 13^{-1} \bmod 14 = 13.$$

Крок 3. Обчислюємо проміжні коефіцієнти u_1 та u_2 :

$$u_1 = h(\tilde{p})w \bmod n,$$

$$u_1 = 9 \cdot 13 \bmod 14 = 47 \bmod 14 = 5,$$

$$u_2 = rw \bmod n,$$

$$u_2 = 7 \cdot 13 \bmod 14 = 7.$$

У результаті обчислень: $u_1 = 5, u_2 = 7$.

Крок 4. Обчислюємо проміжні коефіцієнти f, g та їх суму для знаходження значення x_0 :

$$f = u_1 P,$$

$$g = u_2 Q,$$

$$f + g = (x_0, y_0),$$

$$f + g = 5P + 7Q,$$

де f і g обчислюємо за формулами введених раніше бінарних операцій.

У результаті отримаємо:

$$f = (7, 11), g = (17, 3), f + g = (7, 12), x_0 = 7, y_0 = 12.$$

Крок 5. Обчислюємо параметр для перевірки підпису v :

$$v = x_0 \bmod n,$$

$$v = 7 \bmod 14 = 7.$$

Підпис вірний у тому випадку, коли значення v співпадає з параметром підпису r . У нашому прикладі $v = 7$ і $r = 7$, тобто робимо висновок, що підпис вірний.

Інфраструктура відкритих ключів. Інфраструктура відкритих ключів (*Public Key Infrastructure – PKI*) – це інтегрований комплекс методів та засобів (набір служб), призначених забезпечити впровадження та експлуатацію криптографічних систем із відкритими ключами.

Технологія PKI полягає у використанні двох математично пов'язаних цифрових ключів, що мають такі властивості:

- один ключ може використовуватися для шифрування повідомлення, що може бути розшифровано тільки за допомогою другого ключа;
- навіть якщо відомий один ключ, за допомогою обчислень неможливо визначити другий. Один із ключів відкритий для всіх, а другий має приватний характер і зберігається в захищеному місці. Ці ключі можуть використовуватися для автентифікації чи шифрування цифрового підпису електронних даних.

PKI слугує не тільки для створення цифрових сертифікатів, але і для зберігання величезної кількості сертифікатів і ключів, забезпечення резервування і відновлення ключів, взаємної сертифікації, ведення списків анульованих сертифікатів і автоматичного відновлення ключів та сертифікатів після закінчення терміну їхньої дії. Компоненти інфраструктури відкритих ключів і їхні функції (PKI) мають містити елементи, наведені на рис. 4.22,а.

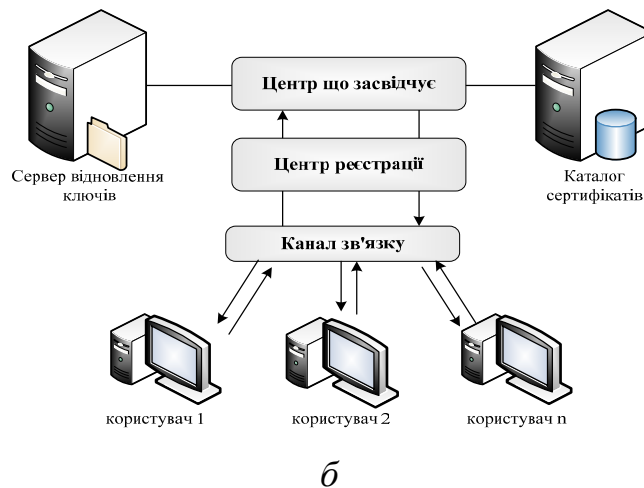
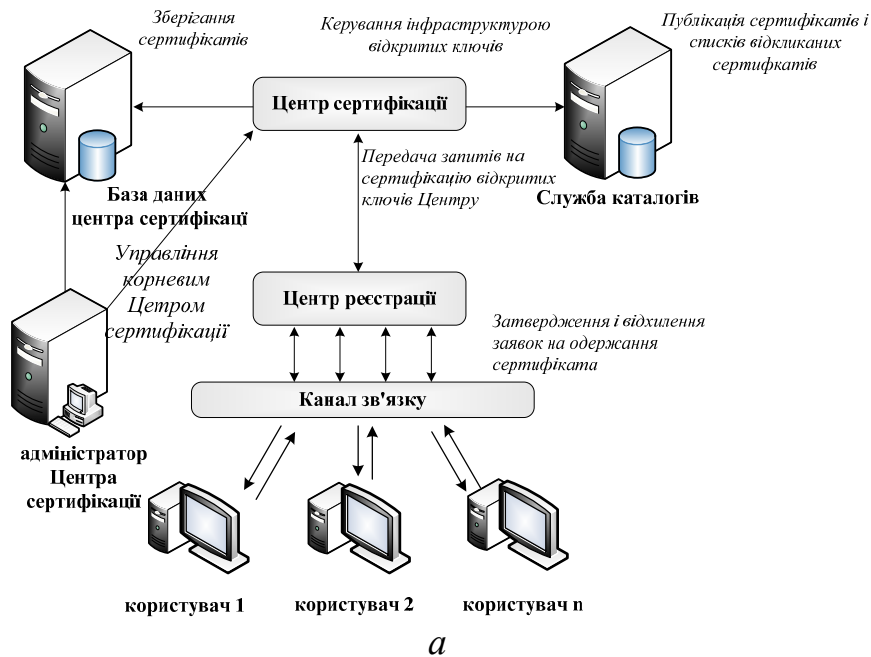


Рис. 4.22. Інфраструктура відкритих ключів:
а – компоненти; *б* – взаємодія між різними компонентами.

Основними атрибутами сертифіката є ім'я та ідентифікатор суб'єкта, інформація про відкритий ключ суб'єкта, ім'я, ідентифікатор і цифровий підпис уповноваженого з видачі сертифікатів, серійний номер, версія і термін дії сертифіката, інформація про алгоритм підпису тощо. Важливо, що цифровий сертифікат містить цифровий підпис на основі секретного ключа довірчого центру.

Центр сертифікації (*Certificate Authority – CA*), або довірчий центр – об'єкт, уповноважений створювати, підписувати та публікувати сертифікати. Центр має також повноваження ідентифікувати користувачів. Основними операціями, що виконує Довірчий центр, є видання, відновлення та анулювання сертифіката.

Дії Центру сертифікації обмежені політикою сертифікації, що диктує йому, яку інформацію він має вміщувати в сертифікат. Центр сертифікації публікує свою політику сертифікації в такий спосіб, щоб користувачі могли перевірити відповідність сертифікатів цій політиці.

Список анульованих сертифікатів (*Certificate Revocation List – Crl*) **CRL** – список сертифікатів, визнаних недійсними в період їхньої дії в разі компрометації секретного ключа чи зміни атрибутів сертифіката з моменту його випуску.

Сховище сертифікатів – спеціальний об'єкт PKI, де зберігаються випущені сертифікати і списки відкликаних сертифікатів. Воно не є обов'язковим компонентом PKI, але значно спрощує доступ до ресурсів і керування системою.

До сховища висувають такі вимоги:

- простота доступу;
- доступ повинний бути стандартним;
- відновлення інформації;
- вбудована система захисту;
- просте керування;
- сумісність з іншими сховищами (необов'язкова вимога).

Сховище спрощує систему поширення сертифікатів.

Фактично чинним стандартом доступу до сховищ є LDAP (*Light-weight Directory Access Protocol*), спрощений протокол доступу до каталогу. Він найбільш адекватний як стандарт для зберігання та витягання сертифікатів після їх генерації, підтримується більшістю серверних операційних систем й баз даних і досить відкритий для того, щоб його могли підтримувати практично будь-які інфраструктури з відкритими ключами.

Центр реєстрації (*Registration Authority – RA*) є додатковим компонентом системи PKI, що дає змогу авторизованому СА автентифікувати користувачів і перевіряти інформацію, що заноситься в сертифікат.

До його функцій можуть належати генерування та архівування ключів, повідомлення про анулювання сертифікатів тощо. У деяких системах СА виконує функції RA. СА видає сертифікат RA (якщо він присутній у системі), причому RA виступає як об'єкт, підлеглий СА. Але RA не може випускати сертифікати.

Кінцевий користувач (*End Entity – EE*) – користувач сертифіката PKI і власник сертифіката. Тобто кінцевий користувач – це об'єкт, що використовує деякі послуги і функції системи PKI. Кінцевий користувач може бути власником сертифіката чи об'єктом, що запитує сертифікат.

Нині не існує загальновизнаного аналога терміна, що бере початок в галузі шифрування з відкритими ключами, – *Certificate Authority*. Це поняття дістало багато різних назв: служба сертифікації, уповноважений з випуску сертифікатів, розпорядник сертифікатів, орган видачі сертифікатів, довірчий центр, центр сертифікації і т. ін. Взаємодію між різними компонентами інфраструктури відкритих ключів ілюструє рис. 4.22,б.

4.6. Засоби криптографічного захисту інформаційно-комунікаційних систем

Як показує практика, виконання криптографічних перетворень у реальному часі найефективніше здійснювати на основі апаратного шифрування, основу якого складають спеціальні апаратні криптографічні засоби, швидкодію яких можна забезпечити через застосування оригінальних технічних рішень для реалізації алгоритмів як симетричної, так і асиметричної криптографії.

У більшості симетричних криптосистем фейстелевського типу (наприклад, таких як DES, ГОСТ і т. ін.) реалізується базова функція, яка n-кратне (залежно від системи) число разів здійснює обробку вихідного тексту.

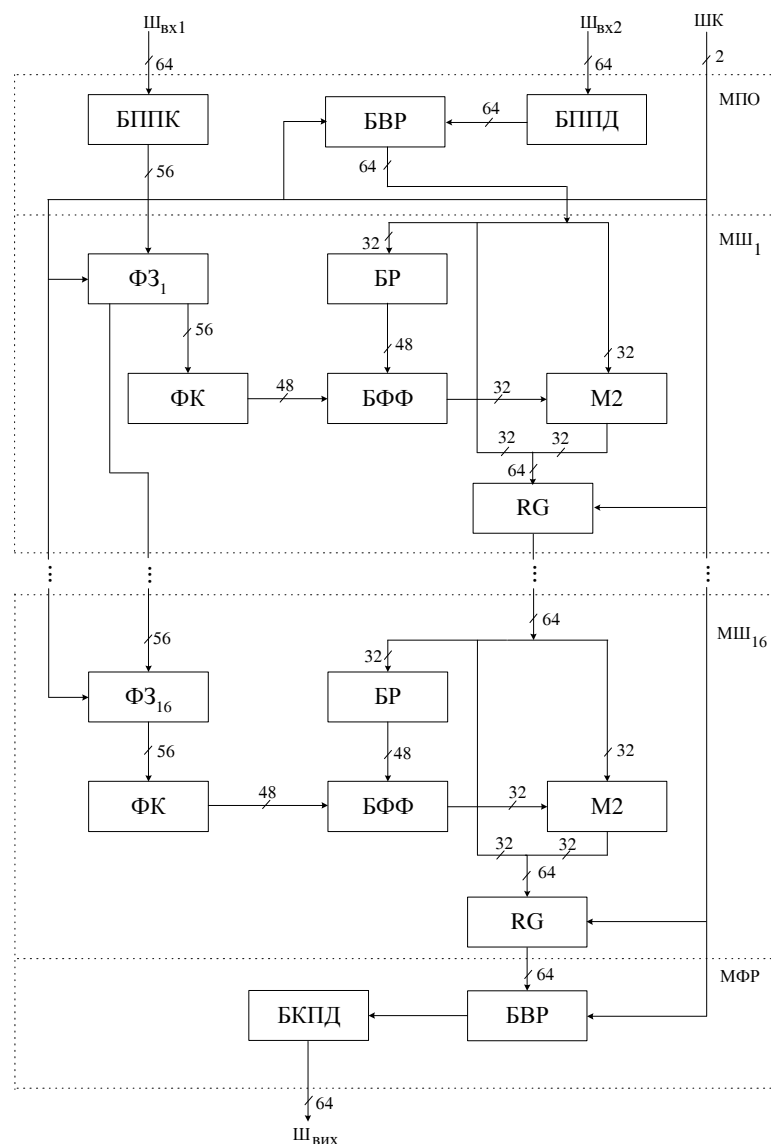


Рис. 4.23. Структурна схема систолічного криптографічного обчислювача

Дану особливість можна використовувати для підвищення продуктивності цифрових пристроїв, які реалізують криптографічні

перетворення. Для цього необхідно побудувати алгоритм, який передбачає організацію конвеєра даних, і відобразити його на систолічну структуру, у якій черговий блок, що виконує функцію шифрування, одержує дані з попереднього.

З метою мінімізації затримок у проектованих структурах обчислювачів деякі перетворення (перестановка, зсув, додавання чи вилучення бітів) потрібно виконувати через відповідні комутаційні сигнальні лінії шин даних. Середня швидкість шифрування одного блока даних у криптографічних систолічних обчислювачах буде зростати зі збільшенням обсягу оброблюваної інформації. Як ілюстрацію викладеного, побудуємо систолічний криптографічний обчислювач КрО – (рис. 4.23), який реалізує систему шифрування DES (рис 4.20).

Він містить модуль (М) початкової обробки (МПО), 16 М шифрування (МШ_i, $i = \overline{1,16}$), М формування результату (МФР), дві 64-бітові шини входу (Ш_{вх1} і Ш_{вх2}), розряди яких є масив, упорядкований відповідно до вихідної матриці (ВМ) (табл. 4.3), 64-бітову шину виходу (Ш_{вих}) і дворозрядну

Таблиця 4.3 шину керування (ШК), через перший розряд якої надходить стробований сигнал запису результату і-ї ітерації шифрування чи дешифрування (Ш/Д), другий – визначає режим роботи КрО Ш/Д.

Вихідна матриця

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

У МПО входять блок початкової підготовки ключа (Кл) (БППК), блок початкової перестановки даних (БППД) і блок вибору режиму (БВР).

Блоки БППК і БППД містять групу контактів (ГК), комутуючих розряди Ш_{вх1} і Ш_{вх2} відповідно на базі матриці початкової підготовки Кл (МППК) (табл. 4.4) і матриці початкової підготовки даних (МППД) (табл. 4.5) відносно ВМ.

Таблиця 4.4

Матриця початкової підготовки ключа

57	49	41	33	25	17	09
01	58	50	42	34	26	18
10	02	59	51	43	35	27
19	11	03	60	52	44	36
63	55	47	39	31	23	15
07	62	54	46	38	30	22
14	06	61	53	45	37	29
21	13	05	28	20	12	04

Таблиця 4.5

Матриця початкової підготовки даних

58	50	42	34	26	18	10	02
60	52	44	36	28	20	12	04
62	54	46	38	30	22	14	06
64	56	48	40	32	24	16	08
57	49	41	33	25	17	09	01
59	51	43	35	27	19	11	03
61	53	45	37	29	21	13	05
63	55	47	39	31	23	15	07

Б

лок
БВР

(рис. 4.24) складається з вузла перестановок (ВП), який містить ГК, комутуючих вихід БППД відповідно до матриці зв'язків (МЗ) (табл. 4.6) і мультиплексора (MUX).

На виході MUX в залежності від режиму роботи Ш/Д формується або значення, що надійшло на вхід даного вузла, або значення, перетворене за допомогою ВП.

Цикли Ш/Д реалізуються за допомогою 16 МШ_i ($i=\overline{1,16}$), що складаються з формувачів організаторів зсувів (ФЗ) (ФЗ_i, $i=\overline{1,16}$) і формувачів Кл (ФК), блоків розширення (БР) і формування функції (БФФ), схем суми за модулем 2 (М2) і регістрів (RG).

Модулі МШ_i ($i=\overline{1,16}$) відрізняються від ФЗ_i ($i=\overline{1,16}$), які у черговій

Таблиця 4.6

Матриця зв'язків

33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64
1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32

ітерації Ш/Д формують нове значення для ФК, що генерує Кл шифрування (Кл_i, $i=\overline{1,16}$). Організація зсувів у ФЗ₁ (рис. 4.25), ФЗ_i ($i=\overline{9,16}$) (рис. 4.26), ФЗ_i ($i=\overline{3,8,10,15}$) (рис. 4.27) здійснюється за допомогою організаторів зсувів ліворуч (ЗЛ) (ЗЛ_i, $i=\overline{1,2}$) чи праворуч (ЗП) (ЗП_i, $i=\overline{1,2}$) на основі матриць зсувів, наведених у кожній з табл. 4.7 – 4.10 відповідно.

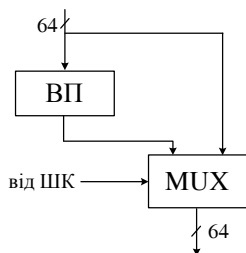


Рис. 4.24.

Структурна схема
блока вибору режиму

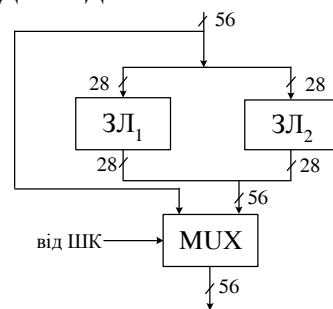


Рис. 4.25. Структурна
схема організатора зсувів у
ФЗ₁

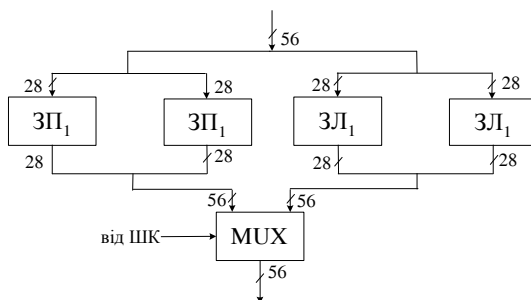


Рис. 4.26. Структурна схема організатора зсувів у ФЗ_i ($i=\overline{9,16}$)

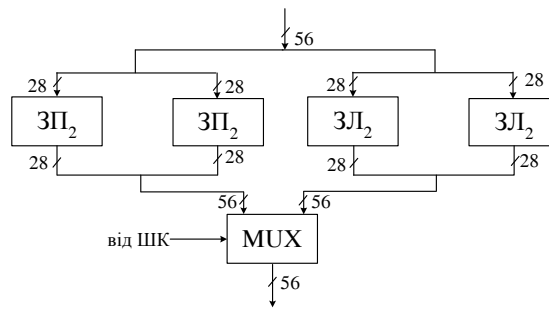


Рис. 4.27. Структурна схема організатора зсувів у ΦC_i , ($i=3,8,10,15$)

Таблиця 4.7
Матриця зсувів

ЗЛ₁

0	1	2	3	4	5	6	3
7	8	9	0	1	2	4	5
6	7	8					

Таблиця 4.8
Матриця зсувів

ЗЛ₂

							0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8						

Таблиця 4.9
Матриця зсувів

ЗП₁

8							
	0	1	2	3	4	5	
6	7	8	9	0	1	2	3
4	5	6	7	8	0	0	1

Таблиця 4.10
Матриця зсувів

ЗП₂

7	8						
		0	1	2	3	4	
5	6	7	8	9	0	1	2
3	4	5	6				

Таблиця 4.11
Матриця завершальної
обробки ключа

14	17	11	24	01	05
03	28	15	06	21	10
23	19	12	04	26	08
16	07	27	20	13	02
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Таблиця 4.12
Матриця розподілу

32	01	02	03	04	05
04	05	06	07	08	09
08	09	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	01

Мультиплексори формувачів $\Phi 3_i$ ($i=\overline{1,16}$) призначені для комутації 56-бітового коду, утвореного $ЗП_i$ ($i = 1,2$) і $ЗЛ_i$ ($i = 1,2$). Формувач $\Phi К$ містить $ГК$, комутуючих виходи $БФФ$ відповідно до матриці завершальної обробки $Кл$ ($МЗОК$) (табл. 4.11), а $БР$ включає $ГК$, комутуючих виходи $БВР$ відповідно до матриці розподілу ($МР$) (табл. 4.12).

Блок $БФФ$ (рис. 4.28) складається з $М2$, постійного запам'ятовувального пристрою ($ПЗП$), в якому зберігається матриця перетворення ($МП$), вузла формування ($ВФ$), що містить $ГК$, комутуючих виходи $ПЗП$ відповідно до матриці перестановок (табл. 4.13).

У RG зберігаються результати $Ш/Д$, одержані на кожній ітерації в $МШ_i$ ($i=\overline{1,16}$). За допомогою RG у структурі $КрО$ формується конвеєр

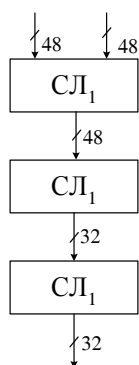


Рис. 4.28. Блок формування функції

даних, завдяки якому ефективно реалізується функція шифрування.

У модуль $МФР$ вміщений $БВР$ і блок кінцевої перестановки даних ($БКПД$), який містить $ГК$, комутуючих виходи $БВР$ відповідно до матриці завершальної обробки даних ($МЗОД$) (табл. 4.14).

Сформована систолічна структура $КрО$ функціонує таким чином. Шестидесятичотирибітовий $Кл$ через $Ш_{вх1}$ надходить до $БППК$, де вилучаються контрольні розряди (8, 16, 24, 32, 40, 48, 56, 64) $ВМ$. Отримане 56-бітове значення надходить до $МШ_1$. Вихідний текст, який піддається $Ш/Д$, у вигляді 64-бітових блоків даних ($БД$) через $Ш_{вх2}$ надходить паралельним кодом у $БППД$. Перетворене у $БППД$ 64-бітове слово надходить до $БВР$ і передається на виходи його $МУХ$, який керується сигналом $Ш/Д$, що надходить із $ШК$. Підготовлені до $Ш/Д$ 64-бітові $БД$ надходять потактно до $МШ_i$ ($i=\overline{1,16}$), у яких зазначені дані розділяються на два $БД$: $БД_1$ і $БД_2$ розмірністю 32 біти кожний.

Молодші розряди, що містяться в $БД_1$, надходять на вхід $М2$, а старші, що містяться в $БД_2$, – на $БР$. Розряди $БД_1$, що надійшли до блок $БР$, розширюються до 48 біт і утворюють новий код.

Сформоване в $БППК$ 56-бітове значення початкового $Кл$ надходить у $\Phi 3_i$ ($i=\overline{1,16}$), де розбивається на старшу і молодшу частини розмірністю 28 біт кожна, які обробляються організаторами зсувів (рис. 4.25 – 4.27

Таблиця 4.13

Матриця завершальної обробки даних

40	08	48	16	56	24	64	32
39	07	47	15	55	23	63	31
38	06	46	14	54	22	62	30
37	05	45	13	53	21	61	29
36	04	44	12	52	20	60	28
35	03	43	11	51	19	59	27
34	02	42	10	50	18	58	26
33	01	41	09	49	17	57	25

Таблиця 4.14

Матриця перестановок

16	07	20	21
29	12	28	17
01	15	23	26
05	18	31	10
02	08	24	14
32	27	03	09
19	13	30	06
22	11	04	25

відповідно), виходи яких підключені до MUX. Сформоване 56-бітове слово на виходах MUX ΦZ_i МШ_i ($i=\overline{1,16}$) надходить до ΦZ_{i+1} МШ_{i+1} ($i=\overline{1,15}$) і ФК МШ_i ($i=\overline{1,16}$).

П'ятидесятишестибітовий БД, який надходить до ФК перетворюється у 48-бітовий, що являє собою значення K_{Li} ($i=\overline{1,16}$) для i -ї ітерації Ш/Д. Ключ, який містить 48 розрядів, K_{Li} ($i=\overline{1,16}$), і 48-бітові дані, сформовані БР, передаються до БФФ (див. рис. 4.28), перетворюються у М2 БФФ і надходять на адресні входи ПЗП БФФ, з якого зчитується БД, переданий до ВФ БФФ.

Із ВФ БФФ 32-розрядний код надходить на перший вхід М2 МШ_i ($i=\overline{1,16}$), на другий вхід якого передаються молодші 32 біт БД, що утворюються на виході БВР МПО для першої ітерації Ш/Д чи RG МШ_i ($i=\overline{2,15}$) – для i -ї ітерації Ш/Д ($i=\overline{2,16}$). Результуючі 32 біт поєднуються зі старшими 32 біт БД БВР МПО для першої ітерації Ш/Д чи RG МШ_i ($i=\overline{2,15}$) – для i -ї ітерації Ш/Д ($i=\overline{2,16}$). Утворений при цьому 64-бітовий код записується у RG за стробуючим сигналом, який надходить із ШК.

Результат, що зберігається в RG МШ_i ($i=\overline{1,16}$), зашифроване чи розшифроване повідомлення для i -ї ітерації (одного циклу Ш/Д). За допомогою МШ_i ($i=\overline{1,16}$) у КрО реалізований 16-ступеневий конвеєр Ш/Д даних. Отриманий в RG МШ_i ($i=16$) 64-бітовий БД передається до МФР, де обробляється у БВР і БКПД. Сформоване 64-бітове повідомлення надходить на 64-розрядну шину виходу ($\text{Ш}_{\text{вих}}$).

У разі конвеєрної обробки середній час Ш/Д одного блока визначається за формулою

$$T_{\text{сер}} = (n \cdot T + 2 \cdot T_{\text{mux}} + (N-1)T) / N,$$

де n – кількість ступенів конвеєра; T – час шифрування для однієї ітерації; T_{mux} – час перемикавання MUX; N – кількість блоків Ш/Д даних.

Наприклад, при $T=86$ час для повідомлення розміром 1024 біт $T_{\text{сер}}$ склало 0,168 мкс, при цьому продуктивність КрО відповідає 45,4 мбайт/с. Для Ш/Д БД більшої довжини, наприклад $N \rightarrow \infty$, $T_{\text{сер}}$ буде наближуватися до T . У цьому випадку гранична продуктивність Ш/Д для цього типу КрО наближається до 88,7 мбайт/с. Якщо зазначену структуру реалізувати на ПЛІС, то продуктивність КрО зросте не менше ніж на порядок.

Як видно, така швидкодія досягається за рахунок використання систолічної організації обчислювача для реалізації криптографічного алгоритму.

Велику зацікавленість для реалізації апаратного шифрування викликають асиметричні схеми, наприклад, метод RSA та його модифікації. Проблема використання RSA подібних алгоритмів під час їх реалізації пов'язана з повільною швидкістю обробки даних. Для реалізації швидкого криптографічного перетворення даних можна використати апаратне шифрування на основі паралельного асиметричного криптопроцесора (КП), що реалізує вищевказаний метод за такими залежностями:

$$C = M^E \bmod N, M = C^D \bmod N,$$

де M – відкритий текст ($0 < M < N$); C – шифротекст ($0 < C < N$), E – відкритий ключ; D – секретний ключ.

Крім операції шифрування і дешифрування (табл. 4.15) КП виконує псевдотекст на простоту за виразом $b^{p-1} \bmod p = 1$.

У табл. 4.15 наведено потрібні ВД, що надходять на три вхідні шини пристрою ($Ш_{вх1}$, $Ш_{вх2}$, $Ш_{вх3}$) і результат, який видається на вихідну шину ($Ш_{вих}$).

Таблиця 4.15

Дані на шинах КП відповідно до ініційованих операцій

Операція	Основа степеневі функції $Ш_{вх1}$	Показник степеня $Ш_{вх2}$	Модуль $Ш_{вх3}$	Результат $Ш_{вих}$
Шифрування	M	E	N	C
Дешифрування	C	D	N	M
Псевдотест на простоту	b	$p-1$	p	-

Такий КП (рис. 4.29) містить пристрій керування (ПК), модулі початкової обробки (МПО): множення (МдМ); ділення (МД); показник степеня (МПС), а також три 512-бітові вхідні шини ($Ш_{вх1}$, $Ш_{вх2}$, $Ш_{вх3}$) і 512-бітову вихідну шину ($Ш_{вих}$).

Модуль МПО призначений для пересилання даних внутрішньою шиною і обчислення кількості тактів, необхідних для множення, і складається з регістрів RGX (512 розрядів), RGV (512 розрядів), RGK (5 розрядів) і комбінаційної схеми KC1. Регістри RGX і RGV використовуються відповідно для зберігання даних, які надходять з $Ш_{вх1}$, і кінцевого результату, а KC1 – для обчислення кількості тактів множення, значення якої записується у RGK.

Модуль МдМ використовується для множення двох 512-розрядних чисел і складається з трьох 512-розрядних регістрів RGA, RGB і RGR, мультиплексорів MX1 і MX2, лічильника СТ1, комбінаційної схеми KC2, помножувача MPL (16×512 розрядів) і тривходового накопичувального 528-розрядного суматора SM1. Регістри RGA і RGB використовуються для зберігання співмножників. Тридцятидвоканальний MX1 передає 32 16-розрядних блоків даних, які знаходяться в RGB, на вхід DX MPL.

Двоканальний MX2 здійснює вибір другого оператора (RGA чи RGB), а для підрахунку блоків застосовується п'ятирозрядний СТ1, вихід якого керує адресою MX1. Схема KC2 порівнює дані СТ1 і RGK, еквівалентність яких сигналізує про виконання останньої операції поблокового (секційного) множення. Суматор SM1 здійснює нагромадження чергових результатів поблокового множення, а зсувний RGR потактно записує молодшу частину добутку.

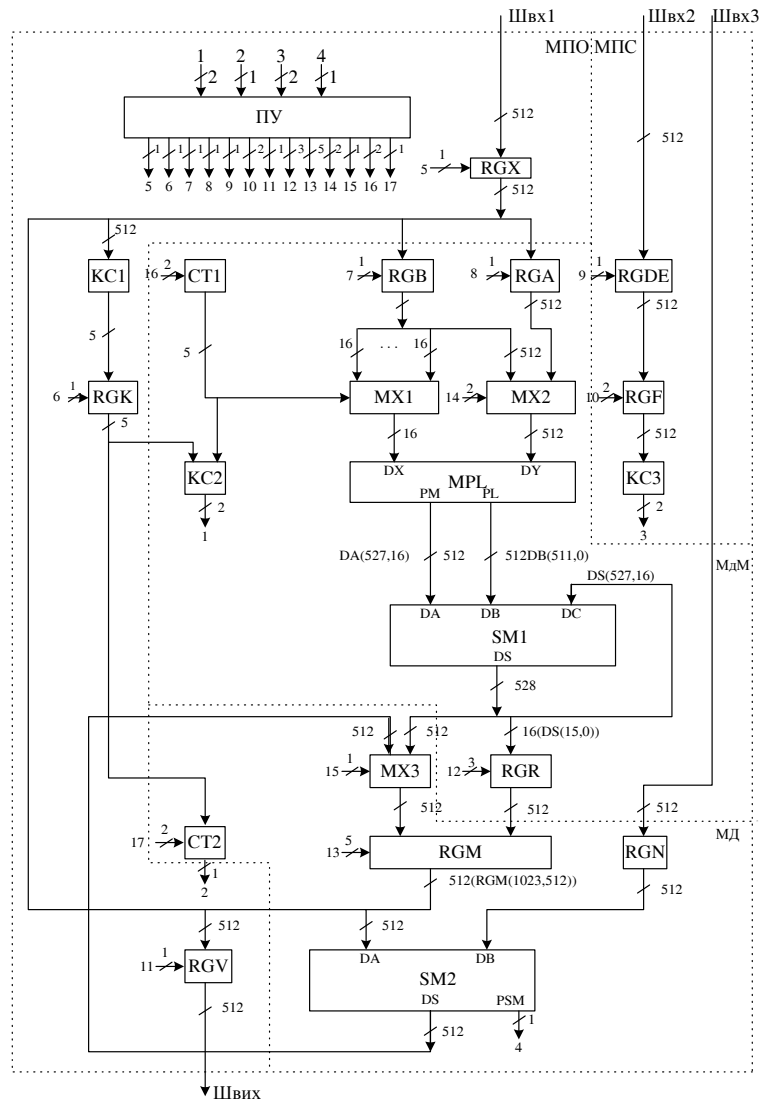


Рис. 4.29. Структурна схема паралельного асиметричного КП

Модуль МД призначений для обчислення залишку від ділення на операнд, що надходить із Ш_{вх3} і складається з регістрів RGM (1024 розрядів) і RGN (512 розрядів), мультиплексора MX3, лічильника CT2 і суматора SM2. Зсувний RGM зберігає ділене чи остачу від ділення, а RGN – значення модуля ділення. Мультиплексор MX3 комутує дані, які надходять у RGM, а SM2 обчислює різницю 512 старших розрядів RGM і вмісту RGN, результат якої записується в RGM, якщо він більше нуля. Дев'ятирозрядний лічильник CT2 підраховує кількість зсувів RGM, і коли їх 512, виробляється сигнал закінчення операції ділення.

Модуль використовується для визначення послідовності виконання операцій множення і ділення та складається з регістра RGDE (512 розрядів), регістра зсуву RGF (512 розрядів) і комбінаційної схеми KC3. Регістри RGDE і RGF використовують відповідно для зберігання і зсувів на один розряд праворуч показника степеня. Схема KC3 обчислює значення двох сигналів: перший визначає значення нульового розряду RGF, другий вказує на те, що RGF дорівнює нулю (ознака кінця обчислень).

Після завантаження в RGX, RGDE, RGN даних (табл. 4.15) і надходження сигналу «пуск» пересилається вміст із RGX у RGA і RGB, які зберігають значення співмножників. Паралельно дані з RGX надходять до KC1, яка вираховує число K ($0 < K < 31$, K – параметр, від якого залежить кількість тактів операції множення), що надходить до RGK. Дані з RGDE заносяться в RGF для виконання зсувів, а CT1 скидається.

Далі в ПК аналізується значення нульового розряду RGF, що надійшов через KC3 і формується сигнал керування для MX2, комутуючий RGA чи RGB до входу DY MPL. Якщо значення вказаного розряду дорівнює одиниці, то виконується множення вмісту RGB і RGA, інакше – RGB і RGB. Мультиплексор MX1 залежно від значення CT1 комутує блоки розміром 16 біт, що зберігаються в регістрі RGB, на вхід DX MP.

У результаті множення утворюються два 512-бітові числа – старша і молодша частина секційного множення. Старша частина апаратно зсувається на 16 розрядів ліворуч і надходить на вхід DA SM1, молодша частина – на вхід DB, а на DC – результат попереднього додавання. Обчислена 528-бітова сума надходить на вихід DS SM1, молодші 16 біт якого записуються в RGR, а інші 512 надходять на вхід DC SM1, апаратно зсунуті на 16 розрядів праворуч.

З метою підвищення швидкодії підсумовування і множення виконуються паралельно (конвеєрні обчислення), тобто під час множення i -х 16 розрядів RGB, результати $(i-1)$ -го множення складаються з попередніми. Повне перетворення здійснюється максимум за 33 цикли обчислень (32 множення і 32 додавання, зсунутих відносно множення на один цикл).

Після виконання чергового множення і додавання CT1 збільшується на одиницю, а на вхід MP надходять наступні 16 біт RGB і виконується чергове множення і додавання. Якщо значення CT1 $>$ RGK, то реалізація множення припиняється і виконується останнє додавання. Результат множення (512 молодших розрядів якого зберігаються в RGR, а 512 старших розрядів надходять з виходу SM1) передається у RGM для ділення на модуль, а інверсне значення RGK надходить до CT2.

Для підвищення швидкості перетворень в КП виконується аналіз молодшого біта RGF, якщо він дорівнює одиниці, то не чекаючи обчислення остачі від ділення, МдМ підносить до квадрата вміст RGB.

Після отримання добутку в RGM аналізується його старший розряд і якщо він дорівнює нулю, то відбувається зсув RGM вліво на розряд і значення CT2 інкрементується. Якщо зазначений розряд дорівнює одиниці, то зі старших 512 розрядів RGM віднімається (за допомогою SM2) дільник, що зберігається в RGN. Якщо результат позитивний, то він записується в старші 512 розрядів RGM і цикл віднімання продовжується до завершення ділення, яке припиняється при значенні CT2=512, а остача зберігається в 512 старших розрядах RGM.

Після цього результат заноситься в RGA чи RGB залежно від того, чи їх дані збільшувалися в МдМ. Потім виконується наступний цикл множень і ділень.

Після закінчення кожного циклу відбувається зсув RGF на розряд праворуч. Якщо всі розряди RGF стали дорівнювати нулю, то виконання операції піднесення до степеня числа закінчено і результат з RGM заноситься до RGV. Після закінчення обчислень виробляється сигнал «дані готові» і через $\Pi_{\text{вих}}$ зчитуються з КП.

На основі сучасних технічних рішень в Україні розроблені та серійно випускаються засоби криптографічного захисту для інформаційно-комунікаційних систем. Розглянемо розробки науково-впроваджувального підприємства НВФ «Криптон».

До пристроїв захищеної передачі інформації можна віднести виріб «ТОПАЗ-8000», який призначається для шифрування даних та підключається в розрив з'єднання комп'ютера (або іншого термінального обладнання) і стандартного модему, під'єданого до комутованих або виділених д्रोсяних або мобільних каналів зв'язку. Швидкість передачі даних пристрою до 115000 біт/с і він може працювати в мобільній мережі передачі із використанням модему GSM та дозволяє організувати захищену мережу між 2-ма і більш абонентами (максимальне число абонентів 10 000). Також підтримується віддалене підключення до Ethernet.

Засіб на основі ГОСТ 28147-89 реалізує шифрування потоку даних інтерфейсу RS-232 (криптоперетворенню піддається вся інформація, за винятком АТ-команд). Пристрій забезпечує ключову систему методу відкритих ключів Діффі-Хеллмана у варіанті Ель-Гамала з довжиною відкритої частини ключа 1024 біта (довжина сеансового ключа складає 256 біт). Також реалізований алгоритм аутентифікації, а довготривалий ключ (ДК) завдовжки 512 бітів для алгоритму шифрування є однаковим для всіх пристроїв однієї мережі і зберігається в недоступній ззовні пам'яті пристрою. Разовий ключ (РК) повинен бути унікальним для кожного напрямку зв'язку і вибирається з масиву РК (довжина РК складає 256 біт), а при завершенні часу його використання проводиться автоматична зміна зі знищенням старого РК.

Існує декілька варіантів застосування цього пристрою.

Варіант 1 – з'єднання двох віддалених комп'ютерів через телефонну мережу загального користування (рис. 4.30). Даний варіант є простим прикладом застосування пристрою «Топаз» для криптографічного захисту інформації, що передається абонентами комутованими або виділеними каналами зв'язку.



Рис. 4.30. Схема підключення «Топаз» за варіантом 1

Також можливе з'єднання абонентів через GSM мережу (на основі GSM модемів) або через супутникову мережу з фіксованими каналами передачі.

Варіант 2 – створення повнозв'язної мережі «кожен з кожним» (рис. 4.31) з максимальним числом 1000 абонентів, що входять в один сегмент мережі, тобто кожний з цих 10000 абонентів може підтримувати один з одним захищений зв'язок з використанням ключів, унікальних для кожної пари абонентів.

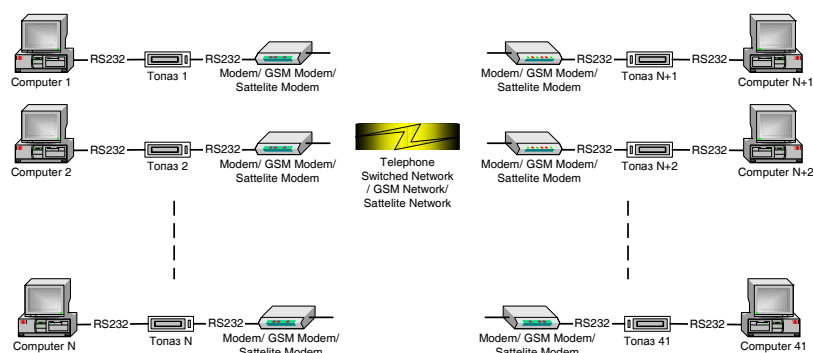


Рис. 4.31. Схема підключення «Топаз» за варіантом 2

Варіант 3 – віддалений доступ до мережі, який використовується у разі необхідності організації такого доступу через Dial-Up або виділеним каналом зв'язку (рис. 4.32).

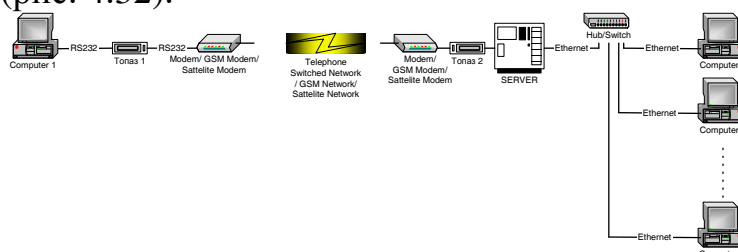


Рис. 4.32. Схема підключення «Топаз» за варіантом 3

Варіант 4 – з'єднання віддалених фрагментів мережі при необхідності організації зв'язку двох і більше віддалених локальних фрагментів однієї захищеної мережі (рис. 4.33).

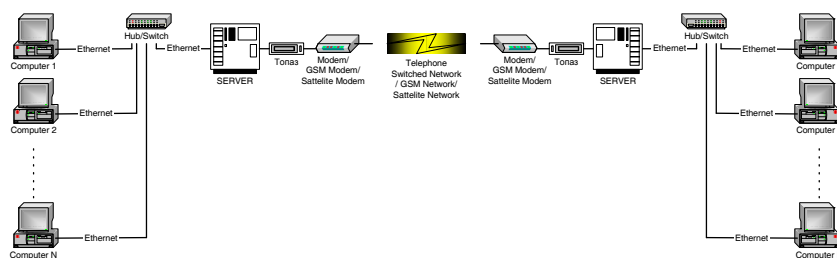


Рис. 4.33. Схема підключення «Топаз» за варіантом 4

Варіант 5 – змішана мережа, що використовується для організації захищеного зв'язку як між фрагментами, так і між окремими абонентами мережі (рис. 4.34).

Комплекс попереднього шифрування на основі «Кокон-М» може підтримувати мережу із 256 абонентів і забезпечувати:

- криптографічне перетворення інформації за ГОСТ-28147-89 у режимах простої заміни, гамування, гамування зі зворотнім зв'язком та виробленням імітовставки;
- генерацію та формування випадкової послідовності;
- неможливість зчитування змісту ключових даних зовнішнім програмним забезпеченням;

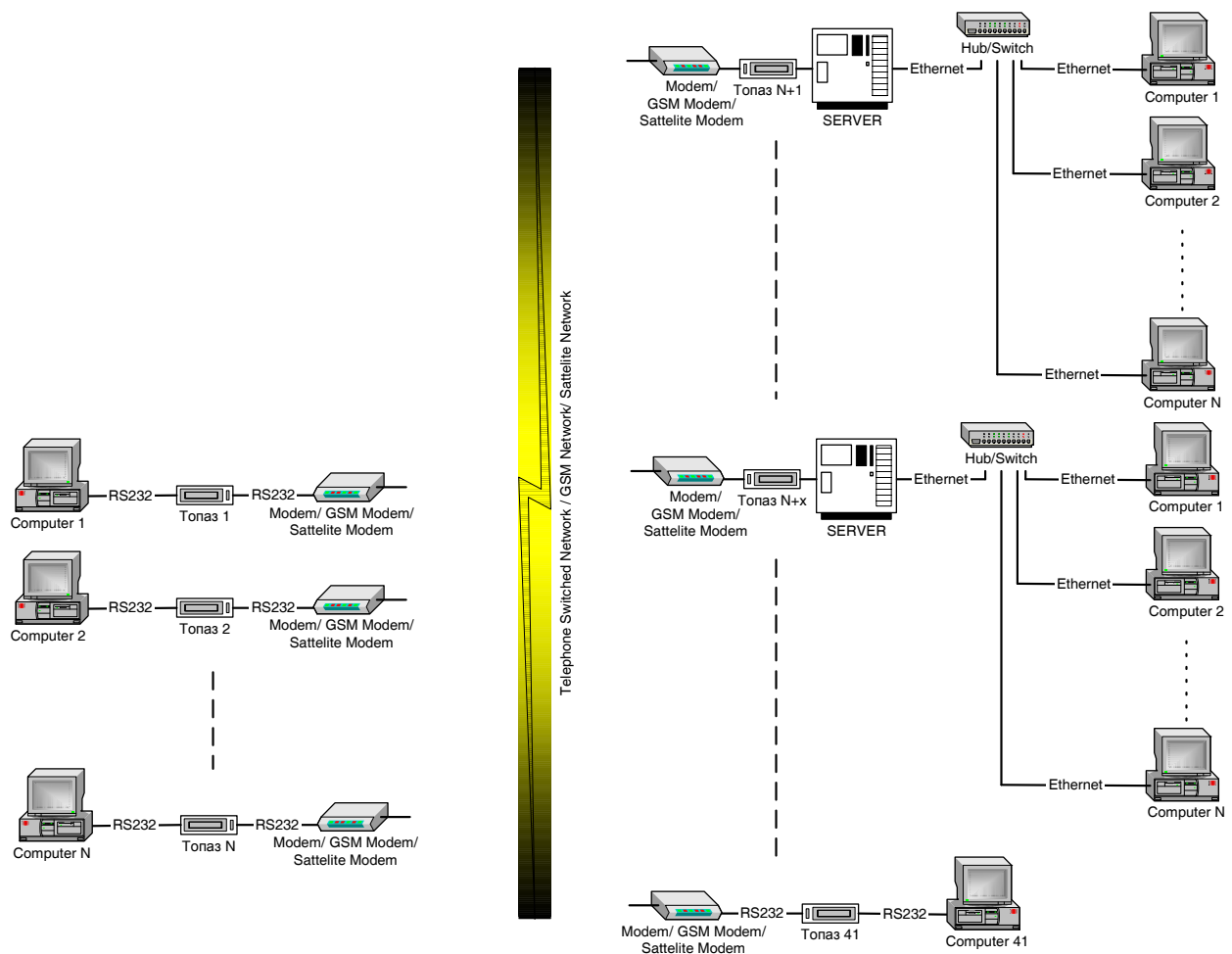


Рис. 4.34. Схема підключення «Тоназ» за варіантом 5

- знищення ключових даних у пристрої;
- перевірку працездатності модуля та стану ключової системи;
- розмежування доступу до функцій пристрою за допомогою паролів.

Завантаження ключових даних у модуль здійснюється за допомогою апаратно-програмного засобу виготовлення ключів. Алгоритм роботи комплексу забезпечує можливість «гарячої» заміни модуля, а знищення усіх даних, відкритих повідомлень та паролів, що зберігаються в

оперативному запам'ятовуючому пристрої, здійснюється відразу після завершення його безпосереднього функціонування.

Комплекс «Кокон-М» має наступні режими роботи:

- «Самоконтроль» (перевірка цілісності ПЗ та наявності усіх необхідних драйверів та файлів на початку роботи);
- «Контроль» (автоматична перевірка працездатності модуля та ідентифікації оператора введення паролю доступу PAS-WORK).
- «Шифрування» (зашифрування та розшифрування інформації за командою оператора за умови підключення модуля до комп'ютера та позитивної перевірки працездатності в режимі «Контроль»);
- «Адміністрування» (знищення ключових та файлів даних, зміна паролю доступу PAS-WORK, встановлення модуля у початковий стан, а також створення та редагування адресної книги абонентів мережі зв'язку);
- «Журнал» (перегляд вмісту журналу, його збереження наприкінці сеансу роботи у текстовому форматі).

«ОНІКС-200» – комплекс тунельного шифрування інформації для віртуальних приватних мереж призначено для криптографічного перетворення даних, які передаються відкритими каналами зв'язку мереж загального користування між локальними фрагментами корпоративної IP-мережі. Апарат вмикається в розрив з'єднання мультиплексного обладнання локальної і глобальної мережі і дозволяє створювати віртуальні приватні мережі (VPN), що містять до 1024 локальних фрагментів побудованих на базі 128 ключових напрямів зв'язку. Пристрій реалізує алгоритм ГОСТ 28147-89 за допомогою модуля апаратного шифрування, за допомогою якого здійснюється криптоперетворення всього IP-пакету, що направляється абонентові мережі (пропускна спроможність пристрою – до 92 Мбіт/с). Підтримується робота в мережах, що використовують технологію VLAN (IEEE 802.1Q).

Ключ ДК (512 біт) є однаковим для всієї віртуальної мережі і зберігається в недоступній ззовні пам'яті апарату, а (РК) (256 біт) є унікальним для кожної пари абонентів мережі і вибирається із масиву РК відповідно до IP-адреси абонента. Після завершення часу дії РК, він знищується і автоматично формується новий. Введення ключової інформації реалізується за допомогою модуля ключових даних, який є флеш-картою MMC.

Структура шифратора забезпечує 100% апаратне дублювання функцій шифрування і контролю. При вмиканні живлення пристрій виконує систему тестів, а в процесі роботи проводиться тестування трактів шифрування/розшифрування. Безпека підтримується системою контролю і знищення критичної інформації, як за командою оператора, так і при виявленні атаки на апаратуру.

Застосування цього пристрою промодельовано на наступному прикладі. Нехай відділення підприємства знаходяться в обласних центрах країни і мають свою локальну комп'ютерну мережу, що включає 3 і більше комп'ютерів. Відділенням постійно необхідно обмінюватися конфіденційною інформацією, для чого слід організувати захищену віртуальну мережу підприємства на базі технології INTERNET.

Для цього у кожній локальній мережі організується доступ до виділеного каналу INTERNET, перед яким і встановлюється пристрій (рис. 4.35).

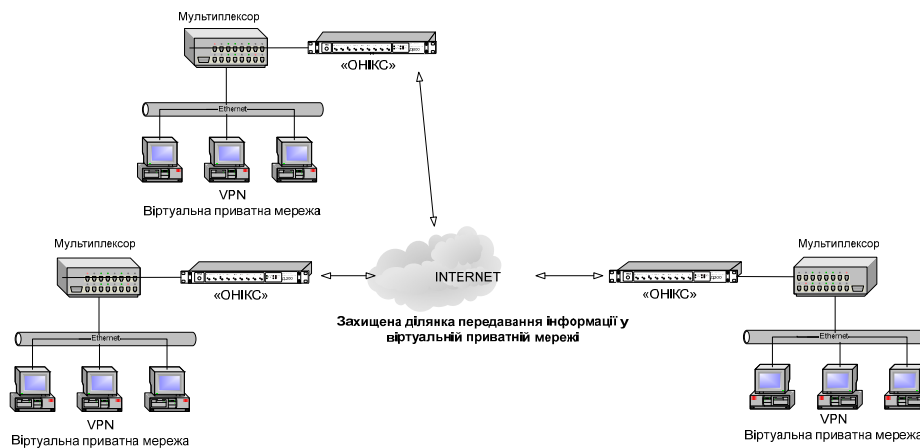


Рис.4.35 Схема підключення «ОНІКС»

Для захисту інформації, що передається комутованими каналами, використовується низка пристроїв, серед яких і абонентський пристрій криптографічного захисту інформації «СЕКМОД-К», який здійснює захист конфіденційних даних під час передачі мовних сигналів телефонними комутованими каналами (фізичними лініями).

Пристрій виконано у вигляді телефонного апарату, який включає:

- вокодер (швидкість передачі даних 5600 біт/с);
- модуляр (криптографічний перетворювач сигналів мовного спектру);
- модем (рекомендації V.34, V.42) для передачі шифрованих параметрів мови між однотипними апаратами;
- шифратор ГОСТ 28147-89;
- контролер криптопротоколу, тестів і блокувань.

Пристрій забезпечує ключову систему за методом відкритих ключів Діффі-Хеллмана у варіанті Ель-Гамала з довжиною відкритої частини ключа 1024 біти (сеансовий ключ складає 256 бітів) та містить масив з 16-ти ДК (512 бітів), які для кожного сеансу зв'язку вибираються випадково.

Пристрій має алгоритм аутентифікації та використовується для підприємств з розгалуженою мережею дилерів в різних містах, для яких необхідно забезпечити захист телефонних переговорів. Для цього замість стандартних телефонних апаратів, необхідно встановити криптографічний телефонний апарат «Секмод-К», що забезпечує як звичайні переговори, так і захищені (рис. 4.36).

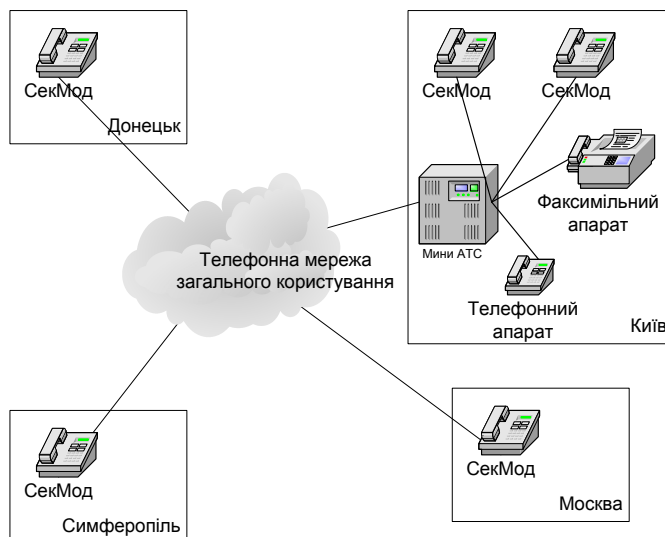


Рис. 4.36. Схема підключення криптографічного телефонного апарату «Секмод-К»

Але якщо власник не бажає змінювати телефонні апарати, то між ними і телефонною мережею загального користування (або міні АТС) встановлюється пристрій криптографічного захисту інформації «Криптон-4М7» (рис. 4.37). У даному варіанті здійснюється і захист передачі факсиміле.

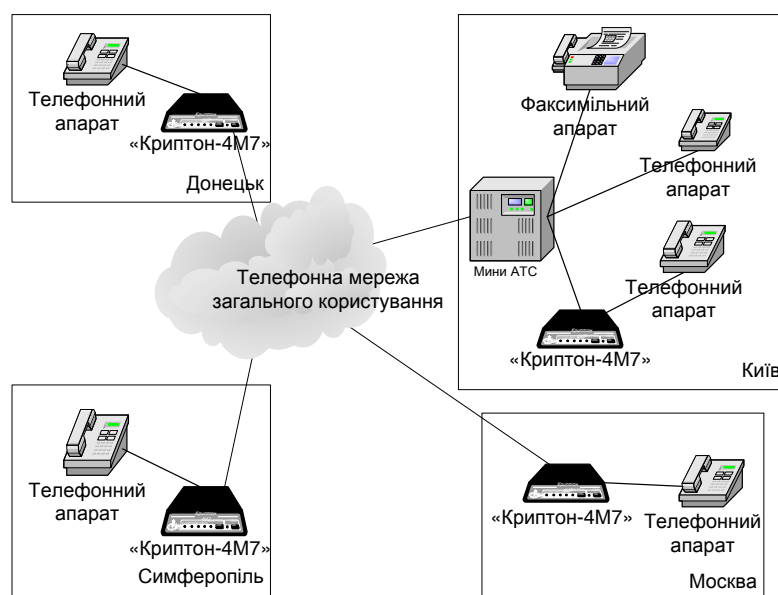


Рис.4.37 Схема підключення «Криптон-4М7»

Якщо для своїх співробітників потрібно організувати окрему мережу рухомого зв'язку, то використовують радіостанції «КРІОН» із захищеним каналом зв'язку.

Пристрій «Д-300» призначений для криптографічного захисту конфіденційної інформації, що передається первинними цифровими каналами типу Е1 і здійснює приймання лінійного сигналу потоку Е1 (СЕРТ, РСМ-30) від станційного напрямку, шифрування інформації в режимі гамування відповідно до ГОСТ 28147-89, формування і передачу

закритого сигналу в канал, приймання лінійного сигналу з боку каналу, розшифрування і передачу відкритого сигналу у напрямі станції.

Об'єктом каналного шифрування є фреймований потік E1, відповідний рекомендаціям ITU-T G.703, G.704, G.706, G.732, G.775, G.796, I.431 і системам з часовим розподілом ETSI ETS 300 011 (лінійний код HDB3).

Структура шифратора забезпечує 100% апаратне дублювання функцій шифрування і контролю, крім того, криптоперетворювач дублюється для реалізації зміни ключа «на льоту», коли шифратор з новим ключем починає роботу без розриву зв'язку і без втрат інформації, що передається.

Для захисту одного напрямку необхідно встановити два комплекти «Д-300» в розрив між станційним і каналним обладнанням зв'язку. При щодобовій автоматичній зміні ключів комплекти можуть працювати без обслуговування протягом року.

Пристрій може застосовуватися на наступних ділянках захищеної системи зв'язку:

- підключення УАТС до центральної станції;
- підключення до вузла ISDN;
- підключення до мультиплексорів (центрам комутації);
- підключення до вузла супутникової системи зв'язку;
- зв'язок між сегментами захищеної комп'ютерної мережі.

При включенні живлення пристрій виконує систему тестів, зокрема тести стандарту FIPS 140-2. В процесі роботи проводиться тестування трактів шифрування/розшифрування і безперервна перевірка якості каналу зв'язку. Таким чином застосовуються всі заходи для виключення неправильної роботи шифраторів.

Безпека «Д-300» підтримується системою контролю і знищення критичної інформації як за командою оператора, так і при виявленні атак на апаратуру.

Розглянемо способи застосування і схеми підключення пристрою.

Варіант 1. Є мережа рівня підприємства, яка містить 80 комп'ютерів. Необхідно створити віддалений фрагмент мережі з 30 комп'ютерів із захищеною інформацією, що передається між фрагментами. Для цього необхідно орендувати один фреймований потік E1 між фрагментами, встановити два комплекти «Д-300» та перетворювачі Ethernet в E1. Після застосування таких засобів реальна пропускна здатність каналу між фрагментами може складати 1,3-1,6 Мбіт/сек. Схема підключення наведена на рис. 4.38.

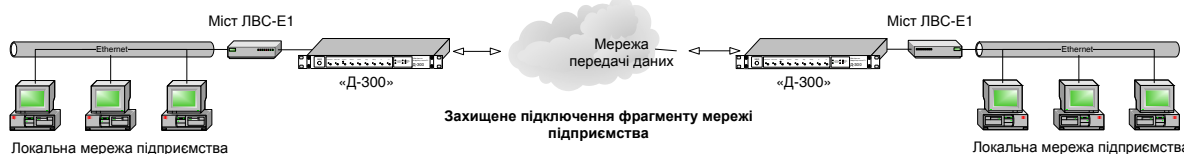


Рис. 4.38 Схема підключення «Д-300» за варіантом 1

Варіант 2. Для захисту інформації, що передається між підприємством і філією необхідно орендувати один фреймований потік E1 між УАТС та встановити два комплекти «Д-300». Таке рішення буде ефективним при кількості абонентів від 50 до 300 для кожної УАТС. Схема підключення наведена на рис. 4.39.

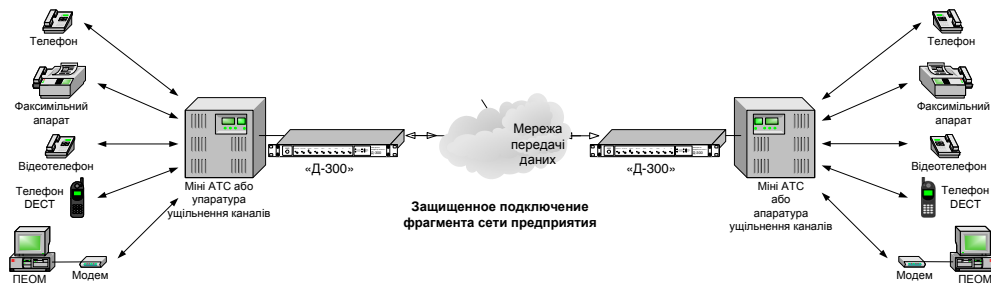


Рис. 4.39. Схема підключення «Д-300» за варіантом 2

Для генерації і запису ключових даних розроблено пристрій «Д-300/Ц», що є автономним блоком, призначеним для формування комплекту ключів для апаратів «Д-300» і записи їх в модулі ключових даних «МКД».

«МКД» – це носій (виконаний у вигляді 8-ми контактного роз’ємного екранованого і герметичного з’єднувача), призначений для транспортування ключової інформації від центру генерації ключів до апаратів криптографічного захисту інформації. Модуль застосовується, як правило, в системі безпечного розподілу ключів на основі принципу «розбиття секрету», при цьому ключова інформація транспортується в двох модулях – «МКД1» і «МКД2».

Ключі РК формуються з даних, що генеруються криптографічно стійким джерелом випадкових чисел, а ДК – на основі даних, представлених на диску. Ключі піддаються різносторонньому тестуванню, а запис ключових даних здійснюється одночасно до двох комплектів носіїв з розбиттям секрету на дві частини, записувані в «МКД» та «Д-300Ц» оснащений системою самотестування і контролю, яка при щонайменших відхиленнях параметрів від норми блокує роботу центру генерації ключів і виключає запис недостовірних ключових даних в «МКД».

Модуль ключових даних підтримує послідовний периферійний інтерфейс SPI із швидкістю обміну до 20 Мбіт/с, а обсяг пам’яті «МКД» достатній для річного запасу ключів за 40 напрямками при щодобовій зміні ключів.

Модуль генератора випадкових чисел «МКЕ-5237» призначений для високопродуктивної генерації послідовностей випадкових чисел в апаратурі засобів криптографічного захисту інформації для формування ключових даних і випадкових параметрів криптографічних алгоритмів і протоколів.

Пристрій відноситься до класу модулів розширення шини PCI і формує аналогові сигнали шуму за допомогою його фізичних джерел, окремі з яких постійно контролюються на стабільність статистичних характеристик. Продуктивність модуля складає не менше 4 Мбайт/с, а для генераторів фізичного шуму потужність джерела шумового сигналу перевищує потужність власних шумів і зовнішніх наведень не менше ніж на 20 дБ.

Генератор випадкових біт «МКЕ-5102» призначений для генерації випадкових бітових послідовностей в апаратурі засобів криптографічного і технічного захисту інформації та відноситься до класу гібридних

інтегральних мікросхем, виготовлених з використанням малогабаритних напівпровідникових приладів, безкорпусних конденсаторів і резисторів, виконаних за SMD-технологією.

Мікросхема є комбінованим аналого-цифровим пристроєм, що включає генератор аналогового шумового сигналу і мікроконтролер з вбудованим аналого-цифровим перетворювачем. Пристрій забезпечує генерацію випадкових бітових послідовностей і передачу їх зовнішнім пристроям із швидкістю 100 Кбіт/с.

Запитання для самоконтролю

1. Назвіть моделі і системи шифрування.
2. Що таке «ключ»?
3. Чим відрізняється «криптографія» від «криптоаналізу»?
4. Що таке «криптографічна система шифрування»?
5. Який процес, обернений до шифрування?
6. Які існують вимоги до сучасних криптографічних систем захисту інформації?
7. Як класифікуються криптографічні методи?
8. Що називається «функцією-пасткою»?
9. Алгоритм шифрування Ель-Гамала.
10. Дайте визначення «цифровому підпису».
11. Назвіть стандарт цифрового підпису (алгоритм DSS).
12. Поясніть, як відбувається в межах криптографії захист прав на цифрову інтелектуальну власність.
13. Як класифікуються спектральні методи цифрової криптографії?
14. Що називається «хеш-функцією»?
15. Які повноваження має центр сертифікації?
16. Які існують основні види атак на криптографічну систему?
17. Які існують основні типи криптоаналітичного розкриття інформації?
18. Який принцип покладено в основу алгоритмів з підстановним і перестановним шифром?
19. Чому асиметричні алгоритми називаються алгоритмами «з відкритим ключем»?
20. Яка різниця між симетричною та асиметричною криптосистемами?
21. Назвіть алгоритми та системи симетричного і асиметричного шифрування.
22. У чому різниця блокового і потокового шифрування і до яких з методів шифрування вони належать?
23. Класифікація блокового шифрування.
24. Які базові криптографічні перетворення використовуються в алгоритмі шифрування RSA?
25. Які існують методи криптоаналізу?
26. Сучасні засоби криптографічного захисту інформації.

Розділ 5. ОСНОВИ ЗАХИСТУ ВІД РУЙНІВНИХ ПРОГРАМНИХ ВПЛИВІВ

5.1. Захист програмного забезпечення. Класифікація загроз

Наприкінці ХХ ст. змінився підхід до самого поняття – «інформація». Цей термін все частіше став використовуватися для ідентифікації особливого виду товару, вартість якого найчастіше перевищує вартість інформаційної системи, у рамках якої він існує.

Проблема захисту ІКСМ стає ще більш серйозною й у зв'язку з розвитком і поширенням обчислювальних мереж, територіально розподілених систем та систем з віддаленим управлінням доступом до інформаційних ресурсів.

Вагомим аргументом для підвищення уваги до питань безпеки ІКСМ є бурхливий розвиток і поширення так званих комп'ютерних вірусів або руйнуючих програмних впливів – програм, здатних потай існувати в системі і здійснювати потенційно будь-які несанкціоновані дії (процеси), що перешкоджають нормальній роботі користувача й самої системи та безпосередньо завдає шкоди властивостям інформації.

Незважаючи на розробку спеціальних програмних засобів захисту від руйнівних програмних впливів, кількість нових програмних вірусів постійно зростає. Щодня з'являється близько 300 нових вірусів та їх модифікацій. Зазначені цифри показують, що існує необхідність звернути особливу увагу на проблему вірусології інформаційного середовища.

Зазвичай користувачі нехтують елементарними заходами безпеки. При цьому, мало хто замислюється про можливі втрати організації у випадку, якщо черговий вірус знищить базу даних бухгалтерії або перетворить у мішанину байтів базу даних клієнтів. Ще менше хвилює людей збиток від діяльності макровірусів, що заважають нормальній роботі співробітників, яким день у день доводиться витрачати певний робочий час на боротьбу із примхами заражених офісних пакетів [68].

Антивірусні програми для індивідуальних користувачів ІКСМ добре відомі й їх існує достатня кількість як комерційних, так і безкоштовних. Менш відомі програмні продукти антивірусного захисту призначені для комплексного захисту корпоративних систем.

Захист програмного забезпечення (ПЗ) – процес встановлення і підтримки стану безпеки програмного забезпечення ІКСМ і її ресурсів, а також збереженої й оброблюваної інформації на базі використання методів, засобів та заходів, що здійснюються згідно з визначеною політикою безпеки.

Слід зазначити, що під інформацією розуміються всі дані, які можуть зберігатися на комп'ютерах користувачів, серверних платформах та іншому устаткуванні ІКСМ, що підлягає захисту. До інформації відносяться всі програмні продукти, що підтримують функціональні можливості ІКСМ, її ресурси й послуги, згідно з визначеними задачами та вимогами. У більшості ж випадків, під поняттям програма мається на увазі процес, який виконується по командах даної програми в межах ІКСМ.

Безпека або захищеність ПЗ – це стан інформації й програмних продуктів, що відповідає встановленому статусу їхнього збереження і використання, згідно з визначеною політикою безпеки та функціями системи.

Поняття «захист» для будь-яких інформаційних об'єктів має конкретний сенс у відповідності до мети та задач захисту ПЗ. Побудова самої системи захисту, відповідно до встановленої цілі, здійснюється шляхом виконання таких трьох базових етапів:

- аналіз структури й принципів функціонування системи, частиною якої є інформаційні об'єкти захисту та ПЗ;
- виділення на основі аналізу вразливих елементів інформаційної системи та ПЗ, які впливають на безпеку цих об'єктів;
- визначення й аналіз можливих загроз зазначеним елементам ПЗ, а також формування переліку організаційних, нормативних, функціональних і технічних вимог до системи захисту;
- розробка системи захисту ПЗ відповідно до пред'явлених вимог та встановленої політики безпеки.

Ціль захисту інформаційного й програмного забезпечення ІКСМ є процес протидії впливу на будь-яку інформаційну систему та її програмне забезпечення, якщо даний вплив виконується з метою їх знищення, зниження ефективності функціонування або несанкціонованого доступу до ресурсів та послуг. Зазначений вплив може бути реалізовано технічно або організаційно, тільки у тому випадку, коли відома інформація про принципи функціонування ІКСМ, її структуру та ПЗ тощо. Базовими причинами припинення функціонування систем є збої й відмови в роботі ПЗ, які частково або повністю перешкоджають функціонуванню ІКСМ, можливостям доступу до інформаційних ресурсів та послуг системи. Крім того, збої й відмови в роботі програм є однією з основних причин втрати даних. Цілі захисту ПЗ, згідно з встановленою метою, представлені на рис. 5.1.



Рис. 5.1. Цілі захисту ПЗ

Класифікація загроз ПЗ ІКСМ. Базовою процедурою формування вимог до створюваної системи захисту ПЗ є аналіз загроз інформації та ПЗ ІКСМ, а також етапи їх виявлення, що відіграють винятково важливу роль в проектуванні системи захисту.

Загроза ПЗ – можливість реалізації будь-якої навмисної або випадкової дії (процесу), що може привести до порушення встановленої політики безпеки ПЗ та інформації, що зберігається і обробляється у ІКСМ.

Відповідно до загальних задач захисту інформації та її властивостей захист ПЗ також можна класифікувати з умов порушення:

- конфіденційності ПЗ;
- цілісності ПЗ;
- надійності та доступності ПЗ.

З точки зору використання та організації підсистем доступу до інформаційних ресурсів і послуг системи, загрози навмисних не авторизованих дій у своїй більшості, мають дві фази реалізації (прояву):

- фазу проникнення, що полягає в спробі несанкціонованого доступу до ресурсів та послуг ІКСМ та безпосередньо до її ПЗ;
- фазу впливу на ПЗ, що полягає в несанкціонованому використанні ресурсів ІКСМ, після успішного доступу до них.

Залежно від способу реалізації, можна виділити такі основні види загроз програмному забезпеченню інформаційної системи (рис. 5.2).

1. Загрози несанкціонованого доступу до ресурсів та ПЗ:

- загрози доступу з боку несанкціонованих користувачів;
- загрози доступу з боку несанкціонованих програм;
- загрози доступу несанкціонованих користувачів від імені санкціонованих (загроза маскуванню зловмисника).

2. *Загрози несанкціонованого використання ресурсів та ПЗ:*

- загрози несанкціонованого використання даних (копіювання, модифікації й ін.);
- загрози несанкціонованого копіювання програм;
- загрози несанкціонованої модифікації програм;
- загрози несанкціонованого дослідження програм;
- загрози несанкціонованого перевикористання даних.

3. *Загрози некоректного використання ресурсів та ПЗ:*

- загрози випадкового доступу з боку прикладних програм до розділів основної пам'яті;
- загрози випадкового доступу до системних областей дискової пам'яті;
- загрози некоректної зміни бази даних (введення невірних даних, порушення цілісності даних, тощо);
- загрози виникнення помилок у роботі користувачів або обслуговуючого персоналу ІКСМ.

4. *Загрози прояву помилок у програмних й програмно-апаратних засобах, що допущені при розробці даних засобів:*

- загрози прояву помилок, допущених при проектуванні специфікацій на розроблювальні засоби ПЗ;
- загрози прояву помилок, допущених при проектуванні розроблювальних засобів ПЗ;
- загрози прояву помилок, допущених при реалізації проектів розроблювальних засобів ПЗ.

5. *Загрози перехоплення потоку даних, що циркулює в лініях зв'язку ІКСМ з метою розкрадання, знищення, модифікації або переадресації інформації.*

6. *Загрози відправлення даних в ІКСМ від імені іншого користувача з метою розкрадання, модифікації інформації або завдання збитків власнику інформації чи системі.*

7. *Загрози несанкціонованої реєстрації електромагнітних випромінювань з метою розкрадання інформації чи подальшої її модифікації.*

8. *Загрози розкрадання документів, носіїв інформації й пристроїв, що входять до інфраструктури ІКСМ.*

9. *Загрози несанкціонованої зміни складу компонентів ІКСМ або злочинного виводу їх з ладу.*

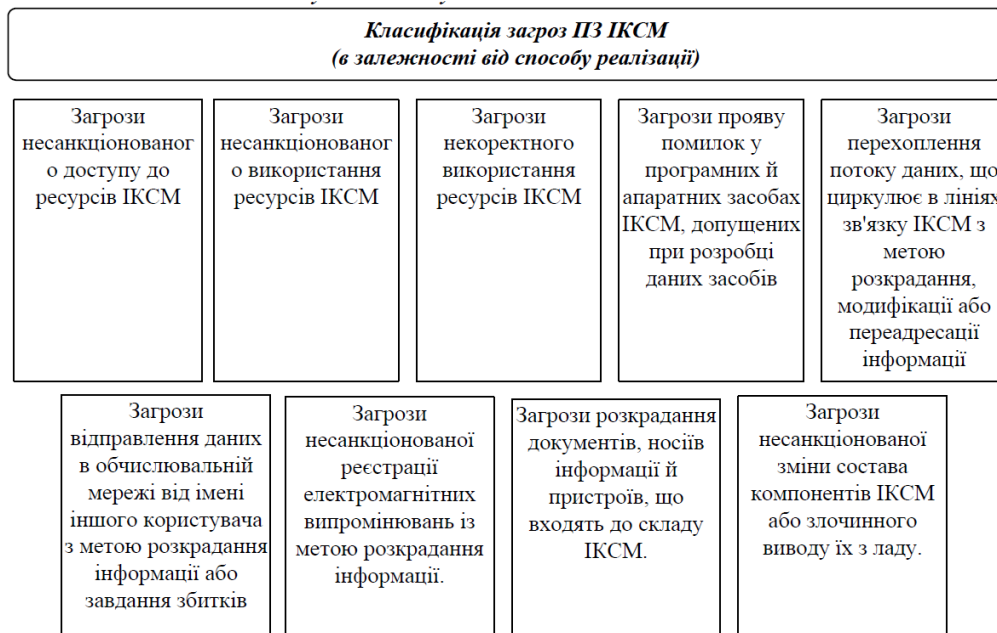


Рис. 5.2. Класифікація загроз залежно від способу реалізації

Реалізація будь-яких загроз виконується через вразливі елементи *ІКСМ*. Під вразливими елементами *ІКСМ* розуміються ті її компоненти програмного та програмно-апаратного устаткування, за допомогою яких можлива реалізація несанкціонованого доступу до інформаційних і програмних ресурсів взагалі.

Слід зазначити, що одним з основних вразливих компонентів *ІКСМ*, безпосередньо є програмне забезпечення інформаційної системи. Зазначений висновок зроблено з урахуванням того, що з допомогою ПЗ можлива реалізація будь-яких несанкціонованих процесів в системі та організація доступу до будь-яких ресурсів ІКСМ.

Для формування повного переліку вимог до розроблювальної системи захисту ПЗ, крім виявлення всіх можливих загроз, повинен бути проведений аналіз цих загроз на основі їхньої класифікації по ряду базових ознак. Кожна з ознак класифікації загроз відбиває одну з узагальнених технічних або організаційних вимог до системи захисту. При цьому загрози, що відповідають кожній ознаці класифікації, дозволяють деталізувати вимоги до системи захисту взагалі.

Класифікація загроз ПЗ ІКСМ може бути проведена за такими базовими ознаками (рис. 5.3).

За безпосереднім джерелом загроз, тобто загрози, безпосереднім джерелом яких є:

- людина (наприклад, загроза несанкціонованого копіювання секретних даних користувачем ІКСМ);
- санкціоновані програмно-апаратні засоби (наприклад, загроза виникнення відмови в роботі операційної системи);
- несанкціоновані програмно-апаратні засоби (наприклад, загроза форматування жорсткого диска програмним вірусом).

За положенням джерела загроз:

- загрози, джерело яких розташовано у межах ІКСМ (наприклад, загрози некоректного використання ресурсів ІКСМ);
 - загрози, джерело яких розташовано поза межами ІКСМ (наприклад, загроза реєстрації випромінювань від ліній зв'язку).
- За ступенем залежності від активності ІКСМ:*
- загрози, які можуть проявлятися незалежно від активності ІКСМ (наприклад, загрози розкрадання документів і носіїв інформації у ІКСМ);
 - загрози, які можуть проявлятися тільки в процесі автоматизованої обробки даних (наприклад, загрози виконання й поширення програмних вірусів).
- За ступенем прояву:*
- загрози випадкової дії (наприклад, загрози прояву помилок програмно-апаратних засобів ІКСМ);
 - загрози навмисної дії (наприклад, загрози дій злоумисника для розкрадання інформації).
- За ступенем впливу на ПЗ:*
- пасивні загрози, які при реалізації нічого не міняють у структурі й змісті ПЗ ІКСМ (наприклад, загроза копіювання секретних даних);
 - активні загрози, які при впливі вносять зміни в структуру й зміст ПЗ ІКСМ (наприклад, загроза навмисної модифікації інформації).
- За етапами доступу користувачів або програм до ресурсів:*
- загрози, які можуть проявлятися на етапі доступу до ресурсів ІКСМ (наприклад, загрози несанкціонованого доступу у ІКСМ);
 - загрози, які можуть проявлятися після дозволу доступу до ресурсів ІКСМ (наприклад, загрози несанкціонованого або не коректного використання ресурсів ІКСМ).
- За способом доступу до ресурсів ІКСМ:*
- загрози, спрямовані на використання прямого стандартного шляху доступу до ресурсів ІКСМ (наприклад, загроза маскуванню під іншого користувача);
 - загрози, спрямовані на використання прихованого нестандартного шляху доступу до ресурсів ІКСМ (наприклад, загроза несанкціонованого доступу до ресурсів ІКСМ шляхом використання не документованих можливостей ОС).
- За місцем розташування інформації, що зберігається та оброблюється у ІКСМ:*
- загрози доступу до інформації на зовнішніх запам'ятовувальних пристроях (наприклад, загроза несанкціонованого копіювання секретної інформації з жорсткого диска);
 - загрози доступу до інформації в основній пам'яті (наприклад, загроза доступу до системної області оперативної пам'яті з боку прикладних програм);
 - загрози доступу до інформації, що циркулює в лініях зв'язку (наприклад, загроза перехоплення потоку даних);

- загрози доступу до інформації, що відображається на терміналі або при друкуванні даних на принтері (наприклад, загроза запису відображуваної інформації на приховану відеокамеру). Загальна кількість загроз програмному забезпеченню інформаційних систем достатньо велика, однак згідно з статистичними даними є категорія загроз, що найбільш часто реалізується не санкціонованими користувачами системи.

Базові загрози інформаційним ресурсам та ПЗ ІКСМ, що найбільш часто реалізовані несанкціонованими користувачами інформаційної системи:

- розкрадання зовнішніх інформаційних носіїв із секретними даними;
- несанкціоноване копіювання секретних даних, після одержання доступу до ресурсів обчислювальної системи та його ПЗ;
- різке зниження продуктивності обчислювальної системи або повне припинення функціонування ІКСМ, через неконтрольоване розмноження комп'ютерних вірусів;
- розкрадання секретної інформації, що зберігається в інформаційній системі, за допомогою комп'ютерних вірусів або іншого ПЗ;
- втрата інформації внаслідок деструктивних дій комп'ютерних вірусів або іншого спеціалізованого ПЗ;
- неможливість завантаження операційної системи, як наслідок дій (процесів) після зараження комп'ютера програмним вірусом і виконання ним деструктивних дій;
- навмисне псування або модифікація інформації з метою завдання матеріальних збитків;
- втрата інформації внаслідок виникнення збоїв і відмов у роботі програмно-апаратного забезпечення;
- матеріальні збитки власника інформації ІКСМ або користувачів інформаційної системи, шляхом підробки або модифікації відповідних даних (відомостей, протоколів, іншої документації) у базах інформаційних ресурсів;

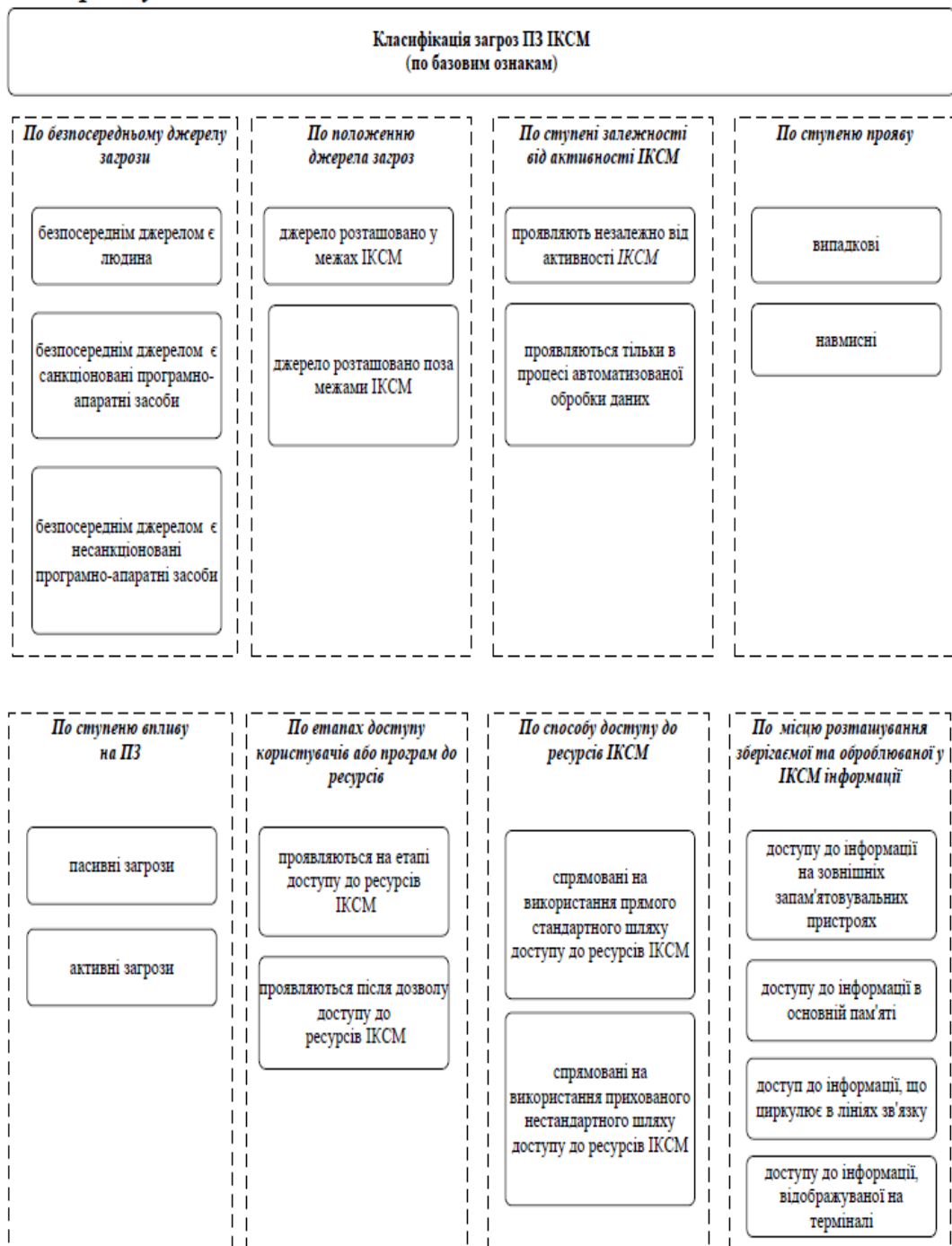


Рис. 5.3. Класифікація загроз програмному забезпеченню ІКСМ

- випадкове руйнування секретної інформації через некоректні дії користувачів або програмних засобів;
- збої й відмови в роботі критичного програмного забезпечення, що призводять до катастрофічних наслідків;
- збої й відмови в роботі програмно-апаратних засобів через випадкове або навмисне руйнування використовуваних ними інформаційних структур;
- перехоплення секретних даних, що циркулюють у лініях зв'язку;
- одержання по мережі некоректних або підроблених повідомлень;

- відмова від фактів одержання або відправлення повідомлень у мережі з метою завдання матеріальних збитків або технічного розірвання угод тощо.

5.2. Класифікація комп'ютерних вірусів

Руйнівний програмний вплив – це програмний код або його частини, за допомогою яких здійснюється загроза хоча б одній характеристиці безпеки певних ресурсів інформаційної системи. Руйнівні впливи можна поділити на такі групи: комп'ютерні віруси (віруси), логічні бомби, потайні ходи і лазівки; програми розкриття паролів, реплікатори, мережні програмні аналізатори, спеціалізовані утиліти, троянські коні.

Вірус – програмний продукт, здатний до багаторазового самовільного створення свого тіла, який зазвичай заражає (модифікує) інші програми, записані у файлах чи системних областях, для подальшого відтворення нового тіла та одержання управління системою з метою модифікації записів, знищення файлів, завантаження ресурсів і виконання інших руйнівних впливів у інформаційній системі.

Логічні бомби – програмний продукт, що ініціюється з виникненням різних подій, наприклад, відкриття певного файлу, обробка заданих записів та інші дії, з метою порушення характеристик безпеки ресурсів інформаційних систем. Використовуються, наприклад, для розкрадання за допомогою змінювання певним чином (на свою користь) коду програми, що реалізує фінансові операції.

Потайний хід. Уразливість в системі, яку навмисно створив її розробник або яка виникла випадково і фактично є додатковим способом проникнення в систему.

Програми розкриття паролів. Програми, зазвичай призначені для несанкціонованого розкриття паролів (наприклад, архівованих файлів) через перебирання варіантів, можливих для використання символів або проникнення в систему за допомогою словників. Програми, що ґрунтуються на останньому методі, здійснюють зламування системи парольного захисту через перебирання елементів одного або кількох словникових файлів, складених спеціально чи взятих із серверів або жорстких дисків локальних станцій.

Реплікатори. Програми, які при виконанні створюють кілька своїх копій в інформаційній системі. Наприклад, коли реплікатор створює тільки одну копію і після цього виконує її, то пам'ять системи швидко переповнюється, чим обмежується доступ до певних компонентів системи.

Мережні аналізатори. Програмно-апаратні засоби (в окремих випадках програми, що запускаються з робочої станції, підключеної до мережі), призначені для зчитування будь-яких параметрів потоку даних в інформаційній системі.

Суперзапінг. Руйнівний вплив, пов'язаний із несанкціонованим використанням утиліт для подальшої їх модифікації, знищення,

копіювання, розкриття, вставлення, застосування або заборони застосування даних інформаційної системи.

Троянські коні. Спеціалізована програма, що, як правило, виступає від імені інших програм і дозволяє дії, відмінні від визначених у специфікації, що використовуються програмним забезпеченням.

З часом, цей перелік може доповнюватися новими складовими, оскільки рівень зростання програмного і апаратного забезпечення настільки інтенсивний, що його навіть важко спрогнозувати.

Деякі з руйнівних програмних впливів, наприклад логічні бомби або троянські коні, можуть бути реалізовані у вигляді програмних закладок («жучків»), які навмисне впроваджуються в тіло певних програм з метою реалізації руйнівних дій на характеристики безпеки ресурсів інформаційних систем. Наприклад, у командний процесор операційної системи можна встановити програмну закладку, яка є резидентною, виконує функції логічної бомби (активізується під час запуску DISKREET.EXE з нортонівських утиліт) і призначається для запису в певне місце на диску (зазвичай сектор, помічений як збійний) паролів, що вводяться з клавіатури. У цьому разі така закладка порушує не тільки цілісність командного процесора, а й конфіденційність даних, що передаються до потрібної утиліти з клавіатури.

Класифікація комп'ютерних вірусів.

З урахуванням аналізу зазначених руйнівних програмних впливів, їх найзручніше класифікувати за такими ознаками (рис. 5.4):

- за середовищем поширення;
- за способом маскуванню в середовищі;
- за інфікованими об'єктами;
- за способом інфікування об'єкта;
- за способом розміщення в інфікованому об'єкті;
- за руйнівним впливом;
- за здатністю до зміни;
- за стилем написання коду.

За середовищем поширення віруси можна поділити на такі, що функціонують відповідно в середовищі: DOS, WINDOWS, UNIX, NETWARE, INTERNET та інших системах (функції і програмні додатки яких використовують віруси). Назву вірусам дають за іменем середовища, в якому вони поширюються.

За способом маскуванню в середовищі віруси поділяють на видимі і невидимі.

Видимі віруси досить легко виявити, використовуючи найпростіші засоби. Наприклад, за допомогою команди DOS dir, можна побачити зміну розміру інфікованого файлу або, запустивши простий шістнадцятковий редактор, знайти, наприклад, сигнатуру вірусу і т. ін.

Невидимі віруси (stealth; стелс-віруси; віруси-невидимки) містять витончені алгоритми, що дозволяють їм маскуватися в середовищі поширення. Такі віруси, перебуваючи в системі, перехоплюють її

звернення до інфікованих об'єктів і замінюють їхні інфіковані ділянки на оригінальні. Після таких дій, наприклад за командою dir, не можна ідентифікувати зміну розміру файлу, а шістнадцятковий редактор, що використовує у своїй роботі функції ОС, не дасть змоги знайти, наприклад, сигнатуру вірусу і т. ін.

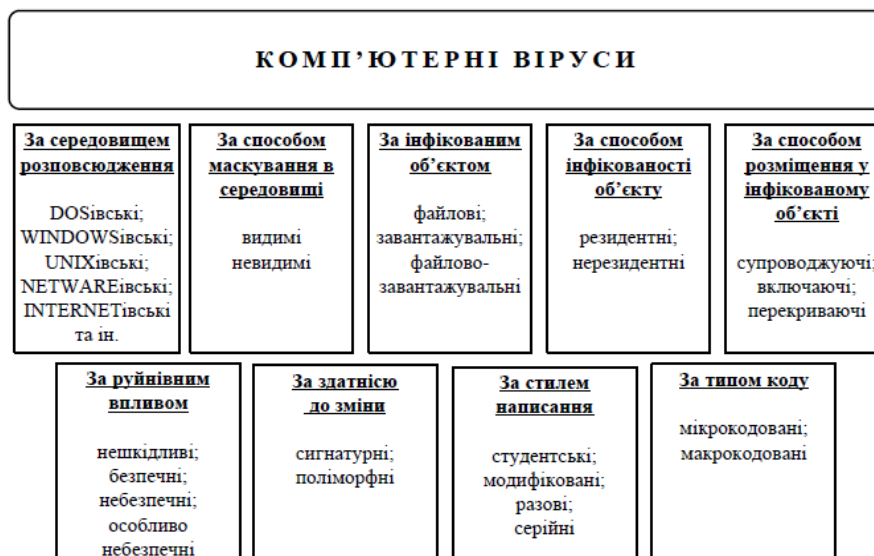


Рис. 5.4. Класифікація комп'ютерних вірусів

За типом інфікованих об'єктів серед вірусів розрізняють: файлові, завантажувальні, файлово-завантажувальні.

Файлові віруси розміщуються у файлах різних форматів (COM, EXE, SYS, DOC і т. ін.) і, як правило, ініціалізуються першими під час їх обробки.

Завантажувальні віруси розміщуються у Boot-секторах дисків або в секторі вінчестера із системним завантажувачем й активізуються під час початкового завантаження ОС.

Файлово-завантажувальні віруси (поєднання файлових і завантажувальних) інфікують як файли, так і зазначені сектори, а алгоритм їхньої роботи значно ускладнюється з урахуванням бінарної дії.

За способом інфікування об'єкта віруси діляться на резидентні та нерезидентні.

Резидентні віруси після запуску залишають в оперативній пам'яті комп'ютера свою резидентну частину, яка перехоплює звернення системи до об'єктів, які підлягають інфікуванню, і заражає їх. Такий вірус залишається в пам'яті аж до вимкнення комп'ютера або його перезавантаження.

Нерезидентні віруси ініціалізуються в період обробки системою інфікованого об'єкта і не є активними (тобто не заражають пам'ять) після цього періоду. Тому нерезидентний вірус не може інфікувати інші файли, якщо не буде ініційовано в момент інфікування файл-носії.

За способом розміщення в інфікованому об'єкті віруси поділяють на супровідні, запускні, перекривальні.

Супровідні віруси трапляються дуже рідко; вони інфікують EXE-файли непрямо, тобто для зазначеного файлу створюється новий з таким самим іменем, але з СОМ-розширенням, де і знаходиться тіло вірусу. У момент запуску файлу з іменем першим активізується СОМ-файл (тобто вірус), який виконує свої функції і далі запускає однойменний EXE-файл.

Запускові віруси вмонтовуються в початок, кінець або у внутрішню частину файлу, при цьому межі останнього розширюються і розміри файлів відповідно збільшуються на розмір впровадженого тіла вірусу, а сам інфікований об'єкт залишається неушкодженим і зберігає свою працездатність.

Перекривальні віруси безповоротно пошкоджують інфікований об'єкт, оскільки в разі його зараження тіло вірусу накладається на код об'єкта. Файли, уражені перекривальним вірусом, не виліковуються і тому, зазвичай, вилучаються.

За руйнівним впливом серед вірусів розрізняють нешкідливі, безпечні, небезпечні, особливо небезпечні.

Нешкідливі віруси відповідно до їх алгоритму не завдають прямої шкоди інформаційній системі, за винятком зайнятого дискового простору і частини оперативної пам'яті (особливо, якщо вірус резидентний). Але будь-який вірус, навіть нешкідливий, може виявити себе інакше в нових умовах (наприклад, у разі зміни версії операційної системи або середовища, характерного для поширення вірусів, форматів дисків і т. ін.) і призвести до непередбачуваних наслідків.

Безпечні віруси характеризуються проявами різних звукових та відео ефектів і, аналогічно нешкідливим вірусам, зменшують розмір вільної пам'яті.

Небезпечні віруси не лише зменшують розмір вільного дискового простору та оперативної пам'яті, а й призводять до серйозних збоїв у роботі системи.

Особливо небезпечні віруси завдають найбільшої шкоди користувачеві та системі. Вони знищують програми, дані, різні записи на дисках та іншу інформацію, що може призвести до безповоротних втрат і серйозних відмов у роботі системи.

За здатністю до змінювання віруси поділяють на сигнатурні та поліморфні.

Сигнатурні віруси завжди мають постійний код, або в тілі вірусу можна принаймні виділити незмінний код (сигнатуру), за яким його можна розпізнати.

Поліморфні віруси не мають постійних пізнавальних груп – сигнатур. Звичні віруси для розпізнавання факту зараження середовища існування розміщують в зараженому об'єкті спеціальну пізнавальну двійкову послідовність або послідовність символів (сигнатуру), яка однозначно ідентифікує зараженість файлу або сектора. Сигнатури використовуються на етапі розповсюдження вірусів для того, щоб уникнути багатократного зараження одних і тих же об'єктів, оскільки при багатократному зараженні

об'єкта значно зростає ймовірність виявлення вірусу. Для усунення демаскуючих ознак поліморфні віруси використовують шифрування тіла вірусу і модифікацію програми шифрування. За рахунок такого перетворення поліморфні віруси не мають збігів кодів. *Поліморфні віруси* дуже складно виявити, оскільки вони не мають сигнатур. Іншими словами, складно знайти два однакові тіла вірусу. Такий ефект досягається через трансформацію його тіла, наприклад за допомогою нескладного шифрування (зазвичай з використанням операції XOR), а також змінюванням програми шифрування. Зазначені віруси називають *привидами* і досить часто при їх побудові використовують стелс-технологію, що робить їх невидимими у відповідному середовищі.

Відповідно до особливостей алгоритму функціонування віруси можна розділити на два класи:

- віруси, що не змінюють середовище існування (файли і сектори) при розповсюдженні;

- віруси, що змінюють середовище існування при розповсюдженні.

У свою чергу, віруси, що не змінюють середовище існування, можуть бути розділені на дві групи:

- віруси-супутники (companion);

- віруси-хробаки (worm).

За стилем написання серед вірусів виділяють студентські, модифіковані, разові та серійні.

Студентські віруси містять зазвичай багато помилок, побудовані за нескладним алгоритмом і є першими спробами авторів у цій області програмування.

Віруси-супутники не змінюють файли. Механізм їх дії полягає в створенні копій виконуваних файлів. Наприклад, в MS-DOS такі віруси створюють копії для файлів, що мають розширення .EXE. Копії привласнюється те ж ім'я, що і виконуваному файлу, але розширення змінюється на .COM. При запуску файлу із загальним ім'ям операційна система першим завантажує на виконання файл з розширенням .COM, який є програмою-вірусом. Файл-вірус запускає потім і файл з розширенням .EXE.

Віруси-хробаки потрапляють в робочу станцію з мережі, обчислюють адреси розсилки вірусу по інших абонентах мережі і здійснюють передачу вірусу. Вірус не змінює файлів і не записується в завантажувальні сектори дисків. Деякі віруси-хробаки створюють робочі копії вірусу на диску, інші – розміщуються тільки в оперативній пам'яті ЕОМ.

За складністю, ступенем досконалості і особливостями маскування алгоритмів віруси, що ***змінюють середовище існування***, поділяються на:

- студентські;

- стелс-віруси (віруси-невидимки);

- поліморфні.

До студентських відносять віруси, творці яких мають низьку кваліфікацію. Такі віруси, як правило, є нерезидентними, часто містять помилки, досить просто виявляються і віддаляються.

Стелс-віруси і поліморфні віруси створюються кваліфікованими фахівцями, обізнаними в роботі апаратурних засобів і операційної системи, а також вододіючими навиками роботи з машино-орієнтованими системами програмування.

Стелс-віруси маскують свою присутність в середовищі існування шляхом перехоплення обігу операційної системи до уражених файлів, секторам і переадресують ОС до незаражених ділянок інформації. Вірус є резидентним, маскується під програми ОС, може переміщуватися в пам'яті. Такі віруси активізуються при виникненні переривань, виконують певні дії, у тому числі і по маскуванню, і тільки тоді управління передається на програми ОС, оброблювальні ці переривання. Стелс-віруси мають здатність протидіяти резидентним антивірусним засобам.

Модифіковані віруси створюють шляхом зміни коду вірусу, який раніше створили інші автори. Разові віруси створюють здебільшого досвідчені програмісти після кропіткої роботи, зазвичай, з метою перевірки своїх професійних здібностей.

Серійні віруси створюють автори або група авторів і виконують їх у єдиному стилі. Досліджуючи їх, можна побачити, як зростає майстерність виробника.

За типом коду віруси поділяють на мікрокодовані та макрокодовані.

Мікрокодовані віруси утворюються, як правило, унаслідок роботи компілятора і є бінарним кодом, що приєднується до інфікованого об'єкта.

Макрокодовані віруси зазвичай обробляються інтерпретатором макрокоду і є послідовністю макрокодів, що зберігаються переважно у файлах (наприклад, із розширенням DOC), створених прикладними програмами, які мають можливість створення макросів (наприклад, MS WORD for WINDOWS).

Будь-який вірус, незалежно від приналежності до певних класів, повинен мати три функціональні блоки: блок зараження (розповсюдження), блок маскуванню і блок виконання деструктивних дій. Розділення на функціональні блоки означає, що до певного блоку відносяться команди програми вірусу, виконуючі одну з трьох функцій, незалежно від місця знаходження команд в тілі вірусу.

Після передачі управління вірусу, як правило, виконуються певні функції блоку маскуванню. Наприклад, здійснюється розшифровка тіла вірусу. Потім вірус виконує функцію проникнення в незаражене середовище існування. Якщо вірусом повинні виконуватися деструктивні дії, то вони виконуються або безумовно, або при виконанні певних умов.

Завершує роботу вірусу завжди блок маскуванню. При цьому виконуються, наприклад, такі дії: шифрування вірусу (якщо функція

шифрування реалізована), відновлення старої дати зміни файлу, відновлення атрибутів файлу, коректування таблиць ОС й ін.

Останньою командою вірусу виконується команда переходу на виконання заражених файлів або на виконання програм ОС.

Для зручності роботи з відомими вірусами використовуються каталоги вірусів. У каталог поміщаються такі відомості про стандартні властивості вірусу: ім'я, довжина, файли, що заражаються, місце упровадження у файл, метод зараження, спосіб проникнення в програмну середу для резидентних вірусів, ефекти, що викликаються, наявність (відсутність) деструктивної функції і помилки. Наявність каталогів дозволяє при описі вірусів вказувати тільки особливі відмінності, опускаючи стандартні властивості і дії.

Структурні особливості побудови вірусів.

Файлові віруси. Файлові віруси можуть прописуватись тільки у файли, що виконують певні дії: командні файли (файли, що складаються з команд операційної системи), файли, що саморозархівовуються і призначені для користувача, і системні програми в машинних кодах, а також в документи (таблиці), що мають макрокоманди. Макрокоманди або макроси є працюючими програмами для автоматизації роботи з документами (таблицями). Тому такі документи (таблиці) можна розглядати як виконуваний файл [95].

Для IBM – сумісних ПЕОМ вірус може прописуватись у файли таких типів: командні файли, завантажувальні драйвери, програми в машинних (двійкових) кодах, документи Word з версії 6.0 і вище, таблиці EXCEL. Макровіруси можуть упроваджуватися і в інші файли, що містять макрокоманди. Файлові віруси можуть розміщуватися на початку, середині і кінці файлу, що заражається (рис. 5.5). Незалежно від місця розташування вірусу в тілі зараженого файлу після передачі управління файлу першими виконуються команди вірусу.

У початок файлу вірус прописується одним з трьох способів. Перший з них полягає в переписуванні початку файлу в його кінець, а на місце, що звільнилося, записується вірус. Другий спосіб припускає зчитування вірусу і зараженого файлу в оперативну пам'ять, об'єднання їх в один файл і запис його на місце файлу. При третьому способі зараження вірус записується в початок файлу без збереження вмісту. У цьому випадку заражений файл стає непридатним.

Вірус		Файл	
Заголовок віруса	Файл	Вірус	Файл
Заголовок віруса	Файл		Вірус

Рис. 5.5. Варіанти розміщення вірусів у файлах

У середину файлу вірус може бути записаний також різними способами. Файл може «розширюватися», а в місце, що звільнилося, може бути записаний вірус. Вірус може прописатись в середину файлу без збереження ділянки файлу, на місце якого поміщається вірус.

Деякі руйнівні програмні впливи, наприклад логічні бомби або троянські коні, можуть бути реалізовані у вигляді програмних закладок (жучків), які навмисно проникають в тіло окремих програм з метою здійснення шляхом певних дій руйнуючого впливу на характеристики безпеки різних ресурсів ІС. Наприклад, в резидентну частину командного процесора системи можна прописати програмну закладку, що виконує функцію логічної бомби, яка активізується при запуску утиліти DISKREET.EXE (шифрування інформації на диску) і записує в певне місце на диску (зазвичай в сектор, помічений як збійний) паролі, що вводяться з клавіатури після ініціалізації зазначеної утиліти. Така закладка порушує не тільки цілісність командного процесора, але і конфіденційність даних, що передаються до утиліти з клавіатури.

Є й більш екзотичні способи запису вірусу в середину файлу. Наприклад, вірус «Mutant», застосовує метод стиснення окремих ділянок файлу, при цьому довжина файлу після упровадження вірусу може не змінитися. Найчастіше вірус прописується в кінець файлу. При цьому, як і у випадку з записом вірусу в середину файлу, перші команди файлу замінюються командами переходу на тіло вірусу.

Алгоритм роботи файлового вірусу

Не дивлячись на різноманіття файлових вірусів, можна виділити дії і порядок їх виконання, які присутні при реалізації більшості вірусів цього класу. Такий узагальнений алгоритм може бути представлений у вигляді наступної послідовності кроків.

Крок 1. Резидентний вірус перевіряє, чи заражена оперативна пам'ять, і при необхідності заражає її. Нерезидентний вірус шукає незаражені файли і заражає їх.

Крок 2. Виконуються дії по збереженню працездатності програми, у файл якої прописується вірус (відновлення перших байт програми, налаштування адреси програм і т. д.)

Крок 3. Здійснюється деструктивна функція вірусу, якщо виконуються відповідні умови.

Крок 4. Передається управління програмі, у файлі якої знаходиться вірус.

При реалізації конкретних вірусів склад дій і їх послідовність можуть відрізнятися від приведених в алгоритмі.

Особливості макровірусів

Особливе місце серед файлових вірусів займають макровіруси. Макровіруси є шкідливими програмами, написаними на макромовах, вбудованих в текстових редакторів, електронні таблиці й ін. Для існування вірусів в конкретній системі (редакторі) необхідно, щоб вбудована в неї макромова мала таку можливість:

- прив'язку програми на макромові до конкретного файлу;
- копіювання макропрограм з одного файлу в іншій;
- отримання управління макропрограмою без втручання користувача.

Таким умовам відповідають редактори MS Word, MS Office, Ami Pro, табличний процесор MS Excel. У цих системах використовуються макромови Word Basic і Visual Basic.

При виконанні певних дій над файлами, що містять макропрограми (відкриття, збереження, закриття і т. д.), автоматично виконуються макропрограми файлів. При цьому управління одержують макровіруси, які зберігають активність до тих пір, поки активний відповідний редактор (процесор). Тому при роботі з іншим файлом у «зараженому редакторі (процесорі)» він також заражається. Тут простежується аналогія з резидентними вірусами по механізму зараження. Для отримання управління макровіруси, що заражають файли MS Office, як правило, використовують один з прийомів:

- у вірусі є автомакрос (виконується автоматично, при відкритті документа, таблиці);
- у вірусі перевизначений один із стандартних макросів, який виконується при виборі певного пункту меню;
- макрос вірусу автоматично викликається на виконання при натисненні певної клавіші або комбінацій клавіш.

Перший макровірус Win Word Concept, що пошкоджує документи Word, з'явився влітку 1995 року. Шкідлива функція цього вірусу полягає в зміні формату документів текстового редактора Word у формат файлів стилів. Інший макровірус Win Word Nuclear вже не такий нешкідливий. Він дописує фразу з вимогою заборони ядерних випробувань, що проводяться Францією в Тихому океані. Крім того, цей вірус щорічно 5 квітня намагається знищити важливі системні файли.

Завантажувальні віруси.

Завантажувальні віруси заражають завантажувальні (Boot) сектори гнучких дисків і Boot-сектори або Master Boot Sector (MBR) жорстких дисків (рис. 5.6).

Завантажувальні віруси є резидентними. Зараження відбувається при завантаженні операційної системи з дисків.

Після включення ЕОМ здійснюється контроль її працездатності за допомогою програми, записаній в постійній пам'яті. Якщо перевірка завершилася успішно, то здійснюється зчитування першого сектора жорсткого диска. Порядок використання дисководів для завантаження задається користувачем за допомогою програми Setup. Якщо диск, з якого здійснюється завантаження ОС, заражений завантажувальним вірусом, то виконуються такі кроки:

Крок 1. Читаний з 1-го сектора диска завантажувальний вірус (частина вірусу) одержує управління, зменшує обсяг вільної пам'яті ОП і прочитує з диска тіло вірусу.

Крок 2. Вірус переписує сам себе в іншу область ОП, найчастіше – на старші адреси пам'яті.

Крок 3. Встановлюються необхідні вектора переривань (вірус резидентний).

Крок 4. При виконанні певних умов здійснюються деструктивні дії.

Крок 5. Копіюється Boot-сектор в ОП і передається йому управління.

Сектор 1	Сектор 2	...	Boot-сектор або MBR	Тіло віруса	
Заголовок вірусу					

Рис. 5.6. Розміщення завантажувального вірусу на диску

Віруси операційних систем. Програми-віруси, що створюються для ЕОМ певного типу, що працюють з конкретними ОС. Привабливість ОС для творців вірусів визначається такими чинниками:

- поширеність ОС;
- відсутність вбудованих антивірусних механізмів;
- відносна простота;
- тривалість експлуатації.

Наявність антивірусних механізмів, складність систем і відносно малі терміни експлуатації, сприяють важкому вирішенню задачі створення вірусів. Тому автори вірусів часто вдаються до використання саме операційних систем для упровадження вірусів.

5.3. Методи та засоби захисту програмного забезпечення

Практичні дослідження щодо проектування та впровадження ІКСМ показують, що найдорожчою складовою інформаційної системи є її програмне забезпечення. Тому розробка програмних засобів захисту інформації з практичного погляду – найбільш актуальне та функціонально-практичне завдання для реалізації процедур підвищення надійності роботи ІКСМ.

Програмні засоби захисту є технічними програмно-апаратними пристроями або безпосередньо програмами, що функціонують згідно з встановленими задачами, алгоритмів та визначеної політики безпеки ІКСМ.

Сучасні тенденції розвитку ІКСМ пов'язані з поширенням та інтеграцією локальних і глобальних мереж, а також технологій «клієнт-сервер», що призводить до зниження ефективності систем захисту інформаційних ресурсів ІКСМ з умов їх територіального рознесення та віддаленого адміністрування. Причиною цьому є швидкий ріст інтенсивності проявів загроз, реалізованих шляхом безпосереднього доступу до ресурсів інформаційної системи. Таким чином, зростає роль так званих *активних засобів захисту ПЗ*, що впроваджуються та функціонують безпосередньо на місці розташування тих чи інших інформаційних ресурсів й пов'язаних з ними послуг.

Методи активного захисту ресурсів ІКСМ діють тільки при функціонуванні інформаційної системи та засновані на використанні її програмно-апаратних засобів [59].

Регламентований метод захисту ПЗ (Регламентация ПЗ) – метод захисту інформаційних ресурсів та ПЗ, що полягає в розробці й реалізації комплексних заходів, що створюють умови для автоматизованої обробки й зберігання інформації, при яких можливість порушення політики безпеки ПЗ зводиться до мінімуму ризиків.

Для ефективного захисту ПЗ необхідно строго регламентувати:

- структурну побудову ІКСМ (архітектура будинків, устаткування приміщень і т.д.);
- технологічні схеми автоматизованої обробки інформації з умов реалізації політики захисту;
- технологічні схеми розробки програмних засобів;
- організацію й забезпечення роботи всього персоналу, зайнятого обробкою, зберіганням та передачею інформації.

Фізичними засобами захисту ПЗ називаються такі засоби, що створюють фізичні перешкоди на шляху до інформаційних ресурсів та ПЗ, а також до процесів їхньої обробки, зберігання та передачі.

До фізичних засобів захисту ПЗ відносяться:

- надвисокочастотні, ультразвукові й інфрачервоні системи, призначені для виявлення об'єктів, що рухаються в межах розташування ІКСМ та її ресурсів з умов визначення їхніх розмірів, швидкості й напрямків переміщення;
- лазерні й оптичні системи, що реагують на перетинання порушниками світлових променів;
- телевізійні системи, призначені для спостереження за охоронюваними об'єктами, в межах яких знаходиться ІКСМ та її ресурси;
- кабельні системи, що використовуються для охорони невеликих об'єктів в межах яких знаходиться ІКСМ та її ресурси.

Апаратні засоби захисту ПЗ (безпосередньо входять до складу устаткування ІКСМ) – засоби захисту процесора й основної пам'яті робочої станції користувача або сервера, пристроїв вводу-виводу інформації, комутаційного устаткування каналів зв'язку, засобів обробки й зберігання інформації та ПЗ.

Апаратні засоби захисту процесора призначені в основному для розмежування доступу до команд процесора з боку ПЗ. Апаратні засоби захисту основної пам'яті забезпечують можливість ізолювання адресних просторів оперативної пам'яті, виділених різним програмам. До апаратних засобів захисту пристроїв вводу-виводу інформації відносяться – блокатори доступу, як інструмент захисту від несанкціонованого використання пристроїв.

Апаратні засоби захисту каналів зв'язку, орієнтовані на криптографічне закриття (шифрування) інформаційних потоків переданих по каналах даних.

До програмних засобів захисту відноситься спеціальне програмне забезпечення, що використовується у ІКСМ для вирішення завдань захисту та безпосередньо захисту самого ПЗ.

Організаційно-технічні засоби захисту ПЗ – сукупність організаційно-технічних заходів, що введені з метою встановлення і підтримки стану безпеки програмного забезпечення ІКСМ і її ресурсів, а також збереженої й оброблюваної інформації згідно з визначеною політикою безпеки.

Нормативно-правові засоби захисту ПЗ – сукупність нормативно-правових та законодавчих заходів, що регламентують процес захисту інформаційних ресурсів і ПЗ та являють собою існуючі в країні або спеціально видані закони й інші нормативно-правові акти і норми даної галузі.

На основі *нормативно-правових та законодавчих* засобів захисту ПЗ регламентуються всі процеси, пов'язані із забезпеченням захисту ПЗ, права й обов'язки всіх осіб і підрозділів, які мають відношення до функціонування ІКСМ. За допомогою даних засобів також установлюється відповідальність за дії, наслідком яких може бути порушення рівня захищеності ПЗ.

Оптимальний вибір засобів, необхідних і достатніх для вирішення заданої сукупності завдань захисту ПЗ, здійснюється на основі встановленої політики безпеки з умов мінімізації ризиків для процесів функціонування ІКСМ.

Ефективність захисту ПЗ ІКСМ досягається тільки у випадку об'єднання використовуваних для цієї цілі методів і засобів у єдину систему комплексного захисту, яка повинна бути функціонально самостійною підсистемою ІКСМ.

Із системних позицій захист ПЗ забезпечується цілим комплексом засобів, що починається законодавчими актами і закінчується конкретними апаратно-програмними розробками. Відомі такі категорії засобів захисту програмного забезпечення (рис. 5.7): власні, у складі інформаційної системи, із запитом інформації, активні та пасивні.

Засоби власного захисту визначають елементи захисту, що містяться в самому програмному забезпеченні або супроводжують його. До них належать документація, розповсюдження продукції у вигляді виконавчих модулів, супроводження програм розробником, обмеження застосування, проектування на замовлення, вбудовані ідентифікаційні мітки власника та авторське право.

До *засобів захисту у складі інформаційних систем* відносять захисні механізми пристроїв інформаційних систем, замки захисту доступу та зміну функції в системі.

Серед механізмів захисту дисків потрібно виокремити дві групи:

1. Перешкода безпосередньому копіюванню програм із диска на диск.
2. Захист програм від реасемблювання і налагоджувачів.

Реасемблери та налагоджувачі дають змогу подати програму у формі, більш доступній для сприйняття, а також допомагають вивчити логіку захисту і оперативно здійснити модифікацію програм.

Перша група захищає програму від несанкціонованого відтворення, друга – від несанкціонованої ревізії. Ці групи не взаємозв'язані, оскільки програми, призначені для вільного розповсюдження, можуть бути захищені від налагоджувачів і реасемблерів, і навпаки, різні програмні продукти можуть бути захищені не тільки від копіювання. Найбільш надійний захист забезпечується одночасним застосуванням двох груп, оскільки її подолання у програмі, скопійованій із захищеного диска, буде пов'язане з подоланням захисту другої групи. Отже, програми, захищені від налагоджувачів і реасемблерів, які містяться на стандартному диску, можуть бути легко скопійовані, а ті, що розташовані на захищеному диску і не містять другої групи, можуть бути легко вивчені та модифіковані з метою подолання механізмів захисту.



Рис. 5.7. Категорії засобів захисту програмного забезпечення

Програми, що використовують *засоби захисту із запитом інформації* для подальшого виконання призначених функцій, здійснюють запит на введення додаткової інформації, поданої, наприклад, у вигляді ключових слів. До структури зазначених засобів входять паролі, криптографічні шифри, сигнатури на основі унікальних характеристик інформаційних систем і апаратура захисту.

Засоби активного захисту поділяють на зовнішні і внутрішні; вони активізуються у разі виникнення певних (нештатних) обставин, що підпадають під контроль, наприклад, таких як неправильно введені паролі, вичерпаний час користування, вичерпана кількість запусків, неправильна контрольна сума ділянок програми тощо.

Засоби пасивного захисту охоплюють методи ідентифікації програм, пристрої контролю подій, водяні знаки, що перешкоджають створенню копії, і психологічні заходи. За допомогою цих засобів здійснюється підтвердження справжності, контроль доступу, пошук доказів несанкціонованого копіювання тощо.

Програмні засоби захисту є найважливішою і необхідною частиною механізму захисту сучасних інформаційних систем і можуть бути як автономними, так і входити до складу різного програмного забезпечення. Це насамперед пов'язано з такими їхніми властивостями, як універсальність, гнучкість, надійність, простота реалізації, можливість модифікації та удосконалення. З універсальністю пов'язана можливість розв'язання програмними засобами широкого кола завдань захисту. Гнучкість асоціюється з тим, що вони можуть адаптуватися до конкретних умов функціонування інформаційних систем, а також у структурі інформаційних систем, наприклад, бути складовою частиною операційної системи (ОС), функціонувати як самостійні пакети програм захисту, розподілятися між окремими компонентами системи і т. ін. З надійністю пов'язана висока програмна стійкість у разі тривалої безперервної роботи і задоволення високих вимог щодо достовірності впливів управління за наявності різних дестабілізуючих факторів. Простота реалізації програмних засобів захисту очевидна порівняно з можливістю реалізації будь-яких інших засобів. Можливості їх модифікації й удосконалення визначаються самою природою.

Основними недоліками їх використання є те, що вони додатково завантажують процесор, що призводить до збільшення часу реагування на запити і, відповідно, до зменшення ефективності роботи, а також до зменшення ємності доступної і зовнішньої оперативної пам'яті. Слід зазначити, що у разі випадкової чи зловмисної модифікації програми вона може втратити здатність виконувати функції захисту, а також стати додатковим каналом несанкціонованого отримання інформації. Крім цього, жорстка орієнтація на архітектуру певних типів ПК, а також залежність від ОС доповнює зазначені недоліки.

Перелік програмних засобів захисту може бути будь-яким, а виконувані ними функції можуть бути такі: перевірка прав доступу (за простим паролем, за складним паролем, за разовими паролями); розпізнавання користувачів за різними ідентифікаторами та компонентів програмного забезпечення і елементів баз даних; розмежування доступу до захищених даних за матрицею повноважень, рівнем секретності та іншими ознаками; керування доступом до задач, програм і елементів баз даних за спеціальними мандатами; реєстрація звернень до системи, задач, програм і елементів захищених даних; підготовка до видачі конфіденційних документів (формування і нумерація сторінок, визначення і присвоєння грифа обмеження доступу, реєстрація виданих документів тощо); перевірка адресата перед видачею захищених даних у канали зв'язку; керування видачею даних у канали зв'язку; криптографічне перетворення

даних; контроль процесів обробки і видачі захищених даних; знищення залишкової інформації у постійному запам'ятовувальному пристрої після виконання запитів користувачів; сигналізація спроб несанкціонованих дій; блокування роботи користувачів, які порушують правила захисту інформації; організація псевдо роботи з порушником з метою відвернення його уваги; забезпечення комплексних засобів і систем захисту; комплексний захист від вірусів та інших програмних руйнівних впливів; забезпечення проведення експертиз і сертифікації; керування ризиком та організація дій у кризових ситуаціях тощо.

Слід зазначити, що індустрії цього напряму властива стихійність розвитку програм захисту, що, з одного боку, не дає гарантій повноти наявних засобів, а з другого – не виключає дублювання тих самих завдань захисту. З огляду на сказане, можна відокремити три принципи вимог до формування програмних засобів захисту: функціональна повнота, гнучкість і уніфікованість використання.

Що стосується першої вимоги, то неважко переконатися, що за наведеним щойно переліком можна створити комплексний продукт, який найповніше охоплює всі класи захисту.

Задоволення інших двох вимог залежить від форм і способів подання програм захисту. Аналіз показав, що найповніше вимоги гнучкості й уніфікованості задовольняє така сукупність принципів: наскрізна модульна побудова, повна структуризація, подання машино-незалежною мовою.

Принцип наскрізної модульної побудови полягає в тому, що кожному з програм будь-якого рівня (обсягу) подавати у вигляді системи модулів, кожний з яких має бути цілком автономним і мати стандартні вхід і вихід, що забезпечують комплексування з будь-якими іншими модулями.

Подання машинонезалежною мовою означає, що програмні модулі мають бути такими, щоб їх із мінімальними зусиллями можна було включати до складу програмного забезпечення будь-якої інформаційної системи. Повну універсалізацію подання модулів можна забезпечувати поданням їх у вигляді блок-схеми, деталізованої настільки, щоб кожний блок можна було реалізовувати малою кількістю операторів найбільш поширених мов високого чи низького рівня.

5.4. Методи боротьби з вірусами

Масове розповсюдження вірусів, серйозність наслідків їх дії на ресурси ІКСМ викликали необхідність розробки і використання спеціальних антивірусних засобів і методів їх застосування. Антивірусні засоби застосовуються для вирішення таких задач:

- виявлення вірусів в ІКСМ;
- блокування роботи програм-вірусів;
- усунення наслідків дії вірусів.

Виявлення вірусів бажано здійснювати на стадії їх впровадження або, принаймні, до початку здійснення деструктивних функцій вірусів. Необхідно відзначити, що не існує антивірусних засобів, що гарантують

виявлення всіх можливих класів вірусів. При виявленні вірусу необхідно зразу ж припинити роботу програми-вірусу, щоб мінімізувати збиток від його дії на систему. Усунення наслідків дії вірусів ведеться у двох напрямках:

- видалення вірусів;
- відновлення (при необхідності) файлів, областей пам'яті.

Відновлення системи залежить від типу вірусу, а також від елементу часу виявлення вірусу по відношенню до початку деструктивних дій. Відновлення інформації без використання дублюючої інформації може бути нездійсненним, якщо віруси при упровадженні не зберігають інформацію, на місце якої вони поміщаються в пам'ять, а також, якщо деструктивні дії вже почалися і вони передбачають зміни інформації.

Для боротьби з вірусами використовуються програмні і апаратурно-програмні засоби, які застосовуються в певній послідовності і комбінації, утворюючи методи боротьби з вірусами. Можна виділити методи виявлення вірусів і методи видалення вірусів.

Методи виявлення вірусів

Відомі такі методи виявлення вірусів:

- сканування;
- виявлення змін;
- евристичний аналіз;
- використання резидентних сторожів;
- вакцинація програм;
- апаратурно-програмний захист від вірусів.

Сканування – один з найпростіших методів виявлення вірусів. Сканування здійснюється програмою-сканером, яка проглядає файли у пошуках пізнавальної частини вірусу – сигнатури. Програма фіксує наявність вже відомих вірусів, за винятком поліморфних вірусів, які застосовують шифрування тіла вірусу, змінюючи при цьому кожного разу і сигнатуру. Програми-сканери можуть зберігати не сигнатури відомих вірусів, а їх контрольні суми. Програми-сканери часто можуть видаляти знайдені віруси. Такі програми називаються поліфагами.

Метод сканування застосовується для виявлення вірусів, сигнатури яких вже виділені і є постійними. Для ефективного використання методу необхідне регулярне оновлення відомостей про нові віруси.

Метод виявлення змін базується на використуванні програм-ревізорів. Ці програми визначають і запам'ятовують характеристики всіх областей на дисках, в яких звичайно розміщуються віруси. При періодичному виконанні програм-ревізорів порівнюються характеристики, що зберігаються, і характеристики, одержувані при контролі областей дисків. За наслідками ревізії програма видає відомості про можливу наявність вірусів.

Звичайно *програми-ревізори* запам'ятовують в спеціальних файлах образи головного завантажувального запису, завантажувальних секторів логічних дисків, характеристики всіх контрольованих файлів, каталогів і

номера дефектних кластерів. Можуть контролюватися також обсяг встановленої оперативної пам'яті, кількість підключених до комп'ютера дисків і їх параметри.

Головною перевагою методу є можливість виявлення вірусів всіх типів, а також нових невідомих вірусів. Досконалі програми-ревізори знаходять навіть стелс-віруси.

Є у цього методу і недоліки. За допомогою програм-ревізорів неможливо визначити вірус у файлах, які поступають в систему вже зараженими. Віруси будуть знайдені тільки після розмноження в системі.

Програми-ревізори непридатні для виявлення зараження ресурсів, оскільки документи і таблиці дуже часто змінюються.

Евристичний аналіз порівняно недавно почав використовуватися для виявлення вірусів. Як і метод виявлення змін, даний метод дозволяє визначати невідомі віруси, але не потребує попереднього збору, обробки і зберігання інформації про файлову систему.

Суть евристичного аналізу полягає в перевірці можливих середовищ існування вірусів і виявлення в них команд (груп команд), характерних для вірусів. Такими командами можуть бути команди створення резидентних модулів в оперативній пам'яті, команди прямого звернення до дисків, минувши ОС. Евристичні аналізатори при виявленні «підозрілих» команд у файлах або завантажувальних секторах видають повідомлення про можливе зараження. Після отримання таких повідомлень необхідно ретельно перевірити ймовірно заражені файли і завантажувальні сектори всіма наявними антивірусними засобами. Евристичний аналізатор є, наприклад, в антивірусній програмі Doctor Web.

Метод використання *резидентних сторожів* заснований на застосуванні програм, які постійно знаходяться в ОП ЕОМ і відстежують всі дії решти програм.

У разі виконання якою-небудь програмою підозрілих дій (звернення для запису в завантажувальні сектори, переміщення в ОП резидентних модулів, спроби перехоплення переривань і т. п.) резидентний сторож видає повідомлення користувачу. Програма-сторож може завантажувати на виконання інші антивірусні програми для перевірки «підозрілих» програм, а також для контролю всіх файлів (із змінних дисків, флешек, по мережі), що поступають ззовні.

Істотним недоліком даного методу є значний відсоток помилкових повідомлень, що заважає роботі користувача, викликає роздратування і бажання відмовитися від використання резидентних сторожів.

Під *вакцинацією програм* розуміється створення спеціального модуля для контролю її цілісності. Як характеристика цілісності файлу, зазвичай використовується контрольна сума. При зараженні вакцинованого файлу, модуль контролю знаходить зміну контрольної суми і повідомляє про це користувача. Метод дозволяє знаходити всі віруси, у тому числі і незнайомі, за винятком стелс-вірусів.

Найнадійнішим методом захисту від вірусів є використання *апаратурно-програмних антивірусних засобів*. В даний час для захисту ПЕОМ використовуються спеціальні контролери і їх програмне забезпечення. Контролер встановлюється в роз'єм розширення і має доступ до загальної шини. Це дозволяє йому контролювати всі звернення до дискової системи. У програмному забезпеченні контролера запам'ятовуються області на дисках, зміна яких в звичних режимах роботи не допускається. Таким чином, можна встановити захист на зміну головного завантажувального запису, завантажувальних секторів, файлів конфігурації, виконуваних файлів й ін.

При виконанні заборонених дій будь-якою програмою контролер видає відповідне повідомлення користувачу і блокує роботу ПЕОМ.

Апаратурно-програмні антивірусні засоби володіють рядом переваг перед програмними:

- постійно працюють;
- знаходять всі віруси, незалежно від механізму їх дії;
- блокують недозволені дії, що є результатом роботи вірусу або некваліфікованого користувача.

Недолік у цих засобів один – залежність від апаратурних засобів ПЕОМ. Зміна останніх веде до необхідності заміни контролера.

Методи видалення наслідків зараження вірусами

У процесі видалення наслідків зараження вірусами здійснюється видалення вірусів, а також відновлення файлів і областей пам'яті, в яких знаходився вірус. Існує два методи видалення наслідків дії вірусів антивірусними програмами.

Перший метод припускає відновлення системи після дії відомих вірусів. Розробник програми-фага, що видаляє вірус, повинен знати структуру вірусу і його характеристики розміщення в середовищі існування.

Другий метод дозволяє відновлювати файли і завантажувальні сектори, заражені невідомими вірусами. Для відновлення файлів програма відновлення повинна завчасно створити і зберігати інформацію про файли, одержану в умовах відсутності вірусів. Маючи інформацію про незаражений файл і використовуючи відомості про загальні принципи роботи вірусів, здійснюється відновлення файлів. Якщо вірус піддав файл необоротним змінам, то відновлення можливе тільки з використанням резервної копії або з дистрибутива. При їх відсутності існує тільки один вихід – знищити файл і відновити його самостійно.

Якщо антивірусна програма не може відновити головний завантажувальний запис або завантажувальні сектори, то можна спробувати це зробити самому. У разі невдачі слід відформатувати диск і встановити ОС.

Профілактика зараження вірусами комп'ютерних систем

Щоб забезпечити ЕОМ від дії вірусів, користувач, перш за все, повинен мати уявлення про механізм дії вірусів, щоб адекватно оцінювати

можливість і наслідки зараження ІКСМ. Головною ж умовою безпечної роботи в ІКСМ є дотримання ряду правил, які випробувані на практиці і показали свою високу ефективність.

Правило перше. Використовування програмних продуктів, одержаних законним офіційним шляхом, тобто – програмні продукти повинні бути ліцензовані.

Ймовірність наявності вірусу в піратській копії у багато разів вища, ніж в офіційно одержаному програмному забезпеченні.

Правило друге. Дублювання інформації. Перш за все, необхідно зберігати автономні носії програмного забезпечення. Бажано обирати носії, на яких відсутня функція повторного запису. Слід особливо поклопотатися про збереження робочої інформації. Переважно регулярно створювати копії робочих файлів на змінних машинних носіях інформації із захистом від запису. Якщо створюється копія на внутрішньому носії, то бажано її створювати на інших ЗЗП або ЕОМ. Копіюється або весь файл, або зміни, що тільки вносяться. Останній варіант застосовується, наприклад, при роботі з базами даних.

Правило третє. Регулярно використовувати антивірусні засоби. Перед початком роботи доцільно запускати програми-сканери і програми-ревізори. Антивірусні засоби повинні регулярно оновлятися.

Правило четверте. Особливу обережність слід проявляти при використуванні нових зовнішніх носіїв інформації та файлів. Нові диски та флешки обов'язково повинні бути перевірені на відсутність завантажувальних і файлових вірусів, а одержані файли – на наявність файлових вірусів. Перевірка здійснюється програмами-сканерами і програмами, що здійснюють евристичний аналіз. При першому виконанні робочого файлу потрібно користуватись резидентними сторожами. При роботі з одержаними документами і таблицями доцільно заборонити виконання макрокоманд засобами, вбудованими в текстових і табличних редакторів (MS Word, MS Excel), до завершення повної перевірки цих файлів.

Правило п'яте. При роботі в розподілених системах або в системах колективного користування доцільно нові зовнішні носії інформації і файли, що вводяться в систему, перевіряти на спеціально виділених для цієї мети ЕОМ. Доцільно для цього використовувати автоматизоване робоче місце адміністратора системи або особи, що відповідає за безпеку інформації. Тільки після всебічної антивірусної перевірки дисків і файлів вони можуть передаватися користувачам системи.

Правило шосте. Якщо не передбачається здійснювати запис інформації на носій, то необхідно обирати диски CD/R, DVD/R (тобто диски де відсутня повторна можливість запису).

Постійне проходження всім приведеним рекомендаціям дозволяє значно зменшити ймовірність зараження програмними вірусами і захищає користувача від безповоротних втрат інформації.

У особливо відповідальних системах для боротьби з вірусами необхідно використовувати апаратно-програмні засоби.

Порядок дій користувача при виявленні зараження ЕОМ вірусами

Навіть при скрупульозному виконанні усіх правил профілактики можливість зараження ЕОМ комп'ютерними вірусами повністю виключити не можна. Якщо вірус все ж таки потрапив в ІКСМ, то наслідки його перебування можна звести до мінімуму, дотримуючись певної послідовності дій.

Про наявність вірусу в ІКС користувач може судити за такими ознаками:

- поява повідомлень антивірусних засобів про зараження або про передбачуване зараження;
- явні прояви присутності вірусу, такі як повідомлення, що видаються на монітор або принтер, звукові ефекти, знищення файлів й інші аналогічні дії, що однозначно вказують на наявність вірусу в ІКСМ;
- неявні прояви зараження, які можуть бути викликані й іншими причинами, наприклад, збоями або відмовами апаратурних і програмних засобів ІКСМ.

До неявних проявів наявності вірусів в ІКСМ можна віднести «зависання» системи, уповільнення виконання певних дій, порушення адресації, збої пристроїв і т. п.

Одержавши інформацію про передбачуване зараження, користувач повинен переконатися в цьому. Вирішити таку задачу можна за допомогою всього комплексу антивірусних засобів. Переконавшись у тому, що зараження відбулося, користувачу слід виконати таку послідовність кроків:

Крок 1. Вимкнути ЕОМ для знищення резидентних вірусів.

Крок 2. Здійснити завантаження еталонної операційної системи із змінного носія інформації, в якій відсутні віруси.

Крок 3. Зберегти на змінних носіях інформації важливі для вас файли, які не мають резервних копій.

Крок 4. Використовувати антивірусні засоби для видалення вірусів і відновлення файлів, областей пам'яті. Якщо працездатність ЕОМ відновлена, то здійснюється перехід до кроку 8, якщо не відновлена – до кроку 5.

Крок 5. Здійснити повне стирання і розмітку (форматування) зовнішніх пристроїв пам'яті.

Крок 6. Відновити ОС, інші програмні системи і файли з резервних копій, створених до зараження.

Крок 7. Ретельно перевірити файли, збережені після виявлення зараження, і, при необхідності, видалити віруси і відновити файли.

Крок 8. Завершити відновлення інформації всебічною перевіркою ЕОМ за допомогою всіх антивірусних засобів, що є у розпорядженні користувача.

При виконанні рекомендацій по профілактиці зараження комп'ютерними вірусами, а також при умілих і своєчасних діях у разі

зараження вірусами, збиток інформаційним ресурсам ІКСМ може бути зведений до мінімуму.

5.5 Захист програмного забезпечення від реасемблерів та налагоджувачів

Організовуючи захист ПЗ, важливо включити механізми, що перешкоджають впровадженню руйнуючого алгоритму, які можна здійснити в двох режимах: статичному і динамічному. У статичному режимі бінарний код програми перетворюється в початковий текст (дизасемблюється), який вивчається з метою подолання механізму захисту. У динамічному режимі здійснюється трасування програми, тобто виконання її на комп'ютері за допомогою засобів, що дозволяють динамічно здійснювати доступ до регістрів і ділянок пам'яті та зупиняти програму в контрольних точках (КТ) та ін.

Сучасний ринок ПЗ пропонує засоби, що дозволяють не тільки перетворити бінарний модуль в мнемочод асемблера (з коментарями), але й застосовувати широкий набір функцій динамічних методів дослідження, які реалізуються за допомогою налагоджувачів.

Вбудовуючи в ПЗ механізми захисту, важливо передбачити, щоб вони протистояли одночасно дизасемблюванню і налагоджувачам, оскільки захищена тільки від налагоджувача програма може бути легко дизасембльована, і, навпаки, захищена тільки від дизасемблювання програма може легко трасуватися.

Для дослідження внутрішньої поведінки програм застосовують спеціальні програмні засоби (*debug tools*), що мають можливість трасування (введення в програму точок зупину, за якими переривається її виконання, наприклад, з метою оцінки результатів), перевірки і модифікацій значень змінних. Базовими для налагоджувачів є методи покомандного виконання і КТ.

Для встановлення режиму покомандного виконання використовується спеціальний засіб, що міститься в сучасних універсальних процесорах. Так, в регістрі стану процесора є біт (ознака TF) по командного виконання. Якщо TF=1, то процесор після кожного виконання команди генерує переривання INT 1h (одиначний крок), за яким підключається відповідна програма обробки. На початку процесу її виконання TF скидається, і процесор переходить в нормальний режим, а після її завершення значення ознаки відновлюється, і процесор повертається в покроковий режим. Метод КТ базується на тому, що в тіло програми динамічно, замість вказаної команди, вставляється, наприклад, переривання INT 3h (точка зупину), за яким нормальне її виконання припиняється і виконується необхідна спеціальна обробка. Далі, після виконання процедури КТ, код, заміщений перериванням INT 3h, відновлюється і виконання досліджуваної програми продовжується. Крім цього, в процесорах передбачені спеціальні регістри, що дозволяють одночасно встановити до чотирьох КТ, через які можна контролювати, наприклад, звернення до

пам'яті, зміну її ділень, вибірку команди за певною адресою та ін. У таких процесорах генерується переривання під час звернення до попередньо заданого порту введення-виведення або зміни чи читання регістра у разі реалізації задачі в режимі віртуального процесора.

Усі зазначені чинники потрібно враховувати, будуючи розглянуті нижче засоби захисту.

Захист програм від статичних методів дослідження

Для істотного ускладнення аналізу програм статичними методами дослідження використовують багато різних захисних механізмів, комплексне застосування яких надає серйозну протидію хакерам і зводить результати їх зусиль щодо вивчення логіки програми практично нанівець. Розглянемо найбільш відомі засоби протидії дизасемблерам.

Неявні переходи. Передаючи управління певному кодовому модулю, потрібно змінювати вміст регістра IP, що автоматично здійснюється за виконанням команди передачі управління JMP. Якщо, наприклад, в процесі виконання програми із стека в IP за допомогою команди RET занести новий код адреси, то здійсниться неявний перехід до нової ділянки коду і, таким чином, буде прихована точка передачі управління.

Конкатенація з навантажувальним кодом. У випадку, коли програма дуже маленька, потрібно навантажувати її тіло додатковими модулями, що містять багато команд, які не мають відношення до алгоритму роботи. У вказаних модулях рекомендується, наприклад, застосувати переривання 21h і 13h, які часто використовуються в побудові систем захисту. Такі вклучення, як правило, ускладнюють пошук захисних механізмів.

Приєднання універсального захисного модуля до бінарного коду програм. Дуже зручно до готової незахищеної програми приєднати універсальний захисний модуль. Якщо таке захоплення перетворює, наприклад, заголовок бінарного файлу, то це, як правило, істотно ускладнює аналіз коду, отриманого шляхом стандартного дизасемблювання захищеного модуля.

Криптографічне перетворення коду. Один з найбільш стійких засобів захисту засновується на трансформації програмного коду шляхом складних (наприклад, на основі DES) криптографічних перетворень в процесі роботи виконуючого модуля. Іншими словами, та частина програми, яку потрібно засекретити, міститься у файлі в зашифрованому вигляді і після дизасемблювання буде сформований безглуздий код. У процесі роботи програма безпосередньо в пам'яті комп'ютера поблоково розшифровує свою секретну частину перед її виконанням.

Захист програм від динамічних методів дослідження. Для захисту ПЗ від динамічних методів дослідження використовують прийоми, направлені, в основному, на виявлення засобів стеження за захищеною програмою і, у разі їх виявлення, реалізують протидію.

Дозвіл і заборона переривань. Використання в захищеній програмі команд, що періодично змінюють значення ознаки TF, ускладнює

налагоджувачам встановлювати КТ, які допомагають дослідженню виконуючого модуля.

Контроль програми в пам'яті. Після завантаження програми в пам'ять, хакер з метою її вивчення за допомогою налагоджувача встановлює КТ, а також може робити інші зміни в кодовому модулі. Виявити модифікації можна шляхом включення (в певних точках програми) модулів підрахунку контрольної суми коду, що знаходиться в пам'яті. У разі, якщо підрахована сума не збігається з відомим значенням в програмі вироблюються протидії налагоджувачу.

Контроль часу виконання. Виявити захоплення програми налагоджувачем і переривання її роботи в процесі дослідження можна шляхом контролю часу виконання окремих бінарних модулів. Не збіг контрольного часу виконання програми з поточним у бінарному коді реалізується перехід до захисних дій.

Відновлення векторів переривань. Багато програм, особливо резидентних, призначених для дослідження захищених програмних засобів, після свого запуску перевизначають вектори переривань, які у більшості випадків пов'язані з дисковими операціями і функціями DOS. Для виявлення стеження і забезпечення власного захисту у ПЗ в разі необхідності повинні бути передбачені процедури відновлення адрес у векторах переривань, очищення пам'яті, а також перевірки автентичності початкових команд обробників вказаних вище переривань.

Перевизначення векторів переривань. Досліджуючи захищену програму, хакер намагається виявити захисні механізми, що часто будуються на перериваннях за дисковими операціями і зверненнях до функцій DOS. З метою маскування вказаних звертань доцільно перевизначити вільні номери переривань, наприклад, 40h і 50h визначити як 13h і 21h, тобто вміст пам'яті за адресами 4Ch-4Fh і 84h-87h скопіювати відповідно в 100h-103h і 140h-143h. Далі під час звернення в програмі до переривань 40h або 50h насправді будуть оброблятися 13h або 21h. Також можна застосовувати переривання, які мало використовуються, наприклад, 5h.

Перевірка вільної пам'яті. Якщо кодовий модуль захоплений налагоджувачем або контролюється іншими програмними засобами, то обсяг вільної пам'яті в поточному режимі буде суттєво відрізнятися від обсягу у разі автономної роботи захищеної програми. Дану залежність можна використати як ознаку для генерації протидії в разі не збіг очікуваного діапазону значень вільної пам'яті після її перевірки.

Перевірка доступних областей пам'яті. Спільна робота програми з налагоджувачем або іншими засобами дослідження відрізняє вміст різних програмно доступних областей пам'яті, наприклад, відео-пам'яті. Тоді на певних етапах автономного виконання захищеної програми можна попередньо визначити контрольну суму вказаної відео-пам'яті і порівняти її, наприклад, з поточним значенням (у разі спільного виконання з іншими

програмами). Відмінність величин у цьому випадку буде служити сигналом для передачі управління до протидіючого механізму.

Блокування консолі. З метою ускладнення аналізу захисного механізму в період його роботи рекомендується здійснювати блокування роботи клавіатури і відеотерміналу. Для цієї мети застосовують комплекс різноманітних заходів. До них відносяться: заборона відеосигналу і роботи клавіатури шляхом скидання третього і сьомого бітів відповідно в портах 3B8h, 3D8h і 61h, використання спеціальних ресурсів DOS, наприклад, підфункції 1 функції 44h переривання 21h, перевизначення векторів переривань, що використовуються для роботи з консоллю та ін.

Використання специфіки функціонування налагоджувальних засобів комп'ютерних систем. Більшість налагоджувальних засобів мають свої особливості, які виявляються в процесі функціонування та якими можна скористатися, будуючи захисні механізми. Наприклад, відомо, що в префікс програмного сегмента (Program Segment Prefix – PSP) активної транзитної програми за зміщенням 2Eh MS DOS розміщує покажчик стека в разі звернення до системних функцій, оскільки внутрішній стек DOS використовується під час системних викликів. Якщо програма виконується під налагоджувачем, то першим обробку 21h переривання виконає саме він, а його покажчик буде розміщений в даній чотирибайтовій області активного PSP. Перевіривши її, можна виявити роботу налагоджувача.

Використання специфіки функціонування апаратних засобів комп'ютерних систем. Різна апаратура має свої функціональні особливості, які можна використовувати, будуючи системи захисту. Особливої уваги завжди заслуговують процесори. Вони мають механізми буферизації оперативної пам'яті, що забезпечують тимчасове зберігання підлягаючих виконанню команд. Пристрій обробки мікропроцесора, виконуючи команди, витягує їх із буферу, не вимагаючи доступу до каналу. Пристрій сполучення каналу мікропроцесора стежить за станом буферів, поповнюючи їх, коли інші системні елементи не займають пам'ять. Виконуючи команди передачі управління буфери можуть скидатися і після завершення переходу в місце передачі управління починаються заповнюватися знову. У покроковому режимі обробки програми для виконання чергової команди потрібно кожний раз здійснювати звернення до пам'яті. Якщо, наприклад, попередній код перетворює наступну команду на команду безумовного переходу, то в нормальному режимі виконання буде модифікований тільки код в ОП, а виконається той, який в буфері. Тоді у разі покрокового виконання буде виконаний безумовний перехід.

Мікропроцесори мають свої особливості функціонування, які часто пов'язані з апаратними помилками. Один з процесорів Intel має одну особливість, що виявляється в покроковому режимі роботи. Вона полягає в тому, що після команд пересилки сегментних реєстрів, наприклад, MOV ax, dx; POP ds; POP ss та ін. втрачається одне трасоване переривання, і процесор пропускає одну команду. У процесорі також втрачається

трасування в разі сегментних переривань і використання стекового системного реєстра. З урахуванням цієї особливості здійснюється виявлення налагоджувача.

Слід зазначити, що вдале використання всіх можливостей сучасних налагоджувальних засобів дозволяє ефективно дослідити і «зламати» захисні механізми в ПЗ, але це, у більшості випадків, залежить від професіоналізму зловмисника.

5.6 Системний підхід до захисту ПЗ

Системний підхід захисту ПЗ – це технологія організації і реалізації процесу створення, впровадження та супроводу підсистеми захисту ПЗ з умов її здійснення на всіх етапах життєвого циклу ПЗ й ІКСМ з урахуванням комплексного використання всіх наявних засобів і методів захисту.

При цьому усі засоби, методи й заходи повинні використовуватися для захисту ПЗ найбільш раціональним чином та поєднуватися в єдиний цілісний механізм – систему, що повинна забезпечувати так званий – *багаторівневий захист*. Зазначений процес захисту реалізується не тільки від зловмисників, але й від некомпетентних або недостатньо підготовлених користувачів і персоналу ІКСМ [59].

Комплексна система захисту ПЗ повинна включати чотири захисних пояси (рис. 5.8):

- зовнішній, що охоплює всю територію, на якій розташована вся інфраструктура ІКСМ;
- рівень споруд або приміщень, у яких розташоване устаткування ІКСМ, а також лінії передачі інформації;
- рівень компонентів системи (технічних засобів, зовнішніх носіїв, на яких зберігається ПЗ);
- рівень технологічних процесів обробки даних (внутрішня обробка, передача даних по внутрішніх локальних або корпоративних лініях зв'язку).

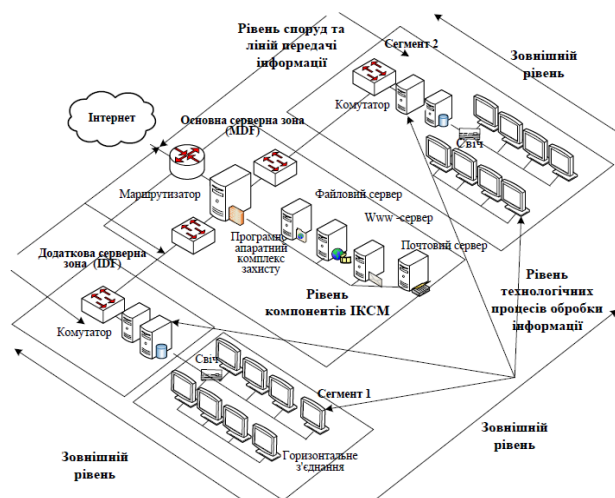


Рис. 5.8. Комплексна система захисту ПЗ

Перші три рівні забезпечують захист компонентів ІКСМ, включаючи ПЗ, шляхом фізичної перешкоди доступу (використання систем огороження, сигналізації, контрольно-пропускних пунктів й ін.). Слід зазначити, що не завжди вдається належним чином забезпечити фізичний захист ліній передачі інформації. Для підвищення безпеки інформаційного обміну в цьому випадку необхідно передбачити альтернативні або резервні канали передачі даних.

Останній рівень забезпечує захист ПЗ на основі *логічної перешкоди доступу* при умові, що фізичний доступ до компонентів ІКСМ вже реалізований.

Оптимальним варіантом побудови комплексної системи захисту є її орієнтація на виконання всіх перерахованих вимог для протидії кожній можливій загрозі. Таким чином, система захисту повинна мати *багаторівневу структуру* з умови того, що зловмиснику для порушення встановленої політики безпеки ПЗ, «необхідно буде пройти» всі визначені рівні захисту.

Концептуальними рівнями захисту ПЗ, що відповідають перерахованим вище вимогам, є:

- *зовнішній рівень* – рівень перешкоди прояву загроз;
- *граничний рівень* – рівень захисту ПЗ від впливів реалізованих загроз;
- *внутрішній рівень* – рівень усунення наслідків впливів реалізованих загроз.

Таким чином, система захисту ПЗ для підтримки встановленої політики безпеки, повинна забезпечувати виконання таких функцій:

1. *На зовнішньому рівні:*

- виявлення умов, що породжують прояв загроз;
- ліквідація умов, що породжують прояв загроз;
- створення умов, що перешкоджають прояву загроз;

2. *На граничному рівні:*

- виявлення проявів загроз;
- перешкода доступу реалізованих загроз до ресурсів ІКСМ;
- попередження впливів реалізованих загроз на ПЗ;

3. *На внутрішньому рівні:*

- виявлення впливів на ПЗ;
- локалізація впливів на ПЗ;
- ліквідація наслідків впливів на ПЗ.

Тільки всі вище перераховані функції системи захисту ПЗ для кожної з можливих загроз за умови їх точного й своєчасного виконання, забезпечать ефективний захист ПЗ та інформації, яка обробляється та зберігається в ІКСМ.

Вся безліч функцій системи комплексного захисту повинна бути достатньою для забезпечення необхідної безпеки ПЗ у будь-який момент часу. Безліч активних функцій, визначається поточними умовами зберігання й обробки інформації у ІКСМ.

Функція захисту виконується відповідно до використовуваного методу захисту за допомогою спеціально створених для її виконання засобів.

У загальному випадку під методом (засобом) захисту ПЗ розуміється опис процесу реалізації якої-небудь функції захисту. Використовуючи схожість понять функція й завдання, можна також сформулювати, що під методом захисту розуміється опис способу вирішення якого-небудь завдання захисту. Методи захисту ПЗ можна класифікувати на: неформальні й формальні.

Неформальний метод – описує процес реалізації якої-небудь функції, що не може бути виражена в узагальнених алгоритмах. При цьому під алгоритмом ми розуміємо точний опис, що визначає послідовність дій, необхідну для одержання встановленого результату захисту.

Формальний метод – задає узагальнені алгоритми реалізації якої-небудь функції завдання для виконання встановленої задачі захисту.

Окремі методи можуть бути комбінованими або напівформальними, коли одна частина відповідає формальній ознаці, а інша – неформальній.

Для використання методів захисту ПЗ на практиці створюються засоби захисту, що в свою чергу також розділяються на формальні й неформальні.

Систематизація методів захисту ПЗ

Систематизація методів захисту дозволяє виділити узагальнені (концептуальні) й більш деталізовані функції захисту ПЗ ІКСМ (рис. 5.9, 5.10, 5.11). Узагальнений та деталізований підходи до побудови підсистеми захисту ПЗ ефективніше реалізують політику безпеки ІКСМ з умов підвищення рівня захисту [59].

Слід зазначити, що на представлених нижче рисунках, відображені як функції так і методи захисту ПЗ, тому що: будь-яка функція захисту реалізується за допомогою відповідних методів, які можна визначити, як – методи реалізації даної функції.

Методи захисту ресурсів ІКСМ й ПЗ у сукупності з методами їх несанкціонованого використання можна назвати *методами захисту від несанкціонованих дій користувачів і програмних продуктів*.

Методи захисту від несанкціонованого доступу до ресурсів ІКСМ можна поділити на: методи захисту від дій несанкціонованих користувачів та несанкціонованих програм (комп'ютерних вірусів).

Методи захисту від несанкціонованого використання ресурсів ІКСМ можна поділити на: методи захисту програмних й інформаційних ресурсів.

Класифікуємо функції і методи системи захисту залежно від поставленої цілі, щодо політики захисту ПЗ ІКСМ.

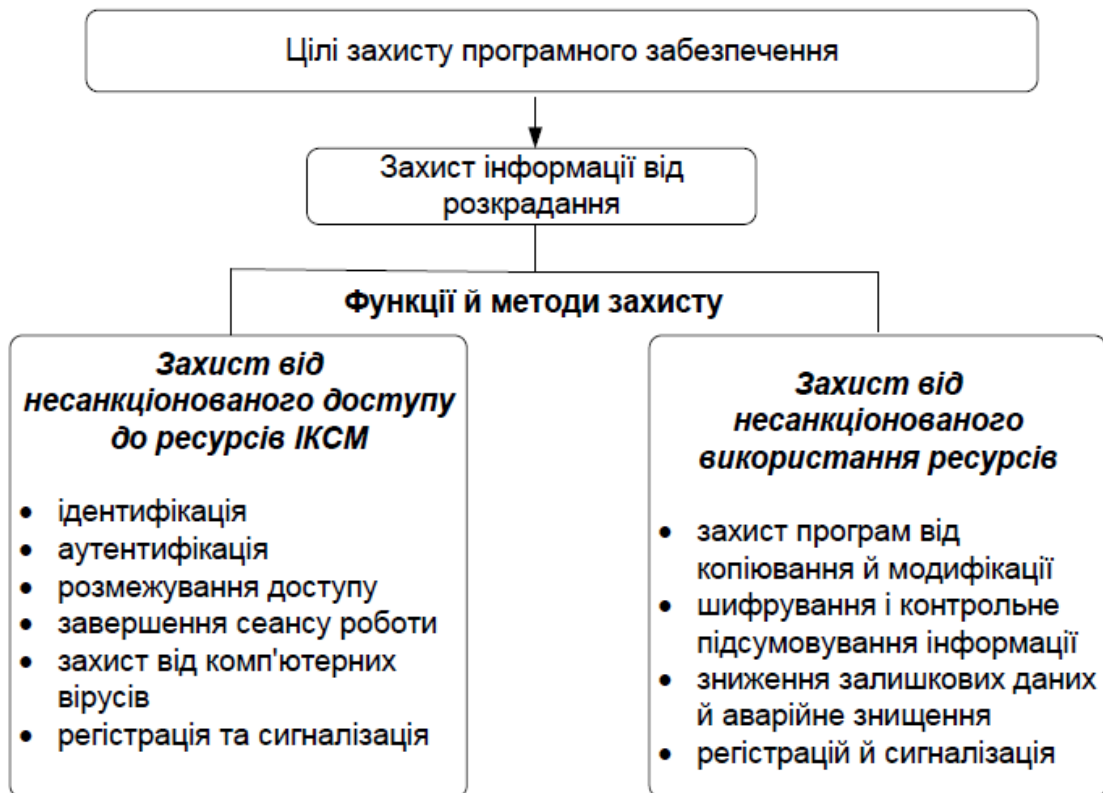


Рис. 5.9. Функції і методи системи захисту ПЗ ІКСМ від розкрадання

При захисті інформаційних ресурсів та ПЗ ІКСМ від несанкціонованих дій, повинна здійснюватися реєстрація всіх спроб доступу до ІКСМ, а також звертань до її інформаційних ресурсів та послуг системи. Крім того, необхідно реалізувати процедуру «сигналізації» (повідомлення служби безпеки) про всі спроби несанкціонованого входу у ІКСМ і доступу до ресурсів системи.

В сучасних ІКСМ достатньо широко впроваджуються «реєстрація» й «сигналізація», як методи захисту ПЗ від некоректного використання, а також у процедурах внесення інформаційної й функціональної надмірності з умов підвищення рівня захищеності ІКСМ. Однак, у цьому випадку реєстрація й сигналізація носять інший характер і застосовуються для підтримки фізичної й логічної цілісності збережених й оброблюваних даних, а також для відновлення й самовідновлення працездатності ІКСМ після виникнення збоїв і відмов програмно-апаратних засобів.

Реєстрації при цьому підлягають всі дії користувачів і програм, що були впровадженні (або спроба впровадження) з умов модифікації даних та ПЗ.

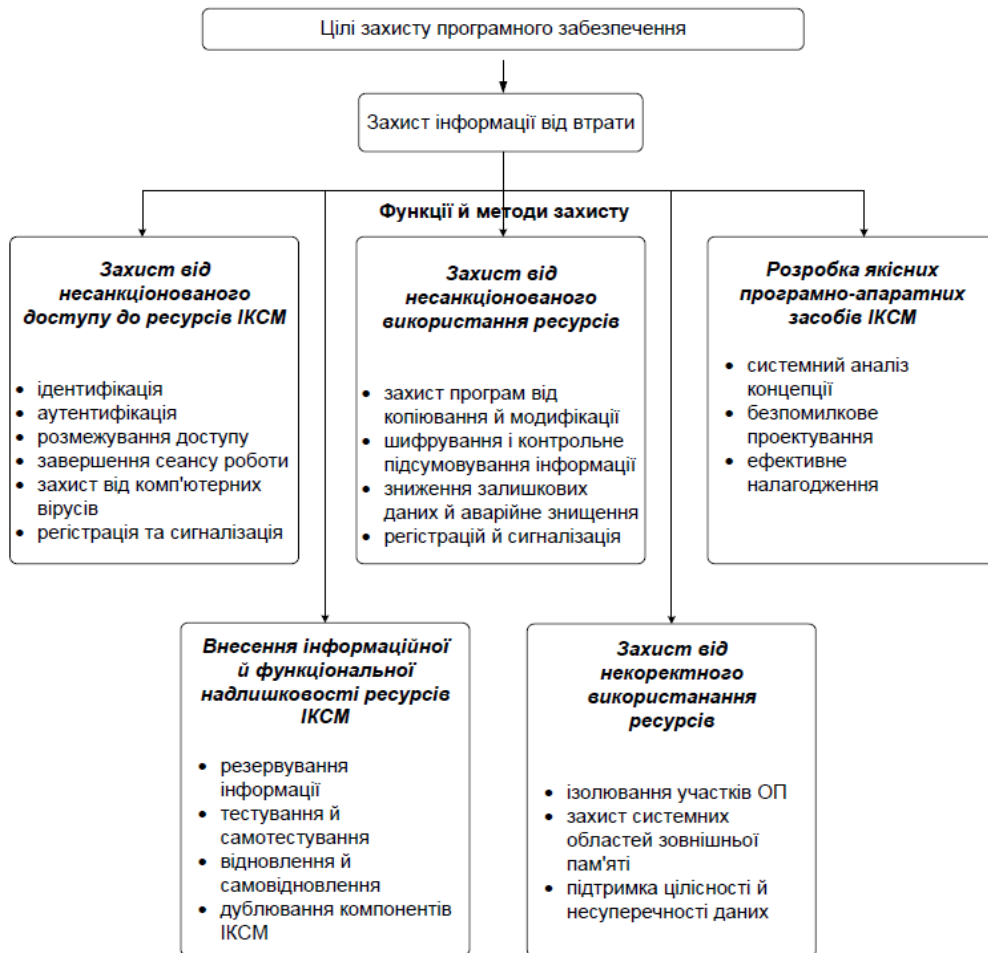


Рис. 5.10. Функції і методи системи захисту ПЗ ІКСМ від втрати

Сигналізація у даному випадку, повинна використовуватися для повідомлення відповідних компонентів системи захисту й адміністрації про випадки: некоректного використання ресурсів, а також при виникненні збоїв і відмов програмно-апаратних засобів та їх забезпечення.

Захист від несанкціонованих дій користувачів і програм повинен реалізовуватися, як на рівні операційної системи, так і на рівні загальносистемних і прикладних програм, наприклад систем управління базами даних або систем управління послугами.

Методи ізолювання ділянок оперативної пам'яті й захист системних областей зовнішньої пам'яті, що відповідають методу захисту від некоректного використання ресурсів ІКСМ, повинні бути реалізовані також на рівні операційних систем.

Методи підтримки цілісності й несуперечності даних по захисту від некоректного використання ресурсів ІКСМ, а також методи внесення інформаційної й функціональної надмірності ресурсів, реалізуються на всіх рівнях захисту програмного забезпечення. Особливо важливу роль для забезпечення безпеки обробки інформації відіграє ефективність реалізації даних методів на рівні операційних систем і систем управління базами даних.



Рис. 5.11. Функції і методи системи захисту ПЗ ІКСМ від збоїв і відмов

Ефективна система захисту інформаційних ресурсів та ПЗ є інтеграційний комплекс, який засновано на всезагальному обліку й комплексному використанні та реалізації всіх представлених на рис. 5.9, 5.10, 5.11 функцій і методів захисту ПЗ ІКСМ. Ігнорування кожної з визначених функцій захисту приводить до безперешкодної реалізації загрози інформаційним ресурсам та ПЗ, а отже надає можливість порушення встановленої політики безпеки ІКСМ.

Запитання для самоконтролю:

1. Мета та задачі захисту ПЗ.
2. Загрози інформаційним ресурсам та ПЗ. Класифікація.
3. Наведіть класифікацію комп'ютерних вірусів.
4. Назвіть ознаки класифікації комп'ютерних вірусів.
5. Поясніть принцип дії стелс-вірусів і поліморфних вірусів.
6. Приведіть структуру файлового вірусу і поясніть алгоритм його роботи.
7. У чому полягають особливості алгоритмів функціонування макровірусів і завантажувальних вірусів?
8. Дайте характеристику методів виявлення вірусів.
9. Назвіть методи видалення наслідків зараження вірусами.

10. Перерахуйте профілактичні заходи запобігання зараженню вірусами ІКСМ.
11. Порядок дій користувача при виявленні зараження ЕОМ вірусами.
12. Дайте коротку характеристику основних засобів захисту програмного забезпечення.
13. Методи та засоби захисту програмного забезпечення.
14. Класифікація методів захисту програмного забезпечення.
15. Класифікація засобів захисту програмного забезпечення.
16. Приведіть приклади програмних кодів вірусів.
17. Наведіть приклади програмних кодів виявлення вірусів.
18. Поясніть сутність комплексного підходу до побудови системи захисту ПЗ.
19. Що таке «системний підхід до захисту ПЗ»?
20. Багаторівневі системи захисту інформаційних ресурсів та ПЗ.

Розділ 6. ЗАГАЛЬНІ ПОЛОЖЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ МІЖНАРОДНИХ СТАНДАРТІВ

Сучасний етап розвитку інформаційної безпеки потребує комплексного підходу до розробки та впровадження методів і засобів захисту інформаційних ресурсів підприємств, як на технічному, так і на організаційному рівні, тобто реалізації інтегрованого процесу – **управління інформаційною безпекою** [*information security management*]. Зазначений процес забезпечує механізми, які дозволяють реалізувати політику інформаційної безпеки організації чи об'єкта інформаційної діяльності в цілому. Інформаційна безпека – реалізація процесу захисту інформації від широкого діапазону загроз, що здійснюється з метою забезпечення безперервності бізнесу підприємства або відокремлених робочих процесів, доведення до мінімуму збитку бізнесу компаній і доведення до максимуму повернення інвестицій і виконавських функцій організації. Гостро стає необхідність розгляду інформаційної безпеки, як складової бізнес-процесів підприємств з різними формами власності, а також адоптації визначень, норм, вимог, тощо до цих процесів.

Інформація – це майно (або активи), що, подібно іншим важливим діловим активам, має цінність для організації й повинна бути захищена відповідним чином [12].

На об'єктах інформаційної діяльності або безпосередньо в інформаційно-комунікаційних системах інформація може існувати в різних формах та надана від різних джерел. Вона може бути надрукована або написана на папері, збережена в електронному вигляді, передана поштою або з використанням електронних засобів, показана на плівці або озвучена в бесіді. Безвідносно, звідки береться інформація, або за допомогою яких засобів вона розподіляється в інформаційних мережах або зберігається й обробляється, вона повинна бути завжди відповідно захищена.

Інформаційна безпека досягається реалізацією відповідної безлічі заходів щодо управління процесами бізнесу, які можуть бути представлені визначеними політиками, методами, процедурами, організаційними структурами, устаткуванням й функціями програмного забезпечення, тощо. Ці заходи управління безпекою необхідно встановлювати таким чином, щоб забезпечити впевненість у тому, що встановлена мета і цілі безпеки організації досягнуті та контролюються.

Інформація й підтримуючі її процеси, а також автоматизовані системи обробки, збереження й передачі інформації – важливі ділові активи. Конфіденційність, цілісність і доступність інформації можуть бути істотними активами для підтримки конкурентоспроможності підприємств, грошового обігу, прибутковості, юридичній гнучкості й комерційного іміджу організації.

На даний час організації, їх інформаційні системи та мережі зіштовхуються з широким діапазоном джерел загроз безпеці інформації, включаючи несанкціоноване використання й втручання до інформаційних ресурсів, комп'ютерне шахрайство, шпигунство, саботаж, вандалізм,

пожежі тощо. Джерела ушкодження, такі як комп'ютерні віруси, злом системи доступу до ресурсів й напади на систему, типу відмови в обслуговуванні тощо, стають більш звичайними, амбіційними й усе більше й більше складними з технічної точки зору.

Сучасна залежність організацій від інформаційних систем та їх послуг означає, що компанії усе більше уразливі до загроз інформаційної безпеки. Взаємодія суспільних і приватних мереж, а також спільне використання інформаційних ресурсів збільшує труднощі управління доступом та забезпечення ділових процесів й гарантій послуг. Сучасна тенденція до розподілених обчислень послабляє ефективність центрального управління, здійснюваного фахівцем або власником ресурсів.

Багато інформаційних систем спочатку не проектувалися з урахуванням впровадження політики безпеки. Заходи управління інформаційною безпекою значно дешевші й більш ефективні, якщо вони включені в специфікацію вимог на стадії проектування інформаційної системи. Безпека, що може бути досягнута через технічні засоби, є обмеженою і її варто підтримувати відповідними процесами управління та жорстко визначеними процедурами. Визначення необхідних засобів управління вимагає ретельного планування й уваги до деталізації бізнес-процесів.

Важливо й те, що організація повинна визначити свої вимоги до систем безпеки ще на початковому етапі – розробки таких систем.

Існують три основних джерела визначення вимог до інформаційної безпеки (рис. 6.1).



Рис.6.1. Джерела вимог до систем безпеки

Першим джерелом є оцінка ризиків організації. Через оцінки ризиків ідентифікуються загрози активам, оцінюється їхня вразливість й імовірність виникнення загроз, а також можливий руйнівний вплив при реалізації несанкціонованих дій. Другим джерелом є юридичні, законодавчі, регулюючі й договірні вимоги, які оцінювалися для того, щоб організація, її торговельні партнери, підрядники й постачальники послуг задовольняли один одному та чинному законодавству. Третім джерелом є специфічна кількість принципів, цілей і вимог до обробки інформації, які має або розробила організація, для підтримки своїх дій та послуг.

6.1. Безпека інформаційних ресурсів у ІКСМ

Інформація, яка підлягає технічному захисту в процесі функціонування ІКСМ, може зазнавати впливів цілого ряду загроз, внаслідок чого виникають порушення її цілісності, доступності до неї з боку авторизованих користувачів (див. Закон України «Про захист інформації у автоматизованих системах», «Положення про технічний захист інформації в Україні», Рекомендації Ради Європи №№ R(89)2, R(95)4 та ін.). Спроможність системи технічного захисту інформації (ТЗІ) протистояти впливам загроз визначає рівень захищеності інформаційних ресурсів системи. ІКСМ, як правило, оснащуються штатними і, при необхідності, додатковими (позаштатними) засобами ТЗІ, які при їхньому спільному використанні утворюють комплекс засобів і механізмів захисту (КЗМЗ), що забезпечує потрібний рівень захищеності інформаційних ресурсів цих систем [50, 52].

Основні принципи організації ТЗІ ІКСМ полягають у наступному:
принцип легітимності захисту – ТЗІ у ІКСМ (далі – захист ІКСМ) повинен ґрунтуватися на положеннях і вимогах чинних в Україні нормативно-правових актів і нормативних документів щодо технічного захисту інформації;

- *принцип комплексності захисту* – захист ІКСМ повинен забезпечуватися комплексом взаємопов'язаних нормативних, організаційних заходів і програмно-технічних засобів;
- *принцип безперервності захисту* – захист ІКСМ повинен забезпечуватися на всіх технологічних етапах та режимах її функціонування і надання послуг, зокрема при проведенні ремонтних і регламентних робіт;
- *принцип мінімальної достатності захисту* – захист ІКСМ повинен забезпечувати необхідний рівень захищеності при мінімальних витратах ресурсів;
- *програмно-технічні засоби захисту* не повинні істотно погіршувати основні характеристики ІКСМ (пропускну спроможність, надійність, можливість зміни конфігурації ІКСМ і т. ін.);
- *оцінка ефективності засобів захисту* є невід'ємною частиною робіт з ТЗІ у ІКСМ, що здійснюється згідно з методиками, які враховують всю сукупність технічних характеристик оцінюваного об'єкта, включаючи технічні рішення і практичну реалізацію засобів захисту;
- *впровадження систем управління комплексами засобів захисту ІКСМ* повинні забезпечувати та здійснювати безперервний контроль ефективності засобів захисту, підтримку необхідного рівня захищеності інформаційних ресурсів ІКСМ.

Технічний захист інформації у ІКСМ – процес запобігання за допомогою нормативних, організаційних та інженерно-технічних методів і заходів, реалізаціям загроз для інформаційних ресурсів ІКСМ, що створюються через технічні канали, через канали спеціальних впливів та шляхом несанкціонованого доступу.

Канали спеціальних впливів на елементи ІКСМ – канали, через які впливи на технічні (апаратні, апаратно-програмні) засоби ІКСМ призводять до створення загроз інформаційним ресурсам.

Реалізація загроз інформаційним ресурсам ІКСМ, через канали спеціальних впливів, можлива на базі:

- кількісної недостатності компонентів ІКСМ;
- якісної недостатності компонентів і (або) всієї ІКСМ у цілому;
- навмисної або ненавмисної діяльності осіб, які, в свою чергу, впливають на елементи ІКСМ з використанням програмних і (або) технічних засобів;
- несправностей апаратних елементів ІКСМ;
- виходів за межі припустимих значень параметрів зовнішнього середовища функціонування ІКСМ (у тому числі, пов'язаними зі стихійними лихами, катастрофами й іншими надзвичайними подіями);
- помилок і некоректних дій суб'єктів доступу до ресурсів ІКСМ на стадії її експлуатації.

Функціональна послуга захисту (ФПЗ) – взаємопов'язана множина виконуваних ІКСМ елементарних функцій та процесів, яка дозволяє протистояти певним загрозам інформаційним ресурсам.

База захисту ІКСМ – сукупність всіх елементів системи ТЗІ (методологічних, методичних, проектних, програмних, апаратних, організаційних і т. ін.), що мають відношення до організації (створюють інфраструктуру) протидії загрозам для інформаційних ресурсів у ІКСМ.

Комплекс засобів і механізмів захисту (КЗМЗ) – взаємопов'язаний набір засобів і механізмів ТЗІ, що реалізують обрану модель й політику захисту інформаційних ресурсів у ІКСМ.

Оцінка ІКСМ за критеріями ТЗІ – комплекс спеціалізованих дослідницько-аналітичних та експериментальних робіт, що виконуються з метою визначення відповідності системи захисту інформації у ІКСМ до вимог (специфікацій) нормативних документів з ТЗІ.

Експертиза ІКСМ за критеріями ТЗІ – діяльність, метою якої є дослідження, перевірка, аналіз та оцінка науково-технічного рівня системи захисту інформації у ІКСМ, а також підготовка обґрунтованих висновків для прийняття рішення щодо рівня захищеності інформаційних ресурсів ІКСМ в описаних Заявником умовах експлуатації ІКСМ та рівня довіри до результатів оцінки.

Зміст і послідовність робіт з протидії загрозам повинні відповідати вказаним у державних стандартах ДСТУ 3396.0-96 і ДСТУ 3396.1-96 етапам створення системи захисту інформації і полягати у наступному:

- розробці технічної політики забезпечення захисту інформаційних ресурсів ІКСМ, що знаходиться в експлуатації (охоплює стадії розробки моделі загроз інформаційним ресурсам ІКСМ, розробки технічного та робочого проектів системи ТЗІ у ІКСМ);

- впровадженні, розробленої технічної політики забезпечення захисту інформаційних ресурсів ІКСМ в експлуатаційну практику (охоплює стадію реалізації технічного проекту системи ТЗІ – опції робіт);

- підтримці, впровадженої технічної політики забезпечення захисту інформаційних ресурсів ІКСМ в процесі її експлуатації (охоплює стадію оцінки ІКСМ за критеріями ТЗІ).

Технічну політику забезпечення захисту інформаційних ресурсів іноді скорочено називають **політикою безпеки (ПБ)**. Зазвичай розробка ПБ полягає у розробці та реалізації технологічного робочого проекту системи ТЗІ у ІКСМ.

На початковому етапі для вперше створюваних ІКСМ (таких, наприклад, як інформаційні мережі з розподіленим управлінням і з розподіленим опрацюванням даних або таких, як – системи комутації телефонних каналів зв'язку тощо), повинні бути розроблені вимоги до технічного завдання на проектування та впровадження ТЗІ у ІКСМ за назвою «Вимоги до ТЗІ у ІКСМ». Цей розділ включається до складу загального технічного завдання (ТЗ), що відображає вимоги з ТЗІ у ІКСМ у цілому, і оформлюється згідно з ГОСТ 34.602-89. Крім того, в інших розділах ТЗ на ІКСМ, мають бути враховані інші вимоги з ТЗІ.

Для вже введених в експлуатацію ІКСМ, але не атестованих за критеріями ТЗІ, технічні вимоги (ТВ) до системи ТЗІ у ІКСМ, розроблюються у вигляді окремого документу згідно з ГОСТ 34.602-89.

6.2. Організація технічного захисту інформації

Зазвичай, розробку *технічної політики захисту (політики безпеки, ПБ)* інформаційних ресурсів ІКСМ починають з розробки технічного завдання (ТЗ) або технічних вимог до створюваної системи захисту [97].

У процесі розробки технічного завдання на систему ТЗІ у ІКСМ системах:

- аналізуються інформаційні потоки через ІКСМ, характер і зміст розв'язуваних її користувачами задач, рівень цінності (у т.ч. ступінь конфіденційності) інформації користувачів;

- оцінюються характеристики технологічного середовища експлуатації ІКСМ, що підлягає захисту;

- створюються моделі порушників;

- виявляються дестабілізуючі чинники і загрози для інформаційних ресурсів;

- прогнозуються імовірності прояву загроз, потенційно можливі і припустимі втрати власників та користувачів (інформаційні, економічні, тощо) ІКСМ;

- будується модель загроз;

- надаються вимоги до необхідного рівня захищеності інформаційних ресурсів у ІКСМ.

На стадії розробки ТЗ на систему ТЗІ у ІКСМ (далі – ТЗ) виконуються такі види робіт, що називаються опціями:

- аналіз інформаційного середовища, створеного або створюваного на базі використання ІКСМ, що потребує захисту;
- аналіз середовища користувачів ІКСМ;
- аналіз середовища потенційних порушників;
- о- цінка основних характеристик технологічного середовища функціонування штатних засобів ІКСМ до проведення заходів захисту;
- побудова моделі загроз для інформації у ІКСМ, включаючи аналіз ризиків, що пов'язані із можливими реалізаціями загроз;
- визначення необхідного рівня захищеності інформаційних ресурсів ІКСМ;
- формування основних технічних вимог до розробки моделі захисту ІКСМ, яке здійснюється на стадії технічного проектування.

Метою робіт, що здійснюються на першому етапі розробки ТЗ, є визначення необхідного рівня довіри до коректності створюваної системи ТЗІ. Даний зміст і обсяг потрібних вихідних даних, виконуваних спеціальних досліджень і аналізів, рівень глибини (деталізації, формалізації) необхідних обґрунтувань однозначно залежать від потрібного рівня довіри до коректності системи захисту (див. нормативний документ НД ТЗІ 2.5-003-99).

Аналіз передбачуваних середовищ функціонування ІКСМ виконується на якісному рівні в загальному вигляді. На базі проведених досліджень враховуються основні характеристики об'єктів й особливості взаємовідносин суб'єктів у досліджуваних середовищах. На першому етапі розробки ТЗ визначаються:

- призначення ІКСМ, а також основні розв'язувані на її базі задачі;
- обсяги і ступінь важливості (цінності, у т.ч. конфіденційності) оброблюваної і транспортованої інформації;
- структура основних інформаційних взаємозв'язків;
- основні характеристики технологічного середовища експлуатації ІКСМ, включаючи основні умови, режими й засоби опрацювання і транспортування інформації;
- передбачувані межі зон, що потребують захисту;
- рівні інформативних випромінювань;
- основні види загроз для інформації і технічні канали реалізації цих загроз;
- основні характеристики організаційних структур потенційних порушників.

Вихідними даними для робіт, що виконуються в процесі розробки ТЗ, є:

- розділ ТЗ: «Вимоги до функцій (задач), що виконуються системою» і розділ ТЗ: «Вимоги до видів забезпечення» технічного завдання на вперше створювані і (або) вже створені автоматизовані системи, в складі яких використовується або планується використання ІКСМ (див. ГОСТ 34.602-89);

- організаційно-розпорядницька й експлуатаційна документація на фрагмент (ділянку) інформаційної мережі, у складі якої використовується або планується використання ІКСМ;

- документи, що містять описи організаційних структур користувачів (у т.ч., абонентів) ІКСМ;

- документи, що містять описи організаційних структур потенційних порушників;

- комплект технічної документації, включений до складу поставленої конфігурації ІКСМ;

- нормативні документи ТЗІ.

Результатом виконання першого етапу розробки ТЗ є обране значення необхідного рівня довіри до коректності створюваної системи ТЗІ.

Цілями робіт, що здійснюються на другому етапі розробки ТЗ, є:

- визначення необхідного рівня захищеності інформаційних ресурсів ІКСМ, що потребує захисту;

- розробка основних технічних вимог до забезпечення ТЗІ, з метою їх використання в процесі технологічного робочого проектування системи захисту.

Згідно з встановленими високими рівнями довірчих оцінок, при розробці та впровадженні захищеної ІКСМ, необхідно: розробити модель політики безпеки, повною мірою виконати аналіз середовищ функціонування АТС, створити моделі порушників, створити і проаналізувати модель загроз, виконати аналіз ризиків, обґрунтувати необхідний рівень захищеності інформаційних ресурсів ІКСМ для конкретних або передбачуваних умов її експлуатації.

Результатами виконання другого етапу розробки ТЗ є:

- отриманий перелік суттєвих потенційних загроз для інформаційних ресурсів ІКСМ із зазначеними гранично припустимими рівнями втрат від їх можливих реалізацій;

- основні технічні вимоги до розробки моделі захисту.

У процесі аналізу **інформаційного середовища** ІКСМ досліджується:

- характер та зміст задач користувачів і персоналу телекомунікаційної системи;

- структура інформаційних взаємозв'язків;

- об'ємно-часові характеристики і ступінь важливості (цінності, у т.ч. конфіденційності) інформації, що циркулює у ІКСМ.

У процесі аналізу **середовища користувачів** ІКСМ досліджуються:

- організаційні структури користувачів;

- склад і функціональні обов'язки користувачів;

- повноваження користувачів.

У процесі аналізу **технологічного середовища** ІКСМ досліджуються:

- основні характеристики ІКСМ;

- характеристики середовища транспортування інформації;

- умови і способи опрацювання інформації штатними засобами ІКСМ, що потребує захисту із позицій ТЗІ;

- зовнішні чинники середовища експлуатації ІКСМ (у т.ч. спеціальні дослідження) із позицій ТЗІ.

У процесі аналізу **середовища потенційних порушників** досліджуються:

- організаційні структури потенційних порушників;
- склад і можливості потенційних порушників, що реалізують загрози для інформації у ІКСМ;
- моделі потенційних порушників.

У процесі аналізу **середовища функціонування** ІКСМ виконується аналіз ризиків, пов'язаних із можливими реалізаціями загроз та побудова моделі загроз.

За результатами побудови моделі загроз визначається необхідний рівень захищеності інформаційних ресурсів ІКСМ.

На заключному етапі визначаються основні технічні вимоги до розробки моделі захисту ІКСМ.

У процесі технологічного робочого проектування системи ТЗІ у ІКСМ послідовно розроблюються:

- технічний проект – модель захисту інформаційних ресурсів ІКСМ;
- робочий проект – проект комплексу засобів і механізмів захисту.

Створення моделі захисту містить у собі проробку таких аспектів:

- визначення множини функціональних послуг захисту, які у необхідній мірі протидіють загрозам, що включені в модель загроз (для АТС див. НД ТЗІ 2.5-001-99);

- визначення мінімально необхідних рівнів стійкості механізмів захисту, що реалізують послуги захисту з обраної множини функціональних послуг;

- оптимізація проекту моделі захисту за критеріями діяльності (для АТС див. НД ТЗІ 3.7-002-99);

- забезпечення функціональної достатності моделі захисту;

- усунення функціональної надмірності моделі захисту.

З метою спрощення процесу проектування системи ТЗІ і полегшення сприйняття результатів оцінки захищеності інформації у ІКСМ за аналогією з Європейськими критеріями безпеки (ITSEC) доцільно специфікувати перелік так званих стандартних профілів захищеності інформації у ІКСМ для різних умов їхнього застосування.

Створення проектної документації повинно включати проробку таких аспектів:

- визначення множини засобів і механізмів захисту, які коректно реалізують функціональні послуги, що включені в модель захисту;

- проектування (вибір) засобів та механізмів захисту з заданою стійкістю (див. НД ТЗІ 1.1-001-99) від прямих впливів загроз;

- усунення «слабких місць» у проекті з урахуванням передбачуваних умов експлуатації комплексу;

- забезпечення функціональної достатності проекту захищеної ІКСМ;

- усунення функціональної надмірності в проекті, тощо.

Впровадження розробленої технічної політики забезпечення захисту
У процесі реалізації технологічного робочого проекту системи ТЗІ у ІКСМ виконуються такі види робіт:

- програмна і (або) апаратна реалізація розробленого комплексного засобу і методів захисту (КЗМЗ), які забезпечують наведений у ТЗ рівень захищеності інформаційних ресурсів ІКСМ;
- випробування реалізованого КЗМЗ на відповідність нормативним специфікаціям і проектній документації;
- оцінка реальних характеристик технологічного середовища функціонування захищеної ІКСМ після проведення заходів захисту;
- оцінка ефективності нейтралізації «слабких місць» у захисті;
- оцінка досягнутого рівня довіри до коректності реалізованої системи ТЗІ у ІКСМ, що потребує захисту.

Механізми захисту, які включені в проект КЗМЗ, але не реалізовані штатними засобами ІКСМ, створюються на базі програмних і (або) апаратних засобів і включаються до складу поточної конфігурації ІКСМ.

Змістом робіт є випробування реалізованого КЗМЗ на відповідність нормативним специфікаціям і проектній документації. Обсяг і глибина запроваджуваних випробувань, а також повнота охоплення випробуваннями елементів ІКСМ залежить від потрібного рівня довіри до коректності системи ТЗІ і визначається специфікаціями (для АТС наведені в НД ТЗІ 2.5-003-99).

Результат випробувань – підтвердження потрібного рівня довіри реалізованого КЗМЗ на відповідність нормативним специфікаціям (для АТС специфікаціям НД ТЗІ 2.5-003-99) і проектній документації.

Оцінка характеристик технологічного середовища функціонування захищеної ІКСМ

Метою визначення оцінки характеристик технологічного середовища є одержання впевненості в тому, що реальні характеристики технологічного середовища функціонування захищеної ІКСМ після проведення заходів захисту знаходяться в припустимих діапазонах значень, що вказані у нормативних документах. Змістом зазначених робіт є визначення, згідно із спеціалізованими методиками вимірів сигналів та полів від побічних явищ, реальних характеристик і параметрів середовища функціонування захищеної ІКСМ, а також порівняння отриманих оцінок із нормованими припустимими значеннями відповідно до розробленої програми та методики проведення вимірювань.

Обсяг виконуваних спеціальних досліджень середовища, а також повнота охоплення дослідженнями елементів середовища залежить від потрібного рівня довіри до коректності системи ТЗІ і визначається специфікаціями, що для АТС наведені в НД ТЗІ 2.5-003-99.

Результат оцінки – підтвердження впевненості в тому, що реальні характеристики технологічного середовища функціонування захищеної АТС, після проведення заходів захисту, знаходяться в припустимих діапазонах значень.

Підтримка впровадженої технічної політики забезпечення захисту в період експлуатації ІКСМ

Одне з основних завдань персоналу, що експлуатує ІКСМ, у сфері ТЗІ – оцінити достатність і ефективність побудованої моделі захисту, а також повноту, коректність і ефективність реалізації створеним комплексом КЗМЗ функціональних послуг захисту (ФПЗ) у реальних умовах функціонування ІКСМ.

У процесі виконання оціночних робіт на основі матеріалів ТЗ на систему ТЗІ аналізуються умови, в яких повинна працювати ІКСМ, оцінюється слушність вибору необхідного рівня захищеності інформаційних ресурсів, структурованого за видами і далі на основі матеріалів технологічного робочого проекту на систему ТЗІ, технічної документації на ІКСМ (особливо в частині опису комплексу засобів захисту), програми, методики і протоколів випробувань системи ТЗІ перевіряється ефективність і коректність реалізації обраної моделі захисту.

При цьому під ефективністю реалізації моделі розуміється:

- взаємна узгодженість відображених у моделі функцій та профілів (ФПЗ) захисту між собою;
- спроможність механізмів захисту, що реалізують на практиці задані у моделі ФПЗ, протистояти прямим атакам;
- неможливість практичного використання слабостей в архітектурі ІКСМ;
- неможливість практичного використання слабостей в експлуатаційному середовищі;
- неможливість небезпечного конфігурування або використання ІКСМ в умовах, коли засоби, що інформують персонал про перехід станції в небезпечний стан, відсутні або дають помилкові показання.

Під коректністю реалізації моделі захисту розуміється кон'юнкція таких подій:

- проект КЗМЗ містить реалізації усіх без винятку ФПЗ, що включені у модель захисту;
- система ТЗІ, що реально створена на ІКСМ, містить у собі усі без винятку засоби і механізми захисту, які відображені у проекті КЗМЗ;
- технічний проект системи ТЗІ містить опис ФПЗ, що відповідає нормуючим специфікаціям (для АТС – це НД ТЗІ 2.5-001-99);
- робочий проект системи ТЗІ містить опис механізмів захисту, що відповідає нормуючим специфікаціям (для АТС – це НД ТЗІ 2.5-001-99);
- механізми захисту, що включені до складу КЗМЗ, реально функціонують згідно з специфікаціями робочого проекту та нормуючими специфікаціями (за результатами випробувань системи ТЗІ, зокрема її тестування у процесі експлуатації).

Аналіз слабких місць робиться в контексті забезпечення необхідного рівня захищеності інформаційних ресурсів. Наприклад, можливо примиритися з наявністю таємних каналів передачі інформації, якщо відсутні вимоги до навмисних порушень конфіденційності. Слабкість

конкретного захисного механізму стосовно певного виду загроз може не мати значення, якщо вона компенсується іншими засобами забезпечення безпеки.

6.3.Методика і критерії оцінки захищеності інформації

У даному розділі розглянуто основні положення нормативного документу (НД): «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» (далі – Критерії, НД ТЗІ 2.5-004-99), що установлює критерії оцінки захищеності інформації, оброблюваної в комп'ютерних та телекомунікаційних системах з комутацією пакетів, від несанкціонованого доступу. Критерії є методологічною базою для визначення вимог із захисту інформації у вищеназваних системах від несанкціонованого доступу (НСД), створення захищених комп'ютерних та телекомунікаційних систем і засобів захисту від НСД, оцінки захищеності інформації у цих системах та їхньої придатності для обробки критичної інформації (тобто, інформації, що вимагає захисту) [95].

Побудова та структура критеріїв захищеності інформації

У процесі оцінки спроможності ІКСМ системи забезпечувати захист оброблюваної інформації від НСД розглядаються вимоги двох видів: вимоги до функціональності послуг безпеки, що надаються ІКСМ системою, та вимоги до забезпечення гарантій захисту.

В контексті Критеріїв ІКСМ система розглядається, як система, що надає користувачам певний набір функціональних послуг із захисту інформації (іноді ці послуги називають послугами безпеки). Функціональні послуги із захисту інформації у Критеріях, що наведені у НД ТЗІ 2.5-004-99, розбиті на чотири групи, кожна з яких описує вимоги до послуг, що забезпечують захист від загроз одного із чотирьох основних видів.

Конфіденційність. Загрози, що відносяться до несанкціонованого ознайомлення з інформацією, становлять загрози конфіденційності.

Цілісність. Загрози, що відносяться до несанкціонованої модифікації інформації, становлять загрози цілісності.

Доступність. Загрози, що відносяться до порушення можливості використання ІКСМ систем або оброблюваної інформації легальними (авторизованими, санкціонованими) користувачами, становлять загрози доступності.

Обережність. Ідентифікація, автентифікація, авторизація користувачів ресурсами ІКСМ системи, контроль за діями користувачів, забезпечення керованості ІКСМ становлять предмет послуг обережності і керованості.

Аналізуючи функціональність представлених послуг безпеки, необхідно упевнитись, що більшість послуг є незалежними одна від одної. Проте існує кілька залежних послуг, тобто послуг, реалізація яких неможлива без одночасної реалізації певних інших послуг безпеки.

Слід зазначити, що необхідною умовою користування будь-якими функціональними послугами безпеки є обов'язкова реалізація послуги

«Цілісність комплексу засобів захисту», хоча б на першому рівні її ефективності.

У Критеріях проблема боротьби із НСД розглядається, виходячи із того, що конфіденційна інформація може переміщуватись в одному з двох напрямів – від користувача цієї інформації до якогось об'єкта цієї системи або навпаки від об'єкта до користувача. Вважається, що конфіденційність забезпечується через додержання вимог політики безпеки щодо переміщення інформації від об'єкта до користувача або до процесу.

Послуга *«Довірча конфіденційність»*, дозволяє користувачеві керувати потоками інформації від захищених об'єктів, що належать його домену безпеки, до інших об'єктів ІКСМ системи. Як правило, під об'єктами, що належать домену безпеки користувача, маються на увазі об'єкти, власником яких є користувач.

Послуга *«Адміністративна конфіденційність»* дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від захищених об'єктів до користувачів.

Послуга *«Повторне використання об'єктів»* забезпечується, якщо перед наданням користувачеві або якомусь процесові прав доступу до об'єкта, до якого організується доступ, не залишається інформації, що пов'язана із попередньою роботою цього об'єкта, а також якщо скасовуються попередні права доступу до цього об'єкта.

Послуга *«Конфіденційність при обміні»* дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, під час їх експорту/імпорту через незахищене середовище.

Вважається, що цілісність, як і конфіденційність, забезпечується через додержання вимог політики безпеки щодо безпечного переміщення інформації від об'єкта до користувача або до процесу. Санкціоноване (припустиме) переміщення може здійснюватися лише авторизованим користувачем або процесом.

Розглянемо послуги, функціональність котрих спрямована на забезпечення захисту інформації від несанкціонованої модифікації (зокрема, від її знищення). Специфікації цих послуг надані в одному із розділів Критеріїв (див. НД ТЗІ 2.5-004-99).

Послуга *«Довірча цілісність»* дозволяє авторизованому користувачеві керувати потоками інформації, що надходять від інших користувачів до захищених об'єктів, які належать його домену захисту.

Послуга *«Адміністративна цілісність» (ЦА)* дозволяє адміністратору чи авторизованому користувачу керувати потоками інформації від користувачів і процесів до захищених об'єктів.

Послуга *«Відкат»* забезпечує можливість відновлення роботи ІКСМ системи після помилок користувачів, після збоїв програмного забезпечення (ПЗ) або апаратних засобів цієї системи, дозволяє підтримувати цілісність баз даних, прикладних застосувань, побудованих на транзакціях і т. ін. Дана послуга забезпечує можливість відмінити

операцію або послідовність операцій і повернути (тобто, «відкатити») захищений об'єкт до попереднього стану.

Послуга «Цілісність при обміні» (ЦВ) дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час експорту/імпорту цих об'єктів через незахищене середовище. Найчастіше ця послуга реалізується з використанням механізмів криптографічного захисту, наприклад, як складова при реалізації цифрового підпису.

Для того, щоб інформаційна система могла бути оцінена на відповідність критеріям доступності, засіб криптозахисту цієї системи, повинен надавати послуги щодо забезпечення можливості авторизованим користувачам на певному проміжку часу мати безперешкодний доступ до ресурсів системи в цілому, до окремих її функцій, зокрема до оброблюваної інформації, і гарантувати спроможність ІКСМ функціонувати у разі відмови її компонентів.

Послуга «Використання ресурсів» дозволяє контролювати використанням послуг ІКСМ та її ресурсів.

Найм'якішою формою контролю за використанням ресурсів є застосування так званих квот. Усі захищені об'єкти системи (наприклад, дисковий простір, тривалість сеансу користування ресурсами, час використання центрального процесора і т. ін.) повинні пройти ідентифікацію і контролюватись диспетчером доступу шляхом накладення обмежень на максимальний обсяг даного ресурсу, що може бути виділений користувачу.

Послуга «Стійкість до відмов» забезпечує доступність інформаційної системи після відмови її компонентів. Стійкість до відмов гарантує доступність до ІКСМ, після відмови її компонента.

Послуга «Гаряча заміна» (ДЗ) дозволяє гарантувати доступність ресурсів ІКСМ (зокрема, можливість використання її інформаційних ресурсів, окремих функцій або ІКСМ системи у цілому) не тільки після, але і в процесі заміни окремих компонентів цієї системи. Основна мета, яка досягається внаслідок реалізації цієї послуги, полягає в тому, що на проміжках часу, коли встановлюється нова версія ПЗ або коли здійснюється заміна несправного компонента системи, забезпечується безперервність захисту.

Послуга «Відновлення після збоїв» (ДВ) забезпечує повернення інформаційної системи до відомого захищеного стану після відмови або після переривання обслуговування. В одних випадках процес відновлення після збоїв може вимагати втручання оператора, а в інших більш високих рівнях ефективності реалізації цієї послуги. У цих випадках КЗЗ має бути здатним продукувати відновлення працездатності автоматично без втручання оператора. Ця послуга забезпечує повернення ІКСМ системи у відомий захищений стан після відмови або переривання обслуговування.

Послуга «Реєстрація» (НР) дозволяє контролювати небезпечні з точки зору захисту інформації дії щодо ІКСМ. Реєстрація — це процес

розпізнавання, фіксування й аналізу дій і подій, що пов'язані з дотриманням політики безпеки інформації. Рівні даної послуги ранжируються залежно від повноти і вибіркової контролю, складності засобів аналізу даних журналів реєстрації і спроможності вияву потенційних порушень.

Послуга «Ідентифікація і автентифікація» (НІ) дозволяє комплексній системі захисту визначити і перевірити особистість користувача (фізичної особи), який намагається одержати доступ до ресурсів системи. Хоч поняття «ідентифікація» відрізняється від поняття «автентифікація», на практиці обидва ці процеси важко буває поділити. Важливо, щоб в кінцевому підсумку були підстави стверджувати, що система має справу з конкретним відомим їй користувачем. За результатами ідентифікації і автентифікації користувача система (точніше, КЗЗ), по-перше, приймає рішення про те, чи дозволено даному користувачеві увійти у систему, і, по-друге, використовує одержані результати надалі для здійснення розмежування доступу на підставі атрибутів доступу користувача, що увійшов.

Послуга «Достовірний канал» (НК) дозволяє гарантувати, що користувач взаємодіє безпосередньо з комплексом захисту і ніякий інший користувач або процес не може втручатись у взаємодію (підслухати або модифікувати інформацію, що передається).

Послуга «Розподіл обов'язків» (НО) дозволяє знизити ймовірність навмисних або помилкових неавторизованих дій користувача або адміністратора і, отже, величину потенційних збитків від таких дій. Роль адміністратора безпеки повинна бути визначена так, щоб обов'язки, що мають відношення до безпеки, могли бути виконані тільки в цій ролі. Ролі не обов'язково мають бути абсолютно взаємовиключаючими, оскільки деякі функції або команди можуть знадобитись і адміністратору, і користувачу, або різним адміністраторам і т. ін.

Послуга «Цілісність комплексу засобів захисту» (НЦ) визначає міру спроможності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами.

Послуга «Самотестування» (НТ) дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій ТЛК системи.

Послуга «Ідентифікація і автентифікація при обміні» дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію.

Послуга «Автентифікація відправника» (НА) дозволяє протидіяти відмовам від авторства і однозначно встановлювати належність певного об'єкта певному користувачу, тобто той факт, що об'єкт був створений або відправлений даним користувачем.

Послуга «Автентифікація одержувача» (НП) дозволяє протидіяти відмовам від одержання і дозволяє однозначно встановити факт одержання певного об'єкта певним користувачем.

У процесі оцінки захищеності ІКСМ системи від НСД розглядаються вимоги двох видів:

- вимоги до функцій (послуг) забезпечення безпеки;
- вимоги до рівня гарантій.

Виконання вимог першого виду забезпечується розробником системи захисту в процесі її проектування (розробки) і перевіряється експертною комісією в процесі оцінки її якості. Виконання вимог другого виду забезпечується як діями розробника, проте вже на всіх стадіях життєвого циклу системи, так і спільними діями розробника і експертної комісії в процесі оцінки. Наведені в критеріях гарантій вимоги регламентують передусім дії розробника. Дії експертної комісії регламентуються іншими документами.

Специфікації послуг безпеки були розглянуті вище. Більшість з вимог критеріїв гарантій, являють собою конкретизацію положень стандартів серії ДСТУ ISO 9000 щодо створення КЗЗ у ІКСМ і для їх викладення використовується термінологія з області управління якістю продукції (ДСТУ 3230-95).

Критерії гарантій включають вимоги до архітектури КЗЗ, середовища розробки, послідовності розробки, середовища функціонування, документації і випробувань КЗЗ. У цих критеріях вводиться сім рівнів гарантій, які є ієрархічними. Вимоги викладаються за розділами. Для того, щоб система захисту ІКСМ одержала певний рівень гарантій (якщо вона не може одержати більш високий), повинні бути задоволені всі вимоги, визначені для даного рівня в кожному з розділів.

Процес розробки. Від Розробника вимагається визначити всі стадії життєвого циклу ІКСМ, розробити, запровадити і підтримувати в робочому стані документально оформлені методики своєї діяльності на кожній стадії.

Управління конфігурацією. Управління конфігурацією є необхідною і невід'ємною частиною робіт із створення будь-якої інформаційної системи. Система управління конфігурацією повинна бути орієнтована на вирішення чотирьох основних завдань: визначення конфігурації, регулювання конфігурації, облік стану і перевірка якості конфігурації.

Відповідно до Критеріїв система управління конфігурацією включає в себе технічні та організаційні заходи. Система управління конфігурацією повинна охоплювати розробку і супроводження програмного, апаратного, програмно-апаратного забезпечення, розробку документації, тестів і т. ін.

Вимоги до процесу проектування забезпечують гарантії того, що на кожній стадії розробки (проектування) існує точний опис інформаційної системи, а реалізація ІКСМ точно відповідає вихідним вимогам (політиці безпеки).

Вимоги до процесу проектування передбачають наявність чотирьох основних рівнів деталізації ІКСМ у процесі її створення: функціональна специфікація, проект архітектури, детальний проект, реалізація. У процесі перевірки дотримання вимог виконується аналіз коректності опису інформаційної системи для кожного рівня деталізації і його відповідності опису попереднього рівня. У документах, в яких наведені описи для кожного рівня деталізації, можуть використовуватись посилання на інші документи. Вимоги до середовища функціонування ІКСМ системи забезпечують гарантії того, що система поставляється замовнику без несанкціонованих модифікацій, а також інсталюється і ініціюється замовником так, як це передбачається Розробником. Оцінка забезпечує гарантії того, що ІКСМ-система правильно реалізує політику безпеки і правильно функціонує, і будується на припущенні, що функціонування ІКСМ системи починається з безпечного стану.

Для того, щоб замовник зміг повною мірою використати послуги безпеки, що надаються ІКСМ системою для реалізації політики безпеки, встановленої в його організації, йому необхідна відповідна документація, в якій були б описані ці послуги і дані вказівки щодо їх використання.

6.4. Захист інформації на базі ISO/IEC

На етапі оцінки захищеності інформаційних ресурсів АТС послідовно виконуються такі види робіт (рис. 6.2):

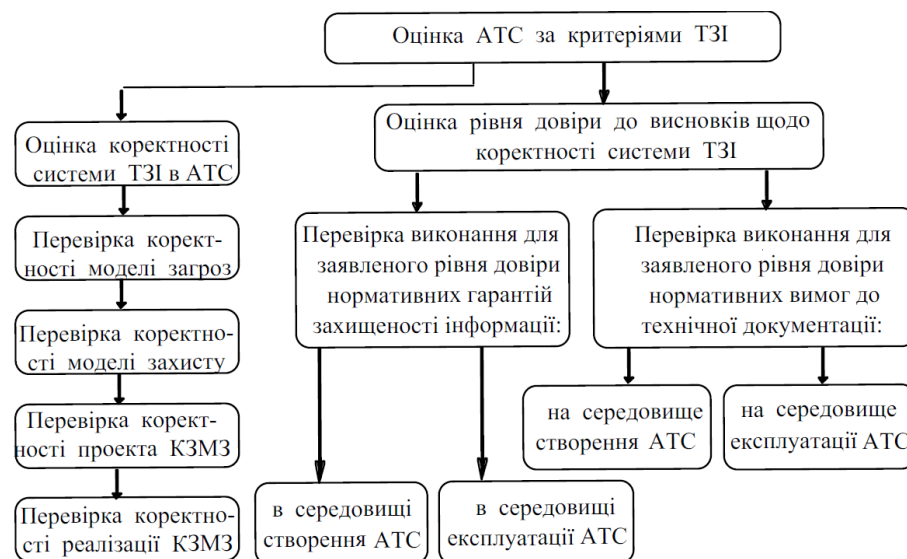


Рис. 6.2. Порядок оцінки АТС за критеріями ТЗІ

Цілями оцінки АТС за критеріями ТЗІ є:

- підтвердження ефективності й коректності розробленої і реалізованої на АТС системи ТЗІ;
- підтвердження заявленого рівня довіри до висновку про коректність системи ТЗІ в оцінюваній АТС.

Процес оцінки АТС за критеріями ТЗІ регламентований базовою методикою оцінки ефективності захисту, викладеною в НД ТЗІ 2.3-001-99.

Ця методика ґрунтується на специфікаціях ФПЗ (див. НД ТЗІ 2.5-001-99), специфікаціях гарантій захищеності інформації (див. НД ТЗІ 2.5-002-99) і специфікаціях довірчих оцінок коректності реалізації захисту (див. НД ТЗІ 2.5-003-99).

Крім того, у процесі оціночних робіт використовуються окремі спеціалізовані методики оцінки якості ТЗІ від НСД, витоків та спеціальних впливів.

Ступінь впевненості в коректності створеної системи ТЗІ у вигляді заявленого до оцінки рівня довіри, а також рівень захищеності інформаційних ресурсів у вигляді певної множини функцій безпеки, для яких зазначені рівні стійкості створених механізмів захисту, вказуються Заявником у процесі оформлення заявки на виконання оціночних робіт. Така заявка направляється на адресу уповноваженого державою експертного органу.

Процес оцінювальних робіт у випадку сертифікації АТС за критеріями ТЗІ регламентується нормативними документами УкрСЕПРО – зокрема, ДСТУ 3413-96.

За результатами оцінки Оцінювач надає Заявнику звіт, в якому вказується результат оцінки.

У випадку негативного висновку в звіті докладно і конкретно з посиланнями на відповідні НД наводяться аргументи і пояснюються причини, що спонукали Оцінювача зробити висновок про невідповідність результатів оцінки до очікуваної цілі.

У випадку позитивного висновку Оцінювачем і Заявником спільно готуються відповідні документи в яких вказуються:

- структура створеної на АТС системи ТЗІ у вигляді множини функцій безпеки з реалізованими рівнями стійкості механізмів захисту, коректність якої підтверджується;

- підтверджене значення рівня довіри до коректності зазначеної в документі структури системи ТЗІ.

У процесі оцінювання за вищими рівнями довіри виникає необхідність у розробці і виготовленні спеціальних схем дослідження «слабких місць», «глибоких тестів на проникнення», моделюванні дій «хакерів», формального опису політики безпеки. Всю вище перераховану роботу повинен узяти на себе Заявник і відповідати за повноту і коректність її виконання. Оцінювач може взяти на себе роботу з перегляду наданих Заявником тестів, моделей, схем, аналізів, обґрунтувань і доказів, має право їх доповнювати й удосконалювати, досліджувати власними методами і засобами слабкі місця у захисті.

Захист інформаційних ресурсів.

Наприкінці 90-х рр. Британський Інститут Стандартів (BSI) розробив національний стандарт щодо управління інформаційною безпекою, який потім одержав назву BS 7799, або «Старий Британський стандарт». При розробці стандарту ставилося завдання забезпечення державних та комерційних організацій інструментом для створення і реалізації

ефективних систем інформаційної безпеки на основі сучасних інформаційних технологій та методів менеджменту. У 2000 р. на базі BS 7799 був розроблений новий стандарт, що визнаний міжнародним, під назвою «International Standard ISO/IEC 17799 (Information technology – Code of practice for information security management)».

ISO (Міжнародна Організація по Стандартизації) і IEC (Міжнародна Електротехнічна Комісія) формують спеціалізовану систему всесвітньої стандартизації. Національні органи, які є членами ISO або IEC, беруть участь у розробці Міжнародних Стандартів через технічні комітети, створені відповідною організацією з метою роботи з специфічними областями технічної діяльності. Технічні комітети ISO й IEC співпрацюють в областях взаємного інтересу. Інші урядові й неурядові міжнародні організації, пов'язані з ISO й IEC, також беруть участь у цій роботі. На даний час сформовано цілий ряд стандартів **ISO/IEC** з урахуванням їх впровадження у галузь «Інформаційної безпеки»: **ISO/IEC 15408** «Критерії оцінювання безпеки інформаційних технологій», а також стандарти серії 27000 – 27001:2005, 27005:2008, 27006:2007, 27003, 27004, 27007, 27022, 27033.

У даному розділі ми розглянемо стандарт ISO/IEC 17799, як найбільш поширений та загальний стандарт для організації системи захисту інформаційних ресурсів та сервісних послуг в інформаційно-комунікаційних системах та мережах.

Стандарт ISO/IEC 17799 – це модель системи менеджменту, яка визначає загальну організацію процесів, класифікацію даних, системи доступу, напрямки планування, відповідальність співробітників, використання оцінки ризику і т. ін. в контексті інформаційної безпеки.

У процесі впровадження стандарту створюється так звана система менеджменту інформаційної безпеки, мета якої – скорочення матеріальних втрат, пов'язаних з порушенням безперервності бізнесу компанії.

Основна ідея стандарту – допомогти комерційним та державним господарським організаціям вирішити достатньо складне завдання: забезпечення надійного захисту інформаційних ресурсів та організація ефективного доступу до даних й процесу їх обробки згідно визначених послуг та вимог.

Основна структура стандарту

Структура стандарту дозволяє вибрати засоби управління, які мають відношення до конкретної організації або сфери відповідальності у середині організації. Зміст стандарту має такі розділи:

- політика безпеки [security policy];
- організація захисту [organizational security];
- класифікація ресурсів та контроль [asset classification and control];
- безпека персоналу [personnel security];
- фізична безпека та безпека навколишнього середовища [physical and environmental security];

- адміністрування комп'ютерних систем та обчислювальних мереж [computer and network management];
- управління доступом до системи [system access control];
- розробка та супроводження інформаційних систем [system development and maintenance];
- планування безперервної роботи організації [business continuing planning];
- виконання вимог (відповідність законодавству) [compliance].

У зв'язку з цим виділяється ряд ключових елементів управління, що подаються як фундаментальні:

- політика інформаційної безпеки;
- розподіл відповідальності за інформаційну безпеку;
- освіта та тренінг з інформаційної безпеки;
- звітність за інцидентами з безпеки;
- захист від вірусів;
- забезпечення безперервності роботи;
- контроль копіювання ліцензованого програмного забезпечення;
- захист архівної документації організації;
- захист персональних даних;
- реалізація політики з інформаційної безпеки.

Як видно, поряд з елементами управління для комп'ютерів та комп'ютерних мереж, стандарт велику увагу приділяє питанням розробки політики безпеки, роботі з персоналом (прийом на роботу, навчання, звільнення з роботи), забезпеченню безперервності виробничого процесу, юридичним вимогам.

Реалізація політики безпеки здійснюється на основі оцінки ризику та ретельно обґрунтовується.

Ризик визначається, як добуток показника можливих втрат на ймовірність того, що ця втрата відбудеться (рис.6.3). Під втратами розуміють матеріальні втрати, пов'язані з порушенням властивостей інформаційного ресурсу:

- конфіденційність;
- цілісність;
- доступність.

Для одержання сертифіката система менеджменту інформаційної безпеки підприємства оцінюється аудитором ISO 17799. Аудитор не може одночасно бути консультантом. Аудит по ISO 17799 складається з аналізу документації з системи менеджменту інформаційної безпеки, а також вибіркового контролю в організації, який дозволяє впевнитися, що реальна практика відповідає опису системи.

Акредитовану сертифікацію можуть здійснювати лише ті сертифікаційні товариства, які пройшли акредитацію ISO. Сертифікат, виданий такою організацією, признається на міжнародному рівні. Суттєве зростання процедур сертифікації відповідно очікується у зв'язку з розвитком електронної комерції та її послуг. Одночасно серйозний інтерес

до ISO 17799 проявляється і з сторони інших секторів державної та комерційної діяльності. До таких галузей відносяться: державні податкові органи та органи внутрішніх справ, банки, фінансові компанії, торговельні фірми, телекомунікаційні компанії, медичні заклади, підприємства транспорту та туристичні фірми і т. ін.

Вимоги безпеки ідентифікуються за допомогою методичної оцінки ризиків безпеки.

Витрати на засоби управління повинні бути збалансовані з урахуванням можливого збитку бізнесу, що може стати результатом порушень безпеки. Методи оцінки ризику можуть застосовуватися для всієї організації або тільки її частини, а також для окремих інформаційних систем, певних компонентів систем або послуг там, де це практично, реально й корисно.

Оцінка ризику – це систематичний розгляд:

- збитку бізнесу, що може з'явитися у результаті порушення безпеки, беручи до уваги можливі наслідки: втрати конфіденційності, цілісності або доступності інформації й інших активів;

- реальної ймовірності такого порушення, що проявляється у світлі переважаючих загроз й засобів управління, що застосовуються у цей час.

Результати цієї оцінки допоможуть направити й визначити відповідні дії по загальному управлінню компанією й пріоритети по управлінню ризиками інформаційної безпеки по реалізації обраних засобів [101].

Важливим є на періодичній основі виконувати *перегляд ризиків безпеки й реалізованих засобів управління* з метою:

- оцінки та введення змін, що стосуються вимог і пріоритетів бізнесу;
- урахування нових видів загроз й слабких місць системі та послугам;
- підтвердження того що засоби управління залишаються ефективними й відповідними.

Перегляд політики безпеки варто виконувати на різних рівнях глибини роботи компанії, залежно від результатів попередніх оцінок і рівнів, що підлягали змінам. Оцінки ризику спочатку виконують на високому загальному рівні для того, щоб визначити пріоритети вкладення ресурсів в області високого ризику, і потім на більш детальному рівні, щоб розглянути специфічні ризики самої системи та її послуг.

Заходи управління

Після ідентифікації вимог безпеки варто вибирати й застосовувати заходи управління, таким чином, щоб забезпечувати впевненість у зменшенні ризиків. Засоби управління можуть бути обрані із стандартів або з іншої безлічі документів та заходів управління визначених для даного класу систем, або можуть бути розроблені, щоб задовольнити потреби компанії відповідно до обраної політики безпеки.

Заходи управління варто вибирати, ґрунтуючись на відношенні вартості реалізації послуг та впровадження систем безпеки й зниження ризиків і можливих втрат, якщо відбудеться порушення. Не грошові

фактори, наприклад, втрата репутації, соціальні тощо, варто також брати до уваги з метою підтримки конкурентоспроможності компанії.

Деякі із заходів управління в стандартах та нормативних документах, можуть розглядатися, як керівні принципи для управління інформаційною безпекою й застосовуються більшістю організацій. Більш докладно це викладено нижче.

Заходи управління (розглянуті із законодавчої точки зору) включають:

- захист даних і секретність особистої інформації;
- охорону інформаційних ресурсів організації;
- права на інтелектуальну власність.

Заходи управління (розглянуті як загальна стала практика для інформаційної безпеки) містять (рис. 6.3):

- документи, що стосується політики інформаційної безпеки;
- розподіл обов'язків, пов'язаних з інформаційною безпекою;
- структуру підрозділів й навчання, пов'язані з інформаційною безпекою;
- повідомлення про інциденти, пов'язаних з безпекою;
- управління безперервністю бізнесу.

Ці заходи управління застосовуються для більшості організацій й у більшості середовищ. Слід зазначити, що, хоча всі заходи управління в стандартах та нормативних документах є важливими, доречність (застосовність) якого-небудь засобу управління повинна визначатися у світлі певних ризиків, з якими зіштовхується безпосередньо зазначена організація. Отже, незважаючи на те, що вищезгаданий підхід розглядається, як відправна точка інформаційної безпеки, він не є догмою та не заміняє вибір заходів управління, заснованих на оцінці ризику.

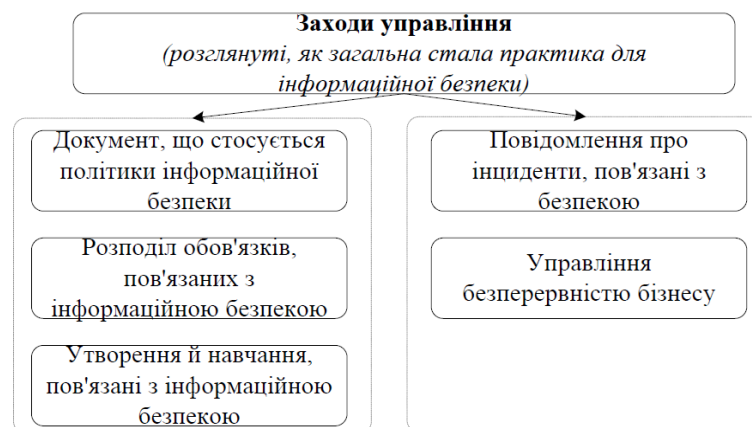


Рис. 6.3. Заходи управління ІБ

Критичними факторами для успішної реалізації інформаційної безпеки в межах організації є:

- політика безпеки, цілі й дії, які відбивають меті бізнесу;

- підхід до реалізації безпеки, що погоджується з культурою та внутрішньою етикою організації;
- підтримка й зобов'язання з боку керівництва;
- правильне розуміння вимог безпеки, оцінки ризику й управління ризиком;
- ефективний маркетинг безпеки для всіх адміністраторів і службовців;
- розподіл повноважень керівництва політикою інформаційної безпеки й стандартами між всіма службовцями й підрядниками;
- забезпечення відповідного тренування й навчання;
- всебічна й збалансована система виміру, що використовується для оцінки ефективності управління інформаційною безпекою й пропозиції в рамках зворотного зв'язку, спрямовані на поліпшення бізнесу;
- оцінка загроз інформації, руйнівного впливу на інформацію і уразливості інформації й засобів обробки, а також ймовірності їхнього виникнення.
- процес визначення ризиків, управління ризиком (*Risk management*) й зменшення або усунення ризиків безпеки, які можуть загрожувати інформаційній системі, у рамках припустимих витрат.

Політика інформаційної безпеки – забезпечує процес управління та підтримки визначеного рівня безпеки об'єкта інформаційної діяльності.

Реалізація процесів управління повинна встановлювати ясні положення політики й показники, зобов'язання стосовно безпеки компанії за допомогою створення й підтримки політики інформаційної безпеки в рамках всієї організації.

Необхідно, щоб документ політики був схвалений керівництвом, виданий і представлений відповідним чином всім службовцям. Він повинен містити зобов'язання по управлінню й викладати підхід організації до управління інформаційною безпекою.

Політика інформаційної безпеки повинна містити такі положення:

1. Визначення інформаційної безпеки, її загальних цілей і можливостей, сфери дії, а також важливості безпеки як механізму, що забезпечує можливість до спільного використання інформації.
2. Визначення намірів управління безпекою, що підтримують мету й принципи інформаційної безпеки.
3. Коротке пояснення політики безпеки, принципів, стандартів і вимог відповідності, що представляють особливу важливість для організації, наприклад:
 - 3.1. узгодження із законодавчими й договірними вимогами;
 - 3.2. вимоги розвитку безпеки;
 - 3.3. запобігання й виявлення вірусів й іншого шкідливого програмного забезпечення;
 - 3.4. управління безперервністю бізнесу;
 - 3.5. наслідки порушень політики безпеки;

3.6. визначення загальних і певних обов'язків по управлінню інформаційною безпекою, включаючи повідомлення про інциденти, що стосуються безпеки;

3.7. посилання на документацію, що може підтримувати політику, наприклад, більше деталізовані політики безпеки й процедури для певних інформаційних систем або правил по безпеці, яким повинні користуватись працівники;

3.8. роз'яснення політики безпеки всім користувачам системи та співробітникам організації у формі, що є доречною, доступною й зрозумілою.

З метою реалізації політики інформаційної безпеки варто створювати процес авторизації управління для існуючих та нових засобів обробки інформації.

Безпека доступу – підтримка процесу інформаційної безпеки на базі засобів обробки інформації й інформаційних активів за допомогою реалізації доступу третіх сторін.

Там, де є ділова потреба в такому доступі третьої сторони, варто виконувати оцінку ризику, для визначення аспектів безпеки й вимог до управління інформаційною системою. Заходи управління варто погоджувати й визначати в контракті із третьою стороною.

Тип доступу, що надано третій стороні, має особливе значення. Наприклад, ризики доступу через мережне з'єднання відрізняються від ризиків, що впливають із фізичного доступу до системи (рис. 6.4).



Рис. 6.4. Типи доступу до системи та її ресурсів

Типами доступу, які підлягають управлінню з точки зору безпеки є:

- фізичний доступ, наприклад, до офісів, комп'ютерних залів й кімнат, кабінетів тощо;
- логічний доступ, наприклад, до баз даних, інформаційних систем та мереж організації.

Третій стороні може бути наданий доступ з ряду причин. Наприклад, є треті сторони, які забезпечують послуги для організації, але не розташовані у тому ж місці. Однак, їм може бути даний фізичний і логічний доступ, як, наприклад:

- коли необхідний доступ на системному або більш низькому рівні прикладної функціональності для підтримки апаратних засобів і програмного забезпечення;
- коли необхідний обмін інформацією, доступ до інформаційних систем або загальних баз даних для торговельних партнерів або спільних підприємств, тощо.

Інформація може піддаватися ризику при доступі третіх сторін з неадекватним управлінням безпекою. Там, де є ділова потреба контактів із третьою стороною, варто проводити оцінку ризику, щоб ідентифікувати будь-які вимоги для певних заходів управління. Варто брати до уваги – тип необхідного доступу, цінність інформації, заходи управління, використовувані третьою стороною та значення цього доступу для інформаційної безпеки всієї організації.

Доступ до інформації й засобів обробки інформації третій стороні не можна забезпечувати, поки не здійснені відповідні заходи управління, і не підписаний контракт, що визначає строки зв'язку або доступу.

Захист від шкідливого програмного забезпечення – захист цілісності програмного забезпечення та інформаційних ресурсів.

Запобігання, виявлення й нейтралізація шкідливого програмного забезпечення потребує специфічних та високопрофесійних заходів та методів управління детально розглянуто у розділі 5.

Програмне забезпечення й засоби обробки інформації уразливі до введення шкідливого програмного забезпечення, такого як комп'ютерні віруси, мережні «хробаки», «троянські коні» і «логічні бомби» тощо. Користувачі повинні бути інформовані про небезпеку неавторизованого або шкідливого програмного забезпечення. Адміністратори інформаційно-комунікаційних систем та мереж повинні впроваджувати спеціальні засоби управління, щоб виявляти, реєструвати й запобігати появі або навмисному введенню шкідливого програмного забезпечення. Зокрема, істотною є необхідність вживання заходів обережності для виявлення й запобігання комп'ютерних вірусів у персональних комп'ютерах та безпосередньо їх поширення по мережі передачі даних.

Заходи управління щодо захисту від шкідливого програмного забезпечення:

- впровадження офіційної політики безпеки, що вимагає наявності ліцензійного антивірусного пакета програм, а також впроваджені системи виявлення та заборони використання неавторизованого програмного забезпечення;

- термінове впровадження офіційної політики захисту інформаційних ресурсів від ризиків, пов'язаних з одержанням файлів й програмного забезпечення із зовнішніх мереж, внутрішніх мереж, або з будь-якого іншого інформаційного середовища у разі коли повинні бути початі захисні заходи;

- установку й регулярне відновлення антивірусних баз і виправлень програмного забезпечення для сканування комп'ютерів і носіїв інформації або при профілактичному контролі у звичайному порядку;

- проведення регулярних переглядів змісту програмного забезпечення й даних для систем, що підтримують критичні бізнес-процеси. Присутність будь-яких не схвалених файлів або неавторизованих виправлень повинне бути офіційно досліджено та зареєстровано;

- перевірку будь-яких вкладень електронних носіїв інформації сумнівного або неавторизованого походження, а також файлів отриманих з мереж чи інформаційних зон на наявність вірусів, ще до їхнього використання;

- перевірку будь-яких вкладень електронної пошти й інформації при її обміні на наявність шкідливого програмного забезпечення ще до їхнього використання. Ця перевірка повинна бути виконана в різних місцях, наприклад, на серверах електронної пошти, на робочих станціях або при вході в мережу організації;

- до процедур й обов'язків фахівців управління безпекою, пов'язаною із захистом від вірусів, повинно входити: навчання по інсталяції та використанню ПЗ, відновлення інформаційних ресурсів та послуг після вірусних нападів тощо;

- відповідні плани по реалізації безперервності бізнесу з урахуванням відновлення інформаційних ресурсів та послуг після вірусних нападів, включаючи всі необхідні заходи, щодо резервування й відновлення даних і програмного забезпечення;

- процедури верифікації всієї інформації й даних щодо шкідливого програмного забезпечення, а також забезпечення точності й інформативності попереджувальних бюлетенів.

Адміністратори інформаційно-комунікаційних систем та мереж повинні забезпечувати впевненість користувачів та керівництва компанії у використанні кваліфікованих джерел щодо постачання й використання впровадженого антивірусного програмного забезпечення. Штат співробітників підрозділів захисту інформаційних ресурсів повинен бути високо обізнаний у питаннях реєстрації помилкових вірусів, а також визначати дії при їх одержанні та установленні розходження між помилковими й реальними вірусами.

Операції по обслуговуванню – організація процесів реалізації політики безпеки з метою забезпечення цілісності і доступності послуг при передачі й обробці інформації в мережах зв'язку.

Обов'язково повинні бути встановлені конкретні процедури виконання погодженої стратегії резервування інформації і даних, а також встановленого циклу процедур їх своєчасного відновлення, реєстрації подій і помилок, моніторинг середовища устаткування при передачі й обробці інформації в мережах зв'язку.

Резервування важливої комерційної інформації, а також системного та прикладного програмного забезпечення повинно виконуватися регулярно з урахуванням можливості відновлення після нещасного випадку або навмисної чи ненавмисної відмови інформаційного середовища. Заходи резервування для кожної окремої системи повинні регулярно перевірятися з метою перевірки відповідності вимогам процесу безперервності бізнесу.

Заходи управління операціями по обслуговуванню:

- мінімальний рівень резервної інформації, разом з точними й повними записами резервних копій інформаційних ресурсів системи і

задокументованими процедурами відновлення, повинні зберігатися у спеціалізованому місці;

- для резервної інформації повинен бути забезпечений відповідний рівень фізичного захисту й захисту середовища. Заходи управління, що застосовуються до середовища на основному місці, повинні мати функції розширення з метою охоплення додаткових та резервних пунктів;

- резервні носії інформації повинні регулярно піддаватися тестуванню для забезпечення технічної відповідності при використанні в надзвичайних ситуаціях;

- процедури відновлення треба регулярно перевіряти і тестувати для забезпечення технічної відповідності.

Управління безпекою мереж – забезпечення безпеки властивостей інформаційних ресурсів в мережах передачі даних, а також реалізація процесу захисту підтримуючої інфраструктури.

Для досягнення й підтримки безпеки в інформаційно-комунікаційних системах та мережах потрібен визначений діапазон засобів та заходів управління. Адміністратори безпеки повинні реалізовувати визначений діапазон для забезпечення інформаційної безпеки і захисту даних від неавторизованого доступу та пов'язаних з цим наданням мережних послуг.

Заходи управління безпекою мереж включають:

- відповідальність адміністраторів безпеки і користувачів за реалізацію політики безпеки при експлуатації мережі й наданні мережних послуг, дані процедури необхідно відокремлювати від процесів обробки даних та інших комп'ютерних операцій;

- необхідно встановлювати спеціальні засоби та впроваджувати заходи управління безпекою систем для забезпечення конфіденційності й цілісності даних, що передаються по загальнодоступних мережах, забезпечувати процедури захисту підключених систем, а також підтримувати доступність мережних послуг і підключених робочих станцій;

- варто встановлювати – обов'язки, відповідальність й процедури для організації процесів з вилученням устаткуванням, включаючи устаткування, розташоване в області дії користувача;

- дії по управлінню безпекою мереж необхідно ретельно розділяти, як за оптимізацією та наданням послуг для бізнесу, так і за забезпеченням послідовного застосування засобів та заходів управління безпекою для всієї інфраструктури обробки інформації.

Розробка й обслуговування систем безпеки – забезпечення процесу розробки, впровадження та експлуатації засобів захисту інформації в інформаційних системах.

Розробка й обслуговування систем безпеки включає повну інфраструктуру інформаційної системи, комерційні додатки й додатки розроблені користувачем тощо. Проектування й реалізація бізнес-процесу, що підтримує додаток або послуги, можуть бути критичними для систем безпеки. Вимоги до систем або заходів безпеки, варто визначати й

погоджувати з керівництвом, технічними можливостями, нормативними актами ще до розробки інформаційних систем.

Необхідно, щоб формулювання вимог бізнесу для нових інформаційно-комунікаційних систем або вдосконалення існуючих систем були жорстко специфіковані залежно від заходів управління безпекою. У таких специфікаціях варто відокремлено розглядати автоматизовані засоби управління, які включені в систему, а також необхідність їх підтримки та супроводу. Такі специфікації варто враховувати при оцінці пакетів програм для комерційних додатків.

Необхідно, щоб вимоги й заходи управління безпекою відбивали комерційну цінність інформаційних ресурсів, а також можливий потенційний збиток бізнесу, щодо відмови систем безпеки або її відсутності. Структурою аналізу та послідовністю його виконання для визначення вимог безпеки й засобів управління є оцінка ризику й розроблені методики управління ризиком інформаційної системи.

6.5. Задачі організації безпеки інформації

Забезпечення безпеки інформаційних мереж – запобігання ушкодженню інформаційних активів і переривання дій, пов'язаних з реалізацією безперервного процесу бізнесу. Інформаційні ресурси та засоби обробки, поширення інформації повинні бути керовані й фізично захищені.

Повинні бути встановлені відповідні експлуатаційні процедури для захисту документів, носіїв інформації (стрічок, дисків, флешек, касет), обчислювальної техніки, даних, систем введення/виводу й системної документації, які стосуються процесів ушкодження, злодійства й несанкціонованого доступу або інших зловмисних дій.

З даної точки зору необхідно розглядати такі заходи управління:

- фіксація попереднього змісту інформації, яка повинна бути вилучена з організації та розташована на будь-яких носіях багаторазового користування;
- дотримання строгої авторизації всіх носіїв інформації, що видаляється із організації, а також проведення реєстрації всіх видалень для підтримки процедур аудиту;
- носії інформації повинні зберігатися в надійному, безпечному середовищі, відповідно до встановлених вимог.

Всі процедури й рівні авторизації повинні бути чітко задокументовані. Процедури обробки й зберігання інформації варто встановлювати для того, щоб захистити інформацію від неавторизованого розкриття або неправильного впровадження.

Варто встановити процедури для обробки інформації, відповідно до її класифікації у документах, обчислювальних системах, мережах, мобільних засобах зв'язку, пошті, мовній пошті, мовному зв'язку взагалі, системах з комп'ютерним поданням інформації, поштових послугах/засобах

обслуговування, при використанні факсів і будь-яких інших чутливих об'єктів, наприклад, чистих чеків, рахунків.

Заходи управління обробкою й зберіганням інформації (рис. 6.5):

- обробка й маркування всіх носіїв інформації;
- обмеження доступу при ідентифікації неавторизованого персоналу;
- підтримка офіційної реєстрації авторизованих одержувачів даних;
- забезпечення впевненості в тому, що введені дані є повними та обробка завершується належним чином, а також є підтвердження виводу даних;
- захист (записаних у буфер) даних, що очікують виходу на рівень сумісний з їхньою відповідністю;
- зберігання носіїв інформації в середовищі, що відповідає специфікаціям виготовлювачів;
- відомість розподілу даних до мінімуму;
- чітке маркування всіх копій даних, пропонованих увазі авторизованого одержувача.

Системна документація може містити визначений діапазон інформації, наприклад: опис процесів додатків, процедур, структур даних, процесів авторизації тощо. Необхідно розглянути такі заходи управління для захисту системної документації від неавторизованого доступу та використання:

- системну документацію варто зберігати згідно з визначеною політикою безпеки та встановленими стандартами;
- список осіб, що мають доступ до системної документації, варто зводити до мінімуму, а авторизацію варто забезпечувати власникові додатків;
- системну документацію, підтримувану загальнодоступною мережею, або отриману через загальнодоступну мережу, варто захищати згідно з визначеною політикою безпеки та встановленими стандартами.

Безпека обміну інформацією й програмним забезпеченням – запобігання втрат, модифікації або неправильного чи неавторизованого вживання інформації і програмного забезпечення, що підлягає обміну між організаціями та окремими користувачами.

Обмін інформацією й програмним забезпеченням між організаціями та окремими користувачами виконується згідно з встановленими процедурами управління у відповідності чинному законодавству, стандартам або внутрішнім нормативним документам. Обміни варто виконувати на основі угод, або встановлювати внутрішні процедури й стандарти по захисту інформації й носіїв інформації при їх передачі. Дані питання є базовими для процесів безперервності бізнесу і його безпеки з урахуванням питань пов'язаних з електронним обміном даних, електронною торгівлею й електронною поштою, а також вимогами до заходів управління безпекою інформаційних систем.

Угоди обміну програмним забезпеченням повинні включати:

- обов'язки персоналу по управлінню і контролю безпекою та повідомлення про передачу, відправлення й одержання інформації;
- визначені процедури для відправника про передачу, відправлення й одержання повідомлення;
- мінімальну кількість технічних стандартів по формуванню й передачу пакетів;
- стандарти по ідентифікації кур'єра;
- відповідальність й обов'язки у випадку втрати даних;
- використання погодженої системи маркування для чутливої або критичної інформації;
- володіння інформацією й програмним забезпеченням, а також обов'язки по захисту даних, узгодження з авторським правом на програмне забезпечення й аналогічні питання;
- технічні стандарти по запису й зчитуванню інформації й програмного забезпечення;
- будь-які спеціальні засоби управління, які можуть знадобитися, для захисту чутливих об'єктів, таких як криптографічні ключі тощо.

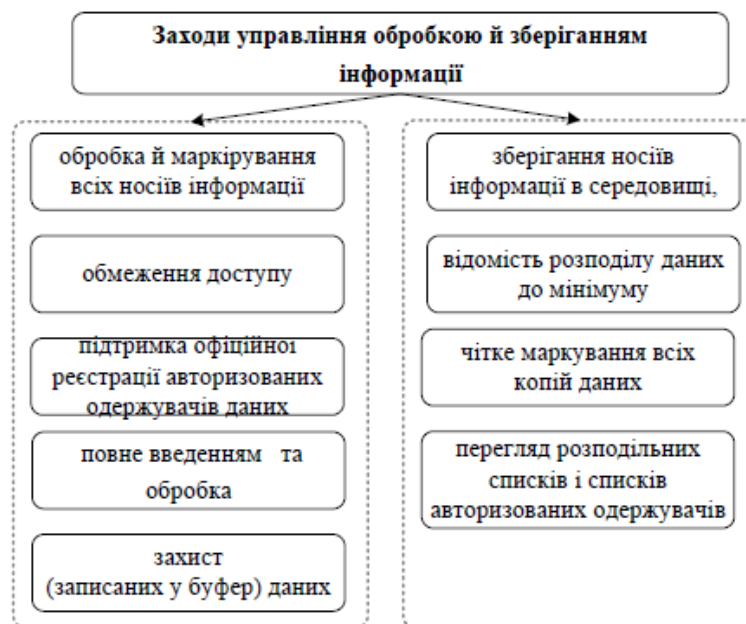


Рис. 6.5. Заходи управління обробкою інформації

Інформація може бути вразливою до неавторизованого доступу, неправильного вживання або спотворення під час фізичного транспортування, наприклад, при пересиланні носіїв інформації через поштову службу або через кур'єра. Варто застосовувати такі засоби управління для охорони комп'ютерних носіїв інформації, що транспортують між пунктами:

- варто використовувати надійний транспорт або кур'єрів. Список авторизованих кур'єрів необхідно погоджувати з керівництвом, а також варто реалізовувати процедуру перевірки ідентифікації кур'єрів;

- варто застосовувати спеціальні засоби та заходи управління безпекою для захисту чутливої інформації від неавторизованого розкриття або модифікації.

Електронна торгівля – процедури обміну електронними даними (EDI), даними електронної пошти й оперативними транзакціями в глобальних інформаційно-комунікаційних мережах, що проводяться з метою реалізації процесу безперервного бізнесу.

Електронна торгівля уразлива до ряду мережних загроз, які можуть бути результатом шахрайської діяльності, заперечування контракту, а також розкриття або модифікації інформації. Щоб захистити електронну торгівлю від таких загроз, необхідно застосовувати відповідні заходи управління безпекою.

Заходи управління безпекою електронної торгівлі:

- аутентифікація (користувачів, даних, додатків, послуг тощо.);
- авторизація (авторизований перелік цін, ключових торговельних документів, партнерів, користувачів, керівництва тощо);
- аудит всіх гілок фізичних та авторизованих процедур реалізації процесу безперервного бізнесу;
- управління процесами, пов'язаними з конфіденційністю контрактів й заявками на підряд, тощо;
- конфіденційність інформації про ціноутворення, оплату й поставки.

Визначені вище процедури аутентифікації й авторизації, повинні бути розглянуті із застосуванням криптографічних методів, беручи до уваги відповідність нормативним вимогам та стандартам.

Заходи управління безпекою електронної торгівлі, між торгуючими партнерами, необхідно підтримувати документально оформленою угодою, що приводить обидві сторони до погоджених строків торгівлі, включаючи деталі авторизації користувачів, послуг, тощо.

Обов'язковим є необхідність розгляду стійкості до нападу головного сервера електронної торгівлі, а також питання безпеки будь-якого мережевого чи міжмережевого з'єднання з ним.

Електронна пошта використовується для ділових комунікацій, замінюючи традиційні форми зв'язку, такі як телекс і листи. Електронна пошта відрізняється від традиційних форм ділових комунікацій, наприклад: швидкістю, структурою повідомлення, ступенем неформальності й уразливістю до неавторизованих дій. Необхідно розглядати потребу в заходах управління інформаційною безпекою, для зменшення ризиків безпеки створюваних використанням послуг електронної пошти.

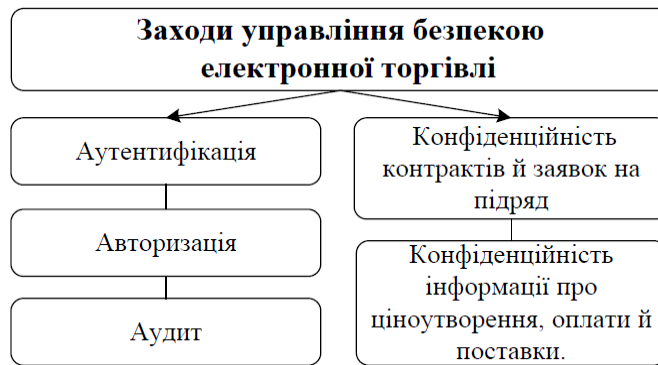


Рис. 6.6. Заходи управління безпекою електронної торгівлі

Ризики безпеки електронної пошти включають:

- уразливість повідомлень при неавторизованому доступі до інформаційних ресурсів, а також модифікації даних або відмов в обслуговуванні;
- уразливість до помилок: неправильна адресація, несанкціонована переадресація, або невірний напрямок маршруту даних трафіку;
- уразливість загальній надійності системи, а також доступності послуги;
- вплив засобів зв'язку на роботу системи та зміни технічних характеристик при передачі інформації (ефект збільшеної швидкості відправлення тощо);
- нормативно-правові й юридичні обмеження процесів та процедур управління безпекою;
- управління доступом вилученого користувача до облікових даних електронної пошти.

Організаціям варто розробляти чітку політику інформаційної безпеки, що стосується використання електронної пошти, включаючи:

- напади на електронну пошту (віруси, перехоплення даних тощо);
- захист підключень та комунікацій електронної пошти;
- провідні вказівки, що визначають процедуру заборони використання електронної пошти;
- обов'язки службовця не компрометувати компанію;
- використання криптографічних методів, для захисту конфіденційності й цілісності електронних повідомлень;
- збереження та знищення повідомлень;
- додаткові засоби управління безпекою для перевірки обміну повідомленнями, що не може бути аутентифіковане.

Політики й керівні принципи безпеки електронних офісних систем розробляються й реалізуються з метою управління бізнесом і ризиками безпеки, пов'язаними з електронними офісними системами.

Електронні офісні системи – забезпечують можливості для більш швидкого поширення й поділу ділової інформації, використовуючи комбінацію: документів, комп'ютерів, мобільних обчислювальних засобів, мобільних засобів зв'язку, пошти, мовної пошти, мовного зв'язку взагалі,

систем з комплексним поданням інформації, поштових послуг засобів обслуговування й факсів.

При розгляді заходів управління безпекою електронних офісних систем та з урахуванням ділового змісту комунікаційних з'єднань й засобів обслуговування до загальної політики безпеки підприємства варто включати питання:

- уразливості інформації в офісних системах (запис телефонних розмов або розмов сполучення конференц-зв'язку, конфіденційність розмов, зберігання факсів, розкриття пошти, розподіл пошти);
- політику безпеки й відповідні засоби управління поділом доступу до інформації та даних;
- категорії чутливої ділової інформації, якщо система не забезпечує відповідний рівень захисту;
- обмеження доступу до інформації реєстраційного журналу аудиту;
- придатність інформаційної системи для підтримки комерційних додатків, таких як передача замовлень або авторизації;
- обмеження обраних засобів обслуговування для певних категорій користувачів;
- ідентифікація статусу користувачів;
- збереження й резервування інформації, що знаходиться в системі;
- вимоги й заходи щодо нейтралізації несправностей тощо.

Варто постійно тримати під контролем підсистеми захисту цілісності інформації, яка видається електронним способом з метою запобігання неавторизованій модифікації даних. Інформацію й дані що виходять, обробляються чи надходять із загальнодоступної відкритої системи (інформація та ресурси Web-сервера, доступного через відкриту мережу Інтернет), необхідно приводити у відповідність із законодавчою, нормативно-правовою базою, внутрішніми правилами й інструкціями, у юрисдикції яких розташована система або здійснюється електронна торгівля. Повинен мати місце офіційний процес авторизації інформації, перед тим як вона стане загальнодоступною.

Програмне забезпечення, дані та іншу інформацію, що вимагає високого рівня цілісності й конфіденційності при її використанні чи обміні у загальнодоступній системі, необхідно захищати відповідними механізмами безпеки з використанням крипто-алгоритмів й цифрового підпису. Для захисту електронних систем публікацій, що мають зворотній зв'язок і пряме введення інформації, варто ретельно дотримуватись того, щоб:

- процедури безпеки та інформація, що надходить до інформаційної системи організації, відповідала стандартам та нормам чинного законодавства з інформаційної безпеки;
- інформація, введена в інформаційну систему, була оброблена повністю й точно, своєчасним способом;
- чутлива до впливів інформація та дані повинні бути захищені в процесі збору, обробки й збереження;

- підсистема доступу до інформаційної системи та її ресурсів, повинна зробити реалізацію процесів ненавмисного або несанкціонованого доступу до мереж неможливою.

6.6. Управління доступом і забезпечення цілісності програмного забезпечення

Забезпечення управління доступом розробляється і впроваджується з метою реалізації авторизованого доступу до інформаційних ресурсів та їх активів, а також з метою управління діловими процесами з урахуванням вимог політики безпеки й авторизації інформації й користувачів.

Загальна політика безпеки інформаційної системи та організації в цілому повинна включати й документувати вимоги бізнесу щодо методів та заходів управління доступом до системи та її ресурсів. Правила управління доступом, права кожного користувача або групи користувачів повинні бути чітко фіксовані у формулюванні політики доступу та її безпеки.

Політика безпеки та впровадження заходів забезпечення процедур управління доступом повинна включати (рис. 6.7.):

- вимоги до безпеки індивідуальних бізнес-додатків;
- ідентифікацію всієї інформації, пов'язаної з бізнес-додатками;
- політики поширення й авторизації інформації (необхідність знання принципів та рівнів безпеки, а також класифікацію інформації що циркулює та обробляється в системі);
- погодженість між політиками управління доступом і класифікацією інформації різних систем і мереж, що співпрацюють;
- відповідне законодавство й будь-які договірні зобов'язання щодо захисту доступу до даних або послуг системи;
- стандартні профілі доступу користувача для загальних категорій роботи;
- управління правами доступу в розподіленому й об'єднаному у мережу інформаційному середовищі, що визнає всі типи доступних зв'язків.



Рис. 6.7. Політика управління доступом

Управління користувальницьким доступом – процес запобігання реалізації неавторизованого доступу до інформаційних систем, її послуг та ресурсів.

Загальна політика безпеки повинна включати офіційні процедури по управлінню та розподілу прав доступу до інформаційних систем та її послуг.

Процедури повинні охоплювати всі стадії в життєвому циклі користувальницького доступу, від початкової реєстрації нових користувачів до кінцевого зняття з реєстрації користувачів, яким більше не потрібен, або заборонений доступ до інформаційних систем і послуг.

Офіційна процедура реєстрації користувача, повинна включати:

- використання унікального ідентифікатора (ID: identification data) користувача для можливості однозначного встановлення взаємозв'язку між діями користувача й відповідальністю за них. Використання групових ID необхідно використовувати тільки там, де вони необхідні, згідно з встановленими правилами політики безпеки:

- перевірку дійсності авторизації користувача інформаційної системи або її послуг;

- перевірку вірності рівня наданого доступу з урахуванням мети бізнесу і структури політики безпеки;

- надання користувачам письмового підтвердження їх прав доступу;

- підпис заяви користувача щодо умов доступу та відповідальності за проведення процедур;

- надання постачальником послуг доступу до інформаційної системи та її ресурсів тільки після проведення завершення процедури авторизації;

- підтримку формального запису всіх осіб, зареєстрованих для використання послуг;

- негайне скасування прав доступу користувачів, які перемінили робоче місце або покинули організацію;

- періодичну перевірку й видалення надлишкових користувальницьких ID й облікових записів;

- запобігання можливості передачі іншим користувачам надлишкових користувальницьких ID ідентифікаторів.

Розподіл і використання привілеїв – методи та засоби багато користувальницької інформаційної системи, які дозволяють користувачеві обходити основні функції системи безпеки або прикладні засоби управління.

Невідповідне використання системних привілеїв – є головним фактором, що породжує відмови інформаційних систем.

У багатьох користувальницьких системах, що мають підсистеми захисту від неавторизованого доступу, повинен існувати розподіл привілеїв керованих через офіційний процес авторизації. З цього приводу необхідно розглянути такі кроки щодо класифікації та впровадження привілеїв:

- надання привілеїв, що пов'язані з роботою з системними програмними продуктами (наприклад операційною системою, системою керування базою даних і кожним додатком, категорії штату службовців, тощо);

- надання привілеїв користувачам з урахуванням необхідного часу знаходження в інформаційній системі для реалізації їхніх функцій;

- необхідність підтримки процесів авторизації, аудиту й запису наданих привілеїв після завершення процедури авторизації;

- заохочення розробки й використання стандартних системних програм для автоматизації та авторизації процедур надання привілеїв користувачам;

- необхідно розділяти призначені привілеї згідно з визначеною класифікацією з урахуванням розподілу між користувачами задач бізнесу.

Пароль є обов'язковим засобом підтвердження ідентифікатора користувача для доступу до інформаційної системи, її ресурсів або послуг що реалізуються в системі.

Процедура розподілу паролів підлягає процесу строгого контролю і управління та повинна включати:

- вимоги до користувачів з приводу підпису заяви, щодо збереження конфіденційності інформації про особисті паролі або інформації про паролі робочої групи;

- забезпечення підтримки власних паролів після позитивної ідентифікації користувача;

- забезпечення процедур безпечної видачі користувачам паролів згідно з визначеними функціями. Варто уникати використання незахищених (відкритий текст) повідомлень електронної пошти або повідомлень електронної пошти третьої сторони з метою запобігання механізмів несанкціонованого вилучення паролів. Користувачам необхідно підтверджувати одержання паролів.

Пароль – засіб забезпечення та підтвердження ідентифікатора користувача, установлює права доступу до засобів обробки інформації, інформаційних ресурсів або послуг інформаційної системи.

Паролі повинні зберігатись в автоматизованій системі тільки в захищеній формі. Інші технології для ідентифікації й аутентифікації користувача, такі як біометрія, перевірка відбитків пальців, перевірка підпису, використання маркерів апаратних засобів є додатковими та доступними заходами для підтвердження функцій користувача в інформаційній системі.

Управління мережевим доступом – процес реалізації захисту внутрішніх та зовнішніх інформаційних ресурсів мережі та її мережових послуг.

Користувачі, що мають авторизований доступ до мереж і мережних послуг, повинні підтримувати режим безпеки мережових послуг та забезпечувати:

- відповідні інтерфейси та інтерфейси безпеки між інформаційною мережею організації й мережами, що належать іншим організаціям, або загальнодоступними мережами;

- відповідні механізми аутентифікації, авторизації для користувачів й устаткування;

- управління процедурами безпечного доступу користувача до інформаційних ресурсів та послуг системи.

Політика безпеки управління мережевим доступом повинна охоплювати:

- інформаційні мережі й мережеві послуги, до яких дозволений доступ;

- процедури авторизації користувачів до визначених мереж і мережних послуг;

- засоби й процедури управління захистом доступу до мережевих підключень і послуг.

Мережеві повинні створюватися таким чином, щоб забезпечувати максимальні можливості для поділу ресурсів і гнучкості маршрутизації. Ці особливості можуть також забезпечити реалізацію неавторизованого доступу до комерційних додатків, або для неавторизованого використання інформаційних засобів обслуговування. Включення заходів управління, які обмежують маршрут між користувальницьким терміналом і мережними послугами, зменшують такі ризики.

Ціль визначення і підтримки маршруту полягає в тому, щоб запобігати вибору користувачами будь-яких інших безпечних маршрутів для реалізації авторизованого здійснення доступу до послуг системи.

Розгалужені інформаційно-комунікаційні мережі, що мають велику кількість зовнішніх зв'язків, створюють достатній потенціал для неавторизованого доступу до інформаційних ресурсів мережі та її послуг. Тому, доступ віддаленими користувачами варто розглядати, як предмет обов'язкової аутентифікації. Аутентифікація віддалених користувачів може бути досягнута при використанні криптографічних методів, маркерах апаратних засобів, фільтрації або організації протоколів виклику/відповіді. Виділені приватні лінії або мережеві засоби перевірки адреси користувача можуть також використовуватися для забезпечення процесу довіри джерелу підключень.

Процедури й засоби управління зворотним викликом, наприклад, використання модемів зі зворотним викликом, можуть забезпечувати захист від неавторизованих і небажаних підключень до засобів обробки інформації організації. Цей тип контролю підтверджує право на доступ користувачів, що намагаються встановити зв'язок з мережею організації з віддалених місць.

Аутентифікація вузла може служити альтернативним засобом аутентифікації груп віддалених користувачів там, де вони приєднані до безпечного, розділеного комп'ютерного засобу.

Інформаційно-комунікаційні системи та мережі усе більше поширюються за традиційні границі організації, оскільки створюються ділові товариства, які використовують спільні інформаційні ресурси, засоби організації й обробки інформації зазначеної мережі та її послуг. Такі розширення інформаційних мереж збільшують ризик неавторизованого доступу до існуючих інформаційних систем та їх ресурсів. При таких обставинах необхідно введення засобів управління безпекою в межах безпосередньо самої мережі з метою розподілу груп інформаційних послуг, користувачів й інформаційних підсистем.

Один з методів управління безпекою інтегрованих інформаційних мереж полягає в тому, щоб розділяти їх на окремі логічні мережеві домени, наприклад, внутрішній мережевий домен організації й зовнішні мережеві домени, кожний з яких захищений певним периметром безпеки. Такий периметр може бути реалізований інсталяцією шлюзу безпеки між цими двома мережами, які повинні бути пов'язані, для управління доступом й інформаційним потоком між цими двома доменами. Цей шлюз варто конфігурувати для фільтрації трафіку між цими доменами і для блокування неавторизованого доступу відповідно до політики управління доступом організації. Приклад цього типу шлюзу – міжмережний екран (рис. 6.8).

Критерії для поділу мереж на домени варто засновувати на реалізації політики управління доступом і вимогах доступу, впливі продуктивності визначеної технології маршрутизації мереж або шлюзів.

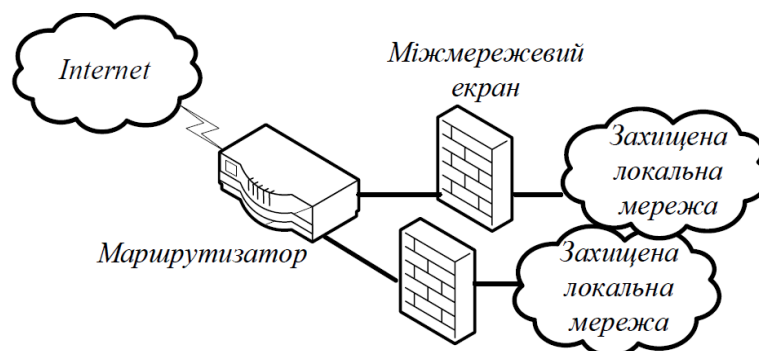


Рис. 6.8. Організація шлюзу безпеки

Вимоги політики управління доступом для розподілених мереж вимагають включення заходів управління з метою обмеження приєднання неавторизованих користувачів. Такі заходи управління можуть бути реалізовані через мережеві шлюзи, які фільтрують трафік за допомогою визначених таблиць або правил. Необхідно, щоб застосовувані обмеження ґрунтувалися на організації політики безпеки й вимогах доступу до комерційних додатків, а також підтримувалися й оновлялися відповідним чином.

Приклади додатків, до яких варто застосувати обмеження:

- електронна пошта;
- одностороння передача файлу;
- передача файлу в обох напрямках;

- інтерактивний доступ;
- доступ до мережі, пов'язаний з датою.

Розподілені мережі, особливо ті, які знаходяться в межах границь організації, можуть вимагати включення засобів управління маршрутизацією з метою підтримки політики управління доступом до комерційних додатків при додаткових приєднаннях користувачів й інформаційних потоків. Необхідно, щоб заходи управління маршрутизацією базувалися на позитивному джерелі й механізмах перевірки адрес призначення.

Сучасні інформаційно-комунікаційні системи та мережі державних або приватних організацій можуть надавати широкий спектр суспільних або приватних послуг. Мережеві послуги можуть мати унікальні або складні характеристики безпеки. Організаціям, що використовують мережеві послуги, необхідно забезпечувати впевненість у тому, що передбачається чіткий опис атрибутів безпеки всіх використовуваних послуг.

Безпека мережевих послуг – запобігання неавторизованому доступу до обчислювальної системи користувача, що встановлений з метою несанкціонованого використання або спотворення інформаційних ресурсів чи зазначених мережевих послуг.

На рівні операційної системи варто використовувати необхідні заходи безпеки для обмеження доступ до персональних інформаційних ресурсів. Необхідно, щоб ці засоби були здатні виконувати наступне:

- ідентифікацію й верифікацію ідентифікатора, і, якщо необхідно, терміналу й місця розташування кожного авторизованого користувача;
- запис успішних і невдалих доступів до системи;
- забезпечення відповідними засобами для аутентифікації;
- обмеження часу приєднання користувачів (у разі потреби).

Інші методи управління доступом, такі як *виклик-відповідь*, можуть бути використані, якщо вони виправдані з погляду ризику бізнесу.

Автоматична ідентифікація терміналу – метод реалізації процесу ініціювання сеансу авторизованих інформаційних послуг з певного місця або комп'ютерного терміналу в межах визначеної інформаційної мережі.

Ідентифікатор у терміналі, або привласнений терміналу, може використовуватися, щоб показати, чи дозволено цьому конкретному терміналу ініціювати або одержувати певні вхідні повідомлення. Може бути необхідним застосовувати фізичний захист терміналу, щоб підтримувати безпеку його ідентифікатора. Необхідно, щоб доступ до інформаційних послуг був досяжний через безпечний процес входу в систему. Процедура реєстрації в комп'ютерній системі варто розробляти так, щоб звести до мінімуму можливість неавторизованого доступу. Тому необхідно, щоб процедура реєстрації розкривала мінімум інформації про систему, щоб уникати надання непотрібної допомоги неавторизованому користувачеві.

Процедура реєстрації повинна:

- не відображати ідентифікатори системи або додатків, поки процес реєстрації не буде успішно завершений;
- відображати загальне повідомлення, яке попереджає, що доступ до системи можуть одержати тільки авторизовані користувачі;
- не забезпечувати повідомлення-підказки протягом процедури реєстрації, які допомагали б неавторизованому користувачеві отримати доступ до ресурсів;
- підтверджувати інформацію реєстрації тільки по завершенні уведення всіх вхідних даних. Якщо виникає помилковий стан, система не повинна показувати, яка частина даних є правильною або неправильною;
- обмежувати число дозволених невдалих спроб реєстрації (рекомендується три) і розглядати: запис невдалих спроб; нав'язування тимчасової затримки перш, ніж будуть дозволені подальші спроби реєстрації або відхилення будь-яких подальших спроб без спеціальної авторизації; роз'єднання приєднань до каналу передачі даних;
- обмежувати максимальний і мінімальний час, дозволений для процедури реєстрації. Якщо воно перевищено, система повинна припинити реєстрацію;
- відображати наступну інформацію щодо завершення успішної реєстрації: дату й час попередньої успішної реєстрації; деталі будь-яких невдалих спроб реєстрації, починаючи з останньої успішної реєстрації.

Унікальний ідентифікатор (користувальницький ID) повинні мати всі користувачі інформаційно-комунікаційної мережі та її ресурсів (адміністратори, адміністратори безпеки, оператори, програмісти, адміністратори баз даних, персонал технічної підтримки тощо):

- з метою особистого використання, щодо реалізації авторизованого доступу до інформаційних ресурсів та встановлених послуг;
- з метою ідентифікації дій, що згодом могли бути простежені відповідальною особою.

Користувальницький ID не повинен давати ніякої ознаки рівня привілею користувача, наприклад, менеджер, контролер тощо.

При виняткових обставинах, де є ясна ділова вигода, може використатися розділений користувальницький ID для групи користувачів або для певної роботи. Для таких випадків схвалення процедур управління варто документувати. Додаткові заходи управління можуть знадобитися для підтримки звітності.

Існують різні аутентифікаційні процедури, які можуть використовуватися для доказу заявленої ідентичності користувача. Паролі – дуже розповсюджений спосіб забезпечення ідентифікації й аутентифікації.

Пароль – один з головних засобів підтвердження повноваження користувача, що здійснює доступ до обслуговуючого комп'ютера.

Управління доступом до додатків – запобігання неавторизованому доступу до інформації та системного ПЗ, що поширюється або обробляється в інформаційних системах.

Варто використати засоби безпеки для обмеження доступу в межах системи та її додатків. Необхідно обмежувати логічний доступ до програмного забезпечення й інформації авторизованих користувачів.

Системні додатки повинні:

- управляти користувальницьким доступом до інформаційних і прикладних функцій системи відповідно до певної ділової політики управління доступом;
- забезпечувати захист від неавторизованого доступу до будь-якої утиліти та програмного забезпечення будь-якої операційної системи;
- не компрометували безпеку інших систем, з якими розділяються інформаційні ресурси;
- забезпечувати доступ до інформації тільки власникові, іншим призначеним авторизованим особам, або певним групам користувачів.

Користувачам прикладних систем, включаючи персонал підтримки, варто забезпечувати доступ до інформаційних і прикладних функцій системи відповідно до певної політики управління доступом, заснованої на вимогах окремих комерційних додатків і сумісної з організаційною політикою доступу до інформації.

Необхідно розглядати застосування таких засобів управління для підтримки вимог обмеження доступу:

- забезпечення інтерфейсу для управління доступом до прикладних функцій системи;
- обмеження знання користувачами інформаційних або прикладних функцій системи, до яких вони неавторизовані здійснювати доступ, з відповідним редагуванням користувальницької документації;
- управління правами доступу користувачів, наприклад, зчитуванням, записом, видаленням і виконанням;
- забезпечення даних виводу з функціонування прикладних систем, що обробляють чутливу інформацію, тільки інформацією, що зазначена протоколами безпеки та відсилається тільки авторизованим терміналам і місцям.

Моніторинг доступу й використання системи – процес виявлення відхилень від реалізації політики безпеки управління доступом до інформаційних ресурсів та мережних послуг з метою фіксації неавторизованих дій.

Проводити моніторинг інформаційної системи необхідно для виявлення відхилень від процесу реалізації політики безпеки управління доступом та запису контрольованих подій з метою забезпечення доказів у випадках інцидентів, що стосуються безпеки інформаційної мережі та її ресурсів. Моніторинг системи дозволяє перевіряти ефективність прийнятих заходів управління безпекою й підтверджує відповідність моделі безпеки системи зазначеній політиці доступу.

Варто створювати журнали аудиту для запису подій, пов'язаних з безпекою інформаційних ресурсів та мережних послуг, і зберігати записи протягом погодженого періоду, з метою надання допомоги в майбутніх розслідуваннях та реалізації процесу моніторингу управління доступом. **Записи аудиту повинні включати** (рис. 6.9.):

- користувальницькі ID;
- дату й час входу й виходу з системи;
- ідентифікатор терміналу або місце розташування, якщо можливо;
- запис успішних і відхилених спроб доступу до системи;
- запис успішних і відхилених даних й інших спроб доступу до ресурсів.



Рис. 6.9. Аудит інформаційної системи

Необхідно встановлювати процедури для моніторингу використання засобів обробки інформації. Такі процедури необхідні для забезпечення впевненості в тому, що користувачі виконують тільки ті дії, на які вони були явно авторизовані. Рівень моніторингу, необхідного для окремих засобів, варто визначати за допомогою оцінки ризику.

Напрями моніторингу інформаційної системи включають (рис. 6.10):

Авторизований доступ містить:

- користувальницький ID;
- дату й час головних подій;
- типи подій;
- файли, до яких був здійснений доступ;
- використовувані програми/утиліти.

Усі привілейовані дії, такі як:

- використання облікового запису супервізора;
- запуск й зупинка системи;
- приєднання/від'єднання пристрою введення/виводу.

Спроби неавторизованого доступу:

- невдалі спроби;

- порушення політики доступу й повідомлення мережних шлюзів і міжмережних екранів;
- попередження від власних систем виявлення вторгнення.
- попередження або відмови системи:
- консольні (термінальні) попередження або повідомлення;
- виключення, записані в системні журнали реєстрації;
- попереджувальні сигнали, пов'язані з керуванням мережею.

Варто регулярно розглядати результат дій по моніторингу системи. Необхідно, щоб частота огляду залежала від передбачуваних ризиків.

Фактори ризику, які необхідно розглядати, включають:

- критичність процесів додатків;
- цінність, чутливість або критичність пов'язаної інформації;
- минулий досвід проникнення в систему й неправильне використання системи;
- ступінь взаємозв'язку систем (особливо загальнодоступних мереж).



Рис. 6.10. Напрями моніторингу інформаційної системи

Перегляд журналу реєстрацій має на увазі фіксацію та подальше розуміння причин й сутності появи загроз, з якими зіштовхується система, і способу їхнього виникнення. Журнал реєстрацій також повинен містити приклади подій, які могли б зажадати подальшого дослідження у випадку інцидентів, що стосуються безпеки мереж.

Системні журнали реєстрації часто містять великий обсяг інформації, більша частина якої є далекою від процесу моніторингу безпеки. Щоб допомогти ідентифікувати значні події з метою проведення моніторингу безпеки, необхідно розглядати автоматичне копіювання відповідних типів повідомлень у другий журнал, а також використання підходящих системних утиліт або інструментів аудита, щоб підготувати файл опитування.

Безпека прикладних систем – запобігання втраті, модифікації або неправильному використанню користувальницьких даних у прикладних системах.

Відповідні засоби управління й журнали аудиту, які відображають діяльність системи щодо поширення інформації та її обробки, повинні бути внесені в роботу прикладної системи, включаючи додатки написані користувачем. Додатки повинні включати підтвердження вхідних даних, а також даних внутрішньої обробки й вихідних даних.

Дані, які були введені правильно, можуть бути спотворені внаслідок помилок, пов'язаних з обробкою, або навмисних несанкціонованих дій. Проведення та підтвердження проведення процедур перевірок необхідно включати в процес стандартного функціонування системи з метою виявлення й локалізації перекручувань та несанкціонованого відтворення даних. Необхідно, щоб структура додатків також забезпечувала реалізацію мінімуму ризику появи відмов в системі, що можуть призвести до втрати цілісності системи та безпосередньо до втрати інформації.

Безпека прикладних систем повинна включати:

- використання й розміщення в програмному забезпеченні системи функцій додавання й видалення, з метою виявлення та запобігання змінам у даних;
- процедури для запобігання впровадженню програмного забезпечення із спотвореними командами, або виконання процедур обробки даних системи після їх ушкодження на етапах попередньої обробки;
- використання коригувальних програм з метою відновлення інформаційного потоку даних після відмов системи, а також з метою забезпечення подальшої правильної обробки даних.

Ауθενфікація повідомлень – метод, що використовується для виявлення неавторизованих змін або спотворень змісту переданого інформаційного повідомлення.

Ауθενфікація повідомлень може бути реалізована в апаратних засобах або програмному забезпеченні, що підтримують фізичний пристрій ауθενфікації повідомлень або програмний алгоритм.

Ауθενфікацію повідомлення необхідно розглядати для додатків, де є вимога безпеки щодо захисту цілісності змісту повідомлення, наприклад: електронні передачі фондів, специфікацій, контрактів, пропозицій і т.п., або інші подібні електронні обміни даних.

Ауθενфікація повідомлень може включати:

- перевірки вірогідності вихідних даних та отримання підтвердження на їх прийняття;
- одержання та узгодження контрольних підрахунків на всіх етапах обробки даних системи;
- забезпечення достатньої кількості інформації щодо визначення достовірності, закінченості, точності і класифікації інформації, що представлена користувачу або наступній системі для подальшої обробки;

- процедури відповідей системи на зазначені тести з метою підтвердження вихідних даних та їх виходу;
- визначення обов'язків усього персоналу, залученого в процесі виводу даних.

Управління криптографічними заходами – процес захисту конфіденційності, доступності і цілісності інформації, а також встановлених мережних послуг на базі криптографічних методів та алгоритмів з метою запобігання несанкціонованому втручанню або змінам.

Криптографічні системи й методи використовуються для захисту інформаційних ресурсів та мережних послуг, що піддаються ризику у разі, якщо інші заходи і методи захисту не є адекватними.

Ухвалення рішення щодо ефективності впровадження криптографічних методів та засобів у конкретну систему, варто розглядати, як частину більш широкого процесу визначення загальної оцінки ризиків всієї інформаційної системи. Необхідно виконувати оцінку ризику для визначення та забезпечення відповідного рівня захисту інформаційних ресурсів та послуг системи. Ця оцінка повинна бути адекватною для визначення того, чи є криптографічний засіб ефективний, який тип управління варто застосовувати, для якої мети і яких бізнес-процесів.

Організація повинна розробляти власну політику використання криптографічних методів і засобів для захисту її інформації та послуг. Політика використання криптографічних методів і засобів впроваджується з метою досягнення максимуму соціального чи фінансового зросту підприємства й зведення до мінімуму ризиків.

Політика використання криптографічних методів і засобів повинна містити такі напрями:

1. Єдиний підхід до використання криптографічних методів і засобів захисту інформаційних ресурсів та послуг у всій організації, включаючи загальні принципи.

2. Єдиний підхід до управління ключами, включаючи методи, що мають справу з відновленням зашифрованої інформації у випадку втрати, компрометації або ушкодження ключів.

3. Ролі, обов'язки та відповідальність за:

3.1. реалізацію політики;

3.2. реалізацію процесу управління ключами;

3.4. визначення відповідного рівня криптографічного захисту;

3.5. визначення відповідної оцінки ефективності використання впровадженого рівня криптографічного захисту;

3.6. єдині стандарти та норми криптографічного захисту, прийняті для ефективної реалізації у всій організації (які рішення використовуються і для яких бізнес-процесів).

При реалізації криптографічної політики організації необхідно враховувати стандарти, нормативні документи, правила й національні обмеження, які могли б застосовуватися при використанні

криптографічних методів у різних географічних зонах. Також враховуються питання, що стосуються потоку зашифрованої інформації, переданої через границю держави. Крім того, варто розглядати заходи управління, застосовувані до експорту й імпорту криптографічної технології.

Цифровий підпис – захід управління інформаційною безпекою, що забезпечує захист доступності й цілісності електронних документів інформаційної системи.

Цифрові підписи можуть застосовуватися для будь-якої форми документа, оброблюваного електронним способом, наприклад, вони можуть використовуватися для підписання електронних платежів, при передачі фондів тощо. Цифрові підписи можуть бути реалізовані при використанні криптографічного методу, що ґрунтується на унікально пов'язаній парі ключів, де один ключ використовується, щоб створювати підпис (особистий ключ), а інший – щоб перевіряти підпис (відкритий ключ).

Варто приділяти увагу типу і якості використовуваного алгоритму підпису й довжині ключів, які повинні бути використані. Необхідно, щоб криптографічні ключі, використововувані для цифрових підписів, відрізнялися від тих, які використали для шифрування загального інформаційного потоку.

При використанні цифрових підписів необхідно розглядати будь-яке відповідне законодавство, що описує умови, при яких цифровий підпис є юридично обов'язковою процедурою захисту інформації.

Будь-яка компрометація або втрата криптографічних ключів може привести до порушення конфіденційності, доступності й/або цілісності інформації та мережних послуг.

Управління криптографічними ключами повинно включати:

- методи із секретними ключами, де дві або більше сторони розділяють той же самий ключ і цей ключ використовується як для шифрування, так і розшифрування інформації. Цей ключ повинен зберігатися в секреті згідно з нормативами організації;

- методи з відкритими ключами, де кожен користувач має пару ключів, відкритий ключ (який має вільний доступ) і особистий ключ (який повинен зберігатися в секреті). Методи з відкритими ключами можуть використовуватися для шифрування і для створення цифрових підписів.

Всі ключі необхідно захищати від модифікації й руйнування, а секретним й особистим ключам необхідний захист від неавторизованого розкриття. Необхідно, щоб система управління ключами ґрунтувалася на погодженій безлічі стандартів, процедур і безпечних методах для:

- формування ключів для різних криптографічних систем і різних додатків;

- формування та одержання сертифікатів з відкритим ключем;

- розподілу ключів призначеним користувачам, включаючи процедури активізації ключів, коли вони отримані;

- зберігання ключів та одержання доступу до ключів авторизованими користувачами;
- зміни або відновлення ключів, включаючи правила змін;
- обігу зі скомпрометованими ключами;
- анулювання ключів, зокрема процедуру вилучення й активізації ключів, наприклад, коли ключі були скомпрометовані, або коли користувач покинув організацію (у кожному випадку ключі необхідно також архівувати);
- відновлення ключів, які загублені або зіпсовані, як частина процесу управління безперервністю бізнесу, наприклад, для відновлення зашифрованої інформації;
- архівування ключів, наприклад, для архівіруваної або відновленої інформації;
- руйнування ключів;
- реєстрації й аудитів дій, пов'язаних з управлінням ключем.

Для зменшення ймовірності компрометації ключів криптосистеми необхідно, щоб ключі мали певні дати активізації й дезактивізації з умов часу обмеженого використання.

Управління цілісністю системного програмного забезпечення – організація захищеного процесу функціонування інформаційної системи, пов'язаного із збереженням достовірності і повноти системного програмного забезпечення та його захистом від несанкціонованих модифікацій.

Управління операційним програмним забезпеченням – процес досягнення мінімуму ризику щодо руйнування або модифікації операційних систем, який повинен забезпечити:

- відновлення бібліотек операційних програм тільки авторизованим користувачем (бібліотекарем програм);
- функціонування операційної системи на базі тільки зазначеного програмного продукту;
- виконання додаткових програм, тільки після підтвердження успішного тестування з умов, що не були оновлені відповідні бібліотеки джерел програмного забезпечення;
- обов'язкову реєстрацію відновлення бібліотек операційних програм в журналі аудиту;
- зберігання попередніх версій програмного забезпечення.

Для захисту операційних даних, що використовуються для задач тестування необхідно застосовувати такі заходи управління безпекою (рис. 6.11):

- процедури управління доступом, що застосовуються для операційних прикладних систем, варто застосовувати й до прикладних систем тестування;
- необхідно, щоб окрема авторизація мала місце щораз, коли операційна інформація копіюється для прикладної системи тестування;
- після того, як випробування закінчене, операційну інформацію варто негайно видаляти із прикладної системи тестування;
- копіювання й використання операційної інформації необхідно реєструвати, щоб забезпечувати визначені процедури аудиту.

Управління доступом до програмних бібліотек вводить з метою зменшення ризику щодо можливостей спотворення програмних продуктів системи, а також підтримки строгого контролю доступу до вихідних бібліотек програмного забезпечення, а саме:

- вихідні бібліотеки програм не слід зберігати в операційних системах;
- необхідно, щоб призначався адміністратор бібліотек програмного забезпечення для кожного додатка;
- персоналу підтримки інформаційних технологій не слід надавати необмежений доступ до вихідних бібліотек програм;
- програми, що перебувають у процесі розробки або супроводі, не слід зберігати в бібліотеках джерел операційного програмного забезпечення;
- відновлення бібліотек і забезпечення програмістів вихідними текстами програмних продуктів необхідно здійснювати тільки призначеному адміністратору бібліотек після авторизації;
- лістинг програм необхідно зберігати в безпечному середовищі;
- треба підтримувати журнал аудитів всіх доступів до вихідних бібліотек;
- старі версії вихідних текстів програм необхідно архівувати, з ясною вказівкою точних дат і часу, коли вони були експлуатаційними, разом з усім програмним забезпеченням підтримки, управлінням роботою системи, визначенням даних і процедур;
- введення й копіювання вихідних бібліотек необхідно впроваджувати з строгими процедурами управління змінами.

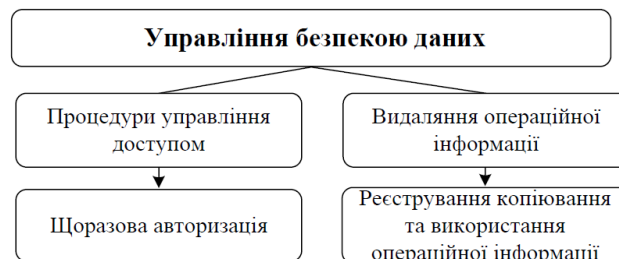


Рис. 6.11. Заходи управління безпекою даних ОС

- Процедури управління змінами операційної системи повинні містити:
- підтримку запису про погодження рівнів авторизації;
 - внесення змін авторизованими користувачами;
 - перегляд засобів контролю й процедур цілісності;
 - ідентифікацію всього програмного забезпечення, даних, компонент баз даних й апаратних засобів;
 - одержання офіційного схвалення для детальних пропозицій перед початком роботи операційної системи;
 - забезпечення того, щоб сукупність документації по системі обновлялася після завершення кожної зміни;
 - підтримку управління версією для всіх відновлень програмного забезпечення;
 - підтримку журналу аудиту для всіх запитів змін;
 - забезпечення вчасного проведення реалізації змін.

Управління безперервністю бізнесу – процес протидії несанкціонованим перериванням дій бізнесу та процес захисту процедур критичних бізнес-процесів. Процес управління безперервністю бізнесу варто реалізовувати для зменшення руйнувань, викликаних нещастями й відмовами систем безпеки (які можуть бути результатом, наприклад, природних нещасть, нещасних випадків, відмов устаткування, навмисних дій тощо), та доведенням їх до визначеного рівня за допомогою комбінування профілактичних заходів та заходів управління відновленням. Необхідно, щоб процес управління безперервністю бізнесу включав заходи ідентифікації загроз й зменшення ризиків, обмеження наслідків руйнівних інцидентів і забезпечення своєчасного поновлення основних дій системи.

Ключові елементи управління безперервністю бізнесу:

- оцінка ризиків організації, з погляду їхньої ймовірності і їхніх впливів, включаючи ідентифікацію й призначення пріоритетів критичних процесів бізнесу;
- визначення переліку впливів, що можуть призвести до переривання бізнесу;
- забезпечення страхування бізнесу;
- формулювання й документування стратегії безперервності бізнесу, сумісної з погодженими бізнес-проектами й пріоритетами;
- формулювання й документування планів безперервності бізнесу відповідно до погодженої стратегії;
- регулярне тестування та відновлення планів й існуючих процесів;
- включення управління безперервністю бізнесу до процесів й структури організації.

Необхідно, щоб безперервність бізнесу починалася з ідентифікації подій, які можуть бути причиною переривання бізнес-процесів, наприклад, відмови устаткування, поведінки або пожежі. Потрібно, щоб це супроводжувалося відповідною оцінкою ризику та визначало вплив цих переривань (як з погляду масштабу ушкодження, так і періоду відновлення). Всі ці дії необхідно виконувати з повною участю власників бізнес-ресурсів і процесів. Ця оцінка повинна розглядати всі бізнес-процеси і не обмежуватися засобами обробки інформації. Залежно від результатів оцінки ризику, варто розробляти план стратегії, щоб визначати звичайний підхід до безперервності бізнесу. Необхідно розробляти плани по підтримці або відновленню бізнес-операцій у необхідні масштаби часу після переривання або відмови критичних бізнес-процесів (рис. 6.12).

Процес планування безперервності бізнесу містить наступне:

- ідентифікацію й узгодження всіх обов'язків і надзвичайних заходів;
- реалізацію надзвичайних заходів з метою регенерації й відновлення в межах необхідного масштабу часу.

Необхідно, щоб процес планування зосереджував на необхідних бізнес-проектах, наприклад, на відновленні певних послуг клієнтам у прийнятний проміжок часу. Варто розглядати послуги й ресурси, які роблять це можливим, включаючи укомплектування персоналом,

неінформаційну обробку ресурсів, а також заходи щодо нейтралізації несправностей для засобів обробки інформації. Варто підтримувати єдину структуру планів по безперервності бізнесу, щоб забезпечувати їх послідовність і ідентифікувати пріоритети для тестування й обслуговування. Необхідно, щоб кожен план по безперервності бізнесу чітко визначав умови його активізації, а також осіб, відповідальних за виконання кожного компонента плану.



Рис. 6.12. Заходи управління безперервністю бізнесу

Методи управління безперервністю бізнесу повинні містити (рис. 6.13):

- високий рівень перевірки різних сценаріїв бізнес-процесів;
- моделювання бізнес-процесів;
- перевірку технічного відновлення інформаційних систем;
- перевірку відновлення на певних місцях використання;
- перевірки засобів обслуговування й послуг постачальника;
- детальні репетиції (які перевіряють, що організація, персонал, устаткування, засоби обслуговування й процеси можуть справлятися з перериваннями).



Рис. 6.13. Система методів управління безперервністю бізнесу

Запитання для самоконтролю

1. Дайте визначення інформації з точки зору бізнес-процесів.
2. Які основні принципи організації ТЗІ у ІКСМ?
3. Через які канали спеціальних впливів можлива реалізація загроз для інформації у ІКСМ?
4. Що таке якісна недостатність компонентів системи ТЗІ?
5. Що таке сертифікований канал можливої реалізації загроз для інформаційних ресурсів ІКСМ?
6. Введіть поняття база захисту ІКСМ.
7. Що таке тест на проникнення?
8. Викладіть зміст і послідовність робіт з протидії загрозам інформаційним ресурсам та їх нейтралізації у ІКСМ.
9. У чому полягає розробка технічної політики безпеки (ПБ)?
10. Що складає зміст технічного завдання на розробку системи ТЗІ?
11. Надайте характеристику процесу розробки моделі захисту.
12. Надайте характеристику процесу розробки комплексу засобів та механізмів захисту (КЗМЗ).
13. Яким чином впроваджується технічна політика безпеки?
14. Яким чином підтримується політика безпеки?
15. Опишіть структуру стандарту ISO/IEC 17799.
16. Дайте визначення політиці інформаційної безпеки з точки зору стандарту.
17. Назвіть основні заходи щодо захисту від шкідливого програмного забезпечення.
18. У чому полягає процедура забезпечення безпеки інформаційних мереж?
19. Назвіть основні заходи управління безпекою електронної торгівлі.
20. Опишіть процедуру організації управління доступом.
21. Що має включати політика безпеки та які існують заходи її впровадження з урахуванням забезпечення процедур управління доступом?
22. Що повинно входити до офіційної процедури реєстрації користувача?
23. У чому полягає автоматична ідентифікація терміналу?
24. У чому полягає моніторинг інформаційної системи?
25. Назвіть основні заходи забезпечення конфіденційності інформації згідно з стандартом.
26. Що таке цілісність системного програмного забезпечення?
27. Введіть поняття «управління безперервністю бізнесу».

СПИСОК ЛІТЕРАТУРИ

1. Алишов Н.И. Организации безопасности информационных ресурсов в системах телекоммуникаций // Праці 4-ї Міжнародної науково-технічної конференції по телекомунікаціям —Телеком-99. – Одеса, 1999. – С. 112-115.
2. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учеб. пособие. – М.: Гелиос АРВ, 2002. – 480 с.
3. Анин Б. Защита компьютерной информации. — СПб.: БХВ-Петербург, 2000. – 384 с.
4. Бабак В.П., Теоритичні основи захисту інформації : Підручник. – К.: НАУ, 2008. – 752 с.
5. Бабак В.П., Корченко О.Г. Інформаційна безпека та сучасні мережеві технології: Англо-українсько-російський словник термінів / – К.: НАУ, 2003. – 670 с.
6. Бабаш А. В., Шанкин Г. П. Криптография. - М.: СОЛОН-Р, 2002. - 512 с.
7. Бабишев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии: Учеб. курс. – М.: Горячая линия – Телеком, 2002. – 175 с
8. Баранов В.Л. Використання системноаналогових обчислювальних структур для адаптивної маршрутизації / Баранов В.Л., Мартинова О.П., Данилівна Г.В., Подлесних Є.Г. Гончарова Л.Л. / Науково-технічний журнал. Інформаційно-керуючі системи на залізничному транспорті. – 2008. – № 1, – С. 24-28.
9. Богущ В.М., Юдін О.К. Інформаційна безпека держави: Навч. посібник. – К.: МК – Прес, 2005. - 432 с.
10. Богущ В. М., Кусин А. М. Інформаційна безпека від А до Я. – К.: МОУ, 1999.–456 с.
11. Бойченко Е.В., Кальфа В., Овчинников В.В. Локальные вычислительные сети. - М., Радио и связь, 2003. - 304 с.
12. Блэк Ю. Сети ЭВМ: протоколы, стандарты, интер-фейсы. М.: Мир, 2002.
13. Бородин Г. А. Коды для полупроводниковых ЗУ, исправляющие однократную и обнаруживающие многократную ошибку // Зарубежная радиоэлектроника. – 1988. – №4. — С. 38 – 56.
14. Баричев С. Криптография без секретов. - М.: Радио и связь 1995 – 204 с.
15. Баричев С. Серов Р. Основы современной криптографии. – М.: ЗАО «Издательство БИНОМ», 2003. – 152с.
16. Бугрименко Д. Многоуровневый модульный дизайн современных безопасных ЛВС с высокой доступностью. – М.:CiscoExpo2006, 2006 – 85с.
17. Бугрименко Д. Многоуровневый модульный дизайн современных безопасных ЛВС с высокой доступностью. – М.:CiscoExpo2006, 2006 – 85с.
18. Бугрименко Д. Технологии виртуализации корпоративных ЛВС. - М.:CiscoExpo2006, 2006 – 74с.
19. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам: Учеб. пособие. – М.: Горячая линия – Телеком, 2005. – 416 с.
20. Бунин С.Г., Войтер А.П. Вычислительные системы с пакетной радиосвязью. – Киев: Техніка, 1989. – 223 с.
21. Вайнштейн А. Основы теории информации. Пер з англ. - М.: 1960. – 360 с.
22. Владимиров А.А. «Wi-фу: боевые приемы взлома и защиты беспроводных сетей. - НТ Пресс, 2005. – 464 с.
23. Высокопроизводительные сети. Энциклопедия пользователя. Марк А. и др.; перев. с англ. – Киев, ДиаСофт, 2003. – 300 с.
24. Гайкович В.Ю., Ершов Д.В. Основы безопасности информационных технологий: Учеб. пособие. – М.: МИФИ, 1995. – 252 с.
25. Гайкович В., Перший А. Безопасность электронных банковских систем. — М.: Изд-во Компания «Единая Европа», 1994. — 363 с.
26. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. – М.: Энергоатомиздат, 1994, Кн.1 и 2.
27. Герасименко В.А., Малюк А.А. Основы защиты информации: Учеб. пособие. – М.: МГИФИ, 1997. – 538 с.
28. Глобус И.А. Легко реализуемые корректирующие коды для совмещенных систем траекторного управления и передачи данных. //Вопросы радиоэлектроники, сер. ОТ, 1977. вып. 8, — С. 32.
29. Голубев В. О. Программно-технічні засоби захисту інформації від комп'ютерних злочинів. – Запоріжжя, 1988. – 144 с.

30. Гончарова Л.Л. Комп'ютерні методи організації мікропроцесорних систем контролю і прогнозу залишкового ресурсу енергетичних об'єктів / Гончарова Л.Л. // Збірник наукових праць. «Моделювання та інформаційні технології», Інститут проблем моделювання в енергетиці – 2009. – № 53 – С. 103-108
31. Гончарова Л.Л. Информационные технологии мониторинга режимов электрических сетей на основе дифференциальных Т-моделей. / Гончарова Л.Л. // Научно-технический журнал. Информационно-управляющие системы на железнодорожном транспорте. – 2009. – № 4 – С. 93-97
32. Гончарова Л.Л. Современные методы компьютерного анализа режимов функционирования сложных электрических объектов. / Гончарова Л.Л. // 36. науч. праць. ІПМЕ НАН України – Вип.56. – К: - 2010. С. 17– 24.
33. Гончарова Л.Л., Максимчук В.Ф., Стасюк А.И. Методи організації комп'ютерної мережі моніторингу параметрів режимів систем електропостачання/ Інформаційно-керуючі системи на залізничному транспорті, науково-технічний журнал, № 2, 2012 –С.35 – 40.
34. Логинов В.В. Обеспечение информационной безопасности средствами IBM S/390 // Экономика и производство, 1999, № 3.
35. ГОСТ 34.311-95 Информационная технология. Криптографическая защита информации. Функция хеширования.
36. ГОСТ 28127-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.
37. Дев'янін П.Н. та інші, Теоретичні основи комп'ютерної безпеки: посібник для ВУЗів. -М.: Радіо та зв'язок, 2000.
38. Дей Д.Д., Зиммерман Ю. Эталонная модель взаимосвязи открытых систем (ВОС)// ТИИЭР. – 1983. – Том 71, № 12. – С. 8-16.
39. Джим Гейер Беспроводные сети.Первый шаг. — СПб.:Вильямс, 2005. — 189 с.
40. Джон Росс. Wi-Fi. Беспроводные сети. Установка. Конфигурирование. – СПб.:ИТ Пресс, – 2006.
41. Диффи У., Хеллман М. Защищенность и имитостойкость: Введение в криптографию. // ТИИЭР, 1979, т. 67, № 3. - С. 71-109.
42. Дмитриев В.В. Прикладная теория информации. – М.: Высшая школа. 1988. – 320 с.
43. Домарев В.В.. К.: ООО —ТИД —ДС, 2001. – 681 с. Часть V. Решения и средства защиты информации. С. 528 –533.
44. Домарев В.В. Безопасность информационных технологий. Системный подход. – К.: ООО «ТИД «ДС», 2004. – 992 с.
45. Дронь М.М., Малайчук В.П., Петренко О.М. Основы теории защиты информации: Навч. посібник. – Д.: Вид-во Дніпропетр. ун-ту, 2001. – 312 с.
46. ДСТУ 3396.0-96 - Захист інформації. Технічний захист інформації. Основні положення;
47. ДСТУ 3396.1-96 - Захист інформації. Технічний захист інформації. Порядок проведення робіт;
48. ДСТУ 3396.2-97 - Захист інформації. Технічний захист інформації. Терміни і визначення;
49. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. – К. Державний комітет України з питань технічного регулювання та споживає політики, 2003. – 31с.
50. Закон України «Про державну таємницю».
51. Закон України «Про захист інформації в автоматизованих системах».
52. Закон України «Про інформацію».
53. Закон України «Про основи національної безпеки України».
54. Закон України «Про електронний цифровий підпис»
55. Закон України «Про електронні документи та електронний документообіг»
56. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000. – 452 с.
57. Зегжда Д. П., Ивашко А. М. Как построить защищенную информационную систему: Технология создания безопас-ных систем. Том 2. — СПб: НПО «Мир и семья -ООО «Интерлайн», 1998. – 256 с.
58. Зима В., Молдовян А., Молдовян Н. Безопасность глобальных сетевых технологий. —СПб.: БХВ-Петербург, 2001. - 320 с.
59. Зима В., Молдовян А.,Многоуровневая защита информационно-програмного обеспечения. — ВККА им. Можайс-кого.: – Петербург, 2000. - 104 с.
60. Игнатов В.А. Теория информации и передачи сигналов. – М.: Рад. радіо, 1979.–280 с.

61. Інформаційна безпека та сучасні мережеві технології: Англо-українсько-російський словник термінів / В.П.Бабак, О.Г.Корченко. – К.: НАУ, 2003. – 670 с.
62. Карасик И. Г. Программные и аппаратные средства защиты информации для персональных компьютеров//Компьютер-пресс. 1992. №3. С. 37-46.
63. Касперски Крис. Защита беспроводных сетей // Журнал Mobi - №8 – К.: 2005. – С. 36-45.
64. Кларк Дж., мл., Кейн Дж. Кодирование с исправлением ошибок в системах цифровой связи // Пер. с англ.; Под ред. В. Герасименко. – М.: —Радио и связь, 1987. – 397 с.
65. Коженевський С.Р., Кузнецов Г.В., Хорошко В.О., Чирков Д.В. Термінологічний довідник з питань технічного захисту інформації/ за ред. Проф. В.О. Хорошка - К. ДУІКТ, 2007 - 365 с.
66. Колмогоров А.Н. Теория информации и теория алгоритмов. М.: —Наука, 1987. 304 с.
67. Конеев И. Р., Беляев А. В. Информационная безопасность предприятия. — СПб.: БХВ-Петербург, 2003. - 752 с.
68. Конахович Г.Ф., Климчик В.П., Паук С.М., Потапов В.Г. Защита информации в телекоммуникационных системах. – К.: МК – Пресс, 2005. – 288 с.
69. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография: Теория и практика. – К.: МК – Пресс, 2006. – 288 с.
70. Конахович Г.Ф., Пузыренко А.Ю., Голубничий О.Г. Оцінка ефективності систем захисту інформації в телекомунікаційних системах. Проблеми інформатизації та управління: Збірник наукових праць. – К.: НАУ, 2009. – Вип.3 (72). – С.75-83.
71. Корченко А.Г. Построение систем защиты информации на нечётких множествах. Теория и практические решения. — К.: «МК-Пресс», 2006. — 320 с.
72. Коцюбинский А.О., Грошев С.В. Современный самоучитель работы в сети Internet. - М.: Триумф, 2003 - 464 с.
73. Крейг Хант. Персональные компьютеры в сетях TCP/IP. – К.: BHV .2001. – 384 с.
74. Кузнецов П. А. Информационная война и бизнес. – Конфидент, 1996, №4, с. 21-24.
75. Кузьмин И.В., Кедров В.А. Основы теории информации и кодирования: Учебник. – К.: Вища школа, 1986. - 238 с.
76. Кунегин. С.В. Системы передачи информации. Курс лекций. М., в/ч 33965, 1997, - 317 с., с ил.
77. Куликовский Л.Ф., Мотов В.В. Теоретические основы информационных процессов: Учеб. пособие для вузов. — М.: «Высшая школа», 1987. — 248 с.
78. Курзанцева Л.И. О применении агентной технологии при создании интеллектуального пользовательского интерфейса – Комп'ютерні засоби, мережі та системи. 2003, № 2. – с. 15-24.
79. Левин В.К., Гайкович В.Ю., Дорошкевич П.В. и др. Информационная безопасность компьютерных сетей// Технологии электронных коммуникаций. – М. 1993. т.5.–128 с.
80. Леонов С.Ю., Гладких Т.В., Загарій Г.І, Стасюк О.І. / Автоматизоване проектування складних систем у комп'ютерній системотехніці, Частина 1, Харків, ПП видавництва «Нове слово», 2012. с.288.
81. Лукацкий А. Обнаружение атак. — СПб.: БХВ-Петербург, 2001. — 624 с.
82. М.В. Гаранин, В.И. Журавлев, С.В. Кунегин. Системы и сети передачи информации – М.: Радио и связь, 2001.–336 с.: ил.
83. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации: Учеб. пос. – М.: Горячая линия – Телеком, 2004. – 280 с.
84. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах: Учеб. пос. – М.: Горячая линия - Телеком, 2005. – 147 с.
85. Мамиконов А.Г. и др. Достоверность и резервирование информации в АСУ. – М.: Энергоиздат, 1986. – 304 с.: ил.
86. Мамиконов А.Г. Основы построения АСУ. – М.: Высш. школа, 1981. – 248 с.: ил.
87. Мафтик С. Механизмы защиты в сетях ЭВМ – М.: Мир, 1993. –300 с.
88. Медведовский И. Д., Семьянов П. В., Леонов Д. Г. Атака на Internet. — 2-е изд. — М.: ДМК. 1999. - 336 с.
89. Михайлов С.Ф., Петров В.А., Тимофеев Ю.А. Информационная безопасность. Защита информации в автоматизированных системах. Основные принципы: учебное пособие, – М.: МИФИ, 1995, –112 с.
90. Михайлов С.Ф., Петров В.А., Тимофеев Ю.А. Информационная безопасность. Защита информации от несанкционированного доступа в автоматизированных системах. Основные концепции: Учеб. пособие. – М.: МИФИ, 1995. – 182 с.

91. Миано Дж. Форматы и алгоритмы изображений в действии. Учеб. Пособ. – М.: Издательство Триумф, 2003 – 336 с.
92. Моисеев Д. Безопасность в компьютерных сетях. Microsoft Internet Security Framework: протоколы SSL и PCT. На сайті <http://www.osp.ru/os>
93. Молдовян А.А., Молдовян Н.А., Советов Б.Я. Крипто-графия. – С.-Пб.: Изд-во Лань, 2000. – 218 с.
94. Молдовян Н. А. Проблематика и методы криптографии. СПб.: Изд-во СПбГУ, 1998. 245 с.
95. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: Введ. —28 квітня 1999 р. № 22.
96. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу
97. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу
98. НД ТЗІ 3.7-002-99 - Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінки захищеності інформації (базова).
99. НД ТЗІ 2.5-001-99 - Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації функціональних послуг захисту.
100. НД ТЗІ 2.5-002-99 - Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації гарантій захисту.
101. НД ТЗІ 2.5-003-99 - Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації довірчих оцінок коректності реалізації захисту.
102. НД ТЗІ 2.7-001-99 - Технічний захист інформації на програмно-керованих АТС загального користування. Порядок виконання робіт.
103. Основы криптографии / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. - М.: Гелиос АРВ, 2001. - 480 с.
104. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы технология, протоколы. - СПб.: Издательский дом —Питер: 2001. - 672 с.
105. Олифер В. Г., Олифер Н. А. Сетевые операционные системы. СПб., 2001 -544 с.
106. Педжман Р., Джонатан Л. Основы построения беспроводных локальных сетей стандарта 802.11. — СПб.:Вильямс, 2004 -302 с.
107. Петраков А.П. Основы практической защиты информации: Учеб. пособие. – М.: Радио и связь, 2000. – 368 с.
108. Петров В.А., Пискарев А.С., Шеин А.В. Информационная безопасность. Защита информации от несанкционированного доступа в автоматизированных системах: Учеб. пособие. – М.: МИФИ, 1995. – 396с.
109. Петров А. А. Компьютерная безопасность. Криптографические методы защиты.- М.: ДМК.2000.- 448 с.
110. Пролетарский А. В., Баскаков И. В., Чирков Д. Н. Беспроводные сети Wi-Fi. – Интернет-университет информационных технологий - ИНТУИТ.ру, БИНОМ. Лаборатория знаний, 2007. – 216 с.
111. Проскурин В. Г., Крутое С. В., Мацкевич И. В. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах. — М.: Радио и связь, 2000. — 168 с.
112. Процкевич А.А., Яковишин В.С. Форма хранения и передачи кодированных знаний.// Комплексная защита информации - Вып. 2 – Минск: Ин-т техн. кибернетики НАН Беларуси, 1999. - С.95-103.
113. Пятибратов А.П., Гудыно Л.П., Кириченко А.А. Вычислительные системы, сети и телекоммуникации: Учебник для вузов по специальности — Информационные системы в экономике" / Под ред. А. П. Пятибратова. - М.: Финансы и статистика, 2002 - 398с.: ил.
114. Романец Ю. В. и др. Защита информации в компьютерных системах и сетях. Под ред. В.Ф. Шаньгина. - М.: Радио и связь, 1999. - 388 с.
115. Саломеа А. Криптография с открытым ключом. — М.: Мир, 1995. — 318 с.
116. Скляр Б. Цифровая связь. Теоретические основы и практическое применение / Пер. с англ. – М.: Изд. дом Вильямс, 2004. – 1104 с.
117. Соболева Т. А. Тайнопись в истории России. М.: Междунар. отношения, 1994. 382 с.
118. Соколов А.В., Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах. – М.: ДМК Пресс, 2002. – 656 с.

119. Соловьев Ю. П. Рациональные точки на эллиптических кривых. – Соросовский образовательный журнал, № 10, 1997.
120. Спесивцев А. В., Вегнер В. А., Крутяков А. Ю. Защита информации в персональных – М.: Радио и связь, 1992. – 192 с.
121. Стратонович Р.Л. Теория информации. М.: —Сов. Радио||. 1975, 424. с.
122. Супутникові системи авіаційного зв'язку / В.П. Харченко, С.М. Паук, Л.М. Нестерова, Є.А. Знаковська. — К.: НАУ, 2003. — 188 с.
123. Темников Ф.Е., Афонин В.А., Дмитриев В.И. Теоретические основы информационной техники: Учеб. пособие. – М.: Энергия, 1979. – 512 с.
124. Теоретические основы компьютерной безопасности / П. Н. Девянин, О. О. Михальский, Д. И. Правиков, А. Ю. Щербаков. — М.: Радио и связь, 2000. — 192 с.
125. Тимошенко А. О. Методи аналізу та проектування систем захисту інформації: Курс лекцій. — К.: Політехніка, 2007. — 174 с
126. Фергюсон Н., Шнайер Б. Практическая криптография.: Пер. С англ. – М.: Издательский дом «Вильямс», 2005. – 424 с.
127. Хемминг Р.В. Теория кодирования и теория информации. Пер. с англ. М.: —Радио и связь, 1983.
128. Хетагуров Д.А., Руднев Ю.П. Повышение надежности цифровых устройств методами избыточного кодирования. – М.: —Энергия, 1974. – 290 с.
129. Ховард М., ЛебланкД. Защищенный код / Пер. с англ. — М.: Издательско-торговый дом «Русская редакция», 2003. — 704 с.
130. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации. К.: Изд – во Юниор, 2003. – 504 с.
131. Хоффман Л.Дж. Современные методы защиты информации /Пер. с англ. – М.: Сов. радио, 1980. – 480 с.
132. Шеннон К. Математическая теория связи. В кн.: К. Шеннон. Работы по теории информации и кибернетике. Пер. з англ. М.: 1963, ил.
133. Шеннон К.. Теория связи в секретных системах/ Работы по теории связи и кибернетике. Пер. с англ. – М.: Иностр. литер., 1963. – 498 с.
134. Шеховцов В. А. Операційні системи — К.: Видавнича група BVH, 2005. — 576 с.
135. Шнайер Б. Прикладная криптография.: Пер. С англ. Изд. 2-ое. – М.: Издательский дом «Вильямс», 2001. – 752 с.
136. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. — СПб.: «Наука и техника», 2004. — 384 с.
137. Черешкин Д. С., Смолян Г. Л., Цыгичко В. Н. Реалии информационной войны. – Конфидент, 1996, №4, с. 9-12.
138. ЧмораА. Л. Современная прикладная криптография. — М.: Гелиос АРВ, 2001. — 256 с.
139. Юдін О.К. Кодування в інформаційно-комунікаційних мережах:-Монографія. - К.: НАУ, 2007.-308с.
140. Ярочкин В.И. Информационная безопасность: Учебник. – М.: Академический проект: Трикста, 2005.- 544 с.
141. Autonomic Systems: Concept for Self-Managing IT Infrastructure White Paper. Fujitsu Siemens Computers, March 2003.
142. Brassard G. Modern Cryptology. - N.Y.: Springer-Verlag, 1988. - 107 p.
143. Cisco Systems, Designing a Campus Network for High Availability. – 2006 – 60с.
144. Cisco Systems, Campus Design: Analyzing the Impact of Emerging Technologies on Campus Design. – 2006. – 91с.
145. Cisco Systems, Understanding Rapid Spanning Tree Protocol (802.1w) (Document ID: 24062). - 2006. – 14с.
146. Cisco Systems, Understanding Multiple Spanning Tree Protocol (802.1s) (Document ID: 24248). – 2005. – 14с.
147. David Hucaby. CCNP Self-Study: CCNP BCMSN Exam Certification Guide, Third Edition. – Cisco Press, 2005. – 624с.
148. Dave Hucaby, Steve McQuerry. Cisco Field Manual: Catalyst Switch Configuration. – Cisco Press, 2002. – 560с.
149. Eric Ouellet, Robert Padjen, Arthur Pfund, Ron Fuller, Tim Blankenship —Building a Cisco Wireless LAN|| - Syngress Publishing, Inc, 2002.

Навчальне видання

Гончарова Л.Л., Возненко А.Д., Стасюк О.І., Коваль Ю.О.

ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНИХ ТА КОМП'ЮТЕРНИХ МЕРЕЖАХ

Навчальний посібник

Головний редактор О. В. Ємець
Макет і верстка В. О. Полічева

Підписано до друку 07.10.13. Формат 60х84/16.
Папір – офсетний, друк – на ризографі.
Обл.-вид. арк. 16.03. Ум.друк.арк.17.26.
Зам. № 293-13. Наклад 300.

Надруковано в Редакційно-видавничому відділі ДЕТУТ
(свідоцтво про реєстрацію серія ДК № 3079 від 27.12.07 р.)
03049, м. Київ-49, вул. Миколи Лукашевича, 19