



Б. В. Дурняк, І. М. Лях

# ЗАХИСТ ДАНИХ В ЕЛЕКТРОННИХ ЗАСОБАХ МАСОВОЇ ІНФОРМАЦІЇ



ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Б. В. Дурняк, І. М. Лях

**ЗАХИСТ ДАНИХ  
В ЕЛЕКТРОННИХ ЗАСОБАХ  
МАСОВОЇ ІНФОРМАЦІЇ**

Львів — 2012

**ББК 73**

**Д-84**

**УДК 004.056.5**

**Дурняк Б. В., Лях І. М.**

Захист даних в електронних засобах масової інформації / Б. В. Дурняк, І. М. Лях. – Львів : Видавництво Української академії друкарства, 2012. – 154 с.

У монографії висвітлено основи технології формування систем захисту даних в електронних засобах масової інформації. Розглянуто особливості засобів та методів захисту даних в електронних засобах масової інформації і основні моделі для їх формування. Значну увагу приділено розробленню основних компонент інформаційної технології систем захисту даних та алгоритмів протидії виявленим атакам в засобах масової інформації.

Для студентів магістерської підготовки та спеціалістів в галузях захисту інформації.

**ISBN 978-966-322-372-8**

Друкується за ухвалою

Вченої ради Української академії друкарства  
(протокол № 5/631 від 28.02.2012 р.)

Рецензенти:

**Машков О. А.** – д.т.н., професор  
**Коростіль Ю. М.** – д.т.н., професор  
**Тимченко О. В.** – д.т.н., професор

© Дурняк Б. В., Лях І. М., 2012

© Українська академія друкарства, 2012

# ЗМІСТ

Вступ.....	5
Аналіз методів систем захисту даних в електронних засобах масової інформації.....	7
Основні алгоритми захисту інформації в електронних засобах масової інформації.....	7
Основи захисту даних в електронних засобах масової інформації.....	17
Захист даних в функціональноорієнтованих системах .....	27
Теоретичні основи систем захисту даних в електронних засобах масової інформації.....	37
Моделі систем захисту інформації.....	48
Моделі загроз в системах передачі даних .....	59
Методи оцінки засобів захисту, що використовуються в електронних засобах масової інформації .....	68
Інформаційні засоби розв'язку задач систем захисту даних в електронних засобах масової інформації .....	74
Інформаційні засоби моделей захисту даних.....	74
Формування інформаційної моделі системи захисту .....	84
Синтез моделей захисту даних з інформаційними моделями .....	94
Організація інформаційної моделі загроз в засобах масової інформації .....	99
Розробка основних компонент інформаційної технології систем захисту даних в електронних засобах масової інформації.....	111
Організація способів функціонування процесів, що реалізуються в інформаційних моделях.....	111
Розробка алгоритмів протидії виявленим атакам.....	122
Загальна організація функціонування інформаційної технології системи захисту засобів масової інформації.....	133
ВИСНОВКИ.....	142
CONCLUSIONS .....	144
Список джерел .....	146

## ВСТУП

Інтенсивний розвиток електронних засобів масової інформації дозволяє збільшити кількість користувачів та розширити асортимент послуг, що надається з використанням телекомунікаційних і мобільних систем. Дослідження в галузі досить інтенсивно проводяться як в Україні, так і за її межами фірмами, що спеціалізуються на виробництві різних компонент мобільних систем. Цей попит опирається в значній мірі на політику зниження цін на мобільні послуги, яку проводять телекомунікаційні фірми, що працюють на ринку надання послуг в системах масової інформації. Важливим аспектом досліджень в цій галузі є проблема захисту інформації, яка передається в засобах масової інформації, при наданні інформаційних послуг. Оскільки засоби масової інформації використовують мобільний зв'язок для надання приватних послуг, що можуть носити конфіденційний характер, а також для послуг, що не пов'язані безпосередньо із встановленням зв'язку між абонентами, а носять особистий характер, наприклад, визначення місця знаходження абонента, надання інформаційної довідки абоненту тощо, то проблема захисту інформації, що передається через мобільну систему, є надзвичайно актуальною.

У зв'язку з цим важливою проблемою для систем масової інформації є створення гнучких засобів захисту, які можна було б адаптувати до потреб окремих абонентів. Створення гнучких засобів захисту інформації є актуальною проблемою ще й тому, що захист інформації, при реалізації послуг, призводить до збільшення ціни на відповідну послугу. Можливість управляти рівнем захисту дозволяє розв'язувати задачі персоніфікації рівня захисту послуги в залежності від вимог абонента.

Актуальність задач підвищення безпеки функціонування електронних засобів масової інформації, особливо у випадку використання мобільних систем, обумовлюється й тим, що ці системи знаходять досить широке застосування в державних організаціях, де здійснюється обмін конфіденційною інформацією.

Цю тематику досліджують такі вчені України, як: д.т.н., професор Тимченко О. В.; к.т.н., доцент Швайко І. Г.; к.т.н., доцент Щербина І. С.; к.т.н., доцент Катков Ю. І.; к.т.н., доцент Дробик О. В.; к.т.н., доцент Колченко О. В.; к.т.н., доцент Трофименко О. Р. та інші.

Таким чином, монографія є цікавою не тільки з точки зору висвітлення можливостей запропонованих підходів до підвищення рівня захисту інформації, але й має важливе практичне значення для використання існуючих електронних засобів масової інформації, що свідчить про актуальність роботи для галузі інформаційних технологій.

Автори висловлюють щире подяку рецензентам книги: д.т.н., професору Машкову О. А., д.т.н., професору Коростілю Ю. М., д.т.н., професору Тимченку О. В. за поради та цінні вказівки при підготовці видання.

Всі зауваження і пропозиції будуть сприйняті з вдячністю.

# АНАЛІЗ МЕТОДІВ СИСТЕМ ЗАХИСТУ ДАНИХ В ЕЛЕКТРОННИХ ЗАСОБАХ МАСОВОЇ ІНФОРМАЦІЇ

## Основні алгоритми захисту інформації в електронних засобах масової інформації

Широке розповсюдження електронних засобів масової інформації призвело до необхідності дослідження і розв'язку низки задач інформаційної безпеки при використанні мобільних систем. Це пов'язано з тим, що обмін приватною інформацією між двома користувачами може полягати у передачі даних, які є комерційною чи приватною таємницею. Захист інформації в системах масової інформації пов'язаний також із захистом від зловживань засобами зв'язку, що полягають у використанні чужих мобільних телефонів для власних потреб, у несанкціонованому використанні послуг, які може отримувати власник телефону без оплати останніх і т.д.

В залежності від можливостей систем масової інформації та алгоритму послуг, які можна отримати завдяки використанню систем масової інформації, можна створити значний перелік різних небезпек, з якими можуть зіткнутися як окремий користувач, так і власники систем масової інформації. Щоб більш системно визначитися з небезпеками, які існують відносно абонентів, насамперед визначимо базові типи небезпек, що можуть впливати на роботу системи масової інформації в проекції на проблеми захисту інформації, що передається по каналах систем масової інформації. Основні небезпеки, що існують відносно інформації в засобах масової інформації (ЗМІ), визначені в рамках систем, що використовують криптографію як один з важливих способів захисту інформації і являють собою стандартизовані поняття, вказані на рис. 1.

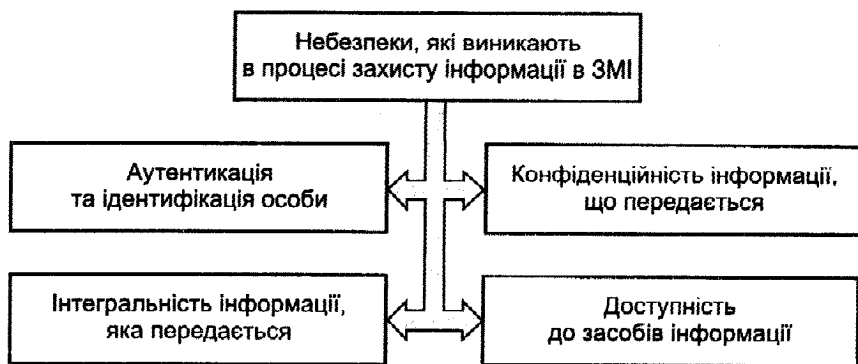


Рис. 1. Основні небезпеки, які виникають в процесі захисту інформації в електронних ЗМІ

Забезпечення аутентифікації джерела інформації реалізується різними механізмами ідентифікації, найбільш поширеним серед яких є використання паролів, кодів, таємних ключів. Крім того, з такою метою в галузі інформаційних технологій використовуються механізми ідентифікації, що полягають в:

- ідентифікації мітками часу;
- ідентифікації, що ґрунтується на використанні алгоритмів шифрування та інші.

Ідентифікація мітками часу реалізується кількома методами. В першому випадку використовується фіксований інтервал часу, за який отримана інформація повинна бути розпізнана як така, що дійсно походить від легального абонента. Цей час використовується на дешифрування, якщо повідомлення було зашифроване, чи реалізацію інших алгоритмів, які використовуються для забезпечення контролю даних, що передаються. Другий спосіб використання часу полягає у приписуванні переданим даним мітки часу, яка відповідає часу надання даних відповідним джерелом. Для зазначених способів ідентифікації характерною є вимога, яка полягає у тому, що мусить дотримуватися режим реального часу при роботі відповідних апаратних та програмних засобів.

Другий спосіб аутентифікації, що ґрунтується на використанні шифрування з симетричним ключем, хоч і має свої недоліки, але



досить широко використовується при передачі даних. Часто для таких цілей використовуються асиметричні шифри, які мають таємний ключ і явний ключ, найбільш відомим асиметричним алгоритмом шифрування є алгоритм RSA. Процес аутентифікації можна реалізувати, використовуючи код MAC разом з ключами шифрування. В цьому випадку до повідомлення додається код MAC, що формується на основі використання цього повідомлення і разом з повідомленням передається до адресата. Адресат на основі отриманого повідомлення за відомим адресатові алгоритмом вираховує код MAC і порівнює вирахований код MAC з кодом MAC, який передано адресату разом з повідомленням. Якщо порівнювані коди збігаються, то повідомлення приймається як таке, що відповідає оригіналу.

Один з основних методів забезпечення конфіденційності інформації, що передається каналами систем масової інформації, полягає у шифруванні даних. В кожній з областей захисту інформації використовуються різні класи шифрів, починаючи від перестановочних шифрів та закінчуючи складними шифрами, що ґрунтуються на використанні модульної арифметики, теорії груп та інших математичних дисциплін, що дозволяють розв'язувати основні задачі шифрування. До таких задач належать:

- перетворення кодів, що зашифровуються таким способом, який не дозволяє без знання таємних ключів виконати операцію дешифрування за актуальний період часу;
- задача вибору чисел, які б можна було використовувати у ролі ключів шифрування;
- задача мінімізації часу необхідного для реалізації шифрувальних функцій;
- доведення необхідної міри стійкості розроблених алгоритмів та методів шифрування відносно атак на системи шифрування, що є гарантією безпечності кожної окремої криптосистеми.

Інтегральність інформації, яка передається, означає, що в отриманій адресатом інформації немає частин, які не відповідають оригіналу. Найбільш актуальним є забезпечення інтегральності в сферах фінансової діяльності, де зміна одного фрагмента даних

може призвести до катастрофічних для легальних абонентів наслідків. До методів забезпечення інтегральності належать метод, що ґрунтується на використанні MAC, про який вже йшлося вище.

Другим методом забезпечення інтегральності є метод, що полягає у використанні цифрового підпису. Цифровий підпис створюється шляхом редукції тексту, який передбачається передавати з допомогою однонаправлених функцій, типу H-функцій, та шифрування H-образу тексту з допомогою несиметричних алгоритмів. При шифруванні абонент використовує приватний ключ, який є таємним, і скорочений зашифрований текст, який являє собою цифровий підпис, що разом з текстом, який може бути зашифрований з допомогою симетричного шифру або бути відкритим, передаються адресату. Адресат, використовуючи публічний ключ, розшифровує H-образ тексту повідомлення, через прийнятий по каналу зв'язку тексту, формує його скорочений образ і, якщо цей образ збігається із скороченим образом, який отримано з цифрового підпису, то це є гарантією, що текст повідомлення не було модифіковано.

Доступність означає можливість управління доступом до засобів масової інформації, до інформації, яка вміщується в системі масової інформації, до засобів шифрування даних, що передаються, та інших компонент, несанкціонований доступ до яких може призвести до порушення роботи системи масової інформації та неможливості надання послуг легальним користувачам. Таким чином, небезпека, що пов'язана з несанкціонованим доступом до системи масової інформації, є досить багатогранною за способами взаємодії з системою масової інформації.

Однією з компонент, що протидіє такій небезпеці, є використання паролів та ідентифікаційних номерів PIN. Розвиток електронно-апаратних засобів дозволяє використовувати більш складні методи для контролю доступу. На сьогодні вже є можливим використання низки біометричних засобів для ідентифікації споживачів послуг перед наданням їм послуг. До таких засобів зокрема належать:

- ідентифікація за райдужною оболонкою ока;
- ідентифікація за відбитком долоні;

— ідентифікація за відбитком пальців;

— ідентифікація за голосом.

Одним з базових методів захисту даних в засобах масової інформації є скремблювання мови. Методи скремблювання використовуються для аналогових систем і являють собою методи шифрування аналогового сигналу. Для того, щоб шифрувати сигнал мови, необхідно поміняти кореляцію між такими параметрами, що визначають аналоговий сигнал:

— часом;

— частотою;

— амплітудою.

Скремблювання частоти полягає у виділенні окремих частотних смуг в сигналі і переставлянні фрагментів сигналів цих частотних смуг в зміненому порядку. Скремблювання в часі полягає у перестановці виділених фрагментів сигналу з однієї часової послідовності в іншу. Скремблювання аналогового сигналу за одним параметром називається однопараметричним. Якщо скремблювання реалізується за кількома параметрами, то воно називається багатопараметричним.

В електронних системах масової інформації широко використовуються цифрові канали. Тому для захисту даних і розв'язку інших задач безпеки систем масової інформації використовується цифрове шифрування. Досить широко в системах масової інформації використовується потокове шифрування, яке можна легко реалізувати апаратними засобами. Принцип функціонування поточкового шифру полягає у наступному. Сигнал мови перетворюється на послідовний цифровий код. Ключ шифрування являє собою в більшості випадків генератор псевдовипадкових бітів, що синхронно з кодами шифрованого сигналу подаються на суматор по модулю два. На виході такого суматора формується зашифрована послідовність відповідного коду. При дешифруванні зашифрованої послідовності бітового коду на суматор по модулю два подається зашифрований код, а на другий вхід суматора подається в тій же послідовності ідентична псевдовипадкова послідовність одиниць і

нулів бітового коду. Формально таке шифрування записується у вигляді:

$$C = K \oplus W,$$

де  $C$  – зашифроване повідомлення,  $K$  – ключ шифрування,  $W$  – повідомлення, яке зашифровується. Основними недоліками такого способу шифрування є такі особливості цього шифру:

- ключ шифрування повинен бути за довжиною рівним з довжиною повідомлення, яке зашифровується;
- для забезпечення дешифрування необхідно забезпечити надійну синхронізацію ключа із зашифрованою послідовністю, оскільки виникнення розсинхронізації в одній позиції коду призведе до неможливості дешифрування всієї частини повідомлення, яка залишилась нерозшифрованою;
- генератори псевдовипадкових бітових послідовностей у двох абонентів, що обмінюються повідомленнями, повинні бути ідентичними.

При використанні блокового шифрування з'являється можливість скоротити розмір ключа, оскільки шифрування в цьому випадку проводиться поблочне. Зазвичай розмір блоків становить 64 або 128 бітів. Основні типи блокових шифрів наведені на рис. 2.

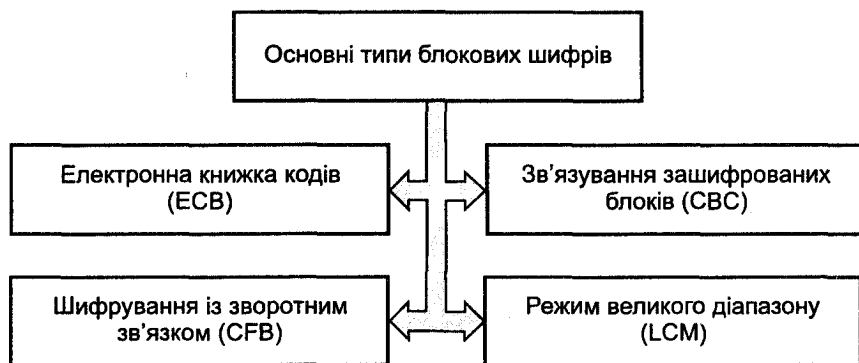


Рис. 2. Основні типи блокових шифрів

В методі шифрування ЕСВ однакові блоки відкритого тексту зашифровуються в однакові блоки зашифрованого тексту. Це означає, що для різних блоків тексту явно використовуються різні зашифровані тексти. Тому спосіб шифрування називається шифруванням по електронній книжці, в якій для різних блоків тексту розміщуються різні ключі.

В методі СВС на першому кроці шифрування кожного блоку відкритого тексту відбувається аналогічно до методу ЕСВ, але кожний зашифрований блок подається в буферний регістр і складається побітово по модулю два з наступним блоком відкритого тексту. Тому кожний зашифрований блок є залежним від всіх інших блоків, які передували цьому блоку. Через це таке шифрування називається зв'язуванням зашифрованих блоків.

На відміну від попередніх способів шифрування в методі СFB можна шифрувати послідовності бітових кодів, які є коротшими від блоків в 64 чи 128 бітів. В ролі ключа використовується псевдовипадковий бітовий код. Зашифрований код одного байта повідомлення по зворотному зв'язку передається на суматор XOR і сумується з біжучим кодом наступного байта відкритого тексту.

Недоліком перерахованих вище методів шифрування є їх висока чутливість до методів синхронізації, оскільки її порушення призводить до неможливості розшифрування зашифрованого повідомлення. Крім того, бітова помилка у відкритому тексті впливає на весь зашифрований текст.

Шифрування типу LCM використовує спосіб шифрування, аналогічний до шифрування потокового, але в ролі шифрувального ключа використовується лічильник. Тому в цьому випадку неможливе поширення помилкового біта на все зашифроване повідомлення.

Крім вищезазначених потокових шифрів, в системах масової інформації використовуються й інші методи та системи шифрування. Таке шифрування ґрунтується на використанні асиметричних шифрів. Використання шифрів цього типу вимагає розвинутої системи управління ключами шифрування, яка є гарантом і однією з важливих умов забезпечення стійкості алгоритмів до атак, що

направлені на несанкціоноване дешифрування даних, які циркулюють в системі масової інформації.

Розглянемо на загальному рівні основи функціонування симетричних та асиметричних алгоритмів шифрування. Симетричні алгоритми шифрування розглядаються як цілі системи, оскільки в цілому алгоритми, що реалізують симетричне шифрування, є досить складними. Для симетричних криптосистем характерним є використання блоків, на які розбивається шифрований текст, а кожний блок окремо зашифровується і, відповідно, дешифрується. Найбільш поширеним розміром блока є блок, який складає 64 біти. Основа цілого класу блочних шифрів являє собою конструкцію Фейстеля. Ця конструкція передбачає наступну послідовність дій з реалізації алгоритму шифрування. Блок відкритого тексту розбивається на дві половини – праву і ліву, тому довжина блока повинна бути парною. На кожному циклі одна з частин блока перетворюється за допомогою функції  $f$  і допоміжного ключа  $k_1$ , який формується на основі початкового ключа. Результат перетворення сумується по модулю два з другою частиною блока. Після цього ліва частина і права частина міняються місцями. На останньому кроці використання схеми Фейстеля ґрунтується на уявленнях про інволюційні функції. Функція  $f(x)$  називається інволюційною, якщо  $f(f(x)) = x$ , для всіх  $x$ . Наприклад, функція  $f(x) = 7x$  є інволюцією, оскільки  $f(f(x)) = 7(7x) = x$ , функція  $f(x) = x \oplus c$  також є інволюцією, оскільки:

$$f(f(x)) = (x \oplus c) \oplus c = x \oplus c \oplus c = x.$$

Якщо криптографічне перетворення позначити символом  $E^k_1(*)$ , при  $1 < i < n$ , де  $k$  – ключ, то шифротекст  $C$  можна отримати в результаті перетворення:

$$C = E^k_n(E^k_{n-1}(\dots E^k_2(E^k_1(P))\dots)),$$

де  $P$  – відкритий текст. Якщо функція  $E^k_1(*)$  є інволюцією, то відкритий текст можна отримати на основі використання співвідношення:

$$P = E^k_1(E^k_2(\dots E^k_{n-1}(E^k_n(C))\dots)).$$

Основною проблемою більшості блочних шифрів є те, що для розкриття одного блока тексту достатньо дешифрувати один блок шифротексту. Для вирішення цієї проблеми Ріверст запропонував метод побудови ресепарабельного режиму шифрування, який описано нижче.

За допомогою спеціального перетворення послідовність блоків  $P_1, \dots, P_n$  перетворюється у псевдоблоки  $P'_1, \dots, P'_n$ , а послідовність зашифрованих блоків  $C_1, \dots, C_n$  формується на основі шифрування псевдоблоків способом, що реалізується в типі блокового шифру ЕСВ на таємному ключі  $k$ . Функція перетворення послідовностей блоків  $P_1, \dots, P_n$  повинна бути зворотною. Обчислювальна складність процедури розрахунку блока відкритого тексту, якщо немає хоча б одного псевдоблока, повинна бути експоненціальною. Для прикладу, наведемо схему Ріверста, в якій використовується фіксований нетаємний ключ  $k_0$ . Ця схема складається з нижчезазначеної послідовності дій. Для використання перетворень блоків у псевдоблоки генерується випадковий ключ  $k^*$ . Послідовність псевдоблоків обраховується за допомогою перетворення:

$$P^i = P_i \oplus E(k^*, i), \text{ де } i=(1,2,\dots,S),$$

$$P'_{S+1} = k^* \oplus h_1 \oplus h_2 \oplus \dots \oplus h_S,$$

де  $h_i = E(k_0, P_i \oplus i)$ , для  $i=(1,2,\dots,S)$ , а ключ  $k_0$  є не таємним ключем. Ця схема подібна до схеми ЕСВ з тою відмінністю, що ключ перетворення не є фіксованим, а для кожного нового тексту, який необхідно зашифрувати, генерується заново. Наведене вище перетворення є зворотним, або:

$$k^* = P'_{S+1} \oplus h_1 \oplus h_2 \oplus \dots \oplus h_S,$$

$$P_i = P'_i \oplus E(k^*, i) \text{ для } i=(1,2,\dots,S).$$

Типовим представником асиметричних шифрів є система RSA. Криптостійкість RSA ґрунтується на трудомісткості розкладу на множники великих чисел, оскільки відкриті і таємні ключі є функціями двох великих простих чисел. Для генерації парних ключів використовуються два великі випадкові прості числа  $p$  і  $q$ .

Потім обраховується їх добуток  $n = p \cdot q$ . Тоді випадковим чином вибирається ключ шифрування  $e$  такий, щоб він задовольняв умови:  $e$  і  $\varphi(n) = (p-1) \cdot (q-1)$  повинні бути взаємно-простими числами. Алгоритм Евкліда використовується для обрахунку ключа дешифрування  $d$ , який повинен відповідати співвідношенню:  $ed = 1 \pmod{\varphi(n)}$ . Це означає, що виконується співвідношення:  $d = e^{-1} \pmod{\varphi(n)}$ . При цьому,  $d$  і  $n$  є взаємно-простими числами. Числа  $e$  і  $n$  є відкритими, число  $d$  – таємним ключем. Числа  $p$  і  $q$  зберігаються в таємниці. Для шифрування повідомлення розбивається на окремі блоки, кожний з яких повинен бути меншим від  $n$ . Шифрування окремих блоків в цьому випадку зводиться до:  $C_i = m_i^e \pmod{n}$ .

При дешифруванні кожний зашифрований блок  $C_i$  вираховується у відповідності із співвідношенням:  $P_i = C_i^d \pmod{n}$ .

Справедливість цих співвідношень впливає з такої послідовності перетворень:

$$C_i^d = (m_i^e)^d = m_i^{ed} = m_i^{r \cdot \varphi(n) + 1} = m_i \cdot m_i^{r \cdot \varphi(n)} = m_i \cdot 1 = m_i.$$

У цій послідовності перетворень всі обчислення проводяться за модулем  $n$ .

В сучасних засобах масової інформації для розв'язку задач ідентифікації та аутентифікації поширені алгоритми цифрового підпису. Переважно для реалізації цих процедур використовується криптосистема, яку запропонував Ель-Гамалев. Її стійкість ґрунтується на трудоемності обрахунку дискретного логарифма на скінченному полі. Для генерації ключів в цій криптосистемі вибирається просте число  $p$  і два випадкові числа  $y$  і  $x$ , при цьому  $x < p$  і  $y < p$ . Після цього обраховується:

$$y = q^x \pmod{p}.$$

У цьому випадку відкритими ключами є  $y$ ,  $p$  і  $q$ . Таємним ключем є  $x$ . Щоб підписати повідомлення  $M$ , вибирається випадкове число  $k$ , яке є взаємно-простим з числом  $(p-1)$ . Після цього



вираховується:  $a = q^k \bmod p$ . За допомогою алгоритму Евкліда знаходять число  $b$  з рівняння:

$$M = (xa + kb) \bmod (p - 1).$$

Підписом в цьому випадку є пара чисел  $a$  і  $b$ . Випадкове число  $k$  повинно зберігатися в таємниці. Для перевірки цифрового підпису необхідно перевірити, чи виконується таке співвідношення:

$$y^a a^b \bmod p = q^M \bmod p.$$

Існує перелік криптосистем, які використовують несиметричні ключі, що ґрунтуються на використанні дискретного логарифма і використовуються для реалізації схем передачі ключів, завдяки чому їх можна віднести до протоколів обміну ключами. Прикладом реалізації такого протоколу може бути наступна послідовність дій. Одна сторона вибирає випадкове велике число  $X$  і посилає його другій стороні  $X = q^x \bmod n$ . Друга сторона вибирає випадкове велике число  $y$  і посилає його першій стороні  $Y = q^y \bmod n$ . Перша сторона обраховує  $k = Y^x \bmod n$ , друга –  $k' = X^y \bmod n$ . При цьому  $k$  і  $k'$  рівні  $q^{xy} \bmod n$ . Для обрахунку  $x$  і  $y$  необхідно вираховувати дискретний логарифм. Тому  $k$  є таємним ключем для двох сторін.

## **Основи захисту даних в електронних засобах масової інформації**

На сьогодні поширеною мобільною системою є система GSM. Тому доцільно проаналізувати основні задачі та методи захисту даних, що циркулюють в рамках цієї системи та методах захисту самої системи і окремих її компонентів. У зв'язку з цим розглянемо базову структуру системи GSM. На рис. 3 наведено структурну схему основних компонент мобільної системи GSM.

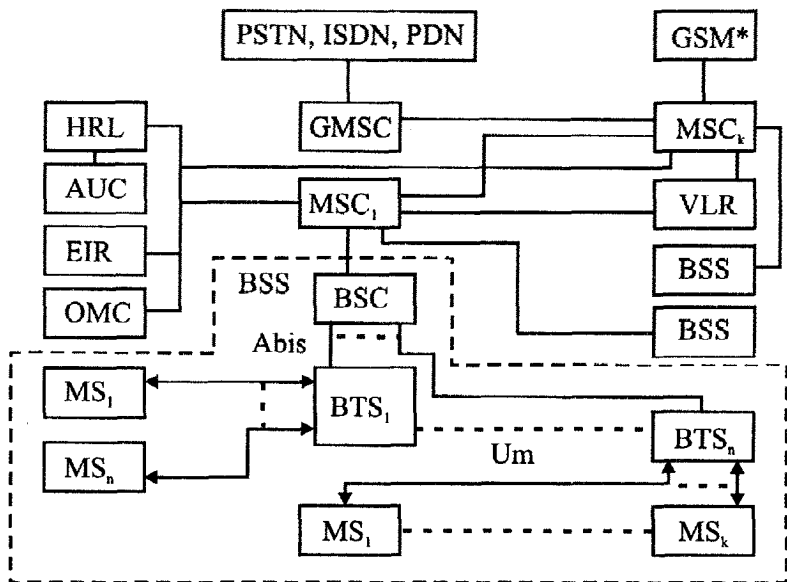


Рис. 3. Структурна схема основних компонент GSM

На рисунку використовуються такі позначення:

$MS_1 - MS_n$  – рухомі, або мобільні станції;

BTS – базова трансиверна станція, що складається з антени, приладів обробки сигналів, підсилювачів і утворює одну чи декілька сот;

BSC – контролер базових станцій, який управляє станціями BTS, він здійснює резервування частот, переключення з однієї станції BTS на іншу, пошук мобільних станцій, ущільнення радіоканалу для сполучення із стаціонарними мережами зв'язку;

MSC – центр комутації мобільних служб, який встановлює зв'язок з іншими MSC та контролерами BSC, центри MSC створюють стаціонарну магістральну мережу системи GSM, шлюз MSC додатково об'єднаний з іншими стаціонарними мережами, крім того, MSC виконує всі функції, що необхідні для додаткових служб;

HLR – реєстр початкового положення, що являє собою базу даних, в якій зберігається вся інформація про користувача, а саме: номер ISDN мобільного абонента, оплачені послуги і ключ аутентифікації, дані про біжучі зміни зони мобільної станції;

VLR – реєстр місцезнаходження абонентів, зв'язаний з кожним центром MSC, являє собою базу даних, кожний VLR належить до окремої соти, таким чином, VLR копіює всю інформацію про абонента, який потрапляє у відповідну соту;

OMC – центр експлуатації та обслуговування, який здійснює спостереження за інформаційним обміном, управління безпекою і абонентами, а також ведення рахунків за надані послуги;

AUC – центр аутентифікації, який складається з алгоритмів аутентифікації, ключів шифрування, цей центр розміщується в окремій захищеній частині бази даних HRL або реалізується окремо;

EIR – реєстр обладнання, що являє собою базу даних для розпізнавання IMEI, цей реєстр вміщує ідентифікаційну інформацію про всі пристрої, зареєстровані в мережі, крім того, він формує «чорний список» викрадених мобільних телефонів;

GSM\* – інша мережа мобільного зв'язку GSM, з якою з'єднується дана GSM;

GMSC – шлюз MSC для підключення мережі GSM до мереж зв'язку інших типів;

PSTN – загальна комутована телефонна мережа;

ISDN – цифрова система зв'язку з інтеграцією послуг, яка може бути транзитною мережею;

PDN – мережа передачі даних загального користування;

Um – радіоінтерфейс, в якому реалізуються механізми ущільнення і доступу до середовища, наприклад, в системі GSM 900 використовується схема FDMA зі 124 каналами шириною по 200 кГц;

Abis – інтерфейс зв'язку між базовими станціями BTS і контролером BSC.

В системі GSM використовується низка стандартних елементів захисту. На рис. 4 наведена схема основних компонент таких засобів. Очевидно, що ці засоби захисту реалізуються в компонентах, які формують систему масової інформації, тому на рисунку наведено схематичне зображення компонент, що реалізуються з метою реалізації захисту даних в GSM.

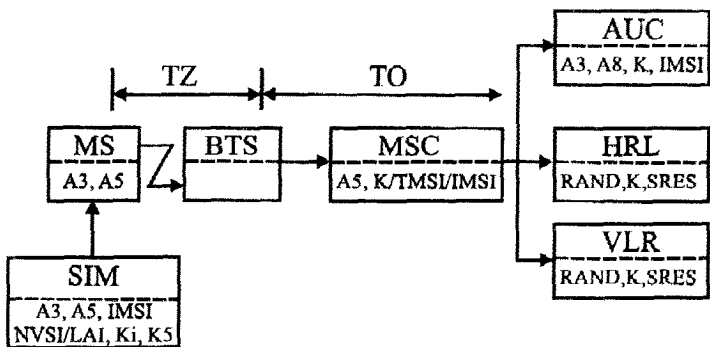


Рис. 4. Схе́ма основних засобів захисту

На рисунку використовуються такі позначення:

A3 – алгоритм шифрування, який використовується для ідентифікації користувача;

A5 – алгоритм шифрування тимчасового номера ідентифікації абонента, що використовує послуги роумінгу;

A8 – алгоритм шифрування, що використовується для аутентифікації MS за псевдовипадковим числом RAND і ключем абонента Ki;

IMSI – міжнародний ідентифікаційний номер мобільного абонента;

TMSI – тимчасовий ідентифікаційний номер мобільного абонента;

LAI – ідентифікатор власного мобільного образу абонента;

Ki – ключ до алгоритму шифрування A3;

SRES – 32-бітова послідовність, яка утворюється в результаті шифрування псевдовипадкового числа довжиною в 128 бітів RAND, яке присилається з мережі до мобільного терміналу і використовується в алгоритмі шифрування A8;

K5 – ключ, що використовується алгоритмом шифрування A5, який є потоковим і шифрує дані, що передаються з рухомої станції MS;

TZ – трансмісія, що зашифровується, переважно ця трансмісія стосується радіоканалу;

TO – трансмісія відкритої передачі даних, яка у відповідності до архітектури системи GSM реалізується через провідні канали.

Інші позначення MS, BTS, MSC, AUC, HLR і VLR відповідають позначенням, що використовуються на рис. 3, за винятком позначення SIM, яке визначає ідентифікаційну карту, або модуль

ідентифікації, який розміщується в мобільному телефоні у кожного абонента GSM.

Розглянемо більш детально, в чому полягають захисні функції кожної з компонент, що наведені на рис. 4.

Центр ідентифікації і аутентифікації реалізує функції захисту доступу абонента до мережі. Для цього використовується таємний ключ абонента  $K_i$ , який вміщується у карті SIM, алгоритм шифрування  $A_3$ , який також реалізовано в MS і AUC, та механізм формування псевдовипадкового числа довжиною в 128 бітів, яке генерується в AUC. При співпраці центра з MS використовується реєстр HLR власних станцій MS. Ідентифікація мобільної станції відбувається наступним чином. Центр аутентифікації генерує випадкове число RAND довжиною в 128 біт, яке передається в мобільну станцію MS. В MS на карті SIM знаходиться таємний ключ  $K_i$  і алгоритм шифрування  $A_3$ . Використовуючи ключ  $K_i$  і алгоритм  $A_3$ , станція MS шифрує прийняте число RAND і формує 32-бітне зашифроване число SRES, яке передається через BTS, MSC в AUC. Центр аутентифікації, використовуючи той же алгоритм  $A_3$  і таємний ключ  $K_i$ , які ідентичні ключу і алгоритму, що знаходяться на карті SIM у санкціонованого абонента, розшифровує випадкове число RAND, яке було передане на станцію MS. Якщо прийняте із станції число SRES і число, сформоване в AUC, однакові, то мобільна станція вважається санкціонованою.

Реєстр власних станцій HLR вміщує дані кожного користувача, який зареєстрований в мережі GSM. Реєстр HLR, разом з такими даними, як виконання виплат за надані послуги кожною станцією, вміщує алгоритм  $A_3$ , що використовується для аутентифікації, алгоритм  $A_8$ , що використовується для шифрування повідомлення, та таємний ключ  $K_i$ . Реєстр HLR також бере участь у формуванні псевдовипадкового числа RAND, яке передається з AUC в MS і забезпечує необхідні параметри випадковості.

Реєстр зовнішніх станцій VLR вміщує дані рухомих станцій, що в поточний момент переміщуються в зоні, яка обслуговується цим GMSC. Він вміщує тимчасові ідентифікаційні номери TMSI мобільних абонентів, які перебувають в чужій підсистемі GSM. Ці

номери замінюють номери IMSI. Реєстр VLR визначає реальне місцезнаходження мобільної станції, яка перебуває в чужій зоні. Крім того, цей реєстр бере участь в процедурі аутентифікації чужої станції, коли гострова станція MS перший раз гостює в чужій мережі.

Карта SIM є модулем, який вміщується в мобільній станції і забезпечує аутентифікацію абонента. Карта SIM являє собою апаратний засіб, на якому розміщується мікропроцесор та пам'ять. В карті розміщується міжнародний номер мобільного абонента IMSI та два алгоритми шифрування A3 і A8. Крім того, на карті зазначено індивідуальний ключ Ki, а також її елемент контролю доступу, яким є номер PIN. Карти SIM, що використовуються в мобільних телефонах, крім цієї інформації, вміщують номер IMSI, PUK, LAN і TMSI. Інформація, що відповідає PUK, являє собою персональний ключ розблокування, який використовується у випадку блокування карти SIM. Блокування карти SIM відбувається тоді, коли карта SIM встановлюється в телефон і для її розпізнавання вводиться її PIN. Якщо введений при ініціалізації карти PIN не відповідає номеру, який має карта, то після трьох спроб ввести неправильний номер, карта блокується. Тоді розблокувати її можна за допомогою персонального ключа PUK. Ідентифікатор TMSI використовується тільки у випадку, коли абонент перебуває в зоні чужої системи GSM. Для того, щоб для ідентифікації мобільної станції не треба було передавати в мережу IMSI, реєстр VLR реалізує процедуру аутентифікації з використанням шифрування алгоритмом A5 та передачу TMSI, який розпізнається рухомою станцією, що підтверджує отримання відповідного тимчасового ідентифікатора. Крім того, аутентифікується LAI, який є ідентифікатором власної системи GSM для цієї станції MS.

Відповідно до зазначеного вище, карта SIM являє собою апаратний засіб захисту доступу до мобільної станції, забезпечує захист перед несанкціонованою інсталяцією карти SIM в мобільному телефоні, наприклад, коли карта SIM є викраденою, реалізує захист при ідентифікації мобільної станції у випадку, коли санкціонований абонент використовує послугу роумінгу шляхом

присвоєння та ідентифікації станцій за тимчасовим номером TMSI. Всі ці процедури використовують алгоритми шифрування інформації, яка при реалізації процедури передається через радіоканал.

Наступним елементом засобів захисту, який вміщується в самій станції MS, є алгоритм A5, що використовується для шифрування повідомлень. Таким чином, в системі GSM реалізуються механізми захисту доступу до мобільних станцій при встановленні з ними зв'язку та механізми, що ґрунтуються на алгоритмах шифрування для захисту трансмісії даних через радіоканал у всіх випадках, коли ці дані передаються від MS в мережу зв'язку.

В мобільній системі існує перелік елементів, які тою чи іншою мірою сприяють підвищенню безпеки. Одним з таких елементів є реалізація сеансу зв'язку через радіоканал з перескакуванням по частотах. Реалізація переходів з однієї частоти на іншу протягом одного сеансу зв'язку зв'язана з подоланням явища втрат в каналах, що працюють на радіочастотах. Оскільки алгоритм перескоків реалізується в BSC, то несанкціонований моніторинг радіоканалу з метою перехоплення даних стає неможливим, якщо невідомий алгоритм, що управляє таким перескакуванням.

Крім вищезазначених засобів захисту мобільних систем, можна говорити і про нестандартні засоби захисту систем масової інформації, які доступні для користувача системи GSM. Одним із таких засобів є реалізація стратегії шифрування «від точки до точки». Така стратегія забезпечує збереження приватності розмови незалежно від того, чи реалізується з'єднання між станціями мобільними, чи між станціями GSM і мережею PSTN. Одним із підходів до реалізації цієї стратегії є виділення окремого каналу зв'язку. Справа у тому, що захищеним каналом в сучасних мобільних системах є тільки радіоканал. Тому для реалізації стратегії захисту «від точки до точки» необхідно, щоб в оператора була можливість, з точки зору можливостей апаратних засобів, такий канал виділити. Апаратура, яка забезпечує оператору можливість реалізації такої стратегії, є досить дорогою. Тому не кожен оператор має можливість реалізувати таку послугу. Переважно такими послугами користуються урядовці, особи, що обіймають

високі посади, та інші абоненти, для яких забезпечення захисту з рівнем, вищим ніж рівень стандартних засобів безпеки, є обґрунтованим.

Другим підходом до реалізації нестандартних засобів захисту в мережах GSM є використання нестандартних процесів шифрування. Для того щоб детальніше розглянути можливість використання нестандартного процесу шифрування, необхідно детальніше зупинитися на схемі мобільного телефона (рис. 5).

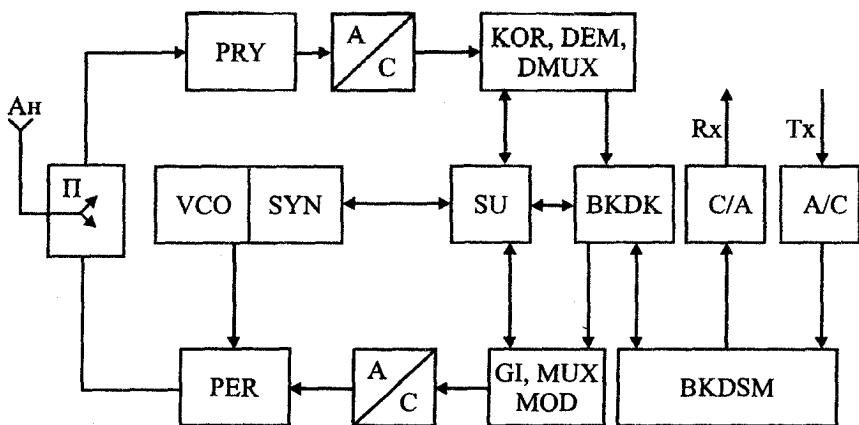


Рис. 5. Блок-схема мобільного телефона GSM

На рисунку використовуються такі позначення:

PRY – приймач;

П – перемикач;

Ан – антена;

PER – передавач;

A/C – аналого-цифровий перетворювач;

VCO – генератор, що управляється напругою;

SYN – синтезатор;

SU – система управління;

GI – генератор імпульсів;

MUX – мультиплексор;



MOD – модулятор;  
BKDSM – блок кодування-декодування сигналів мови;  
BKDK – блок кодування-декодування каналів;  
KOR – коректор;  
DEM – демодулятор;  
DMUX – демультимплексор;  
C/A – цифро-аналоговий перетворювач;  
Tx – вхідний сигнал;  
Rx – вихідний сигнал.

Демультимплексор використовує нумерацію кадрів для вибору даних з різних часових щілин і формування з них логічних каналів. Блок кодування-декодування в режимі прийому відтворює параметри людської мови з блоків, що складаються з 260 бітів, і передає сформований цифровий сигнал на ЦАП, а в режимі передачі здійснює компресію цифрового сигналу мови. Генератор імпульсів формує імпульси, що передаються в канал, та збільшує кількість каналів у відповідності до структури кадру. Генератор VCO генерує всі необхідні частоти для несучої частоти, а також генерує синхронізуючі сигнали для блоку управління.

У цьому випадку нестандартний засіб захисту являє собою шифрувальний модуль, який включає кодуючий/декодуючий пристрій та модуль вокодера. Завдяки модулю кодера-декодера досягається висока якість розпізнавання голосу. Для шифрування використовується алгоритм потокового шифрування. Очевидно, що для використання цього нестандартного засобу захисту між двома абонентами, ці два абоненти повинні використовувати однаково модифіковані мобільні станції. При цьому встановлення зв'язку відбувається стандартним чином і тільки при переході на етап передачі даних, якщо абонент замовляє режим шифрування, підключається шифрувальний модуль.

В системах підвищеного рівня захисту використовується декілька алгоритмів шифрування. Один алгоритм використовується для шифрування повідомлення, другий – для забезпечення стійкості на дослідження та виявлення ключів шифрування, а третій – для управління ключами шифрування всередині мережі.

При використанні нестандартних засобів безпеки у вигляді алгоритмів шифрування повідомлень відповідний модуль реалізується як окремий модуль, який можна під'єднати до інтерфейсу телефону. В цьому випадку модуль шифрування, як правило, вміщує відповідні апаратні елементи (рис. 6).



Рис. 6. Основні компоненти, що входять в модуль шифрування

При використанні додаткових нестандартних засобів захисту, що ґрунтуються на використанні додаткового шифрування повідомлень, виникає задача управління ключами шифрування в системах масової інформації, що ускладнює використання нестандартних засобів захисту.

## **Захист даних в функціональноорієнтованих системах**

Крім систем загального користування типу GSM, існують локальні та спеціалізовані системи масової інформації, для яких питання безпеки є першочерговими. Прикладом таких систем можуть слугувати системи масової інформації, що орієнтовані на надання можливостей ведення переговорів між просторово розділеними абонентами. Функціональна орієнтація таких систем в більшості випадків визначається прикладною предметною областю, в якій такі системи передбачається використовувати.

Може скластися враження, що існування універсальної системи масової інформації, прикладом якої може слугувати система зв'язку Internet, повністю витіснить різноманітні специфічні системи масової інформації. Цього на сьогодні не сталося, оскільки універсальність системи масової інформації призводить до існування низки факторів, які недопустимі в багатьох функціонально орієнтованих системах. Наприклад, універсальність системи масової інформації передбачає можливість її використання широким класом користувачів, що спричиняє додаткові складності при розв'язанні задач безпеки процесу передачі даних. Універсальність системи масової інформації, здебільшого передбачає її більш високу експлуатаційну вартість, у порівнянні з вартістю функціонуючої функціонально орієнтованої мережі. В універсальних мережах існує значно менше можливостей проводити модифікацію останніх, якщо вона обумовлена специфікою тої предметної області, для якої вона використовується. Можна навести перелік інших прикладів з конкретних прикладних областей використання універсальної системи масової інформації, наприклад, системи Internet, що призвело до суттєвих проблем при її використанні для розв'язку задач в кожній окремій прикладній галузі. Тому розглянемо деякі спеціалізовані, або функціонально орієнтовані, системи масової інформації з точки зору розв'язку в таких системах задач забезпечення їх безпечного функціонування.

Розглянемо системи масової інформації, що призначені для забезпечення розмов між просторово розділеними абонентами. Такого типу системи масової інформації, незважаючи на розвиток

мобільних систем чи розвиток мережі Internet, в наш час досить широко застосовуються, наприклад, будь-яка корпоративна система зв'язку з власною, окремою, або внутрішньою АТС, яка підтримує послуги із забезпечення переговорів між абонентами окремої корпорації. Основним засобом, що орієнтований на розв'язок задачі безпечного зв'язку, є засіб шифрування – скремблер. Типова структурна схема, що реалізує цього типу шифрування аналогового сигналу, наведена на рисунку 7.

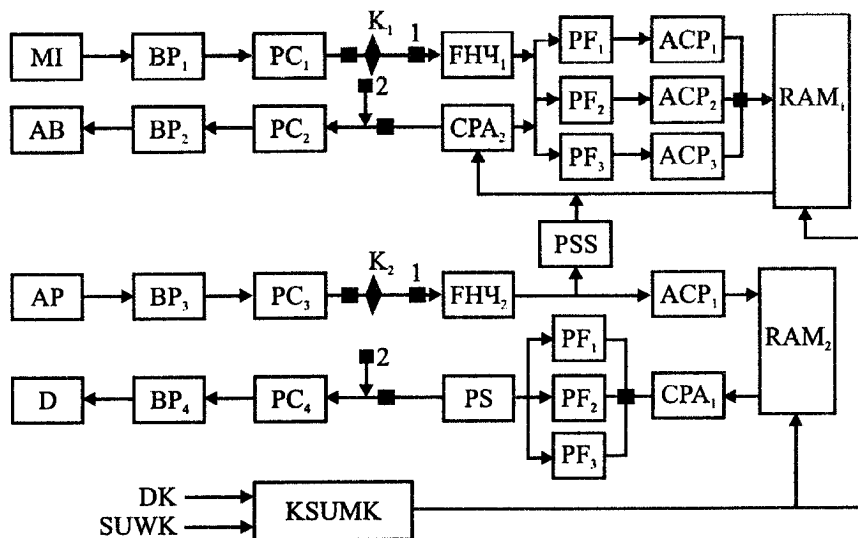


Рис. 7. Структурна схема аналогового кремблера

На рисунку використовуються такі позначення:

- MI – мікрофон або інший аналоговий вхід голосового сигналу;
- BP1 – BP4 – вхідні узгоджувальні перетворювачі;
- PC1 – PC4 – підсилювачі вхідного сигналу;
- ФНЧ1 – ФНЧ2 – фільтри низької частоти (3кГц);
- PF1 – PF3 – смугові фільтри;
- PS – сумуючий підсилювач;
- АСР1 – АСР4 – аналогово-цифрові перетворювачі;
- СРА1, СРА2 – цифро-аналогові перетворювачі;

AB – випромінююча антена;  
AP – приймаюча антена;  
D – динамік або інший пристрій для відтворення аналогового сигналу людської мови;  
RAM1, RAM2 – оперативна пам'ять;  
PSS – процесор синхронізації;  
KSUMK – модуль контролю шифрування, управління монітором і клавіатурою;  
DK – дані ключа шифру;  
SUWK – сигнали управління та вибору ключа;  
K1, K2 – ключі режимів роботи скремблера.

Охарактеризуємо функціонування скремблера. Вхідний блок  $BP_1$ , узгодження сигналу, що приходиться з мікрофона  $MI$ , формує сигнал і подає його на підсилювач  $PC_1$ , який з сигналу в кілька мілівольт низької частоти підсилюється до  $+30$  dB, що необхідно для стабільної роботи фільтрів і аналогово-цифрових перетворювачів. Якщо перемикач  $K_1$  перебуває в положенні 1, то буде відбуватися скремблювання сигналу. В цьому випадку вхідний сигнал подається на фільтр низької частоти з ціллю обмеження смуги сигналу в межах 3 кГц. Після цього сигнал подається на смугові фільтри, які ділять його на різні піддіапазони частот. Сигнали кожної частотної смуги перетворюються в цифрову форму на  $ACP_1$  і записуються в пам'ять  $RAM_1$ . У відповідності з роботою мікропроцесора, що управляє процесором шифрування, записані сигнали у порядку, що відповідає алгоритму шифрування, зчитуються з пам'яті і подаються на цифро-аналоговий перетворювач  $CPA_2$ . Аналоговий сигнал підсилюється на підсилювачі  $PC_2$ , перетворюється в блоці  $BP_2$  у відповідності з вимогами випромінюючої антени AB і передається з AB в радіоканал. З радіоканалу сигнал подається на прийомну антену AP через блок  $BP_3$  та підсилювач  $PC_3$  подається на перемикач  $K_2$ , положення якого відповідає положенню перемикача  $K_1$  на передачій частині. Через фільтр низької частоти  $FHЧ_2$  та аналого-цифровий перетворювач  $ACP_4$  сигнал в цифровій формі записується в пам'ять  $RAM_2$ . Сигнал,

що був записаний в  $RAM_1$ , зчитується з  $RAM_1$  на CPA не у тій послідовності, в якій він виділявся на різні частотні смуги, а в послідовності, яка визначається ключем шифрування. Таким чином зчитаний сигнал був зашифрований шляхом перестановок його частотних смуг у вибраній послідовності. При зчитуванні цього сигналу з  $RAM_2$ , який прийшов на AP з радіоканалу, порядок зчитування частотних смуг буде таким, який є зворотним до порядку, в якому цей сигнал зчитувався з  $RAM_1$ . Таким чином здійснюється дешифрування аналогового сигналу мови, що полягає у перестановці частотних смуг сигналу. Зчитуваний з  $RAM_2$  сигнал перетворюється на CPA в аналогову форму, подається на смугові фільтри, що ідентичні смуговим фільтрам в каналах шифрування, і на сумуючому пристрої PS сигнал відновлюється у явній формі. Після цього голосовий сигнал потрапляє через модулі  $PC_4$  і  $BP_4$  на модуль відтворення повідомлення, який може являти собою звичайний динамік. Модуль KSUMK передає ключ шифрування в  $RAM_1$  і  $RAM_2$ , який визначає зміну порядку запису складових сигналу в пам'ять, завдяки чому здійснюється шифрування. На вхід цього модуля подаються вхідні дані, ключі шифрування, здійснюється вибір ключа в рамках модуля та подаються зовнішні управляючі сигнали.

Крім скрамблерів, в засобах масової інформації такого типу використовуються також шифратори, які забезпечують вищий рівень захищеності, оскільки в цьому випадку використовуються потокові алгоритми шифрування. Але для використання шифрувальних алгоритмів потокового типу ширина частотної смуги в 3 кГц, з якою може працювати скремблер, недостатня. Цифрове шифрування потребує смуги частот не менше ніж 10 кГц. Це призводить до необхідності підвищення швидкості передачі голосових сигналів, що можна реалізувати, використовуючи в каналах трансмісії вокодер, що, крім того, призводить до підвищення якості передачі голосових сигналів.

Структура такої системи подібна до системи, наведеної на рис. 7. Різниця полягає в тому, що сигнал після підсилення подається на вокодер, на виході якого ми отримуємо цифровий потік, що подається на суматор по модулю два (XOR), на другий

вхід цього суматора подається поточковий ключ шифрування, і на виході суматора ми отримуємо цифровий потік зашифрованого голосового сигналу, який подається на вихідний вокодер, що з цифрового потоку формує вихідний сигнал, який через випромінюючу антену передається в радіоканал. Приймочна сторона працює аналогічно, використовуючи еквівалентний поточковий ключ для розшифрування голосових даних.

При використанні такого способу шифрування надзвичайно важливою є задача синхронізації роботи системи шифрування і системи розшифрування. Проблема синхронізації може розв'язуватися різними способами. Один з таких способів наведено на рис. 8.

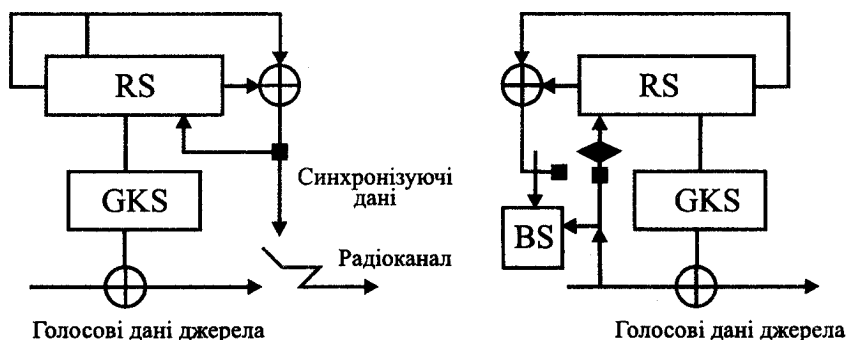


Рис. 8. Схема реалізації синхронізації ключів

На рисунку використовуються такі позначення:

- RS – регістр синхронізації;
- GKS – генератор шифрувальних ключів;
- BS – блок синхронізації.

Після ініціалізації викликаючим оператором режиму шифрування починає генеруватися послідовність даних синхронізації. Ці дані пересилаються до станції-приймача перед висиланням голосового сигналу. В приймачі перевіряється, чи отримані дані є синхронізуючими даними. При цьому існують дві можливості. В одному випадку бітова послідовність, що передана в приймач, порівнюється з еталоном, який може знаходитися в приймачі. В другому

випадку приймач в послідовності бітових даних відшукує однакові послідовності. Якщо однакові послідовності виявлено, то така послідовність приймається як послідовність синхронізуюча, і після того в приймачі починається розшифровування голосових даних. При такому способі розпізнавання синхронізуючої послідовності існує можливість уникнення помилок, пов'язаних з втратою окремих бітів, що часто трапляється в радіоканалі.

Широке використання приватних систем масової інформації, що використовують радіоканал в різних частотних діапазонах, обумовлює актуальність задач розробки та використання методів побудови радіоелектронних засобів захисту. Засоби радіоелектронного захисту складаються з двох компонент:

1. Радіоелектронного розпізнавання, яке полягає у:

- відшукуванні;
- перехопленні радіовипромінювань джерела, що підлягає розпізнаванню;
- локалізації;
- ідентифікації радіоелектронного зв'язку і його джерел;

2. Радіоелектронний захист, що полягає у протидії наперед визначеним небезпекам, які можуть бути розпізнані. Найбільш поширеними небезпеками, які можуть бути джерелом атак або основою для реалізації радіоатак, є:

- перехоплення повідомлень, що захищаються;
- дезорієнтація;
- радіолокація;
- радіоподавлення передаючої станції.

Перехоплення повідомлення можна обмежити регулюванням потужності передаючої станції. Автоматичне управління потужністю передавача здійснюється наступним чином. При зменшенні потужності збільшується кількість помилок в бітовій послідовності, яку приймає приймач. Потужність передавача зменшується до того рівня, поки кількість помилок в прийнятій бітовій послідовності не досягне гранично допустимої величини. Крім того, протидія перехвату здійснюється використанням вузьконаправлених



антен, що використовуються в мікрохвильових діапазонах радіоканалів, в яких працює мережа радіозв'язку.

Дезорієнтування полягає в передачі, у відповідності з метою використання цього способу протидії небезпекам, фальшивих даних.

Радіолокація переважно використовується для подальшого знищення передаючої станції. Протидією для такої небезпеки є використання направлених антен, управління потужністю випромінювання і т. д.

Радіоподавлення по суті направлене не на станцію, що передає повідомлення, а на станцію, яка ці повідомлення приймає, і полягає здебільшого, у зашумленні тих діапазонів частот, які використовуються для здійснення зв'язку.

Найбільш відомим способом протидії атакам на радіоканали є спосіб, який полягає у розширенні смуги радіоканалу. Відомі такі технічні розширення смуг:

- використання транкінгових систем;
- використання трансмісії пакетів;
- безпосереднє частотне розширення потоку;
- перескакування, або переключення частот каналу передачі повідомлення;
- гібридні методи протидії.

Найбільш поширеним способом протидії подавлення радіоканалу є переключення частоти каналу у відповідності з алгоритмом, який являє собою ключ методу протидії. Для реалізації цього методу будується скорельована послідовність переключення частот для групи сіток каналів, які між собою не корелюють. Сітка таких каналів вважається ортогональною. В звичайному радіоканалі використовується канал шириною 25 кГц у смузі УВЧ, наприклад, 289 МГц. При зміні частоти на 373 МГц смуга частот в 25 кГц стане перенесеною на 79 каналів. Група каналів радіозв'язку називається сіткою каналів. В радіомережі, що використовує техніку перескакування з каналу на канал, можна використовувати більше ніж одну сітку каналів в один і той же час, тому вживається термін групи сіток каналів. В системі з перескакуванням частоти можна

використовувати до 80 сіток каналів, наприклад, впорядкованих в 10 групах. На рис. 9 наведено структурну схему реалізації перескакування з каналу на канал.

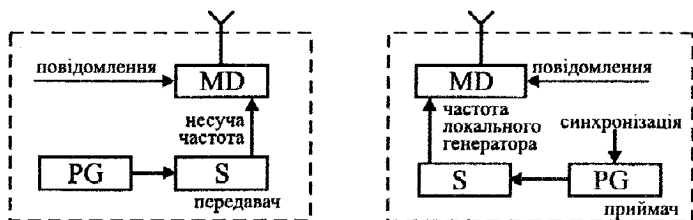


Рис. 9. Структурна схема реалізації переходів з частоти на частоту при реалізації сеансу передачі повідомлення

На рисунку використовуються такі позначення:

MD – модулятор;

S – синтезатор;

PG – псевдовипадковий генератор.

Наведена на рисунку схема реалізації переходів з однієї частоти на іншу має сенс лише тоді, коли зміна частот в передавачі та приймачі синхронізовані. При переходах або перескакуваннях з частоти на частоту (в цьому випадку мова йде про несучі частоти) частотний спектр повідомлення розширюється на цілу доступну смугу частот, завдяки чому подавлення радіоканалу стає неможливим. Найкраще розширення доступних каналів досягається в смузі УВЧ з частотами від 225 до частоти 400 МГц, що дозволяє створити до 700 каналів з шириною смуги частот 25 кГц. Параметром, що характеризує швидкодію системи перескакувань з частоти на частоту, є параметр  $z$ , що визначається як десятковий логарифм відношення ширини смуги частот, що може використовуватись для перескакування з частоти на частоту (SPD) до ширини смуги частот повідомлення (SPW), що записується у вигляді співвідношення:

$$z = 10 \log(SPW / SPD).$$

Для вищенаведеного прикладу смуги частот цей параметр буде рівний:

$$z = 10 \log(400 \text{ МГц} - 225 \text{ МГц}) / 25 \text{ кГц} = 36 \text{ dB}.$$

Захист, який здійснюється шляхом переключення частот, є захистом каналу радіозв'язку, який будемо називати TRANSEC. Для реалізації такого захисту необхідно використовувати такі вхідні параметри:

- таємні ключі (переважно 8 ключів);
- точний час;
- вибір каналу або сітки каналів оператором радіоапаратури;
- допустима або дозволена множина частот.

Параметри, що необхідні для реалізації алгоритму генерації вихідних управляючих даних, є такими:

- еталони синхронізації;
- параметри використовуваної сітки каналів;
- послідовність перескакування з однієї частоти на іншу;
- потік шифрувального ключа.

В рамках технології захисту, що ґрунтується на частотному перескакуванні, цей метод повинен застосовуватись не тільки для передачі повідомлення, але й для передачі сигналу синхронізації. Перескакування переданого сигналу синхронізації вміщує еталон даних, специфічних для використовуваної сітки. Станція приймаючої сторони здійснює моніторинг очікуваної частоти синхронізації для виявлення перескакування частоти синхронізації. В момент виявлення перескакування синхронізації в приймаючій станції виконується встановлення першопланового годинника. Після закінчення комунікації приймач повертається до тактової частоти власного синхронізуючого генератора. Для того щоб запізнення при виявленні синхронізації в станціях прийому не призвело до збоїв у роботі і втрат повідомлень, в таких системах використовуються головні станції, які слідкують за тим, щоб у різних приймачів не накопичувались допустимі запізнення, що може призвести до того, що час, яким обмежується період очікування сигналів синхронізації, може бути збільшеним. Впровад-

ження сітки реалізується через будь-яку станцію, що перебуває в режимі прийому. Така підлегла станція висилає ідентифікатор часу ( $TRQ_1$ ) до центральної станції, яка також мусить бути в режимі очікування. Після отримання сигналу  $TRQ_1$  центральна станція висилає сигнал  $TRP_1$  до всіх підлеглих станцій, які знаходяться в режимі очікування. Відповідь на сигнал  $TRP_1$  відбувається на частоті поточного перескакування, як сигнал  $TRP_2$ . Цей спосіб організації централізованої синхронізації називається hailing (привітання). Він дозволяє співпрацювати в режимі перескакування з частоти на частоту із станціями, які працюють на сталій частоті комунікації, станціям, що використовують перескакування з частоти на частоту. При реалізації цього способу захисту радіоканалу необхідно здійснювати координацію використання сіток каналів, інакше можуть виникнути колізії використання каналів. Це може призвести до самоподавлення передаючої станції.

# ТЕОРЕТИЧНІ ОСНОВИ СИСТЕМ ЗАХИСТУ ДАНИХ В ЕЛЕКТРОННИХ ЗАСОБАХ МАСОВОЇ ІНФОРМАЦІЇ

Необхідність захисту даних в електронних засобах масової інформації обумовлена наявністю небезпек, що існують відносно даних, які передаються по системах масової інформації і до систем в цілому. Тому засоби захисту являють собою сукупність технічних рішень із захисту, кожний з яких орієнтований на певний тип відомих небезпек. Створення теоретичних основ захисту даних засобів масової інформації (ЗМІ) передбачає можливість створення засобів та систем захисту, що дозволили б розв'язувати задачі забезпечення безпеки функціонування ЗМІ при виникненні не тільки відомих раніше небезпек. Завдяки таким теоретичним засобам існує можливість формувати математичні моделі системи захисту даних в ЗМІ, і на основі таких моделей не тільки створювати системи захисту з більш широкими захисними можливостями, а й досліджувати процеси, що беруть участь у реалізації процедур захисту та процедур протидії атакам. Перш ніж розглядати математичні основи опису системи захисту, необхідно визначитися з основними поняттями, які будемо використовувати у дослідженнях. До таких понять належать:

- загроза;
- небезпека;
- атака;
- засіб захисту;
- система захисту.

Під загрозою будемо розуміти таку властивість, або параметр об'єкту захисту, використання якого дозволяє здійснити несанкціоновану взаємодію об'єкта захисту із зовнішніми об'єктами або дозволяє здійснити несанкціоноване втручання у функціонування об'єкта чи несанкціоновані його зміни.

Під небезпекою, для окремого конкретного об'єкта, будемо розуміти певний зовнішній об'єкт або процес, які можуть ініціювати дії, що направлені на несанкціоновану взаємодію з об'єктом захисту.

Під засобом захисту будемо розуміти таку компоненту об'єкта захисту чи окремих засобів, що існують незалежно від об'єкта, які розпізнають процес несанкціонованого втручання та здійснюють протидію відповідному втручання. При цьому засоби захисту не беруть участі у функціонуванні об'єкта і реалізації його основних функцій.

Система захисту являє собою певним чином організовану сукупність засобів захисту в єдиній структурі, в рамках якої окремі засоби захисту взаємодіють між собою з метою розв'язку задач розпізнавання та протидії несанкціонованому втручання в роботу об'єкта, який передбачається захищати.

Під атакою будемо розуміти послідовність дій, яка ініціюється певною небезпекою для здійснення несанкціонованого втручання і для цього використовує загрози. Атака може бути успішною і неуспішною. Успішною називається така атака, в результаті якої реалізована або досягнута ціль, яка повинна формуватися небезпекою, що ініціює і формує відповідну атаку.

Виходячи з наведених вище якісних визначень, можна досить конкретно виділити основні особливості, що характеризують небезпеку як таку. До таких особливостей належать:

- наявність інформації про об'єкт, який передбачається атакувати;
- можливість формування окремої атаки;
- здатність формувати атаку як таку, що може досягти сформованої в рамках безпеки цілі.

Відзначимо, що небезпеку як деякий зовнішній об'єкт чи зовнішній процес не будемо ототожнювати з об'єктами чи процесами, які складають природне зовнішнє середовище, в якому функціонує об'єкт охорони, незважаючи на те, що це зовнішнє середовище або його фрагменти можуть впливати на функціонування об'єкта таким чином, що останній не зможе розв'язувати свої функціональні

задачі, для яких його було створено. Дія зовнішнього середовища, в якому передбачається функціонувати об'єкт і який передбачається охороняти, призводить до передбачуваного впливу цього середовища на об'єкт, і цей вплив повинен враховуватися при проектуванні об'єкта. Результат такого впливу, величина та характер якого можуть змінюватися в процесі функціонування об'єкта, може бути відомим, або передбачуваним, чи непередбачуваним. Такий вплив може призводити, у випадку ЗМІ, до зашумлення каналу, до втрати бітів в потоці даних, що передаються через канал, та до виникнення несправностей в програмних чи апаратних засобах, що реалізують ЗМІ. Для розв'язку задач захисту від таких факторів, в цьому випадку ЗМІ використовується системами діагностики, використовуються різноманітні програми, алгоритмічні чи апаратні засоби підвищення надійності системи. Прикладом протидії проти втрати бітів в каналі, при передачі їх послідовностей через канал, можуть слугувати методи використання коректуючих кодів для передачі даних.

Виходячи з викладеного вище, під небезпекою слід розуміти деякий створений об'єкт чи процес, який за визначенням не є частиною природного зовнішнього середовища. Тому небезпека являє собою штучно створений об'єкт або процес, який формувався або створювався з метою реалізації відповідної небезпеки. Таким чином, в склад небезпеки повинні входити досить конкретні компоненти, до яких належать такі:

- підсистему формування атаки;
- підсистему збору і аналізу інформації стосовно об'єкта, який передбачається атакувати;
- підсистему формування цілі атаки;
- підсистему використання результатів успішно проведеної атаки;
- підсистему маскування.

Система масової інформації являє собою не тільки статичну структуру, а й систему динамічну, в якій відбуваються досить складні процеси, пов'язані з передачею даних, вибір необхідного трафіка та інших процесів, що є необхідними складовими всього

процесу функціонування ЗМІ. Крім того, загальноновизначеним є факт існування небезпек для функціонування ЗМІ, які ініціюють відомі атаки. Існує низка розроблених засобів захисту ЗМІ, які ефективно використовуються в задачах забезпечення безпечного функціонування ЗМІ. Більшість засобів захисту, що використовуються в ЗМІ, має в своїй основі розвинутий математичний апарат, в рамках якого можна розглядати не тільки задачі, зв'язані з даними конкретним засобом, а й задачі, що стосуються узагальнень можливостей цих засобів при їх синтезі в загальну систему захисту. Тому розглянемо теоретичні основи засобів захисту, що використовуються, та можливості їх розширення. Одним із засобів, що найбільш широко використовується, є шифрування даних, що передаються по каналах зв'язку. Використання цього засобу захисту пов'язано з протидією найбільш поширеним атакам, що полягають у:

- перехопленні даних з ціллю несанкціонованого використання інформації, що описується відповідними даними;
- заміні інформації, що передається;
- реалізації шифрування в режимі реального часу даних, що передаються через канал;
- реалізації управління ключами в режимі реального часу, який визначається швидкістю передачі даних через канал;
- обмеженні періоду актуальності ключів, шифрування, що реалізуються безпосередньо в каналі;
- використанні ключів, що є співвимірними з розмірами даних, які передаються через канал.

Перехоплення даних з ціллю використання інформації, яку ці дані несуть, є атакою не стільки на ЗМІ, скільки на методи укриття інформації, для опису якої використовуються відповідні дані. Ця особливість обумовлена тим, що перехоплені дані незалежно від каналу можуть піддаватися атакам дешифрування. В цьому випадку ЗМІ розглядається як середовище, яке є більш доступним для атак перехвату, ніж об'єкти, в яких дані перетворюються, аналізуються чи зберігаються. Більше того, засоби захисту, що полягають у шифруванні, можуть не бути пов'язаними безпо-



середньо з каналами передачі, якщо мова йде про передачу цифрових даних. У випадку, коли фізичне джерело даних не є вираженими цифровими даними, а являє собою, наприклад, голосові дані чи деякий реєструючий прилад, що не запам'ятовує реєстровані дані, оскільки таке запам'ятовування є недоцільним, то канал зв'язку, в цьому випадку, є одним з основних засобів, що забезпечує виконання основних прикладних функцій, однією з яких є передача даних. Прикладом таких прикладних задач може бути задача збору даних сейсмічного характеру, які є територіально рознесені, за своєю природою, а обробка таких даних є можлива тільки в деякому централізованому засобі. У зв'язку з цим, до каналних засобів захисту, що являють собою методи шифрування, будемо відносити тільки потокові шифри, для яких характерні прості функції перетворення, оскільки на такі перетворення накладаються обмеження на інтервал часу, який може бути відведений для процесу шифрування. Переважно таке перетворення зводиться до реалізації функції сумування по модулю два (XOR).

Для того, щоб забезпечити високий рівень складності алгоритму шифрування, використовуються більш складні процедури формування ключів, оскільки ключі можуть бути підготовлені до моменту початку передачі даних. Оскільки ключі шифрування і розшифрування повинні бути на двох сторонах каналу передачі, то виникає задача обміну ключами не тільки з точки зору збереження їх таємності, але й з точки зору швидкості такої передачі. Ця задача може розв'язуватися такими способами:

- безпосередньою передачею ключів перед початком сеансу зв'язку;
- формуванням ключа на передаючій і приймальній стороні перед початком сеансу зв'язку;
- використанням наперед вибраних ключів шифрування протягом ряду сеансів зв'язку.

Визначення часу актуальності ключів, що використовуються для шифрування, визначається складністю функцій формування ключів. Але якісно така залежність полягає в наступному. Чим складніша функція формування ключа і чим ключ довший, тим

більшим може бути інтервал часу актуальності ключа. В цьому випадку міра співвимірності ключів потокових алгоритмів з довжиною шифрованих даних є одним з важливих параметрів ключа і міри захисту, яка може бути реалізована в каналі. Але значне збільшення цієї міри може призвести до зниження швидкості передачі даних через канал.

Формально засіб захисту, що ґрунтується на використанні потокових алгоритмів шифрування даних, які підлягають передачі, можна описати таким чином:

$$Z_{sh} = F_{sh} \{D[d(\omega), d(k)], \delta t(k), \varphi(\omega, k), \psi(k)\},$$

де  $d(\omega)$  і  $d(k)$  – довжина повідомлення і довжина ключа повідомлення  $\omega$ ;  $D[d(\omega), d(k)]$  – функція, що характеризує взаємозв'язок між довжиною ключа та довжиною повідомлення;  $\delta t(k)$  – час актуальності ключа  $k$ , який обчислюється в кількості циклів його використання;  $\varphi(\omega, k)$  – функція перетворення  $\omega$  за допомогою ключа  $k$ ;  $\psi(k)$  – функція вибору або функція формування ключа  $k$ ;  $F$  – функція, що пов'язує між собою перераховані вище аргументи. Функція  $F_{sh}$ , записана в явному вигляді, являє собою модель відповідного засобу захисту  $Z_{sh}$ .

Розглянемо, який математичний апарат може бути використаний для побудови моделей  $Z_{sh}$ . Насамперед визначимося з одиницями виміру окремих складових аргументів і самих аргументів. Приймаючи до уваги специфіку роботи каналів передачі даних, довжину повідомлення та довжину ключів будемо вимірювати кількістю біт, з яких це повідомлення та ключ складаються, оскільки будемо розглядати тільки цифрові канали. Значення функції  $D[d(\omega), d(k)]$  буде вимірюватися величинами, які залежать від типу функції  $D$ . Наприклад, якщо функція  $D$  являє собою різницю між  $d(\omega)$  і  $d(k)$ , то  $D$  буде вимірюватися бітами, або  $|d(\omega) - d(k)| = m[\text{Bit}]$ , якщо функція  $D$  буде являти собою спосіб вимірювання кратності довжини ключа відносно довжини повідомлення, то функція  $D$  як аргумент буде величиною безрозмірною,

або  $d(\omega) = m \cdot d(k) = d_1(k) * d_2(k) * \dots * d_m(k)$ , де "\*" – оператор додавання, або оператор, що визначає інший спосіб визначення співвідношення між  $d(\omega)$  і  $d(k)$ . Аргумент  $\delta t(k)$ , що за визначенням вимірюється кількістю циклів використання ключа  $k$ , також вимірюється безрозмірною величиною. Тим не менше, цей аргумент може бути приведено до розмірності часу.

Необхідність в цьому визначається тим, що канал може використовуватись з різною інтенсивністю, і в цьому випадку одна і та ж кількість циклів може відбутися за різні інтервали часу. Це означає, що в атакуючого буде більше або менше часу на визначення ключа і, відповідно, на несанкціоноване розкриття переданого повідомлення. Тому в рамках моделей  $Z_{sh}$  будемо розглядати не параметр  $\delta t(k)$ , а швидкість передачі окремих повідомлень, кожне з яких передається в межах одного циклу. Таку швидкість будемо вимірювати кількістю циклів за вибрану одиницю часу.

Визначення розмірності для функції  $\varphi(\omega, k)$ , як аргумента моделі  $Z_{sh}$ , буде визначатися наступним чином. В системах масової інформації для передачі даних в основному використовуються поточні шифри, оскільки вони забезпечують можливість досягнути максимальної швидкості процесу шифрування. Основною функцією цього шифру є функція XOR для бітових послідовностей повідомлення і ключа. Функцію  $\varphi(\omega, k)$  будемо розглядати окремо для кожного циклу використання ключа. В межах одного циклу використання ключа, який будемо позначати  $t(k)$ , послідовність бітового коду повідомлення будемо позначати  $\omega_i$ . Отже, послідовність бітового коду зашифрованого повідомлення, яке сформовано завдяки функції  $\varphi(\omega, k)$ , будемо позначати  $y_i$ . Тоді можна записати, що  $y_i = \varphi(\omega, k)$ . Очевидно, що  $\omega_i$  може відрізнятися від  $y_i$  такими параметрами:

- хемінговою віддаллю  $h$  між  $y_i$  і  $\omega_i$ ;
- типом розподілу величини  $h(\omega_i, y_i)$  по фрагментах зашифрованого повідомлення  $y_i$ ;

— різницею між десятковими образами  $\omega_i, y_i$ .

Хемінгова віддаль вимірюється співвідношенням :

$$h(\omega_i, y_i) = \sum_{i=1}^k s_i(\omega_i \oplus y_i),$$

що відповідає кількості бітових позицій, якими відрізняються коди  $\omega_i$  і  $y_i$ . Зрозуміло, що  $\max h(\omega_i, y_i) = n$ , де  $n$  — кількість бітових позицій в  $\omega_i$ , що можна записати  $y_i = \bar{\omega}_i$ . Очевидно, що в цьому випадку ефективність  $\varphi(\omega_i, k)$  є мінімальною і її будемо вважати рівною нулю, або  $[h(\omega_i, y_i) = \max] \rightarrow \varepsilon[\varphi(\omega_i, k)] = 0$ .

Також нульова ефективність у функції  $\varphi(\omega, k)$  буде у випадку, коли  $h(\omega_i, y_i) = 0$ , або  $h(\omega_i, k) = \min$ , що можна записати:  $y_i = \omega_i$ . Тому в загальному випадку запишемо наступну умову існування мінімальної ефективності  $\varphi(\omega, k)$ :

$$[h(\omega_i, y_i) = \max] \vee [h(\omega_i, k) = \min] \rightarrow \varepsilon[\varphi(\omega_i, k)] = 0.$$

Визначимо умову збільшення ефективності функції шифрування. Формально таку умову можна записати у вигляді співвідношення:

$$\varepsilon[\varphi(\omega_i, k)] = \alpha \cdot h(\omega_i, y_i), \quad (1)$$

де  $\alpha$  приймає значення з діапазону  $[0,1]$ . За цим співвідношенням можна визначити умову максимальної ефективності функції шифрування на основі дослідження моделі засобу захисту  $Z_{sh}$  і моделі загрози, яка відповідає цьому засобу  $S_{sh}$  та дослідження їх взаємодії.

Коди повідомлення  $\omega_i$  та зашифрованого повідомлення  $y_i$  мають фіксовані розміри, які визначаються кількістю бітових позицій, або  $d(\omega_i)$  і  $d(y_i)$  рівні. Значення  $\varepsilon[\varphi(\omega_i, k)]$  буде максимальним при деякому значенні  $\alpha_i$  у співвідношенні (1). Оскільки  $\alpha \cdot h(\omega_i, y_i)$  в межах всього повідомлення на  $d(y_i)$  може

розміщуватися рівномірно або нерівномірно, що будемо позначати  $\mu[d(y_i), \alpha \cdot h(\omega_i, y_i)]$ .

Приймемо, що  $d(\omega_i) = d(y_i)$  для  $\varphi(\omega, k)$ . Подамо  $d(y_i)$  у вигляді фрагментів, що розміщуються послідовно. Це можна записати у вигляді:  $y_i = y_1(\beta_1) * y_2(\beta_2) * \dots * y_m(\beta_m)$ , де  $\beta_i$  – кількість бітових позицій у фрагмента зашифрованого повідомлення  $y_i$ . Приймемо, що виконується умова:

$$d(y_i) = d[y_1(\beta_1)] + d[y_2(\beta_2)] + \dots + d[y_m(\beta_m)] = \sum_{i=1}^m d[y_i(\beta_i)],$$

де  $d[y_i(\beta_i)]$  – довжина фрагмента  $y_i$ . Очевидно, що кожному фрагменту  $y_i(\beta_i)$  можна зіставити відповідний фрагмент  $\omega_i(\beta_i)$ , і ця відповідність буде визначатися номерами бітових позицій в  $\omega_i$  і  $y_i$ , оскільки  $d(\omega_i)$  і  $d(y_i)$  рівні. Приймемо, що вибрано  $\beta_i = \beta_{const} = \beta^*$ . Тоді можна записати:

$$h(\omega_i, y_i) = h_1[\omega_1(\beta^*)] + \dots + h_m[\omega_m(\beta^*)].$$

Внаслідок того, що  $\beta^* = const$ , можна записати:

$$h(\omega_i, y_i) = h[\omega(\beta^*), y(\beta^*)] \cdot m. \quad (2)$$

Якщо виконується співвідношення (2), то розподіл  $h(\omega_i, y_i)$  є рівномірним, або абсолютно рівномірним по  $m$ , що формально запишемо у вигляді:  $\mu[d(y), \alpha \cdot h(\omega_i, y_i)] = \mu(y_i, m_i)$ , де  $m_i$  – розмір фрагмента в бітах. Очевидно, що параметр  $\mu(y_i, m_i)$  пов'язаний з ефективністю  $\varepsilon[\varphi(\omega_i, k)]$  і цей зв'язок також можна відстежити тільки в рамках моделі засобу захисту  $Z_{sh}$ .

Наступним аргументом моделі засобу захисту  $Z_{sh}$  є функція  $\psi(k)$ , яка, по суті, описує спосіб формування ключа шифрування  $k_i$ . Загальноприйнятий на сьогодні підхід до реалізації методів

створення ключів  $k_i$ , або до реалізації функції  $\psi$  полягає у використанні псевдовипадкових генераторів ключів шифрування.

Такий підхід до реалізації функції  $\psi(k_i)$  не забезпечує можливості використання зворотного зв'язку між величиною захисту, методом шифрування та формуванням відповідного ключа шифрування  $k_i$ , який є таємним, і тим самим є гарантом захищеності зашифрованого повідомлення  $y_i$ , оскільки сама функція шифрування  $\psi(\omega_i, k_i)$ , в більшості випадків, через свою простоту реалізації є відомою, в тому числі і для несанкціонованих учасників чи користувачів системи масової інформації. Завдяки використанню такого параметра, як ефективність шифрування повідомлення, що передається каналом зв'язку, існує можливість пов'язати  $\varepsilon[\psi(\omega_i, k_i)]$  з функцією формування ключа  $\psi(k_i)$ . Спосіб реалізації такого зв'язку тісно пов'язаний з методом реалізації функції  $\psi(k_i)$ . Якщо прийняти, що основою для реалізації  $\psi(k_i)$  будуть псевдовипадкові генератори ключів, що реалізуються переважно на послідовних регістрах із зворотними зв'язками, то один з способів реалізації зворотного зв'язку між моделлю засобу захисту  $Z_{sh}$  і її параметром  $\varepsilon[\psi(\omega_i, k_i)]$  може полягати у модифікації зворотних зв'язків в регістрах, на яких побудовано псевдовипадкові генератори. В цьому випадку алгоритм модифікації ґрунтується на уявленнях про поля багаточленів, при цьому використовуються поля Галуа  $GF(p^n)$ . Такі багаточлени описують регістри генераторів псевдовипадкових послідовностей, причому такі багаточлени повинні бути непровідними.

Розглянемо засоби захисту від втручань в роботу системи масової інформації з метою порушення її штатних режимів роботи  $Z_w$ . Такі засоби захисту особливо актуальні в системах масової інформації, що використовують радіоканали, які фізично доступні для здійснення безпосередніх атак на систему. До такого типу атак належать:

- атаки, що призводять до порушення роботи в радіоканалі, які можна розділити за типом порушень наступним чином:
  - створення вузькосмугових завад;
  - створення завад, що переключаються або перескакують з однієї смуги частот на іншу;
  - створення загальних завад;
  - послідовні завади;
  - широкосмугові завади;
  - імпульсні завади.
- атаки пасивного характеру, що направлені на зміну фізичних параметрів в середовищі розповсюдження електромагнітних полів.

Створення завад полягає у використанні радіостанцій, що випромінюють радіосигнали, найчастіше шумоподібного типу, з метою зашумлення радіосигналів, що несуть інформацію, яка передається активною станцією, що обслуговує відповідний канал зв'язку.

Захист проти таких атак і відповідно таких небезпек потребує організації специфічного способу зв'язку, який будемо називати зв'язком з віддзеркалюванням. Суть цього способу полягає у тому, що передаюча станція передає інформацію окремими посилками, а приймальна станція в перервах між цими посилками в дзеркальному режимі передає кожну посилку назад до передаючої станції. Завдяки цьому передаюча станція має можливість контролювати факт виникнення завад на кожному такті обміну даними. Тоді в залежності від типу завад передаюча станція здійснює такі дії для протидії атакам:

- при вузькосмугових завадах відбувається переключення на інші смуги каналу передачі;
- при створенні імпульсних завад передаюча станція формує окремі посилки даних в проміжках між появою імпульсних завад;
- при завадах, що переключаються з однієї смуги частот на іншу, станція організує переключення передавача таким

чином, щоб смуги, на яких з'являються завади, і смуги, на яких передаються дані, не збігали;

- при виникненні загальних завад, які з'являються в активних смугах частот, передаючі станції переходять на проміжні смуги частот, які не є виділеними для роботи станцій;
- при створенні послідовних завад, що полягають у їх послідовному переході з однієї частоти на іншу, передаюча станція здійснює перехід з однієї смуги на іншу в послідовності, яка не відповідає послідовності надання завад в радіоканалі;
- при використанні широкосмугових завад передаюча станція може збільшувати потужність випромінювальних сигналів або модифікувати спосіб кодування інформації в радіоканалах, який не відтворюється в передавачі, що здійснює відповідну атаку у вигляді шуму.

В цьому випадку засобами захисту є засоби, що підтримують дзеркальний спосіб обміну даними. Очевидно, що цей засіб є розподіленим і знаходиться як в передаючій станції, так і в приймальній станції. Ці засоби дозволяють в автоматичному режимі виявляти атаки, що використовують завади. Другою компонентою засобів захисту є засоби управління режимом передачі даних в залежності від типу розпізнаних радіозавад. Ця складова засобів захисту може знаходитися тільки в передаючій станції, якщо передбачається однонаправлений обмін даними.

Оскільки такі засоби захисту орієнтовані тільки на радіоканали, а в мобільній системі радіоканал використовується лише між MS і MTS, то детально розглядати такі засоби і відповідно загрози, що існують в системах радіозв'язку, ми не будемо.

## **Моделі систем захисту інформації**

Система масової інформації передусім орієнтується на надання послуг широкому колу споживачів, при цьому спектр послуг постійно розширюється з розвитком технічних та програмних засобів реалізації такої системи. Для здійснення обслуговування користувачів системи масової інформації, в рамках останньої, необхідною компонентою є підсистема організації та контролю



доступу. Оскільки ініціатором несанкціонованого доступу в нашому випадку може бути тільки абонент, що володіє мобільним телефоном, то обмежимося механізмами контролю доступу, що реалізуються за участю мобільного телефона. Розглянемо базовий алгоритм, який використовується при аутентифікації абонента системи масової інформації. Оскільки він схематично не є складним, то його доцільно описати у вигляді послідовності дій, які виконуються за структурною схемою, що наведена на рис. 10.

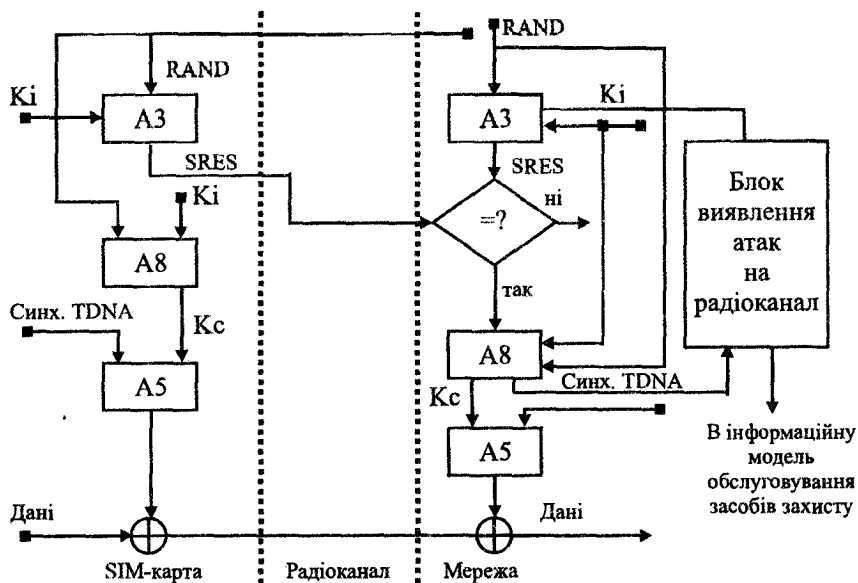


Рис. 10. Структурна схема реалізації функції аутентифікації абонента мобільного телефона

На рисунку прийнято такі скорочення:

A3 – алгоритм аутентифікації абонента;

A5 – алгоритм шифрування даних;

A8 – алгоритм визначення ключа шифрування даних;

RAND – псевдовипадкове число, що формується в мережі зв'язку для кожного окремого сеансу зв'язку;

Ki – ключ для алгоритму A3 (для підтвердження ідентичності абонента);

Kc – ключ для шифрування даних, що передаються по каналах радіозв'язку;

SRES – код ідентифікації ідентичності абонента;

Синх. TDNA – синхронізація кадру передачі даних через радіоканал.

У відповідності з наведеним рисунком аутентифікація абонента відбувається з ініціативи мережі при реєстрації абонента в мережі. Мережа формує псевдовипадкове число RAND і передає його на мобільний телефон, в якому алгоритм A3, що записаний в пам'яті SIM-карти, використовуючи таємний ключ Ki, який також знаходиться на SIM-карті, формує код SRES, який являє собою електронний підпис даного мобільного телефона. Код SRES передається в мережу, де формується з допомогою алгоритму A3 і ключа Ki, такий же код SRES. Якщо ці два коди однакові, то абонента ідентифіковано, і з ним може відбутися сеанс зв'язку. Для цього абонент, використовуючи алгоритм A8, ключ Ki і псевдовипадкове число RAND, генерує ключ Kc для шифрування з допомогою алгоритму A5 даних, що передаються з мобільного телефона в мережу через радіоканал.

Базовою компонентою, що реалізує контроль доступу мобільного телефона до мережі, є спеціалізована мікропроцесорна карта SIM. На цій карті, що вставляється в мобільний телефон, вміщується така інформація:

- Ki – ключ аутентифікації;
- IMSI – індивідуальний ідентифікаційний номер абонента, який складається з коду території, коду мережі та номера абонента;
- A3 – алгоритм шифрування для визначення SRES;
- A8 – алгоритм шифрування для визначення Kc;
- TMSI – тимчасовий реєстраційний номер абонента, який складається з коду території, який використовується для реєстрації абонента в межах чужої мережі (в новому реєстрі VLR);

- LAI – ідентифікатор власного оператора, в якого зареєстровано телефон;
- PIN – персональний ідентифікаційний код, який є паролем абонента і використовується для інсталяції карти SIM для конкретного абонента;
- PUK – персональний ідентифікатор абонента, що використовується для розблокування карти SIM.

З вищенаведеного видно, що процес ідентифікації і аутентифікації виконується на різних етапах функціонування мобільного телефону в системі масової інформації. Базовим елементом, що реалізує ці функції, є змінна мікропроцесорна карта SIM. Параметри, що забезпечують санкціоновану ідентифікацію абонента, розміщуються на карті SIM та в мережі. До таких параметрів належать число RAND, ключ K<sub>i</sub>, персональний ідентифікаційний код та алгоритми шифрування A3 і A8. Для того, щоб можна було говорити про ті чи інші засоби захисту, що стосуються ідентифікації чи аутентифікації абонента, необхідно розглянути небезпеки несанкціонованого доступу. Очевидно, що небезпечні ситуації, які можуть створити несанкціоновані абоненти, потребують, крім телефонного апарата ще й використання комп'ютера та спеціалізованих апаратних засобів. Небезпеки, що направлені на порушення систем санкціонованого доступу, можна розподілити на такі класи небезпек:

1. Небезпеки, що призводять до створення можливості несанкціонованого використання функціонування мобільних станцій (MS);
2. Небезпеки, що призводять до створення можливості несанкціонованого використання чужих ресурсів систем масової інформації або ресурсів санкціонованих абонентів;
3. Небезпеки, що призводять до втрат в системах масової інформації, втрат в оплаті за послуги, які були надані операторами в результаті порушення засобів захисту від несанкціонованого доступу до ресурсів мережі.

Будемо розглядати небезпеку другого типу, яка, по суті, є загальною за своїми наслідками. Перша небезпека відрізняється від

другої тільки способом реалізації атак, а третя небезпека полягає у зміні персоналіфікації осіб, що несуть втрати в результаті здійснення атак.

На загальному рівні атака на засоби захисту від несанкціонованого доступу буде вважатися успішною, якщо в результаті її реалізації несанкціонований абонент ідентифікується системою як санкціонований. Одними з основних параметрів засобів захисту  $Z_{do}$  є персональний ключ  $K_i$  та персональний ідентифікаційний код PIN. Ці два параметри забезпечують два рівні захисту від несанкціонованого доступу. Ідентифікатор PIN захищає доступ на рівні розпізнавання власної карти SIM, яка вміщує інші компоненти захисту. У випадку, коли небезпека розглядається на рівні її моделювання, цей рівень захисту втрачає сенс, оскільки функції та параметри, що вміщено на карті, реалізуються в моделі. Тому будемо досліджувати модель засобу захисту доступу  $Z_{do}$  в таких варіантах:

- коли модель має легальний, зареєстрований в мережі, PIN;
- коли модель не має легального ідентифікаційного номера PIN, що зареєстрований в мережі.

В другому випадку має місце ситуація, коли параметр, що використовується для захисту, носить характер константи, яка формується на основі персональних технологічних характеристик, пов'язаних з виготовленням відповідних мікропроцесорних карт. Прикладом однієї з таких характеристик може бути серійний номер відповідної карти. Такий PIN можна розглядати як пароль, що ідентифікує відповідну мікропроцесорну карту. В цьому випадку засіб захисту типу  $Z_{do}$  в частині, що стосується використання паролів, може описуватися методами, які використовуються для протидії атакам на паролі в системах доступу до комп'ютерних мереж. Іншою особливістю використання PIN в мобільних системах є те, що відповідна карта блокується, коли вводиться неправильний PIN декілька разів підряд. Таким чином, формування такого засобу захисту являє собою суто технічну задачу, оскільки його можна розглядати як засіб захисту, який діє на основі

бінарного алгоритму аналізу, такий засіб захисту будемо називати засобом захисту порогового типу, або  $Z_{do} = Z_{\varphi} * Z_p$ .

Розглянемо засіб захисту  $Z_{\varphi} \in Z_{do}$ , який ґрунтується на використанні персонального ключа  $K_i$  з алгоритмом АЗ. У випадку використання схеми, що наведена на рисунку 10, засіб захисту  $Z_{\varphi} \in Z_{do}$  оперує ключем  $K_i$ , який є, в цьому випадку, гарантом забезпечення захисту при спробі несанкціонованої реєстрації мобільного телефона, оскільки алгоритм АЗ не є таємним, і різні його модифікації виробників телефонних апаратів повинні бути доступними для операторів зв'язку. Засоби захисту  $Z_{do}$  реалізуються не тільки в межах мобільного телефона, але й в компонентах мережі і насамперед в реєстрі HLR. Кожний процес обміну між мобільними телефонами супроводжується передачею IMSI, в якому використовуються персональні номери телефонів та користувачів. Тому засіб захисту  $Z_{\varphi} = Z_{\varphi_1} \cdot Z_{\varphi_2}$ , отже, в загальному можна записати:

$$Z_{do} = f(Z_{\varphi_1}, Z_{\varphi_2}, Z_p).$$

Розглянемо складові засоби захисту  $Z_{do}$ . Спосіб функціонування складової  $Z_{\varphi_1}$  досить простий. Таємний персональний ключ  $K_i$ , що використовується для перетворення випадкового числа RAND з допомогою алгоритму АЗ, є гарантом того, що реєстрація карти SIM, в якій розміщується цей ключ, є правильно авторизованою. Особливістю механізму авторизації карти SIM і, відповідно, мобільного телефона є те, що реєстрація відбувається автоматично при ввімкненні живлення, а другою особливістю є те, що кількість спроб авторизації або реєстрації підряд є обмеженою. Більше того, рішення про реєстрацію приймається в результаті реалізації такої ж схеми, але в системі оператора мережі і MS отримує інформацію тільки про результат відповідної реєстрації. Тому цю компоненту засобу захисту не слід обмежувати лише границями апаратно-програмних засобів MS.

Будь-яка небезпека з визначених вище при реалізації атак не буде обмежуватися тільки однією частиною засобу захисту  $Z_{do}$ , наприклад, частиною  $Z_{pr}$ . Тому необхідно розглядати засіб захисту  $Z_{do}$  в цілому, який включає частину, що знаходиться в MS, і частину, яка знаходиться в AUC.

Насамперед зазначимо, що несанкціоноване використання ресурсів при успішній атаці на засіб захисту  $Z_{do}$  завжди передбачає використання несанкціонованої MS. Під несанкціонованою мобільною станцією будемо розуміти MS, яка дублює легальну MS, що уже зареєстрована в реєстрі HLR. Використання несанкціонованої MS передбачає необхідність здійснення певних маніпуляцій з окремою MS, яку передбачається перевести в статус нелегальної MS (NMS). На відміну від NMS, легальну станцію MS, відносно якої вибирається NMS, будемо позначати LMS. Атаки на засоби  $Z_{do}$  в системах масової інформації, на відміну від подібних атак в комп'ютерних мережах, не виконуються тільки у вигляді програмної реалізації, яка відображає всю послідовність дій, що необхідна, для досягнення атакою відповідної мети, а складаються з послідовності дій, що виконуються з MS з метою переведення її в статус NMS, а нелегальне використання ресурсів мережі здійснюється шляхом легального звертання до системи масової інформації за легальними послугами, що надаються електронними ЗМІ. Першим етапом атаки на  $Z_{do}$  в ЗМІ є сканування радіоканалів з метою вибору MS, яка була би кандидатом на LMS. Зрозуміло, що на роль NMS буде вибрана MS, незареєстрована в мережі, або MS, яка внаслідок різних причин була заблокована в AUC. Після цього всі  $Z_p$  з  $Z_{pr}$  і  $Z_{ps}$  замінюються. Оскільки будь-які порогові засоби являють собою константи, то шляхом модифікації програмних компонент  $Z_{do}$  в MS можна відповідні параметри замінити або обходити. Більше того, така підміна може бути динамічною, що дозволяє своєчасно міняти MS в кандидатах на LMS, що є необхідною умовою уникнення періодично ініціюючих процедур перевірки зі сторони мережі. Очевидно, що NMS, для кожного

конкретного випадку, який може мати місце в мережі відносно MS, повинен формуватись окремо, з врахуванням особливостей цього випадку. При проведенні сканування можна виявити SRES, RAND та IMSI, що передаються по радіоканалу. Для створення NMS необхідно встановити  $k_i$  потенційної LMS. Оскільки можна записати, що

$$\text{SRES} = A3(k_i, \text{RAND}),$$

то при побудові функції  $A3^{-1}$ , можна встановити  $K_i$  у відповідності із співвідношенням  $k_i = A3^{-1}(\text{SRES}, \text{RAND})$ . На сьогодні  $A3$  не є таємним, тому одним з параметрів  $Z_{\varphi_i}$  є міра реалізації зворотного встановлення явного тексту, зашифрованого алгоритмом типу  $A3$ , яку будемо позначати через  $\chi$ . Тоді можна записати:

$$\chi = f\left\{x, \left[A3^{-1}\left[A3(x)\right]\right]\right\},$$

де  $x$  – число, що перетворюється алгоритмом  $A3$ .

Наступним параметром  $Z_{\varphi_i}$ , як і  $Z_{\varphi_s}$  є інтервали часу, через які в мережі проводяться додаткові контролюючі дії, в результаті яких може виявитися факт існування NMS. Прикладом таких дій може бути заміна  $k_i$  або додаткова вимога щодо реєстрації всіх MS. Очевидно, що заміна  $k_i$  потребує безпосереднього втручання в MS зі сторони дистриб'юторів оператора. Це досягається завдяки використанню обмежень на періоди використання SIM-карт та інших умов експлуатації MS. Таким чином, наступним параметром  $Z_{\varphi_i}$  є інтервал часу  $\tau_i$ , що визначається загальним правилом для всіх абонентів електронних ЗМІ. Крім інтервалу часу  $\tau_i$ , який визначається оператором мережі, може встановлюватися іншими правилами, що визначають умови використання MS чи SIM-карти легального абонента. Очевидно, що ці умови будуть враховуватися, при створенні NMS. Такі умови можуть стосуватися різних послуг, наприклад, послуги щодо надання роумінгу та інші. Тому, наступним параметром засобу захисту  $Z_{\varphi_i}$  є параметр умов, який

будемо позначати літерою  $\eta$ . Цей параметр умови використання MS будемо визначати співвідношенням:

$$\eta = \varphi(Q_{op}),$$

де  $Q_{op}$  – додаткові умови оператора системи масової інформації.

Кожний з абонентів деякої системи масової інформації може використовувати перелік послуг, що залежать від можливостей самих MS та від можливості мережі зв'язку GSM. В залежності від кількості можливих функцій MS, що розширюють асортимент послуг, які надаються абонентам, залежить можливість захисту MS від несанкціонованого доступу. Наприклад, якщо використовується в рамках ЗМІ система GPRS і відповідні можливості надаються користувачеві, то виникає додаткова можливість виявлення інформації для формування атак. Наприклад, в рамках системи масової інформації, що підтримує технологію WATM, використовується протокол WAP, який вміщує значно більше інформації про виконувану транзакцію. Такий параметр будемо позначати літерою  $\lambda$  і визначатимемо у відповідності до співвідношення:

$$\lambda_i = \psi_i(Q_{ser}),$$

де  $Q_{ser}$  – номенклатура послуг, що додатково надається системою масової інформації користувачу, наприклад, послуга з визначення місцезнаходження користувача.

Параметр  $\lambda_i$  теоретично являє собою розширення параметра  $\eta$ . Але їх розподіл, в цій роботі, обумовлений доцільністю розрізняти класи послуг, що надаються в межах традиційних на сьогодні технологій ЗМІ, типу WATM, що дозволяють MS працювати з ресурсами мережі Internet.

В загальному вигляді можна записати співвідношення для засобу захисту від несанкціонованого доступу до системи масової інформації:

$$Z_{do} = F\{\chi, \eta, \tau, \lambda\}.$$



Розглянемо засоби захисту від моніторингу  $Z_{mo}$ , що в системах масової інформації орієнтовані на захист радіоканалів. Особливо розвинутими ці засоби захисту є в системах масової інформації, в яких радіоканали значно більші, ніж канали кабельні. Виходячи з цього, до засобів захисту від моніторингу слід відносити всі ті засоби, що орієнтовані на здійснення радіоелектронного захисту. Відомими методами радіоелектронного захисту є такі:

- переключення діапазонів частот радіоканалу в процесі реалізації трансмісії;
- безпосереднє розсіювання потоку, що призводить до збільшення ширини смуги частот, яка надається сигналу при його передачі через радіоканал;
- використання трансмісії пакетів та інші.

Кожний з цих методів характеризується певними параметрами, за якими можна оцінювати міру захисту каналу від радіоперехоплення, чим, по суті, є моніторинг радіоканалу. Наприклад, переключення діапазону частот радіоканалу в процесі трансакції характеризується швидкістю переключення частот, параметрами сітки частот, що використовуються при переключенні каналів, послідовність переключень та інші. Таким чином, можна говорити про параметр засобу захисту, який протидіє перехопленню даних з радіоканалу. Будемо позначати цей параметр буквою  $P_p$ , розглянемо поняття управління радіоканалом. Нехай через деякий радіоканал передаються дані  $x_i$ . Усі дані, що розглядаються в радіоканалах, мають ту чи іншу форму фізичного відображення. Таке відображення реалізується перетворенням даних  $x_i$  в форму, що доступна для їх передачі по радіоканалу, що можна записати:

$$y_i = f(x_i),$$

де  $y_i$  – форма представлення даних  $x_i$ , сприйнятлива для радіоканалу. Під управлінням радіоканалом, в цьому випадку, будемо розуміти додаткове перетворення даних, що представлені у формі  $y_i$ , які залишають форму представлення даних допустимою для радіоканалу, але проводять додаткові зміни у формі представлення,

які ускладнюють можливість перехоплення даних в радіоканалі. Прикладом перетворення  $y_i = f(x_i)$  може слугувати перетворення звукового, або голосового, сигналу в модульовані електромагнітні коливання. Прикладом додаткових перетворень радіосигналів, або радіоданих  $y_i$ , може слугувати перетворення, пов'язане з переключенням діапазонів несучих частот радіосигналів, різні види модуляції, різні способи кодування сигналів та інші перетворення. Таке перетворення запишемо співвідношенням:  $y_i^* = \varphi(y_i)$ . Змінна  $y_i^*$  відрізняється від змінної  $y_i$  в цьому співвідношенні не тільки у відповідності до вигляду функції перетворення, але й у відповідності до таких параметрів, як складність виконання зворотного перетворення, міра зворотності функції  $\varphi$ , яка аналогічна параметру  $\chi$ , що розглядався вище, та інші. Всі ці параметри є досить конструктивними і можуть бути вимірними в кожному конкретному випадку. Наприклад, складність перетворення у відповідності із функцією  $\varphi$  може бути виміряна кількістю математичних операторів, які повинні бути застосовані при реалізації функції  $\varphi$ .

Міра зворотності функції може бути проілюстрована на такому прикладі. Нехай функція  $\varphi$  є перетворенням Фур'є. Тоді точність такого представлення  $y_i$  буде залежати від кількості членів, що використовуються у перетворенні Фур'є. Очевидно, що в кожній практичній реалізації перетворення використовується обмежена кількість частотних складових. Тому при зворотному перетворенні відновлене значення  $y_i' = \varphi^{-1}(y_i^*)$  буде менш точним і не буде повністю збігатися з вихідною величиною  $y_i$ . Таким чином, можна стверджувати, що управління радіоканалом полягає у реалізації додаткових перетворень радіосигналів  $y_i$ . Це можна формально записати таким чином:  $R = \Phi(y_i, \sigma_p)$ , де  $R$  – радіоканал,  $\Phi$  – функція управління радіоканалом  $R$ ;  $\sigma_p$  – параметр, що відображає міру захисту каналу, а точніше, міру захисту перехоплених даних,

що передавались через радіоканал, від їх відновлення у формі  $y_i$  і  $x_i$ . Очевидно, що з точки зору забезпечення безпеки передачі даних через радіоканал велике значення має дальність радіоканалу, яка безпосередньо залежить від потужності передавача. В процесі реалізації трансакції може бути доцільним управляти потужністю передавача таким чином, щоб не позбавити приймача можливості прийняти повідомлення і мінімізувати можливість перехоплення радіоданих. Відповідне управління радіоканалом також буде характеризуватися певним параметром  $\sigma_m$ , який характеризує засіб захисту каналу від моніторингу  $Z_{mo}$ . При формуванні радіоканалів існує можливість управляти направленістю радіоканалів, що дозволяє говорити про параметр  $\sigma_n$  для  $Z_{mo}$  тощо.

### **Моделі загроз в системах передачі даних**

Загрози являють собою деякі властивості об'єкта, що підлягає захисту, і безпосередньо стосуються засобів захисту, що використовуються в кожному конкретному випадку. Необхідність побудови і дослідження моделей загроз зумовлена тим, що зовнішні (відносно об'єктів) небезпеки для реалізації атак на ці об'єкти використовують існуючі в об'єктах загрози. Завдяки дослідженню моделей загроз і моделей засобів захисту та дослідження їх взаємодії з моделями атак, з'являється можливість не тільки створювати процедури виявлення атак, а й можливість їм запобігати завдяки тому, що можна буде в рамках таких моделей їх передбачувати.

Розв'язування задач прогнозу можливих атак та формування нових атак на об'єкт захисту стає можливим завдяки тому, що атаки являють собою послідовність дій, що використовують існуючі загрози або фрагменти таких загроз, які тісно пов'язані з засобами захисту. Зв'язок загроз із засобами захисту в багатьох випадках може обумовлюватися обмеженнями на параметри, що характеризують відповідні засоби захисту. Таким чином, якщо один з параметрів засобу захисту  $Z_{sh}$  являє собою довжину ключа, що використовується для шифрування, а одним з фрагментів атаки

є підбір цього ключа, та у випадку використання методу підбору, який дозволяє ключі такої довжини підбирати за необхідний проміжок часу, то моделлю атаки є модель, що описує відповідний метод підбору ключа. Отже, моделі загроз та моделі атак зв'язані з параметрами і самими моделями захисту.

Якщо має місце ситуація, коли параметр засобу захисту, про який йшла мова вище – довжина ключа шифрування буде збільшена, а відповідна модель атаки або метод підбору ключа уже не зможе за заданий період часу здійснити такий підбір, то відповідна модель загрози перестане відображати собою загрозу, хоча атака як така існує незалежно і від об'єкта захисту і, тим більше, від засобів захисту. В цьому сенсі атака як така має досить конкретну і конструктивну реалізацію в алгоритмах, засобах та методах реалізації тих чи інших дій. При цьому відповідний зовнішній об'єкт відносно об'єкта захисту, до конкретних засобів захисту, може становити або не становити небезпеку. З цього випливає, що деякий об'єкт або методика, яка не становить небезпеки для об'єкта захисту, при зміні параметрів засобів захисту може стати небезпечною для відповідного об'єкта. Наприклад, сканер, що використовується для перехоплення даних з радіоканалу, може бути небезпекою для системи зв'язку, що використовує радіоканали, якщо його чутливість та інші параметри відповідають параметрам MS, з якими останні випромінюють радіосигнали. Якщо існує алгоритм, або методика підбору ключа шифрування, що здійснює такий підбір за час  $\Delta t_i$ , а засіб захисту, що використовує алгоритм шифрування для захисту інформації в об'єкті, визначає допустимий термін, або період часу для визначення ключа більшим або рівним  $\Delta t_g$ , то відповідна методика визначення ключа є небезпекою. Коли цей засіб захисту, інтервал допустимого часу  $\Delta t_g$  зменшити так, щоб  $\Delta t_g < \Delta t_i$ , то відповідна методика або алгоритм перестане бути небезпекою для об'єкта захисту. На відміну від небезпек, що існують відносно об'єктів, загроза як характеристика об'єкта існує завжди, якщо об'єкт використовує засоби захисту.

Розглянемо більш детально моделі загроз, які будемо позначати символом  $U$ . Оскільки кожна загроза безпосередньо зв'язана з різними типами систем захисту та різними типами засобів захисту, то відповідні загрози і їх моделі будемо розглядати відносно окремих засобів захисту. Загрози, що пов'язані з засобами захисту  $Z_{sh}$ , будемо позначати  $U_{sh}$ . Загрози, що пов'язані з засобами захисту  $Z_{mo}$ , будемо позначати  $U_{mo}$  і аналітично відносно  $Z_{do}$  загрози будемо позначати  $U_{do}$ , для  $Z_{vr}$  будемо відповідну загрозу позначати символом  $U_{vr}$ .

Розглянемо метод формування моделі загрози  $U_{sh}$ . Очевидно, що ця модель пов'язана з  $Z_{sh}$ . Цей зв'язок, в першу чергу, полягає у тому, що в моделі  $U_{sh}$  використовуються параметри, які фігурують в  $Z_{sh}$ . Прийmemo, що  $D[d(\omega), d(k)] = h(\omega, k)$ .

Ефективність  $Z_{sh}$  відносно  $h(\omega, k)$  описується:

$$\varepsilon[\varphi(\omega, k)] = \alpha \cdot h_i(\omega, k_i).$$

Прийmemo, що  $\varepsilon[\varphi(\omega, k)] = \alpha_{op} \cdot h(\omega, k_i) = opt$ . Тоді можна записати, що  $U_{sh} = \Delta\varepsilon = \left| \varepsilon - \varepsilon_{op} \right|$ . Відносно параметра  $\delta t(k)$  прийmemo, що  $\delta t(k)$  для кожної конкретної реалізації функції шифрування має свою мінімально необхідну величину  $\delta t_{min}(k)$ . Тоді співвідношення для загрози  $U_{sh}$  можна записати таким чином:

$$U_{sh} = f[\Delta\varepsilon, \Delta\delta t(k)], \text{ де } \Delta\delta t(k) = \left| (\delta t_i(k) - \delta t_{min}(k)) \right|.$$

Функції шифрування  $\varphi(\omega, k)$  в рамках моделі загрози оцінюються алгоритмами криптоаналізу відомого типу шифрів. Прийmemo, що параметри криптоаналітичних алгоритмів відображають не тільки ці алгоритми в абсолютному розумінні цього слова, а й відображають міру наявності додаткової інформації про алгоритм шифрування, яка дозволяє ефективність криптоаналізу суттєво підвищити. Прийmemo, що складність алгоритму крипто-

аналізу залежить від кількості операцій, які необхідно виконати, щоб відновити ключі шифрування, оскільки методи криптоаналізу, насамперед, направлені на встановлення таємних ключів для відомих алгоритмів шифрування. Тоді додаткову інформацію, яка може використовуватись при проведенні криптоаналізу, необхідно зіставляти з кожним фрагментом, або кожним кроком реалізації криптоаналітичної системи. Оскільки алгоритми криптоаналізу досить складні і, по суті, являють собою реалізацію громіздких методів наближених обчислень, тому більш детальний аналіз впливу даних про алгоритми шифрування, що використовуються в системах масової інформації, на рівень загроз, що існують відносно компоненти  $\varphi(\omega, k)$ , яка є компонентою засобу захисту, потребує детального дослідження алгоритмів криптоаналізу.

Однією з важливих функцій загроз, як певної характеристики об'єкта захисту, є забезпечення можливості встановлення зворотного зв'язку між атакою, яка є проявом небезпеки, та засобами захисту, що реалізують процеси протидії атакам, які є гарантом безпечного функціонування об'єктів захисту. З цієї точки зору, загрозу, як характеристику чи параметр засобів захисту, в деяких випадках визначити буває досить складно, особливо, коли загроза як параметр засобу захисту може використовуватись складним алгоритмом або процедурою атаки, яку формує та чи інша небезпека. У зв'язку з цим уявлення про загрозу в багатьох випадках пов'язується з небезпекою. Необхідність створення інформаційних компонент та інформаційних технологій якраз і пов'язана з тим, що загроза як характеристика засобів захисту в багатьох випадках носить інформаційний характер. У випадках з алгоритмами шифрування  $\varphi(\omega, k)$ , що використовуються в системах зв'язку, ця обставина особливо вагома. Тому в загальному вигляді для моделі загроз цю компоненту записують таким чином:

$$U_{sh} = f \{ \Delta \varepsilon, \Delta \delta t(k), I[\varphi(\omega, k)] \},$$

де  $I[\varphi(\omega, k)]$  – компонента моделі загрози  $U_{sh}$ , що визначається інформаційними параметрами системи захисту об'єкта в цілому і компонентами засобів захисту з  $Z_{sh}$ , в конкретному випадку цей параметр стосується систем масової інформації.

Розглянемо компоненту засобів захисту  $\psi(k)$ , яка визначає спосіб вибору таємного ключа  $k_i$ . В системах масової інформації для генерації ключів шифрування використовуються генератори псевдовипадкових кодів, що в більшості випадків реалізуються на основі регістрів зсуву з обмеженими зворотними зв'язками. Тому загрозою для цієї компоненти засобу захисту є ймовірність вибору тією чи іншою небезпекою правильного ключа шифрування  $k_i$  для цієї мобільної станції. Як уже зазначалось, визначення або підбір ключа є однією з основних цілей проведення криптоаналізу. Тому визначення складової частини загрози  $U_{sh}$  тісно пов'язане зі складовою частиною загрози, що стосується компоненти  $\varphi(\omega, k)$ .

Розглянемо модель загроз для засобу захисту  $Z_{do}$ . Параметрами, від яких залежить  $Z_{do}$ , є параметр  $\chi$  – який визначає точність відтворення коду при розшифруванні останнього,  $\eta$  – параметр, що характеризує додаткові умови оператора мережі на спосіб використання послуг,  $\lambda$  – параметр, що характеризує надання додаткових послуг, і  $\tau_i$  – технологічний період функціонування мережі відносно кожної окремої MS, що обслуговується мережею.

Теоретично, при використанні алгоритму АЗ, основою якого є функція  $y_i = k_i \oplus RAND$ , вона є зворотною, виходячи з її визначення. Але в рамках системи зв'язку  $y_i$  передається по каналах зв'язку, які можуть допускати виникнення в  $y_i$  невеликих помилок, наприклад, зміну одного біта на протилежний,  $y_i'$  – це код, який прийнято приймачем.

Тому в рамках приймача і, відповідно, в MS можуть використовуватись коди з автоматичною корекцією помилок. Але

використання таких кодів вимагає використання кодування з надмірністю. Другий підхід до розв'язання цієї задачі полягає в тому, що  $y_i$  допускається приймати з деякою помилкою, наприклад, з помилкою в двох двійкових розрядах. Отже, якщо в результаті дешифрування  $AZ^{-1}(y'_i)$  отримано  $x'_i$ , де  $\Delta x_i = \varphi(x, x')$ , то аутентифікація може бути признаною успішною, якщо  $\Delta x_i \leq \beta_k$ .

Параметр  $\eta$ , що характеризує міру впливу додаткових умов функціонування MS в мережі на можливість використання загроз несанкціонованого доступу, є в більшій мірі параметром, що відображає специфіку мережі, яка може бути пов'язаною з небезпекою несанкціонованого доступу. Цей параметр засобу захисту  $i$ , відповідно, загроза, що пов'язана з цим параметром, може описуватись засобами інформаційного забезпечення, які можуть використовуватись тільки в рамках інформаційних технологій.

Наступний параметр  $\lambda$  також належить до параметрів, які можна розглядати тільки в рамках їх опису інформаційними засобами. На відміну від параметра  $\eta$ , додаткові послуги та додаткові умови, що визначають спосіб функціонування мережі, при виконанні цих умов визначають досить конструктивну інформацію, яка може виявитися доступною для існуючих небезпек. Завдяки цьому, параметр  $\lambda$  можна зобразити у вигляді співвідношення:  $\lambda_m = \varphi(\alpha_1 \dots \alpha_m)$ , де  $\alpha_1 \dots \alpha_m$  – нові дані та параметри, що описують додаткову послугу. Прикладом таких даних може бути тимчасовий ідентифікатор абонента, якщо останній користується послугою роумінгу, або дані протоколу WAP чи протоколу GPRS, якщо MS використовується для зв'язку через Internet. В загальному вигляді модель загроз може бути описана таким чином :

$$U_{do} = f \left\{ I \left[ \eta(\beta_1, \dots, \beta_k) \right], I \left[ \lambda(\alpha_1, \dots, \alpha_m) \right], \tau \left[ P_1, \dots, P_k \right], \chi(m) \right\},$$



де  $\beta_1, \dots, \beta_k$  – дані, що визначають додаткові умови оператора стосовно правил користування мобільним зв'язком,  $\alpha_1, \dots, \alpha_n$  – додаткова інформація, яка пов'язана з наданням додаткових послуг і може бути використана для атаки на  $Z_{do}, P_1, \dots, P_k$  – дії абонента, що регламентуються часовою послідовністю і встановленими інтервалами часу між ними, які необхідно виконувати, щоб задовольнити вимоги оператора,  $m$  – величина допустимого відхилення в кодових послідовностях шифрованих даних, якщо система не використовує кодів з виправленням помилок.

Розглянемо моделі загроз для засобів захисту проти моніторингу радіоканалів передачі даних. Система захисту від моніторингу  $Z_{mo}$  найбільшою мірою залежить від управління каналом. Тому в загальному вигляді систему захисту типу  $Z_{mo}$  можемо описати у вигляді співвідношення:

$$Z_{mo} = F[\rho_p, \rho_m, \rho_i, y_i^*].$$

Загрози, що характеризують цей засіб захисту, описують ті властивості відповідних параметрів, використання яких дозволяє відповідний параметр нейтралізувати відповідно сформованою атакою. Функція  $F$  описує взаємозв'язок між параметрами засобу захисту, які фізично існують в радіоканалі. В нашому випадку ми не будемо розглядати атаки на інші компоненти системи мобільного зв'язку, особливо ті, що побудовані на основі використання спеціалізованих чи універсальних комп'ютерів, які також можна було б віднести до класу небезпек типу моніторингу. Форма представлення сигналів в радіоканалі  $y_i^*$  може використовуватися для захисту від перехоплення в тому сенсі, якщо зворотне перетворення сигналу  $y_i = \varphi^{-1}(y_i^*)$  та  $x_i = f^{-1}(y_i)$ , з точки зору їх реалізації, потребують затрат, які не окупляються вартістю отриманої інформації. Але ця обставина ніколи не береться до уваги, оскільки малоцінна інформація не піддається складним перетворенням типу  $y_i^* = \varphi(y_i)$ . В цьому випадку, коли мова йде про

захист каналу від радіоперехоплення, маються на увазі методи, які протидіють фізичному прийому сигналу радіоканалу несанкціонованими радіоприймальними станціями. Параметр управління потужністю передаючої станції  $\rho_m$ , параметр управління діаграмою направленості  $\rho_i$  та параметр протидії перехоплення  $\rho_n$ , який характеризує управління радіоканалом з точки зору маніпуляції з сигналами, що передаються, за своєю фізичною природою не можуть забезпечити зворотний зв'язок між атакою, яку здійснює відповідна небезпека та засоби зв'язку.

Оскільки основна функція загроз, як сукупність параметрів чи характеристик засобів захисту, яка забезпечує зворотний зв'язок між атаками та засобами захисту, в цьому випадку фізично є неможливою, то відносно засобів захисту типу  $Z_{mo}$  можна говорити про віртуальну загрозу. Тоді за початкову умову приймається факт існування небезпеки по перехопленню, яка буде реалізовувати відповідні атаки на моніторинг радіоканалу. Що стосується параметра  $\rho_m$ , управління потужністю в мобільних системах вже реалізується, і вона залежить від віддалі між MS і BTS. Управління в цьому випадку здійснюється таким чином, що потужність сигналу, який передається, мінімізується. Тому про цей параметр говорити не будемо.

Що стосується параметра засобу захисту  $\rho_i$ , який передбачає можливість управління діаграмою направленості, то тут випадку мова може йти тільки про антени BTS. Для управління діаграмою направленості антен BTS використовують антени типу матричних синфазних антен, або решітчастих антен. Така антена BTS складається з матриці окремих антен, які розміщені між собою на віддалі, що, як правило, дорівнює половині довжини хвилі частотної смуги, на роботу в якій відповідна антена настроюється. Оскільки кожна окрема антена має власний підсилювач, то в залежності від різниці фаз між сигналами, що подаються на різні антени, відповідні сигнали посилюються в більшій чи меншій мірі. Різниця фаз вимірюється у відповідності із співвідношенням:

$$\psi_i = \left[ \left[ 2\pi d(i-1) \right] / \lambda \right] \cdot \sin \theta,$$

де  $\theta$  – кут між площиною антени і площиною фронту сигналу,  $d$  – віддаль між двома суміжними антенами,  $i$  – номер біжучої антени,  $\lambda$  – довжина хвилі радіосигналу, що відповідає середній частоті смуги каналу. Збільшення відношення сигналу до шуму при використанні решітчастих антен збільшується на величину, що обрховується за співвідношенням:

$$G = 10 \log_{10} M (dB),$$

де  $M$  – кількість окремих антенних елементів. Завдяки різниці фаз сигналів на суміжних антенах, в антенній решітці досягається ефект звуження діаграми направленості. Управління орієнтацією діаграми направленості досягається шляхом управління фазою і потужністю кожної окремої антени, що входять до складу антенної синфазної решітки. Це дозволяє не тільки протидіяти атакам перехоплення, завдяки звуженню діаграми направленості, що затрудняє станції перехоплення розмістити антени в зоні дії цієї діаграми, а й вирішувати низку інших задач:

- підвищення об'єму системи масової інформації мобільних телефонів за рахунок того, що стає можливим збільшити кількість користувачів на одиницю площі;
- зменшення потужності випромінюваних сигналів за рахунок створення більш вузького пучка електромагнітних коливань, направлених на конкретну станцію MS;
- спрощення алгоритмів визначення місцезнаходження абонента, одночасно збільшивши точність визначення розміщення абонента.

Загроза, що відповідає цій компоненті засобу захисту від моніторингу, також розглядатися не буде, оскільки при використанні антен типу фазової решітки ширина діаграми направленості радіоканалу формується мінімальною, що ускладнює здійснення радіоперехоплення.

Управління радіоканалом є досить складним і складається з дій, пов'язаних з реалізацією процедур передачі даних. Крім того,

управління каналами відповідає за дотримання вимоги щодо якості обслуговування у відповідності з  $QoS$ . До основних функцій управління належать:

- створення нового носія в радіоканалі, вибір смуги частот для радіоканалу, який передбачається активізувати;
- реконфігурація існуючих носіїв радіоканалів;
- ліквідація носіїв радіосигналів, що призводить до звільнення фізичного каналу;
- реконфігурація транспортних каналів, що може полягати у зміні використовуваного фізичного каналу;
- реконфігурація фізичних каналів.

Важливим елементом управління каналом є управління завантаження каналу зв'язку. При цьому розрізняються завантаження «вверх» (від MS до BTS) і завантаження «вниз» (від BTS до MS). Ці завантаження обчислюються співвідношеннями:

$$B_{BB} = \sum_{k=1}^N \left[ (1 + i_{UL}) \cdot (E_B / N_o)_k \cdot R_k \cdot V_k \right] / \left[ (E_B / N_o)_k \cdot R_k \cdot V_k + W \right]$$

$$B_{BN} = \sum_{k=1}^N \left[ (E_B / N_o)_k \cdot R_k \cdot V_k \cdot (1 - d_k + I_{DL,K}) \right] / W,$$

де  $N$  – кількість з'єднань,  $W$  – смуга з'єднання,  $R_k$  – біжуча трансмісія,  $V_k$  – коефіцієнт активності абонента,  $i_{UL}$  – відношення завад з власної MS до потужності завад з сусідньої MS,  $I_{DL,K}$  – це ж співвідношення тільки між  $MS_k$  і сусідньою MS. Відносно кожної управляючої дії визначаються загрози, які описують залежність між недопустимими значеннями параметрів, якими здійснюється управління при реалізації загального управління радіоканалом між MS і BTS.

## Методи оцінки засобів захисту, що використовуються в електронних засобах масової інформації

Використання засобів захисту в електронних засобах масової інформації обумовлюється необхідністю забезпечення його безпеки. Існуюча тенденція підвищення рівня захисту завдяки використанню нових засобів захисту без оцінки такого захисту призводить до необгрунтованого ускладнення апаратурних і прог-

рамних компонент, що включаються в систему масової інформації та призводить до підвищення цін на захищені послуги. Можливості оцінки міри захисту, які надають різні засоби, дозволяють не тільки оптимізувати необхідний рівень захисту, а й регулювати його величину і, відповідно, вартість використання його засобів захисту. Методи оцінки міри захищеності послуг зв'язку досить складно сформулювати таким чином, щоб можна було безпосередньо пов'язувати різні засоби захисту з єдиною методикою оцінки міри захисту. Більше того, різні засоби захисту орієнтовані на протидію різним небезпекам, що існують відносно системи зв'язку. Тому для розробки загальної методики оцінки рівня підвищення безпеки використання ЗМІ, необхідно розглянути та дослідити такі задачі:

1. Розробити методи оцінки рівня захисту, що забезпечується різними типами засобів захисту;
2. Визначити способи вимірювання величини захисту окремими засобами та визначити міру, яку можна було б застосовувати для таких вимірювань рівня безпеки;
3. Розглянути і дослідити методи інтеграції оцінок міри захищеності, що забезпечується різними засобами захисту, в єдину інтегральну оцінку безпеки використання засобів масової інформації.

Для розв'язку першої задачі необхідно розглянути можливі інтерпретації параметрів, що характеризують відповідний засіб захисту, які допускали б можливість їх вимірювання, а інтерпретація зміни їх значень відповідала б зміні величини захисту, що забезпечується певним засобом. Тому розглянемо окремо різні засоби захисту та їх моделі і покажемо, яким чином можна пов'язати спосіб функціонування відповідного засобу захисту з мірою рівня захисту, який він забезпечує. Розглянемо спосіб захисту, який захищає трансмісію даних через радіоканал в мобільній системі і ґрунтується на використанні поточних шифрів. Основною небезпекою відносно даних, що передаються, є їх перехоплення і, відповідно, несанкціоноване використання. Тому, одним з параметрів, що характеризує процес функціонування відповідного засобу захисту, є криптостійкість відповідного

шифру. В цьому випадку будемо розглядати не криптостійкість, як це прийнято в криптографії, а ефективність шифрування, яка визначається у відповідності із співвідношенням (2.1).

На якісному рівні величина  $\varepsilon(\varphi)$  є тим більшою, чим менш передбачуваною є Хемінгова віддаль між  $\omega$  і  $u$  на різних фрагментах зашифрованого потоку даних  $u$ . Прийнемо, що ключ шифрування  $k_i$  має довжину  $\Delta k_i$  і змінюється від фрагмента  $\Delta \omega_i = \Delta k_i$  до фрагмента  $\Delta \omega_{i+1} = \Delta \omega_i$ . Нехай довжина повідомлення дорівнює  $m$  фрагментів  $\Delta \omega_i$ . Якщо кожному фрагменту зіставити точку на горизонтальній прямій, то на вертикальній осі можна відкладати деяку величину параметра, який характеризує ефективність шифрування на цьому інтервалі. При виборі такого параметра необхідно враховувати такі вимоги:

- відповідний параметр повинен бути придатним для вимірювань;
- вибраний параметр повинен в можливо більшій мірі характеризувати стійкість шифру, або ефективність шифрування;
- вибраний параметр повинен мати визначену фізичну інтерпретацію.

Очевидно, що результат поточного шифрування повідомлення значною мірою залежить від якості генератора псевдовипадкових послідовностей (ГПП). Якість таких ГПП оцінюється різноманітними тестами. Кожний з таких тестів орієнтовано на перевірку тих чи інших ознак, якими можуть характеризуватися псевдовипадкові послідовності. Наприклад, тести перевірки серій дозволяють оцінювати рівномірність розподілу символів в послідовності, що досліджується на основі аналізу частоти появи нулів і одиниць та серій, які складаються з кілобіт, тест перевірки на монотонність, що перевіряє рівномірність розподілу символів в досліджувальній послідовності на основі аналізу ділянок не зростання та не зменшення елементів послідовності та інші. Для отримання числових значень не монотонності використовується статистика:

$$X^2 = \sum_{q=1}^n \left\{ \left[ v_i - \left( \sum_{j=1}^m v_j \right) P_i \right]^2 / \left[ \left( \sum_{i=1}^n v_i \right) P_i \right] \right\},$$

де  $P_i = (1/i!) - (1/(i+1)!)$ ,  $v_i$  – число ділянок не зростання, чи не збільшення, довжина яких дорівнює  $i$ .

Вищезазначені підходи дозволяють оцінити окремі особливості псевдовипадкових величин, але інтерпретація цих особливостей опосередковано пов'язана з ефективністю засобів захисту, в склад яких вони входять. Використання таких параметрів не враховує кодів самого повідомлення при формуванні його шифру. Тому як один з таких параметрів виберемо впроваджений вище параметр ефективності шифрування. Величина значення ефективності шифрування внаслідок прийнятої інтерпретації цього параметра повинна бути обмежена максимально можливою віддаллю між фрагментом вхідного слова  $\omega_i$  та відповідним фрагментом отриманого шифру. Графік відповідного параметра для заданого  $\Delta\omega_i$  наведено на рис. 11.

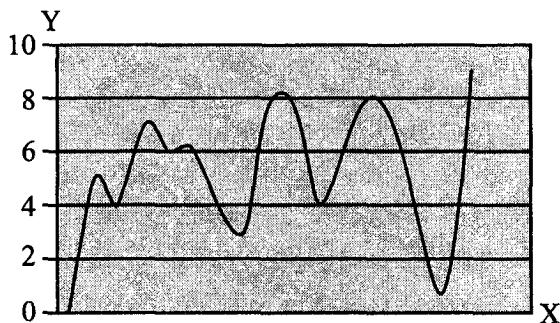


Рис. 11. Крива ефективності шифрування

Наведений графік ілюструє результат експериментів, які проводились на моделі, що реалізує перетворення аналогового сигналу в цифровий, реалізує вибраний генератор ПВП, який програмно можна переналаджувати, та реалізує шифрування вхідного аналогового сигналу, який подається з мікрофона, що підключається до комп'ютера. Крива, зображена на рис. 11, відображає інтегральні

значення ефективності шифрування для серії аналогових сигналів однакової тривалості з вибраною постійною довжиною ключа, що генерується для кожного фрагмента послідовності вхідного слова. В рамках експериментів використовувались вхідні послідовності однакової довжини.

Розглянемо окремі параметри засобу захисту від несанкціонованого доступу до мобільної станції і системи масової інформації в цілому. В загальній формі засіб захисту  $Z_{do}$  записується у вигляді:

$$Z_{do} = F(\chi, \eta, \tau, n).$$

Параметри  $\tau$  і  $\chi$ , виходячи з їх інтерпретації, що наведена вище, є залежними від параметра  $\varepsilon$ , що в певній мірі характеризує засіб захисту  $Z_{sh}$ . В певному наближенні можна стверджувати, що  $\varepsilon$  вимірюється кількістю бітів, а  $\tau$  вимірюється одиницею часу. Зв'язок цих двох одиниць вимірювання реалізується через кількість операцій обчислень, яка необхідна для обчислювальних операцій для виявлення ключа шифрування у випадку різних значень величини ефективності шифрування. Фізична інтерпретація такого зв'язку ґрунтується на тому, що кожна елементарна або приведена операція обчислень виконується протягом деякого інтервалу часу. Таким чином, можна прийняти, що інтервал часу  $\tau$  та ефективність шифрування  $\varepsilon$  зв'язані між собою достатньо однозначною фізичною інтерпретацією. Те саме відбувається між параметром  $\varepsilon$  і параметром  $\chi$ .

Стосовно параметрів  $\eta$  і  $n$  ситуація є складнішою, оскільки останні мають явно виражений семантичний характер. Параметр  $\eta$  можна подати, як послідовність певних дій користувача при використанні окремих послуг ЗМІ. Кожна послуга може бути представлена, як послідовність певних логічних змінних, що об'єднуються логічними зв'язками, яка, наприклад, записується у вигляді:

$$d_1 \rightarrow [(s_1 \& s_2) \vee s_3] \rightarrow s_4,$$



де  $\zeta_1, \zeta_2, \zeta_3$  і  $\zeta_4$  – ідентифікатори окремих дій, що повинні використовуватися користувачем при виборі послуги  $d_1$ . Очевидно, що кожна змінна  $\zeta_i$  описується текстовою інтерпретацією, яка може використовуватися при виборі інших послуг. В цьому випадку для  $\eta$  є можливою наступна інтерпретація. Якщо використання чергової послуги реалізується так, що відповідна  $d_1 = 0$ , то параметр  $\eta = 0$ , і це означає, що використання  $d_1$  призвело до порушення умов коректного використання послуги. В цьому випадку послуга може бути надана, але при цьому рівень безпеки знизився, оскільки потенційна небезпека могла отримати додаткову інформацію. Більше того, при  $\eta = 0$  послуга може бути і не отримана, тим не менше, потенційна небезпека могла отримати додаткову інформацію про MS, що призвело до зниження рівня безпеки користувача.

Оскільки параметри  $\eta$  і  $n$  носять явно виражений семантичний характер, то величина значень цих параметрів встановлюється для кожного окремого випадку на основі експертних оцінок. Наприклад, якщо послуга  $d_1$  призвела до  $\eta = 0$ , то відповідний параметр  $\eta_i$  приймає значення  $\alpha_i$ . Ці відповідності між  $d_1$  і  $\eta_i$  записуються в семантичних словниках у фрагментах структур  $S_c$ , який описує параметр  $\eta$ . Аналогічною є ситуація і для параметра  $n$ .

Оскільки величина значення для  $\eta$  і  $n$  має умовний характер, то їх можна визначити, як міру зміни безпеки системи захисту MS, і їх розмірність при цій інтерпретації узгодити з розмірностями інших параметрів, що характеризують інші типи засобів захисту, які використовуються в мобільній системі.

# ІНФОРМАЦІЙНІ ЗАСОБИ РОЗВ'ЯЗКУ ЗАДАЧ СИСТЕМ ЗАХИСТУ ДАНИХ В ЕЛЕКТРОННИХ ЗАСОБАХ МАСОВОЇ ІНФОРМАЦІЇ

## Інформаційні засоби моделей захисту даних

Інформаційні засоби, що використовуються для моделей захисту даних, орієнтовані на виконання таких функцій в рамках систем захисту:

- інтерпретаційне забезпечення параметрів, що характеризують відповідні моделі;
- розв'язання задач явного представлення залежностей між окремими параметрами, що використовуються в рамках відповідної моделі захисту;
- розв'язок задач прогнозування можливих атак на об'єкти захисту, які ґрунтуються на аналізі моделей загроз та цілей потенціальних атак;
- розв'язок задач оцінки рівня безпеки об'єктів, що підлягають захисту;
- розв'язок задач забезпечення заданого рівня безпечного функціонування інформаційних технологій;
- розширення асортименту послуг, які характеризуються замовленим рівнем конфіденційності зі сторони ініціатора послуг.

Серед асортименту інформаційних засобів, що можуть використовуватися в рамках інформаційної технології, орієнтованої на забезпечення безпеки передачі даних, існують базові компоненти, що складають основу технологічної системи, та спеціалізовані компоненти, що орієнтовані безпосередньо на розв'язок задач захисту інформації в мобільних системах.

В рамках монографії не розглядається задача підвищення рівня захисту даних взагалі, оскільки така постановка задачі є занадто загальною і до певної міри некоректною. Її некоректність обумовлена тим, що засоби захисту інформації, в залежності від рівня захисту, який вони забезпечують, мають різну вартість, що призводить до зміни вартості послуг, які надаються користувачам

мобільної системи. Тому кожний із користувачів повинен мати можливість самостійно визначати міру захисту даних, які він хоче передавати через засоби мобільного зв'язку в кожній окремій транзакції, яку користувач ініціює. В цьому випадку в рамках системи захисту повинна існувати можливість адаптації засобів захисту до вимог користувача, який платить за використання відповідних засобів захисту.

Крім захисту інформації, в рамках системи масової інформації існує проблема захисту персоніфікованих компонент мобільної системи, які кожний із користувачів оплачує або купує, якщо хоче користуватися відповідною системою масової інформації. Тому в рамках відповідної інформаційної технології повинна забезпечуватись можливість вибору таких персоніфікованих засобів, які б забезпечували різний рівень їх захисту, в залежності від побажань користувачів. Засоби захисту цих компонент також повинні забезпечувати можливість їх адаптації до вимог потенційного користувача, оскільки в залежності від рівня захисту, який вони забезпечують, визначається вартість відповідних персональних засобів. Такими персональними засобами є мобільні телефони та SIM-картки. Завдяки адаптаційним можливостям відповідних засобів стає можливим суттєво знизити ціни на мобільні телефони, послуги зв'язку та інші інформаційні послуги, які можуть надаватися через мобільну систему. Це призводить до збільшення кількості можливих користувачів системи масової інформації.

Система захисту даних в ЗМІ повинна функціонально орієнтуватися на різні типи загроз, до яких належать загрози несанкціонованого використання інформації, що передається через канали зв'язку, які позначались  $U_{sh}$ , загрози несанкціонованого доступу  $U_{d0}$  та загрози моніторингу  $U_{m0}$ . В цьому випадку ми не розглядаємо загрози системного характеру  $U_s$ , які направлені на дискредитацію всієї мобільної системи шляхом ініціації в ній несправностей, ініціації в ній відмов у наданні типових послуг та інших форм дискредитації мобільної системи масової інформації.

До інформаційних засобів, що дозволяють розв'язувати задачі інтерпретаційного забезпечення параметрів, та моделей, що розглядаються в роботі, належать такі компоненти:

- семантичні словники різної функціональної орієнтації, які пов'язані з основними задачами захисту в мобільних системах;
- системи правил розширення інтерпретаційних описів окремих компонент системи масової інформації;
- системи правил виводу нових складених інтерпретаційних описів, складних об'єктів.

Семантичні словники  $C_S$ , в більшості випадків, це структури, які можна розділити на окремі компоненти словника. Першою компонентою такого словника є ідентифікатор об'єкта, що інтерпретується, а другою – переважно текстовий опис на мові користувача інтерпретаційного розширення для відповідного ідентифікатора. Таким чином, ідентифікатори являють собою слова формальної мови, що використовуються для абстрактного опису відповідних моделей. Семантичні словники, здебільшого, використовуються для відображення об'єктів та процесів на природній мові споживача. Доцільність такого відображення зумовлюється існуванням необхідності у взаємозв'язку між споживачем і системою, який відображається з допомогою семантичних словників. Формально окрема компонента словника  $C_S$  записується у такому вигляді:

$$C_{S_i} = X_i : \langle \alpha_1 \rangle | \langle \alpha_2 \rangle | \dots | \langle \alpha_m \rangle ,$$

де  $x_i$  – ідентифікатор компоненти об'єкта,  $\alpha_i$  – слово або фраза з природної мови, яке використовується для опису ідентифікатора  $x_i$  на мові користувача.

Семантичні словники  $C_S$  використовуються не тільки для перетворення формальних описів у мову споживача, а й для узгодження між собою різних областей інтерпретації.

Функціональна орієнтація семантичних словників може визначатися характером ідентифікаторів, що описуються у словнику. Наприклад, такими ідентифікаторами можуть позначатися окремі

об'єкти системи, окремі функціональні зв'язки між об'єктами, що складають систему, яка описується в цілому системою словників, окремими ідентифікаторами можуть позначатися процеси, які відбуваються в системі, та інші компоненти, виділення яких в окрему групу вважається доцільним. В цьому випадку система словників може бути описана у вигляді:

$$C_s = \{C_s(X), C_s(f), C_s(P), \dots, C_s(M)\}.$$

Таку функціональну орієнтацію семантичних словників називатимемо технологічною функціональною орієнтацією (ТФО), оскільки вона впливає на технологічні методи організації процесів використання семантичних словників.

Іншим типом функціональної орієнтації є такий розподіл словників на окремі складові, який визначається характером задач, що передбачається розв'язувати в рамках інформаційної технології. До таких задач належать:

- задачі визначення рівня захисту послуг в системі масової інформації, який відповідає певному поточному моменту часу її функціонування;
- задачі управління рівнем захисту або рівнем безпеки, який необхідно забезпечити для певного класу послуг на деякий планований період часу;
- задачі аналізу запитів користувачів на забезпечення певного рівня безпеки використання послуги конкретного типу;
- задачі виявлення атак на системи масової інформації та організацію протидії виявленим атакам і т. д.

В рамках такої функціональної орієнтації семантичних словників, яку будемо називати конструктивною функціональною орієнтацією (КФО), можна використовувати словники з ТФО.

Семантичні словники  $C_s$ , що сформовані в деякий початковий момент реалізації системи захисту ЗМІ, в процесі її експлуатації можуть підлягати змінам. Це обумовлюється тим, що мобільні системи безперервно розвиваються, а це спричиняє зміни в різних компонентах і, відповідно, в процесах, що відбуваються в системах

масової інформації. Такі зміни можуть мати не тільки кількісний характер, а й якісний характер, що потребує корекції семантичного опису відповідних компонент системи. Наприклад, впровадження нової послуги, яку може надавати ЗМІ своїм користувачам, може вимагати використання додаткових або нових засобів захисту. Прикладом такої ситуації може слугувати впровадження послуги для визначення місця знаходження абонента при появі відповідного запиту на таку послугу. В цьому випадку семантичні словники необхідно розширювати, оскільки, мова йде про виникнення якісно нової компоненти, якою є процес надання відповідної послуги. Розширення семантичних словників може здійснюватися таким чином:

- доповненням  $C_s$  новою компонентою з власним інтерпретаційним розширенням;
- модифікацією інтерпретаційного розширення існуючих в семантичному словнику інтерпретаційних розширень.

Для кожного із зазначених випадків необхідно мати окремі системи виводу нових компонент, тому необхідно мати системи правил модифікації існуючих інтерпретаційних розширень. В цьому випадку семантичні словники будемо розглядати як засоби, що орієнтовані на розв'язання таких задач:

- задач створення та обслуговування засобів зв'язку між користувачами і системою захисту ЗМІ;
- задач, пов'язаних з узгодженням та встановленням залежностей між різними підсистемами ЗМІ при розв'язку задачі створення, модифікації чи аналізу системи захисту послуг, що надаються користувачам, та захисту системи масової інформації в цілому.

Необхідність встановлення таких залежностей обумовлюється таким фактором. Засоби захисту, що використовуються в рамках різних компонент, в багатьох випадках необхідно пов'язувати між собою, особливо у випадку, коли розв'язується задача загальної оцінки рівня захисту системи та задача визначення залежності рівня захисту окремої послуги чи окремого абонента від засобів

захисту, що реалізується в рамках баз даних VLR чи інших компонент системи ЗМІ.

При розв'язку першої задачі інтерпретаційне розширення реалізується у вигляді тексту на мові користувача. При розв'язку другої задачі інтерпретаційне розширення являє собою опис залежності між компонентою, для якої реалізується таке розширення, і компонентою, в якій це розширення описується. Наприклад, в рамках мобільного телефона однією з компонент захисту, яка входить в склад ЗМІ, є шифрування ідентифікатора, що використовується при аутентифікації абонента. Очевидно, що випадкове число RAND, яке зашифровується потоковим шифром з допомогою персонального ключа  $K_i$ , повинно бути захищене від його розпізнавання в VLR, де воно генерується. Якщо ж такий захист недостатньо високий, то за перехопленим кодом числа SRES, яке передається від абонента в VLR, та розпізнаним числом RAND можна встановити код таємного ключа  $K_i$ , і, завдяки цьому, виникне можливість реалізувати атаку несанкціонованої аутентифікації абонента. Залежність між параметрами цієї компоненти може мати довільний вигляд, який повинен бути конструктивним, що гарантує можливість її практичного використання в рамках інформаційної технології.

Під явним представленням залежностей між параметрами розуміється не стільки форма такого представлення, скільки міра конструктивності використання цього представлення. Міра конструктивності залежностей між параметрами визначається величиною міри однозначності обчислення величини одного параметра за значеннями інших параметрів та за величиною точності такого обчислення, яка визначається характером представленої залежності. На відміну від математичних підходів до встановлення таких залежностей, що здебільшого, ґрунтується тільки на використанні різних механізмів наближеного опису залежностей, в нашому випадку будемо використовувати насамперед підходи, що ґрунтуються на використанні семантичних характеристик параметрів або на використанні їх інтерпретаційних розширень. Після формування семантичного опису зв'язку між параметрами може виявитися

можливим встановлення функціональних, табличних чи інших форм представлення таких залежностей. Покажемо основні методи встановлення залежностей між параметрами на основі аналізу семантичних зв'язків між параметрами.

Приймемо, що всі інтерпретаційні розширення формуються не довільним чином, а у відповідності до системи синтаксичних схем:

$$\Gamma = \{\gamma_1, \dots, \gamma_n\},$$

де  $\gamma_i$  – окрема синтаксична схема. Елементами синтаксичних схем є слова, що об'єднуються в підмножини у відповідності до граматичних типів, яким відповідають ті чи інші слова природної мови споживачів. В цьому випадку будемо розглядати інтерпретаційні розширення  $j(X)$ , що описуються з допомогою природної мови споживача. Кожне слово будемо позначати символом  $\sigma_{ij}$ .

Перший нижній індекс визначає граматичний тип слова, а другий нижній індекс визначає окреме слово цього типу. Аналогічні позначення будемо використовувати й стосовно синтаксичних схем  $\gamma_i$ , де нижній індекс означає тип синтаксичної схеми. Окрема синтаксична схема формує фразу, яку будемо позначати символом  $\psi_i$ . Кожна синтаксична схема описує допустимі взаємозв'язки між словами, що складають окрему фразу. Тому необхідно визначити граматичні зв'язки, що можуть використовуватись в синтаксичних схемах. Очевидно, що такі граматичні зв'язки або синтаксичні функції у порівнянні з семантикою слів є універсальними. Введемо такі синтаксичні функції, які будуть визначатися мірою семантичної коректності використання пари слів у синтаксичній схемі  $\gamma_i$ :

- синтаксична функція абсолютної семантичної коректності, яку будемо позначати символом #;
- синтаксична функція допустимої семантичної коректності, яку будемо позначати символом @;
- синтаксична функція вимушеної семантичної коректності, яку будемо позначати символом \$.



В кожній природній мові можна формувати синтаксично допустимі та семантично абсолютно коректні фрази, наприклад, фраза, яка складається з об'єкта, дії об'єкта та характеристики цієї дії. В цьому випадку відповідна схема  $\gamma_i$  використовує синтаксичну функцію #.

Допустима семантична коректність @ означає використання окремого слова для розширення функції семантичної коректності. Прикладом такого розширення може слугувати використання не одного слова чи ряду слів, що характеризують об'єкт або процес, а використання певної підструктури слів, які можуть являти собою окрему фразу.

Вимушена синтаксична коректність \$ означає таке розширення фрази, яке являє собою суміщення двох окремих фраз. При цьому друга фраза використовує для свого опису елементи першої фрази.

Зрозуміло, що не кожне слово з множини слів певного граматичного типу може бути використане при автоматизованому формуванні нової фрази у відповідності з тією чи іншою граматичною схемою  $\gamma_i$ , оскільки, крім синтаксичних обмежень, в будь-якій мові, що описує реальну предметну область, існують певні семантичні обмеження.

Оскільки мова йде про створення інтерпретаційного розширення, то це означає, що формується нова семантична сутність або ж існуюча семантична сутність розширюється. Це означає, що при виборі чергового слова у відповідності із синтаксичною схемою  $\gamma_i$  повинні виконуватися певні правила. Такі правила тісно пов'язані з аналізом інтерпретаційних розширень, що вже існують в рамках семантичних словників. Наприклад, для побудови фрази нового інтерпретаційного розширення  $j(x_i^*)$ , яке формується у відповідності із схемою  $\gamma_i$ , при виборі слова  $\alpha_j$  для фрагмента  $\alpha_i \# \alpha_j$  необхідно вибирати таке  $\alpha_j$ , яке не використовувалось в уже існуючих інтерпретаційних розширеннях, що відповідають тій же схемі  $\gamma_i$  та відповідають тій же синтаксичній функції # в довільній

схемі  $\gamma_i$ . Крім того, слово, що вибирається, не повинно використовуватись в парі зі словом, що вже використовувалось в тій же синтаксичній функції раніше. Це правило формально можна записати у такому вигляді:

$$\begin{aligned}
 j(x_i^*) &= [\varphi_i(\alpha_{i1}, \dots, \alpha_{i-1}, \gamma_i < \alpha_i, \# \alpha_j >, \dots, \alpha_{ik}) \& \\
 &\& \varphi_j(\alpha_{j1}, \dots, \alpha_{j-1}, \gamma_j < \alpha_j, \# \alpha_i >, \dots, \alpha_{jk}) \& \\
 &\& (\alpha_j \neq \alpha_i)] \rightarrow (\gamma_i < \alpha_i, \# \alpha_j >).
 \end{aligned}
 \tag{3}$$

Для створення автоматизованого способу формування нових  $j^*(x_i)$  необхідно виконати наступне:

- за описом прийнятої предметної області скласти підмножини слів різних граматичних типів;
- на основі існуючих в  $C_S$  інтерпретаційних розширень  $j(x)$  та граматичних правил мови споживача сформуванню систему синтаксичних схем:

$$\Gamma = \{\gamma_1, \dots, \gamma_n\};$$

- сформуванню систему правил виводу нових інтерпретаційних розширень  $j^*(x_i)$ , що відображають семантичні обмеження на способи формування фраз  $\varphi_i$ , що являють собою нові  $j(x_i)$ .

Формування множини з граматично однотипними словами не є проблематичним.

Система синтаксичних схем  $\Gamma$  відрізняється від синтаксичних граматичних правил користувачів тим, що вона стосується тільки нормалізованих фраз  $\varphi_i$ , що допустимі у відповідній мові користувача. Тому формування схеми  $\Gamma$  ґрунтується на перетвореннях допустимих фраз мови користувача у нормалізовану форму.

Система правил побудови нових інтерпретаційних розширень чи правил модифікації інтерпретаційних розширень ґрунтується на основі таких семантичних умов:

**Умова 3.1.** Нове інтерпретаційне розширення  $j^*(x_i)$  не повинно бути семантичною копією уже існуючих інтерпретаційних розширень.

**Умова 3.2.** Модифікація  $j(x)$  не повинна полягати у заміні ідентифікатора об'єкта чи процесу іншим ідентифікатором.

**Умова 3.3.** При формуванні нового  $j^*(x_i)$  і відсутності в множині слів відповідного граматичного типу необхідного слова для формування опису створюється нове слово на основі адаптаційних перетворень слів, запозичених з іншого граматичного класу або з близької предметної області.

**Умова 3.4.** Якщо нове  $j^*(x)$  складається з декількох фраз  $\varphi_1, \dots, \varphi_k$ , то серед цих фраз повинна бути нова для системи фраза  $j(x)$ .

**Умова 3.5.** Різні фрази інтерпретаційних розширень повинні допускати кількісну оцінку відмінностей між ними.

Семантична копія інтерпретаційного розширення являє собою тотожне, з точки зору об'єкта або процесу, який описується, інтерпретаційне розширення. Семантична копія відрізняється від звичайної копії тим, що графічно опис розширення може бути відмінним від оригінального опису, а за своїм семантичним значенням такий опис повністю відповідає оригіналу.

При реалізації модифікації інтерпретаційного розширення не повинно відбуватися заміни одного розширення іншим, яке описує інший об'єкт чи процес. Модифікація і, відповідно, правила перетворень, що реалізують таку модифікацію, полягає у заміні або розширенні описів ідентифікаторів словами, семантичне значення яких не більше від семантичного значення одного або декількох слів в даному розширенні  $j(x_i)$ .

Оскільки опис середовища формується шляхом створення текстового відображення окремих об'єктів, а останнє реалізується на основі використання семантичного словника, то у відповідних підмножинах слів може й не бути ідентифікаторів для нових об'єктів чи процесів, які можуть виникати в середовищі предметної

області. У зв'язку з цим створення нових ідентифікаторів полягає у запозиченні слів з підмножин, які вміщують слова інших предметних областей, що означають дію або ті чи інші характеристики об'єктів.

Четверта умова передбачає недопустимість формування нових  $j^*(x)$ , що являють собою сукупність фраз, які були б семантичними копіями інших складних  $j(x)$ .

Семантичні засоби, що формуються в рамках цієї роботи, призначені не тільки для формування інтерфейсів між користувачами і системою, а й для розв'язування задач кількісного аналізу об'єктів та процесів. Тому необхідно мати можливість не тільки кількісно оцінювати окремі семантичні компоненти, а й проводити перетворення кількісних оцінок окремих семантичних елементів у відповідності із залежностями між ними.

### **Формування інформаційної моделі системи захисту**

Необхідність створення інформаційних моделей системи захисту обумовлюється факторами, що відображають специфіку процесів захисту в системах масової інформації, а саме:

- встановити аналітичні залежності між окремими параметрами одного засобу захисту, між параметрами різних засобів захисту і, відповідно, між окремими засобами захисту в цілому досить складно і здебільшого встановлення таких залежностей в аналітичній формі є неможливим;
- оскільки окремі засоби захисту взаємозв'язані між собою, то такий зв'язок існує щонайменше в рамках інформаційних потоків;
- необхідність розширення засобів захисту в системах масової інформації може зумовлюватися в основному інформаційною структурою та динамічними параметрами інформаційних потоків, що характеризують їх функції захисту відповідними засобами;
- значення параметрів засобів захисту в процесі роботи систем масової інформації змінюються, оскільки остання являє собою

безперервно функціонуючу систему, і такі зміни можуть обумовлюватися змінами вимог користувачів чи змінами в середовищі функціонування, що відображається в інформаційних компонентах систем масової інформації, в інформаційній моделі системи захисту;

- для організації протидії атакам засоби захисту повинні бути взаємозв'язаними з моделями загроз та моделями небезпек, а такий зв'язок може бути реалізованим тільки на рівні інформаційних засобів і, в першу чергу, з використанням інформаційної моделі.

Залежності між параметрами засобів захисту описані в неявній формі в рамках моделей системи захисту. Однією з основних задач інформаційної моделі системи захисту в цілому чи окремих систем захисту, кожна з яких орієнтована на конкретні класи атак, є встановлення та опис відповідних залежностей не стільки в аналітичній формі, скільки у таких формах, які допускають ефективне використання відповідних співвідношень. До таких залежностей належать такі типи залежностей:

- табличні залежності;
- графічні залежності;
- часткові аналітичні залежності;
- логічні залежності;
- мішані форми опису залежностей;
- апріорні залежності;
- семантичні залежності.

Розглянемо основні властивості зазначених вище залежностей з точки зору їх використання в інформаційних моделях.

Табличні залежності являють собою одну з форм залежностей, які досить широко використовуються, в основному в експериментальних дослідженнях. Формально таку залежність можна описати у вигляді співвідношення:

$$T_i(x^1, \dots, x^n) = \forall x^1 \dots \forall x^n [x_i^1 \leftrightarrow x_i^k \leftrightarrow \dots \leftrightarrow x_i^m],$$

де  $x^i$  – параметр, значення якого займають власне поле в таблиці  $T_i$ , “ $\leftrightarrow$ ” – знак, що описує відповідні величини значень  $x^i$  різних параметрів  $x_i^1, \dots, x_i^n$ .

При використанні табличних залежностей в інформаційних моделях, на відміну від їх використання в експериментальних дослідженнях, виникає проблема вибору одиниць вимірювання значень параметрів  $i$ , відповідно, проблема узгодження масштабів значень різних параметрів системи захисту між собою. У випадку експериментальних досліджень ці проблеми розв’язуються шляхом фізичного визначення діапазонів зміни параметрів, методами проведення експериментів, що передбачають вимірювання значень параметрів та можливостями приладів, що використовуються в експериментальній установці.

У випадку формування інформаційної моделі використовуються параметри та їх значення, які отримано з різних джерел, в різних ситуаціях, що між собою на момент їх визначення могли бути незалежними. Інформаційна модель відповідної системи захисту формується на основі аналітичної моделі, яка визначає компоненти, між параметрами яких існують залежності. Інформаційна модель включає такі компоненти:

- конструктивне представлення залежних між собою параметрів;
- явне відображення залежностей між параметрами в одній з наведених вище форм;
- засоби формування неаналітичних залежностей між параметрами моделі;
- інтерфейси взаємозв’язку інформаційної моделі з середовищем, в якому відповідна модель функціонує, або середовищем, з яким вона пов’язана.

Перш ніж розглядати методи побудови інформаційної моделі, розглянемо особливості різних способів опису залежностей між параметрами.

Графічні залежності, в традиційному розумінні цього слова, повинні відображатися у вигляді графіків або сукупності графіків. В рамках інформаційної моделі, яка реалізується аналітично, використання кривих, як деякого графічного образу, не є корек-

тним, і тому переважно такий графічний образ перетворюється в табличну форму представлення відповідних залежностей. У випадку інформаційних моделей такий підхід недопустимо спрощує задачу побудови конструктивного представлення залежностей. Це обумовлюється такими факторами:

- графічні залежності відображають відповідність між параметрами з різною величиною точності, яка залежить від масштабів параметрів, від типу масштабу (лінійні, логарифмічні і т.д.) та від точності, з якою отримано відповідні графічні залежності;
- графічні залежності між різними комплектами параметрів можуть бути між собою неузгодженими за діапазонами вимірювань значень параметрів та за типом масштабів, в яких вони вимірюються;
- графічний спосіб відображення залежностей орієнтований в основному на використання в інтерфейсах та графічних комплексах.

Часткові аналітичні залежності дозволяють більш точно відображати функціональні зв'язки, оскільки вони являють собою аналітичний опис функціональних залежностей в окремих фрагментах діапазонів значень досліджуваних параметрів. В інших фрагментах діапазонів такі залежності можуть подаватися в табличних формах чи в формах певних наближень. Особливістю часткових аналітичних залежностей є те, що вони у вибраних фрагментах забезпечують високу точність відображення, а у фрагментах, що розміщуються між аналітично описаними фрагментами, стає можливим формувати апроксимуючі функції.

Логічні залежності між окремими параметрами є найбільш ефективними для дослідження зв'язків між ними. Особливостями логічних залежностей є такі фактори:

- логічні залежності здійснюють найбільш загальну апроксимацію зв'язків між параметрами;
- для побудови логічних залежностей використовуються ефективні або критичні величини параметрів, множина яких відображається на дискретну область значень  $\{0,1\}$ ;

- для вибору логічних функцій, що зв'язують між собою окремі критичні точки різних параметрів, необхідно виходити з фізичних моделей, процесів, залежності між параметрами яких встановлюються або вивчаються;
- логічна функція може описувати динаміку одного параметра, якщо останній, в рамках вибраного діапазону значень, має цілий ряд критичних точок, оскільки кожна критична точка може залежати від історії зміни параметра, при реалізації процесу, що описується логічною функцією, а кожна критична точка позначається окремою логічною зміною у відповідній формулі.

Мішані форми опису залежностей включають в себе часткові аналітичні залежності, що узгоджені з фрагментами логічних залежностей. Для формування мішаної системи опису залежностей спочатку формуються критичні точки параметрів та описуються логічні взаємозв'язки між параметрами в межах, що визначаються критичними точками. Фрагменти діапазонів для часткових аналітичних залежностей вибираються в межах виділених критичних точок. Критичними точками, в цьому випадку, є такі значення параметрів, які в межах вибраної критичної точки мають особливості або перестають бути безперервними чи мають розриви. Таке порушення безперервності в критичній точці може мати параметр-функція, чи параметр-аргумент незалежно один від одного. Наприклад, якщо параметр-функція має розрив в критичній точці  $x_i^*$  то і для параметра-аргумента ця точка визначається як критична, незалежно від того, чи цей параметр у відповідній точці має розрив.

Апріорні залежності, на відміну від залежностей аналітичних, формуються на основі експериментальних досліджень, що проводяться з об'єктом чи процесом. Характерним для апріорних залежностей є використання елементарних функцій для опису зв'язків між параметрами, які уточнюються апріорно визначеними константами, коефіцієнтами та іншими штучно використовуваними компонентами, певні значення яких не завжди явним чином впливають з



закономірностей досліджуваних процесів. Типовим прикладом апріорної залежності може слугувати залежність:

$$y = 0.47x + \exp 0.8x .$$

Особливість апріорних залежностей визначають такі фактори:

- апріорна залежність є допустимою тільки в рамках певного діапазону значень параметрів, для яких вона встановлена;
- точність функціонального відображення залежностями апріорного характеру тісно пов'язана з точністю експериментальних даних, на основі яких апріорна залежність будується, та залежить від точності, з якою здійснюється апроксимація відповідного зв'язку між параметрами в точках, які лежать між даними, що отримані в результаті експериментів.

Семантичні залежності між параметрами мають специфічний характер і в найбільшій мірі відображають їх інтерпретацію в рамках предметної області, до якої належить досліджуваний об'єкт чи процес. Семантика, згідно з її визначенням, являє собою опис понятійного відображення досліджуваного процесу, і в цьому сенсі є базою для побудови інших типів залежностей, про які йшла мова вище. Очевидно, що в результаті досліджень об'єктів чи процесів можуть встановлюватися залежності між параметрами, які в предметній області ще не мають свого семантичного відображення. Тому про семантичні залежності, про способи їх побудови будемо говорити тільки при створенні інтерфейсів зв'язку з користувачами. При цьому будемо використовувати описи предметної області інтерпретації та їх розширення, що формуються на основі нових отриманих залежностей між параметрами, які встановлюються в рамках формування чи модифікації системи захисту.

Встановлення зв'язку між параметрами системи захисту, між параметрами моделей захисту та параметрами моделей загроз є необхідним в зв'язку з тим, що ці моделі, при реалізації процесів протидії атакам, взаємодіють між собою. Крім того, необхідно встановлювати залежності між параметрами різних засобів захисту, оскільки вони повинні протидіяти атакам в рамках всієї системи захисту, яка включає в себе всі засоби. Розглянемо кожен окрему

модель захисту і покажемо, як в рамках інформаційної моделі встановлюються такі зв'язки, якщо останні виявляються актуальними для протидії атакам. Система захисту, що використовує як основні елементи захисту алгоритми шифрування, записується таким чином:

$$Z_{sh} = F_{sh} \{ D[d(\omega), d(k)], \delta t(k), \varphi(\omega, k), \Psi(k) \}.$$

Розглянемо метод встановлення залежності  $d(\omega)$  і  $d(k)$ , яка описується функцією  $D$ . Відповідно до відомих способів визначення віддалі між двійковими кодами остання визначається у відповідності із співвідношенням:

$$D = \sum_{i=1}^k (\omega_i \oplus k_i).$$

Тому більш актуальним є встановлення залежностей між  $D(\omega, k)$  та  $\delta t(k)$ ,  $\varphi(\omega, k)$  і  $\Psi(k)$ . Компонента  $\delta t(k)$  є однопараметричною функцією і визначає певний інтервал часу використання ключа. Цей параметр є ефективним з точки зору управління рівнем захисту. Відомо, що чим коротший час використання ключа, тим вищими є його захисні функції, оскільки після завершення інтервалу  $\delta t(k)$  ключ шифрування змінюється. Особливо важливим цей параметр стає при умові, якщо відома необхідна величина часу на розкриття цього ключа. Цей інтервал часу будемо позначати  $\delta t(k)_{kp}$ . Оскільки модель захисту, що ґрунтується на використанні алгоритмів шифрування, крім  $\delta t(k)$  оперує і з іншими параметрами, такими як  $\varphi(\omega, k)$  і  $\Psi(k)$ , то всі компоненти між собою повинні бути зв'язаними і перебувати в певній залежності. Це, з одного боку, обумовлює ситуацію, коли зміна одного параметра, наприклад,  $\varphi(\omega, k)$  призводить до необхідності змін другого параметра  $\delta t(k)$ . З іншого боку, кожний з параметрів може мати окремі причини, що обумовлюють необхідність їх змін і, в цьому випадку, зміна інших параметрів, що входять в  $Z_{sh}$ , є необов'язковою, оскільки ціллю модифікації, наприклад,  $\delta t(k)$ , як і

інших параметрів, є підвищення або пониження рівня захисту  $Z_{sh}$ . Тому розглянемо незалежні причини, що можуть обумовлювати необхідність модифікації параметра  $\delta t(k_i)$ . До таких причин можна віднести:

- дані про кількість атак, направлених на розкриття ключа  $K_i$ , що можуть реєструватися за кількістю невдалих запитів на встановлення зв'язку;
- відсутність атак на ключ  $K_i$  даного абонента, що може зумовлювати можливість продовження часу використання  $K_i$ ;
- параметри псевдовипадкового генератора ключів, які визначають інтервали використання окремого згенерованого ключа.

Розглянемо компоненту  $\varphi(\omega, k)$ . Ця компонента характеризує процес передачі даних, що зашифровуються перед їх передачею в радіоканал. Основні атаки, що реалізуються в системі масової інформації, на успішність яких впливає цей параметр, являють собою атаки перехоплення повідомлень. Тому безпосередня реєстрація таких атак засобами масової інформації є неможлива. Посередній аналіз цього параметра, з метою визначення його впливу на рівень захисту засобами  $Z_{sh}$ , може ґрунтуватися на наступному. Результатом перетворення  $\varphi(\omega, k)$  є деякий код, довжина якого визначається швидкістю передачі даних та часом передачі, що задається інтервалом часу. В рамках засобів захисту обраховується величина  $D_i^* = \omega_i \oplus k_i$  для кожного інтервалу часу  $\Delta t_i$ . Протягом певної кількості інтервалів часу отримуємо послідовність величини  $D_i^* = f(\omega, k_i)$ . Аргументом відповідної функції приймається час  $t$ . Таким чином, можна побудувати функцію  $D^* = f(t)$ . При цьому інтервали  $\Delta t_i$  повинні узгоджуватися з довжиною ключа. Атака на розкриття тексту, що передається по каналу зв'язку, в найпростішому варіанті полягає у підборі слів, що на відповідному інтервалі часу у повідомленні використовуються. Якщо слова в повідомленні розпізнані, то у відповідності із спів-

відношенням  $[\varphi(\omega, k_i) \oplus \omega^*] = k_i$  можна визначити ключ  $K_i$ . Якщо фрагменти даних повідомлення  $\omega_1 * \omega_2 * \dots * \omega_k$  рівні або близькі, то кількість різних слів, які треба розпізнати для встановлення  $\omega^* = \omega$ , є меншою і тому розпізнати їх легше. Слід зауважити, що відповідна атака не проводиться в режимі реального часу, оскільки весь сеанс зв'язку може бути записаним, а розпізнання слів може здійснюватися незалежно від сеансу зв'язку. Отже, на основі аналізу кривої  $D^* = f(t)$  можна оцінювати рівень безпеки або рівень захисту системи масової інформації від атак перехоплення.

Функція  $\Psi(k_i)$  описує умови функціонування генераторів ключа  $k_i$ . Способи підвищення рівня випадковості коду для згенерованого ключа досить детально вивчені, оскільки псевдовипадкові генератори широко використовуються в теорії шифрування. Тому прийемо, що для системи захисту відповідні параметри, які дозволяють генерувати ключі  $k_i$  з різною мірою їх стійкості, що буде залежати від реальних потреб рівня захисту, який повинен забезпечуватися в рамках системи масової інформації, формально можна записати у вигляді:

$$u[\Psi(k_i)] = f[\Psi(k_i), \alpha_1, \dots, \alpha_m],$$

де  $\alpha_i$  – параметри управління псевдовипадковими генераторами ключів  $k_i$ . Явний вигляд співвідношення  $f$  буде залежати від типу псевдовипадкового генератора, що вибраний для генерації ключів  $k_i$ . Прикладом такого генератора може слугувати адитивний генератор, рівняння роботи якого описується співвідношеннями:

$$Q_o(t+1) = \sum_{j=1}^N a_j Q_{j-1} \bmod 2^M$$

$$Q_j(t+1) = Q_{j-1}(t), j = 1, \dots, (N-1),$$

де  $Q_j(t)$  – стан  $i$ -того регістра в момент часу  $t$ , а  $a_i$  – коефіцієнти многочлена  $\Phi(x)$  степеня  $N$ , що є примітивним над  $GF(2)$ . Крім того, використовуються параметри, які вказують на тип псевдо-

випадкового генератора (ПВГ). Як відомо, ПВГ мають періоди, за межами яких можуть повторюватися псевдовипадкові коди. Такі періоди становлять один з важливих параметрів ПВГ. Другим прикладом такого параметра може слугувати степінь многочлена, який прийнято називати формуючими многочленами і т.д.

Для побудови явної моделі захисту типу  $Z_{sh}$  необхідно визначитися з такими факторами:

- зовнішніми факторами, що пов'язані з рівнем захисту, який забезпечується відповідними засобами;
- параметрами, що характеризують можливості реалізованих методів шифрування;
- факторів, що виникають в результаті визначення біжучого стану рівня безпеки.

Зовнішні фактори, що пов'язані з рівнем захисту, зумовлюються існуючими небезпеками. Оскільки небезпеки існують незалежно від об'єкта захисту, то відповідні фактори, що пов'язуються з об'єктом захисту, будемо описувати у вигляді атак, що можуть ініціюватися і здійснюватися завдяки ініціації останніх відповідною небезпекою. Таким чином, можливість реалізації тієї чи іншої атаки будемо пов'язувати з існуванням у відповідному середовищі конкретної небезпеки. Оскільки атака являє собою послідовність дій, що використовують загрози, що є елементами об'єкта, який захищається, то виникає можливість безпосередньо на основі моделювання атаки відтворити необхідну інформацію або уявлення про небезпеку. Слід зауважити, що атаку неможливо описати як деякий рівномірний в часі і, тим більше, безперервний процес, який може бути відображений деякою функціональною залежністю. Особливість атаки як процесу полягає в тому, що вона складається з кількох етапів:

- виявлення інформації про загрози, що існують в об'єкті, який захищається;
- проникнення в об'єкт завдяки використанню можливостей, що надаються загрозами;
- реалізація цілі атаки.

Переважно під атакою розуміють два останні етапи, оскільки вони безпосередньо реалізують взаємодію з об'єктом. В цьому випадку не будемо детально розглядати різні можливі або відомі атаки на систему масової інформації.

Параметри, що характеризують можливості засобів захисту, в нашому випадку будемо розглядати тільки відносно загроз, з якими будемо зіставляти засоби захисту. Таким чином, загрози, які існують в засобах захисту, та їх параметри і будуть внутрішніми факторами, які необхідно відображати в моделях загроз системи масової інформації.

Система масової інформації є системою, що розвивається в часі. Такому розвитку, окрім функціональних засобів, підлягають і засоби захисту. Цей розвиток реалізується шляхом зміни значень параметрів загроз і відображається результатами аналізу зміни кількості вдалих атак, що здійснюються проти ЗМІ. Таким чином, наявність засобів захисту обумовлює необхідність реалізації в рамках ЗМІ системи моніторингу біжучого рівня безпеки функціонування системи.

## **Синтез моделей захисту даних з інформаційними моделями**

Математична модель системи захисту даних являє собою не просто сукупність моделей захисту, кожна з яких орієнтована на окремий клас небезпек, а відображає взаємозв'язок між окремими компонентами різних моделей захисту. Це дозволяє в процесі реалізації та дослідження відповідної системи захисту у вигляді комп'ютерної моделі здійснювати перехід від моделей одного класу до моделей другого класу, в залежності від змін значень параметрів, що використовуються в різних моделях. Зазначені вище обставини обумовлюють актуальність задачі синтезу різних моделей в одну модель системи захисту.

Розглянемо взаємозв'язок між аналітичними моделями  $Z_{sh}$ ,  $Z_{do}$  і  $Z_{mo}$ , що використовуються для опису засобів захисту. Очевидно, що такі взаємозв'язки можуть існувати:

- між аргументами;
- між змінними – функціями;
- між аргументами однієї моделі та змінною функцією іншої моделі.

Такі взаємозв'язки запишемо у вигляді:

$$x_i^j = f_j(x_k^m); y_i^j = f_j(y_k^m); y_j^i = f_k(x_k^m),$$

де  $x_i^j$  – змінна-аргумент моделі  $j$ ,  $x_k^m$  – змінна-аргумент моделі  $m$ ,  $y_i^j$  – змінна-функція моделі  $j$ ,  $y_k^m$  – змінна-функція моделі  $m$ .

Проаналізуємо відповідні взаємозв'язки між моделлю захисту  $Z_{sh}$  і моделлю захисту  $Z_{do}$ . Модель  $Z_{sh}$  записується у вигляді:

$$Z_{sh} = F \{ D[d(\omega), d(k)], \delta t(k), \varphi(\omega, k), \Psi(k) \},$$

$$Z_{do} = F \{ \chi, \eta, \tau, \lambda \}.$$

Насамперед треба зазначити, що в конструктивній або явній формі ці моделі можна представити, лише використовуючи не суто аналітичні способи опису відповідного взаємозв'язку інформаційних компонент. Наприклад, взаємозв'язок між параметром  $\delta t(k)$  і параметром  $D$  може описуватися, з одного боку, на якісному рівні, а з другого боку, на рівні зіставлення окремих значень відповідних параметрів, які можуть бути отримані на основі експериментальних даних чи на основі експертних оцінок, які за своєю природою можуть мати наближений характер. Тому встановлення таких взаємозв'язків може проводитись на основі досить глибокого аналізу предметної області інтерпретації, до якої такі змінні належать. Наприклад, прийнявши до уваги, що  $\delta t(k)$  є інтервалом часу, протягом якого використовується ключ  $k_i$  в алгоритмі поточкового шифрування даних, а  $D[d(\omega), d(k_i)]$  визначає взаємозв'язок між довжиною ключа  $k_i$  і довжиною повідомлення, яке необхідно зашифрувати, на якісному рівні, виходячи з відомого досвіду використання поточкових шифрів, можна стверджувати, що чим більша довжина ключа  $k_i$ , тим складніше його розкрити і тим

довшим може бути період  $\delta t(k_i)$  його використання. Але для реального і конструктивного використання такого якісного твердження необхідно мати інформацію про конкретні довжини ключів (в бітах чи байтах) і відповідні цим довжинам періоди використання ключів. В найпростішому випадку така залежність описується табличними співвідношеннями:

$$T_i = \{D[d(\omega), d(k_i)] \leftrightarrow \delta t(k_i)\},$$

де знак « $\leftrightarrow$ » означає табличну відповідність, а саме табличне співвідношення являє собою компоненту інформаційних засобів. Табличне співвідношення має особливість, яка характерна для певної предметної області інтерпретації. Якщо для зручності позначити  $x_i = D[d(\omega), d(k_i)]$  і  $x_j = \delta t(k_i)$ , то  $T(x_i, x_j) = [x_i \leftrightarrow x_j]$ .

На деякий момент функціонування значення  $x_i$  і  $x_j$  можуть бути визначені для всієї таблиці у всіх точках відповідності певним чином. Протягом функціонування системи відповідні дані можуть змінюватися. Така зміна може обумовлюватися новими даними про значення  $x_i$  і  $x_j$  або зміною співвідношень між відповідними змінними-аргументами. Таким чином, співвідношення для  $Z_{sh}$  можна для цього фрагмента записати:

$$Z_{sh} = F_i \{T_i[D[d(\omega)], d(k)] \leftrightarrow \delta t(k), \varphi(\omega, k), \Psi(k)\},$$

де  $F_i$  – функція, що об'єднує  $T_i$  з  $\varphi(\omega, k)$  і  $\Psi(k)$ .

Для розширення конструктивного представлення співвідношення  $Z_{sh}$  необхідно розглянути такі задачі, що відображають синтез окремих складових моделей засобів захисту:

- виявити взаємозалежність між компонентою  $T_i(x_i, x_j)$  і компонентами  $\varphi(\omega, k)$  та  $\Psi(k)$ ;
- серед  $\varphi(\omega, k)$  і  $\Psi(k)$  вибрати компоненту, яка буде безпосередньо зв'язана з  $T_i(x_i, x_j)$ ;
- визначити взаємозв'язок між компонентами  $\varphi(\omega, k)$  і  $\Psi(k)$ ;



- визначити періоди зміни значень параметрів, що пов'язані між собою;
- визначити періоди зміни способів опису взаємозв'язків між досліджуваними параметрами-аргументами та параметрами-функціями.

Наведені задачі визначають проблеми синтезу моделей різного типу, в такому випадку моделей логічних та інформаційних. Тому розглянемо можливі підходи до розв'язку цих задач.

В першій задачі мова йде про компоненти неявно заданої функції, які необхідно на першому етапі синтезу зв'язати між собою. Вихідними даними для такого вибору є описи інтерпретаційних розширень відповідних компонент  $J(x_i)$ . Такі інтерпретаційні розширення розміщуються в семантичних словниках, і для їх опису використовуються тексти природної мови. Інтерпретаційні розширення  $J(x)$  характеризуються низкою семантичних параметрів  $S_{p1}, \dots, S_{pm}$ , на основі аналізу яких вибираються відповідні компоненти і логічні функції. Аналіз інтерпретаційних розширень ґрунтується на тому, що будь-який опис на природній мові відображає логіку взаємозв'язків між елементами тексту, що складає такий опис. В загальному вигляді можна записати такі співвідношення для  $S_c$ :

$$\Phi[J(x_1, \dots, x_n)] = J(x_1) * J(x_2) * \dots * J(x_n),$$

де «\*» – логічна функція, яка відображається в текстовій формі,  $\Phi$  – функція взаємозв'язку між окремими  $J(x_i)$ . В цьому випадку аналіз  $J(x_i)$  з  $S_c$  полягає у послідовному використанні системи правил, що записуються у вигляді:

$$\left. \begin{aligned} L_1(x_{i1}, \dots, x_{im}) &\rightarrow L_1(x_{ik}) * L_2(x_{im}) \\ \dots &\dots \dots \dots \dots \dots \dots \dots \dots \dots \\ L_m(x_{m1}, \dots, x_{m,j}) &\rightarrow L_1(x_{mn}) * L_2(x_{i,j}) \end{aligned} \right\}. \quad (4)$$

В кожній конкретній реалізації  $S_c$  і відповідно  $J(x_i)$  логічні функції «\*» приймають одне із значень з множини елементарних логічних зв'язків  $\{\&, \vee, \rightarrow, I\}$ . В результаті використання системи (4) для кожної з моделей  $Z_{sh}$ ,  $Z_{mo}$ ,  $Z_{do}$  отримуємо відповідну логічну формулу  $L(Z_{sh})$ ,  $L(Z_{do})$  і  $L(Z_{mo})$ . Кожна логічна формула є структурованою. Така структура відображає пріоритети логічних зв'язків. В найпростішому випадку такі пріоритети відповідають порядку розміщення логічних функцій з врахуванням пріоритетів між цими функціями, які визначаються наступним порядком їх розміщення  $\{\&, \vee, \rightarrow, I\}$ . Якщо виявиться, що  $J(x_i)$  зв'язана з  $J(x_j)$  функцією  $\&$ , то і  $x_i$ ,  $x_j$  пов'язані відповідною функцією. Таким чином, взаємозалежність між окремими компонентами визначається логічними функціями та пріоритетами їх використання.

Наступна задача полягає у визначенні типу зв'язку між окремими компонентами. До таких типів, як вже зазначалось, належать табличні, логічні, частково функціональні емпіричні та мішані, що представляють собою різні комбінації перерахованих типів зв'язків. Тип зв'язку між окремими компонентами вибирається таким чином. В рамках семантичного словника  $S_c$  знаходиться функціонально орієнтований семантичний словник, який може вміщувати опис типу функціональних зв'язків між окремими компонентами. Якщо функціональні зв'язки різних типів позначити символами  $F_1, \dots, F_m$ , то відповідний фрагмент  $S_c$  запишеться у вигляді:

$$S_c(f) := \left\{ \left[ \langle x_1 \rangle F_1 \langle x_2 \rangle \right], \dots, \left[ \langle x_i \rangle F_i \langle x_j \rangle \right], \dots, \left[ \langle x_m \rangle F_m \langle x_n \rangle \right] \right\}.$$

Кожна з функцій може бути складною, наприклад,  $F_i = L_i \rightarrow T_i^j \rightarrow H_e^k \rightarrow T_i^{j+1}$ , де  $T_i^j$  означає табличний зв'язок між двома змінними в діапазоні від  $i$ -того значення змінної до її  $j$ -того значення,  $H_e^k$  – означає емпіричну функцію, що визначена на діапазоні  $[e, k]$ ,  $L_i$  – визначає логічний взаємозв'язок між компонентами, що складають функціональні залежності.

Наступна задача полягає у визначенні інтервалів часу, через які відбуваються зміни біжучих значень параметрів аргументів у співвідношеннях типу  $T_i$ . Ці періоди визначаються на основі таблиць процесів, що описують функціонування інформаційних моделей. В результаті ініціації процесів  $V_i$ , що полягають у перетвореннях даних, які використовуються в процесі функціонування моделей. Таким чином, періоди можливих змін біжучих значень в табличних функціях залежать від:

- моментів ініціації процесів  $V_i$ , що оперують або використовують дані;
- типу перетворень, що реалізуються у відповідних процесах.

Якщо ініційовано процес  $V_i$ , який оперує з даними  $x_i$  або  $V_i(x_i)$ , то період зміни біжучих значень параметрів в  $T_i(x_i, x_j)$  визначається моментом ініціації процесу  $V_i$  та моментом завершення відповідного процесу.

## **Організація інформаційної моделі загроз в засобах масової інформації**

Загрози як компоненти деякої системи можуть існувати тільки в тому випадку, коли в рамках відповідної системи існують засоби захисту чи система захисту. Моделі загроз можна розглядати як компоненти, що доповнюють моделі засобів захисту, якщо ці моделі розглядати як засоби, що дозволяють описувати процеси, які відбуваються в об'єкті захисту. Необхідність використання моделей загроз в системах масової інформації обумовлюється тим, що окрема модель захисту не може передбачити всіх можливих варіантів реалізації атаки зі сторони небезпеки, оскільки будь-який засіб захисту проектується так, щоб він міг протидіяти певним діям, що можуть реалізувати атаки. В процесі реалізації атаки може виникнути ситуація, коли реалізація чергової дії може бути непередбачена системою чи засобом захисту. Такі випадки можуть бути описані в рамках моделей загроз. Це актуально відносно

складних систем та систем, що безперервно функціонують, і їх модифікація здійснюється в процесі функціонування системи.

Оскільки загрози тісно пов'язані з засобами захисту, то будемо розглядати їх моделі на основі аналізу моделей засобів захисту. Як у випадку моделей засобів захисту, так і у випадку моделей загроз останні можуть бути представлені за допомогою інформаційних компонент, оскільки найбільш актуальним є їх конструктивне представлення.

Опис загроз у вигляді інформаційної моделі виявляється єдино можливим внаслідок таких обставин чи причин:

- модель загроз повинна відображати інформацію, що може використовуватися можливими атаками;
- засоби захисту ЗМІ також описуються інформаційними моделями;
- дані про небезпеку, в більшості випадків, являють собою опис певної інформації, яка не відображає можливих атак, що можуть ініціюватися відповідною небезпекою, в явній формі.

Перш за все визначимося з уявленням про інформаційну модель, яка буде використовуватись в нашому випадку. Під інформаційною моделлю  $I(m)$  деякого об'єкта будемо розуміти структуру, що складається з таких обов'язкових компонент:

- окремих елементів, що складають предмет моделі, які надаються у вигляді деякого списку ідентифікаторів цих елементів та інтерпретаційного опису відповідних елементів:

$$X_i := \langle j_1(x_i) \rangle \dots \langle j_n(x_i) \rangle;$$

- зв'язків між елементами  $x_i$  інформаційної моделі  $I(m_i)$ , де  $m_i$ 
  - ідентифікатор відповідної моделі  $I(m_i)$ ;
- процесів, що можуть відбуватися в рамках інформаційної моделі;

Елементи, що складають предмет моделі являють собою окремі компоненти семантичного словника  $C_s$  і в рамках моделі  $I(m_i)$  не мусять вмещувати свого інтерпретаційного розширення. Якщо для формування моделі знадобився новий елемент, то

останній повинен бути введеним в склад семантичного словника  $C_s$  як його розширення.

Зв'язки між елементами моделі  $I(m_i)$  в рамках однієї моделі можуть мати різний характер. Наприклад, взаємозв'язок між елементами моделі  $x_i$  і  $x_j$  може описуватися в табличній формі, зв'язок між елементами  $x_j$  і  $x_k$  може описуватись апріорним співвідношенням або частково аналітичним способом опису. Аналітичні зв'язки між змінними  $x_i$ , якими позначаються елементи моделі, як правило, описують можливі процеси, що виникають в моделі або можуть в моделі відбуватися. У випадку інформаційної моделі, що використовує різні форми опису залежностей між окремими елементами, необхідно забезпечити однозначність при визначенні процесів. Прийmemo, що процес є визначеним, якщо визначені такі фактори:

- параметри-аргументи серед елементів інформаційної моделі —  $x_{ia1}, \dots, x_{jak}$ ;
- один або декілька параметрів функцій моделі  $x_{i\phi 1}, \dots, x_{j\phi m}$ ;
- ціль реалізації процесу у вигляді:

$$\Psi(x_{i\phi 1}, \dots, x_{j\phi m}) \rightarrow f(k_1, \dots, k_m);$$

- процес, який описує послідовність використання залежностей між елементами інформаційної моделі, які необхідні для реалізації процесу, що записується у вигляді:

$$V_i = \left\{ \begin{array}{l} [X_{i\phi j} = \Psi_i(x_{jai}, \dots, x_{kaj})] \rightarrow \dots \\ \dots \rightarrow [X_{k\phi i} = \Psi_k(x_{iam}, \dots, x_{i\phi j})] \rightarrow \dots \\ \dots \rightarrow [X_{m\phi k} = \Psi_m(x_{sak}, \dots, x_{(i+m)ar})] \end{array} \right\},$$

де  $X_{k\phi i} = \Psi_k(x_{iam}, \dots, x_{(i+k)an})$  — залежність між елементом-функцією  $x_{k\phi i}$  і елементами-аргументами  $x_{iam}, \dots, x_{(i+k)an}$ ;

- для кожної залежності  $\Psi_i$ , що описує процес  $V_i$ , визначено діапазони змін значень величин для елементів функцій та для елементів-аргументів:  $x_{i\varphi_j} \Rightarrow [\alpha_{i\varphi}, \beta_{i\varphi}], \dots, x_{i\alpha_j} \Rightarrow [\alpha_{i\alpha}, \beta_{i\alpha}]$ ;
- умови переходу від однієї залежності до іншої при реалізації окремого процесу  $V_i$ ;
- умови ініціації окремого процесу  $V_i$ , визначена локалізація початку процесу та встановлено початкові умови, при яких процес може ініціюватися.

Очевидно, що в рамках однієї інформаційної моделі може бути визначено декілька процесів або один процес. Прийнемо, що окремі процеси  $V_1, \dots, V_k$ , які визначено в рамках однієї інформаційної моделі, безпосередньо не взаємодіють між собою, або  $[V_1(I_j) \rightarrow \dots \rightarrow V_k(I_j)] \Rightarrow \neg V_m(I_j)$ .

Завдяки використанню інформаційних моделей можна досить просто реалізовувати взаємодію різних моделей між собою. Розглянемо наступне визначення.

**Визначення 3.1.** Два процеси  $V_i$  і  $V_j$  мають точку узгодження, якщо вхідні параметри  $x_j$  з  $V_j$  і вихідні параметри  $x_i \in V_i$  зв'язані між собою функціональною залежністю  $x_i(e_i) = f_i[x_j(e_j)]$  і діапазони їх значень  $x_i[\alpha_i, \beta_i]$  та  $x_j[\alpha_j, \beta_j]$  взаємоприводимі.

Взаємна приводимість різних діапазонів означає, що між параметрами, для яких вони використовуються, існує взаємно однозначна залежність. Наприклад, якщо  $x_i[\alpha_i, \beta_i] \leftrightarrow x_j[\alpha_j, \beta_j]$ , то має місце співвідношення  $x_j = f(x_i)$ ,  $x_i = f(x_j)$  і область значень для  $x_i$  і  $x_j$  визначені на множинах  $[\alpha_i, \beta_i]$  і  $[\alpha_j, \beta_j]$  відповідно.

**Твердження 3.1.** Взаємодія двох інформаційних моделей  $I(m_i)$  і  $I(m_j)$  є можливою, якщо в них існують процеси  $V_i(m_i)$  і  $V_j(m_j)$ , які мають хоч би одну узгоджену точку.

Функціонування довільної інформаційної моделі  $I(m_i)$  здійснюється за посередництвом процесів, що можуть бути реалізовані в  $I(m_i)$ . Тому взаємодія між моделями здійснюється за допомогою процесів. Взаємодія процесів  $V_i$  і  $V_j$  в рамках  $I(m_i)$  і  $I(m_j)$  означає, що визначено цілі  $f_i(k_{i1}, \dots, k_{im})$  та  $f_j(k_{j1}, \dots, k_{jk})$ . Тому для взаємодії  $V_i(m_i)$  з  $V_j(m_j)$  необхідно встановити порядок ініціації  $V_i$  і  $V_j$ . Припустимо, що першим ініціюється  $V_i(m_i)$ . Тоді  $C(V_i) = f_i(k_{i1}, \dots, k_{im})$ . Згідно з умовою твердження  $V_i(m_i)$  і  $V_j(m_j)$  мають хоча б одну точку узгодження. Це означає:  $\{\{\forall I(m_i) \exists x_i(e_i)\} \& \{\forall I(m_j) \exists x_j(e_j)\}\} \rightarrow (e_i = f_i(e_j))$ . Кожний елемент з  $I(m_i)$  чи  $I(m_j)$  може описуватися одним чи кількома параметрами, або  $\{x_{i1}(e_i) * x_{i2}(e_i) * \dots * x_{ir}(e_i)\}$ , де кожен  $x_{ij}(e_i) = x_{ij}[\alpha_{ij}, \beta_{ij}] = x_{ij}(g_{ij})$ .

Прийmemo, що для  $I(m_i)$  в процесі  $V_i$  використовуються  $x_i(e_i) \& -x_j(e_j)$ . Тоді  $V_i(m_i) \rightarrow x_i(e_i) = f_i(k_{i1}, \dots, k_{ik})$ . Це означає, що кожна ціль  $C(V_i)$  описується параметрами  $x_i$  елемента  $e_i$  з  $I(m_i)$ . Функція  $f_i(k_{i1}, \dots, k_{ik})$  визначена для окремого  $x_i(e_i)$  на його діапазоні  $[\alpha_i, \beta_i]$ . Тому довільна ціль  $C_i(V_i)$  для  $V_i$  описується певними значеннями  $x_i$  з діапазону  $[\alpha_i, \beta_i]$ . Саме  $f_i$  описує спосіб вибору значень параметра  $x_i$  в діапазоні  $[\alpha_i, \beta_i]$ . Якщо  $f_i(k_{i1}, \dots, k_{ik}) = a = const$ , то це означає, що ціллю процесу  $V_i$  є досягнення параметром  $x_i$  величини  $a$ . Нехай існує  $I(m_j)$  з процесом  $V_j(m_j)$ . Взаємодія між інформаційними моделями означає:

- передачу даних з  $I(m_i)$  в  $I(m_j)$  або навпаки;
- ініціацію процесом  $V_i(m_i)$  процесу  $V_j(m_j)$ ;
- ініціацію за допомогою  $I(m_i)$  кількох процесів  $V_j^*(m_j)$  в моделі  $I(m_j)$ .

Покажемо, що наявність узгоджених точок між  $I(m_i)$  і  $I(m_j)$  є достатньою умовою для взаємодії двох моделей  $I(m_i) \Rightarrow I(m_j)$ . Оскільки спільна точка передбачає використання зв'язаних між собою елементів в  $I(m_i)$  та в  $I(m_j)$ , то у випадку, коли  $e_i$  описується одним параметром  $x_i(e_i)$ , передача даних про біжуче значення параметра є тривіальна, якщо  $x_i(e_i) = f_j x_j(e_j)$ , а  $x_i$  і  $x_j$  є два різних параметри, що описують елементи  $e_i$  і  $e_j$ , то виникає проблема передачі даних про відповідний параметр з  $I(m_i)$  в  $I(m_j)$ . Якщо в  $I(m_j)$ , яка є приймачем даних, існує модель, що являє собою конкретно описану структуру параметрів, то на основі цієї структури проводиться перерахунок інших параметрів.

Розглянемо випадок, коли взаємозв'язок між  $I(m_i)$  і  $I(m_j)$  визначається ініціацією процесом  $V_i(m_i)$  процесу  $V_j(m_j)$ , або коли  $[I(m_i) \rightarrow I(m_j)] \Rightarrow [V_i(m_i) \rightarrow V_j(m_j)]$ . У відповідності з умовою твердження для  $m_i$  і  $m_j$  має місце співвідношення:

$$\forall m_i \forall m_j \exists e_i \exists e_j [X_i(e_i) = f_j [X_j(e_j)]]$$

де  $e_i \in m_i$ ,  $e_j \in m_j$ ,  $x_i$  – параметр, що характеризує  $e_i$ ,  $f_j$  – функція узгодження між  $x_i$  і  $x_j$ . Якщо  $V_i(m_i)$  існує, то для  $V_i(m_i)$  існує ціль  $C(V_i) = f_i(k_{i1}, \dots, k_{in})$ , і  $V_i(m_i) = x_{i1}(e_{i1}) * \dots * x_{ij}(e_{ij}) * \dots * x_{ir}(e_{ir})$ . Оскільки  $x_{ik}(e_{ik})$  є кінцевим елементом процесу, тоді справедливо:  $x_{ik}(e_{ik}) = f_i(k_{i1}, \dots, k_{in})$ , де  $k_{ij}$  – значення параметра  $x_{ir}$  з діапазону,



що позначається, як  $g_i$ . Якщо завершальним елементом  $V_i(m_i)$  є однопараметричний елемент, то функція  $C(V_i) = f_i(k_i)$ . Ця функція визначає початкові умови для параметра  $x_j$  елемента  $e_i$ , який являє собою точку узгодження. Наявність точки узгодження між  $V_i(m_i)$  і  $V_j(m_j)$  є необхідною умовою для ініціації процесу  $V_j(m_j)$  в  $I(m_j)$  по завершенню  $V_i(m_i)$  в  $V_i(m_i)$ . Розглянемо достатню умову. Нехай на поточний момент функціонування  $I(m_j)$  початкове значення  $x_j(e_j) = \alpha_j^*$ . В результаті завершення  $V_i(m_i)$  для  $x_i(e_i)$  у відповідності до цілі  $C(V_i)$  сформувалась величина, що визначається співвідношенням:  $C(V_i) = f(k_i)$ , де  $k_i = \alpha_i$ . У відповідності з  $x_j(e_j) = f_j[x_i(e_i)]$  для  $x_j(e_j)$  визначено значення  $\alpha_j^* = f_j(k_i)$  і  $\alpha_j^* \neq \alpha_j$ . В цьому випадку процес  $V_j(m_j)$  з початковою умовою  $x_j(e_j)$  і початковим значенням параметра  $\alpha_j^*$  буде ініційовано в  $I(m_j)$ . У відповідності з умовою твердження, в цьому випадку, інформаційні моделі  $I(m_i)$  і  $I(m_j)$  є взаємодіючими. Випадок ініціації однією моделлю кількох процесів в іншій моделі є узагальненням випадку ініціації одного процесу. Тому його окремо розглядати не будемо.

Однією з головних особливостей систем захисту є те, що неможливо передбачити всі можливі події, які можуть бути окремими кроками атак на об'єкт захисту. Це означає, що яким би повним відносно атак не був комплект алгоритмів протидії атакам, завжди існує ймовірність виникнення нової атаки зі сторони можливої небезпеки. Оскільки засобами протидії атакам, є засоби захисту, то алгоритмами, що протидіють атакам є процеси, які описуються в рамках інформаційних моделей і можуть ініціюватися, при необхідності, у відповідних моделях. У зв'язку з цим виникають наступні задачі, які повинні розв'язуватися в рамках системи захисту:

- задача розпізнавання атаки;
- задача адаптації системи захисту до нових, непередбачених на етапі проектування, атак на об'єкт захисту;
- задача прогнозування можливих атак.

Задача розпізнавання атаки є необхідною складовою задачею системи захисту. В рамках цього підходу вона перетворюється в задачу ініціалізації процесів в моделі системи захисту, кожний з яких відповідає певному типу атаки. Оскільки небезпеки, що ініціюють ті чи інші атаки, використовують загрози, які існують в об'єкті, що захищається, то основною компонентою, яка розв'язує задачу розпізнавання атаки, є модель загроз. В цьому випадку процеси, що можуть ініціюватися в моделі загроз, повинні являти собою алгоритми розпізнавання атак. Задача розпізнавання атак ускладнюється тим, що атаки на системи зв'язку діляться на два класи – активні атаки і пасивні атаки. Активні атаки при взаємодії з об'єктом, який захищається, призводять у ньому до змін, які можна зареєструвати і таким чином виявити факт існування атаки. Оскільки атаки використовують загрози, що існують, то моделі загроз є тими фрагментами, в рамках яких виявляється факт дії атак. Протидію атакам реалізують засоби захисту, які у відповідності з наведеними вище умовами взаємодії інформаційних моделей, ініціюють процеси, що відповідають алгоритмам протидії виявленим атакам. В цьому випадку приймається, що відповідні процеси описуються в рамках інформаційних моделей та ініціюються в результаті взаємодії з інформаційною моделлю загроз, яка розпізнає відповідні атаки.

Пасивні атаки не можуть бути розпізнані в момент взаємодії відповідної атаки з об'єктом, який захищається, оскільки вони не призводять до змін в об'єкті, що захищається. Такі атаки можуть розпізнаватися лише за аномаліями, що виникають в об'єкті, який захищається. Така атака здійснює вплив на об'єкт захисту шляхом змін, що в ньому можуть відбуватися в процесі штатних способів його функціонування, або шляхом впливу на результати функціонування об'єкта, що захищається, які можуть бути проаналізовані без участі самого об'єкта. Перший тип пасивних атак будемо

називати пасивними атаками безпосередньої дії (ПАБ), а другий тип атак будемо називати пасивними атаками з дією на споживача (ПАС). В цьому випадку в межах об'єкта, що захищається, можуть аналізуватися тільки пасивні атаки типу ПАБ. Атаки типу ПАС розглядати не будемо.

В загальному задачі розпізнавання атак будемо розв'язувати шляхом виявлення відхилень в елементах системи захисту чи елементах об'єкта, що захищається (для випадку атак типу ПАБ). Методи організації такого аналізу можуть мати досить широкий спектр реалізації, починаючи від порівняння з встановленими порогоми значень параметрів елементів і закінчуючи методами обчислення інтегральних оцінок тих чи інших елементів засобів захисту, загроз чи елементів самого об'єкта, який захищається. Методи такого розпізнавання реалізуються у вигляді алгоритмів, що описуються відповідними процесами, які відбуваються в рамках інформаційної моделі загроз та ініціюються у відповідності з прийнятою в кожному випадку дисципліною. Перше ніж розглядати методи розв'язку задач адаптації системи захисту до певних атак, необхідно проаналізувати деякі особливості та можливості інформаційних моделей  $I(m_i)$ . Як зазначалось вище, в склад інформаційної моделі входять описи процесів, які можуть в моделях відбуватися. Опис такого процесу  $V_i(m_i)$  являє собою деяку таблицю, в яку послідовно вписані параметри елементів моделі, тип зв'язку між сусідніми параметрами, діапазони допустимих значень для кожного з параметрів. Для початкових параметрів описуються умови ініціалізації відповідного процесу. Для кінцевого параметра, або групи параметрів записуються умови завершення процесу у вигляді функції цілі. Відносно кожного перетворення, при необхідності, описуються додаткові умови його виконання. В таблиці наведено приклад структури опису процесу  $V_i$  який включається в склад інформаційної моделі  $I(m_i)$ .

При проектуванні систем захисту формуються інформаційні моделі  $I(m_i)$  для загроз та засобів захисту. В склад таких моделей включаються процеси, які в рамках моделей загроз  $U_i(x_{i1}, \dots, x_{im})$

та моделей засобів захисту  $Z_j(x_{j1}, \dots, x_{jk})$  реалізують алгоритм виявлення атак та алгоритм протидії виявленим атаками. Оскільки виявлення атаки відбувається на основі оцінки відхилень, до яких призводить діюча атака, то може мати місце ситуація, коли сукупність виявлених відхилень і їх структура не відповідають жодній атаці, які передбачались на етапі проектування. В цьому випадку, виникає необхідність у генерації нового процесу  $V_j(m_j)$  в моделі засобів захисту на основі даних, отриманих в результаті функціонування процесу в інформаційній моделі загроз. Така генерація може ініціюватись відповідним процесом моделі загроз.

Табл.

**Фрагмент опису процесу  $V_i(m_i)$**

№ $\lambda$	Параметри	Діапазон	Граничні значення	Функція	Умови переходу
1	$X_{i,1}$	$[\alpha_{i1}, \beta_{i1}]$	$X_{i1} = \alpha_{i1}^*$	$\varphi_1(X_{i1})$	
	$X_{i,2}$	$[\alpha_{i2}, \beta_{i2}]$	$X_{i2} = \alpha_{i2}^*$		
2	$X_{i,2}$			$\varphi_2(X_{i2})$	
	$X_{i,3}$	$[\alpha_{i3}, \beta_{i3}]$			
	$\vdots$				$\lambda_2 \rightarrow \lambda_3$
$m-1$	$X_{i,m-1}$	$[\alpha_{im-1}, \beta_{im-1}]$		$\varphi_{m-1}(X_{im-1})$	$C(V_i) \leq \alpha_{im}^*$
	$X_{i,m}$	$[\alpha_{im}, \beta_{im}]$	$X_{im} \leq \alpha_{im}^*$		

Розглянемо запропоновані визначення.

**Визначення 3.2.** Інформаційна модель  $I(m_i)$  називається повною, якщо процеси  $V_i(m_i)$ , що реалізовані в моделі, охоплюють всі її елементи.

$$P[I_i(m_i)] = \forall e_i \exists V_j (e_i \in V_j).$$

**Визначення 3.3.** Інформаційна модель називається насиченою, якщо не існує функціональних зв'язків між елементами  $e_i$  і  $e_j$  таких, які уже не були б використані в реалізованих процесах:

$$N[I_i(m_i)] = \forall \varphi_i(x_i, x_j) \rightarrow \exists \varphi_j(x_k, x_r) [\varphi_j(x_k, x_r) \notin V_i(m_i)].$$

Якщо інформаційна модель засобу захисту  $I_i(m_i, z_i)$  є насиченою, а інформаційна модель загроз ініціює процес  $V_i(U_i)$ , який не має свого розвитку в інформаційній моделі системи захисту, то в цьому випадку  $I(m_i)$  потребує розширення.

**Твердження 3.2.** В моделі  $I(z_i)$  породжується новий процес  $V_i^*(Z_i)$ , якщо  $I(z_i)$  не насичена, і ні один процес  $V_i(U_i)$  з моделі загроз  $I(U_i)$  не має свого розвитку в  $I(z_i)$ .

Оскільки будь-який процес  $V_i$  являє собою послідовність використання залежностей між параметрами, то однією з основних умов формування  $V_i^*(z_i)$  є наявність правил  $V_i^*(z_i) = \{\varphi_{i1}, \dots, \varphi_{ik}\}$ , згідно з якими така послідовність залежностей буде формуватися. Крім правил формування послідовності перетворень, необхідно сформулювати механізм формування цілі функціонування нового процесу  $V_i^*(z_i)$ . Використання правил щодо формування послідовностей з  $\varphi_i$  повинно пов'язуватись з ціллю функціонування  $V_i^*(z_i)$ . Тому перш за все розглянемо формування цілі  $C_i(V_i)$ . Згідно з визначенням цілі  $C(V_i) = f(k_1, \dots, k_m)$ , де  $k_i$  – значення параметра, яке отримано в результаті виконання  $V_i$ , або  $V_i \rightarrow \{k_1, \dots, k_m\}$ . Функція  $f$  описує спосіб розрахунку інтегрального параметра, що характеризує результат функціонування  $V_i$ . Очевидно, що  $V_i(x_{i1}, \dots, x_{im}) \rightarrow C(V_i)$ . Оскільки не в кожному  $\varphi_i(x_i, x_j)$  існує можливість вибору потрібних чи оптимальних значень аргументів  $(x_i \vee x_j)$ , то визначення цілі  $C(V_i)$  полягає у виборі тих чи інших  $x_i$  з  $V_i$ , включаючи  $x_{im}$ , і за їх значеннями визначається

параметр цілі  $C(V_i)$ . Цей параметр, в результаті функціонування  $V_i$ , може виявитися таким, що не відповідає величині чи допустимому діапазону значень  $C(V_i)$ . В цьому випадку приймається, що ініційований процес цілі не досягнув. Припустимо, що  $I(z_i)$  насичена, а  $V_i(U_i) \rightarrow \neg V_i(z_i)$ . Оскільки  $I(z) = N[I(z_i)]$ , то це означає, що не існує в  $z_i$  таких  $\varphi_i(x_i, x_j)$ , які б не використовувались в  $I(z)$ . Оскільки  $I(z_i)$  і  $I(U_i)$  стосуються одного об'єкта, то вони узгоджені. Тому неможлива ситуація, коли в  $I(z_i)$  немає  $V_i(z_i)$ , який був би розвитком для  $V_i(U_i)$ . Якщо в  $I(z_i)$  існує  $V_i(z_i)$  такий, що  $V_i(U_i) \rightarrow V_i(z_i)$ , то  $V_i(z_i)$  є розвитком  $V_i(U_i)$ .

Описувати в загальному вигляді правила  $\Sigma_i$ , що складають систему правил виводу, доцільно на основі даних про конкретні типи засобів захисту та відомих способів протидії певним атакам.

Якщо виникає певний тип атаки  $A_i^*$ , який не відображається в рамках описаних процесів, особливо в моделях загроз  $U_i$ , то в цьому випадку використовуються правила формування відповідних процесів  $V_i(U_i)$ , які складають систему правил  $\Sigma_i$ , що узгоджена з системою правил  $\Sigma_i$ , та відображають окремі методи розпізнавання атак.

# РОЗРОБКА ОСНОВНИХ КОМПОНЕНТ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ СИСТЕМ ЗАХИСТУ ДАНИХ В ЕЛЕКТРОННИХ ЗАСОБАХ МАСОВОЇ ІНФОРМАЦІЇ

## Організація способів функціонування процесів, що реалізуються в інформаційних моделях

Інформаційна модель являє собою основні частини, до складу яких входять:

- опис сукупності основних компонент інформаційної моделі;
- опис способу функціонування інформаційної моделі, яка використовує відповідні компоненти;
- умови ініціації процесу функціонування моделі, умови завершення процесів функціонування;
- засоби інтерпретації результатів та процесу функціонування інформаційної моделі.

Зважаючи на вищезазначений перелік компонент, з яких складається інформаційна модель, виходить, що  $I(m_i)$  може охоплювати системи в цілому або її компоненти, виділення яких обґрунтовується архітектурою системи та архітектурою всіх компонент, що входять в систему. В цьому випадку такими компонентами є засоби захисту, загрози і сам об'єкт, який передбачається захищати. Щодо засобів захисту, то вони являють собою окрему систему захисту, яка є виділеною. Відповідно, ця система є окремою з точки зору процесів, що функціонують в цій моделі. Взаємодія цієї інформаційної моделі з об'єктом, що захищається, відбувається тільки на рівні обміну даними та на рівні взаємодії процесів. Інформаційна модель  $I(z_i)$  об'єднує всі засоби захисту, що використовуються в системі. Основними функціями моделі  $I(z_i)$  є протидія атакам, що ініціюються відносно об'єкта, оцінка рівня безпеки об'єкта в процесі його функціонування та модифікація системи захисту з ціллю забезпечення необхідного рівня захисту. Крім перерахованих основних задач, в рамках

інформаційної моделі системи захисту можуть розв'язуватися задачі прогнозування можливостей небезпек щодо ініціації атак на об'єкт, що охороняється.

Іншою інформаційною моделлю, що використовується для забезпечення безпеки функціонування системи в цілому, є модель загроз  $I(u_i)$ . Оскільки загрози являють собою певні характеристики компонент, або елементів об'єкта, який захищається, то основними компонентами моделі  $I(u_i)$  є елементи об'єкта з тією різницею, що вони в рамках моделі  $I(u_i)$  описуються тільки в тій мірі, в якій вони можуть використовуватися для реалізації атак. Опис цих же компонент як складових об'єкта, що охороняється, в рамках самого об'єкта, відображає їх функціональні можливості і призначення, що орієнтоване на розв'язок задач відповідного об'єкта, в цьому випадку, задач надання послуг зв'язку. Основними задачами  $I(u_i)$  є виявлення атак, прогнозування виникнення нових загроз відносно об'єкта, що захищається, прогнозування нових модифікацій відомих атак та оцінка впливу атаки на об'єкт.

Процеси, що ініціюються в рамках моделі  $I(z_i)$  і  $I(u_i)$ , являють собою алгоритми, що розв'язують задачі, зазначені вище, для кожної моделі. У випадку виникнення необхідності розв'язувати нову задачу породжуються нові процеси в рамках кожної з моделей. Такі алгоритми будуються на основі використання ряду залежностей між параметрами моделі, що складають одну з компонент моделі і встановлюються незалежно від процесів, які функціонують в системі чи породжуються в  $I(m_i)$ .

Розглянемо процеси, що реалізуються в  $I(u_i)$  і орієнтовані на розв'язок основних задач. З функціональної точки зору процеси з  $I(u_i)$  активізують, при необхідності, процеси в  $I(z_i)$ . Першою задачею, яка розв'язується в рамках  $I(z_i)$ , є задача виявлення атак. Відзначимо, що для розв'язку однієї задачі може використовуватися низка процесів, які можуть функціонувати в  $I(u_i)$  незалежно і мати різну орієнтацію в рамках розв'язку однієї задачі. У випадку задачі розпізнавання атак необхідно виділити такі



процеси, що можуть ініціювати один одного в залежності від результатів, які виникають при функціонуванні окремого процесу:

- процес моніторингу ознак, що характеризують появу атак, які діють на об'єкт, що охороняється;
- процес розпізнавання типу атаки за еталонними описами відповідних атак;
- розпізнавання модифікованих атак або атак, стосовно яких в моделі  $I(u_i)$  немає опису еталона.

Необхідність процесу моніторингу обумовлюється тим, що виявляти атаки необхідно ще до того, поки вони не призвели до змін в об'єкті, який охороняється ( $W_i$ ). Тому в рамках  $I(u_i)$  описуються ознаки появи атаки. До таких ознак можна віднести факт зміни параметрів, що характеризують якість надання послуг. Прикладом такої ознаки може бути зміна часу очікування послуги, зміна якості процесу обміну даними і т.д. Оскільки система ЗМІ є розподіленою, то і параметри розподілені в системі. Крім того, один і той же параметр може вимірюватися в рамках різних фрагментів, і тоді виникає необхідність всі результати вимірювань привести до однієї інтегральної ознаки. Більш того, зміна величини тієї чи іншої ознаки може спричинитися не тільки атакою, а й виникненням несправності в окремих компонентах каналу, що реалізує відповідну послугу. У зв'язку з цим модель  $I(u_i)$  повинна взаємодіяти з системами тестування. Тому виникає необхідність розрізняти еталонні образи атак з еталонними образами несправностей. В цьому випадку будемо вважати, що система діагностування функціонує незалежно і, відносно моделі загроз, вона буде лише видавати інформацію про те, чи відхилення параметра обумовлене виникненням несправності, чи ні. Ситуацію, коли ціллю атаки є ініціація виникнення несправності, в цьому випадку розглядати не будемо, оскільки поява несправності означає досягнення відповідною атакою своєї цілі, а реагувати на несправність повинна система діагностики.

Розглянемо процес моніторингу ознак дії атаки на  $W_i$ . Окрема система масової інформації являє собою розподілену систему з

досить великими можливостями з використання системи. Тому процес моніторингу  $V_i(U_i, e_i)$  реалізується у вигляді окремих фрагментів, що функціонують у різних компонентах ЗМІ. Такими компонентами є модулі BSC, які являють собою контролери базових станцій BTS, здійснюють резервування частот, переключення з однієї станції на іншу та пошук мобільних станцій. Очевидно, що в цьому випадку основним каналом для реалізації атаки є радіоканал. Наступною компонентою, в якій функціонує фрагмент процесу  $V_i(U_i, e_i)$ , є модуль MSC, який являє собою цифровий комутатор і разом з іншими модулями MSC системи GSM створює стаціонарну магістральну мережу системи. В цьому випадку входами можливих атак є шлюз GMSC, який з'єднує систему GSM з іншими системами та мережами, наприклад, мережею PSTN та ISDN (суспільна комутована мережа, цифрова мережа зв'язку з інтеграцією послуг), мережею IWF (міжмережна функція обміну) та мережею передачі даних загального користування PDN (наприклад, мережа X.25).

При практичній реалізації відповідного фрагмента процесу в кожному з визначених вище елементів мережі вводити розширення в стандартні засоби масової інформації, як правило, забороняється. Оскільки будь-яка система масової інформації є комерційною або являє собою систему, до якої пред'являються спеціальні вимоги щодо надійності та безпеки, такі обмеження є обґрунтованими. Це означає, що реалізація запропонованих методів підвищення рівня захисту в ЗМІ повинна проводитись в дослідних зразках та випробовуватись в рамках експериментальних досліджень. З іншого боку, запропоновані фрагменти можуть реалізовуватись на резервних системах, якщо їх підключення до діючої системи в режимі дублювання є технологічно допустимим.

Практична реалізація запропонованого підходу для підвищення рівня безпеки роботи ЗМІ може полягати у незалежній реалізації моделей засобів захисту та моделей загроз в рамках додаткового обладнання, на яке з тих чи інших компонент мережі передається інформація, що необхідна для реалізації відповідних

процесів. Така передача може здійснюватися шляхом створення додаткових розгалужень в ЗМІ, які не впливають на штатний режим роботи системи. В цьому випадку результати роботи системи захисту в цілому можуть мати характер додаткової інформації стосовно безпеки функціонування ЗМІ.

У зв'язку з викладеним вище не будемо розглядати проблеми фізичного підключення реалізованої системи захисту до реальної системи масової інформації, а обмежимося методами та алгоритмами реалізації розглянутих задач. Оскільки першою з таких задач є задача моніторингу параметрів, то приймемо, що інформація про зміну значень контрольованих параметрів є доступною.

Виходячи з моделей загроз, видно, що параметри, які фігурують у відповідних моделях, не можуть бути безпосередньо вимірними і потребують окремого обрахунку. Наприклад, в моделі  $U_{sh} = f[\Delta\varepsilon, \Delta\delta t(k)]$  параметр  $\Delta\varepsilon$  являє собою величину ефективності шифрування, або  $\Delta\varepsilon = |\varepsilon - \varepsilon_{op}|$ . На якісному рівні  $\Delta\varepsilon$  означає характер зміни  $\varepsilon$  на різних інтервалах повідомлення  $\omega_i$ , які визначаються довжиною ключа  $K_i$ . В цьому випадку ознакою атаки є факт відхилення біжучого обрахованого значення  $\Delta\varepsilon$  від заданої величини. До цього може призвести типова атака, яка полягає в тому, що на засіб захисту подається упродовж певного часу постійний код, а з виходу знімається шифрограма, за якою здійснюється спроба розпізнати ключ  $K_i$ . Практично, зчитування шифрограми може здійснюватися шляхом підслуховування радіоканалу. Прикладом розпізнавання атак на  $W_i$  по параметру  $\Delta\delta t(k_i)$  може бути наступний сценарій, який в явному вигляді вимагає даних інформаційного характеру, які можуть формуватися в рамках інформаційної моделі. Нехай на певну MS здійснюється атака, що полягає у підборі ключа для АЗ, що використовується при аутентифікації MS. При ідентифікації MS система масової інформації контролює три спроби реєстрації MS. Якщо третя спроба виявляється невдалою, то система блокує відповідну станцію і фіксує факт атаки на відповідну MS. Очевидно, що не всі

абоненти однаково інтенсивно атакуються, в заданому періоді часу, таким способом. Тому для різних MS такий інформаційний параметр, як інтенсивність атак цього типу, буде різним. Процес моделі  $I(u_i)$ , що аналізує  $\Delta\delta t(k_i)$ , відслідковує величину  $\Delta\delta t(k_i)$  для даної MS і аналізує інтенсивність атак підбору ключа  $K_i$ , яка була зареєстрована. Якщо вона зростає в часі і збільшується  $\Delta\delta t(k_i)$  або цей параметр є досить великим, то це означає, що цього типу атаки будуть повторюватись і необхідно зменшувати величину  $\Delta\delta t(k_i)$ , яка в загальному характеризує період використання ключа  $K_i$  для окремої станції MS і, відповідно, абонента. На цьому прикладі видно, що виявлення атаки процесами моделі загроз не можна розглядати традиційно у відповідності із схемою, за якою діє на  $W_i$  певна атака і безпосередньо розпізнається в період її дії. Справа в тому, що атака підробки ключа ідентифікації може мати ціль, що полягає у несанкціонованому використанні чужих ресурсів (оплачених послуг). В цьому випадку відповідна атака може реалізовуватися для цілого класу MS, наприклад, класу MS, що знаходяться у певній соті, або класу MS, що являють собою певний тип MS, чи класу MS, що обслуговується певним оператором. Отже, якщо при великому значенні  $\Delta\delta t(k_i)$  або його зростанні зростає кількість атак для підробки ключа  $K_i$ , то процес  $V_i(U_i, e)$  виявляє факт існування певної інтенсивності атак цього типу. На цьому прикладі видно, що механізм розпізнавання певної інтенсивності атак тісно пов'язаний з інформаційною компонентою моделі  $I(u_i)$ , яка відображає величину росту атак певного типу в часі.

Важливим елементом алгоритму реалізації процесу  $V_i(U_i)$  є дисципліна моніторингу параметрів моделі  $I(u_i)$  з метою виявлення окремих атак чи виявлення їх інтенсивності за даний інтервал часу. В першому випадку виявляється атака на конкретну MS. В другому випадку виявляється факт реалізації атак на окремий клас мобільних станцій.

З наведених вище прикладів випливає, що за різними параметрами моделі загрози розпізнаються різні типи атак та різні модифікації атак окремих типів. З цього виходить, що класифікувати атаки треба не стільки за способом їх реалізації з точки зору певної небезпеки, скільки з точки зору можливих загроз, що існують в об'єкті, який захищається, та з точки зору можливих способів використання цих загроз для реалізації атаки.

Процес моніторингу, що використовується в моделі  $I(u_i)$  для процесу  $V_i(U_i, e_i)$ , являє собою реалізацію адаптивного методу ініціації циклу проведення аналізу біжучих значень ознак та параметрів, що безпосередньо пов'язані з загрозами. Адаптація в цьому випадку стосується вибору періоду між послідовними циклами аналізу, що реалізується фрагментом процесу  $V_i(U_i, e_i)$ . Оскільки функціонування  $I(u_i)$  являє собою процеси, що обслуговують ЗМІ, а не виконують основні функції з надання послуг, то відповідні процеси повинні завантажувати засоби системи певним оптимальним способом. Цей спосіб повинен гарантувати використання мінімальної кількості ресурсів при забезпеченні необхідного рівня безпеки функціонування відповідних процесів. У зв'язку з цим виникає задача оцінки біжучого рівня безпеки функціонування системи. Для розв'язку цієї задачі використовується методика оцінки, що ґрунтується на ймовірнісно-логічних структурах та відповідних засобах визначення рівня небезпеки функціонування ЗМІ. Суть цих методів полягає у наступному. В рамках інформаційної моделі  $I(u_i)$  реєструються всі атаки, що здійснювались відносно системи масової інформації. Кожна атака реалізується у вигляді деякої послідовності дій, які складають окремі кроки атаки. В рамках  $I(u_i)$  зареєстровані атаки розділяються на два класи – атаки, що закінчилися неуспішно, та атаки, що закінчилися успішно. Реєстрація успішних атак певного типу не є проблематичною, оскільки в найгіршому випадку в рамках системи реєструється факт дії відповідної атаки на роботу системи. Тоді

залишається розв'язати задачу розпізнавання типу атаки. Реєстрація невдалих атак потребує більш детального роз'яснення.

Невдалою атакою вважається така атака, яка була виявлена в процесі її реалізації, і системою захисту була реалізована процедура протидії атаці. Прикладом такої атаки та прикладом засобів протидії цій атаці може бути атака на ключ алгоритму АЗ (алгоритм реєстрації MS в системі), що реалізується шляхом підбору ключа  $K_i$ . Засобом протидії цій атаці, у випадку її виявлення, є блокування MS після третьої спроби невдалої реєстрації MS. Очевидно, що наступними кроками такої атаки можуть бути спроби несанкціонованого використання ресурсів системи, що також може бути виявлено, якщо MS формує запит на ресурс, який є заблоковано або який є недоступним даній MS. Попередніми кроками цієї атаки можуть бути дії, пов'язані з формуванням несанкціонованого ключа доступу. Очевидно, що безпосередня дія засобів захисту з ціллю протидії атаці на цьому кроці є неможливою, оскільки фізично така протидія безпосередньо технічними чи програмними засобами захисту є проблематична.

Завдяки тому, що засоби захисту являють собою інформаційну модель, в рамках останньої реєструється інформація про здійснення атак на цьому кроці. На основі аналізу цих даних засоби захисту можуть ініціювати дії, що опосередковано діють на міру успішності реалізації цієї атаки на відзначеному кроці. Така опосереднена дія може полягати у зміні параметрів загроз, що призводить до зменшення ймовірності успіху в реалізації цього кроку атаки. Таким параметром може бути інтервал дії відповідного ключа. Якщо час на генерацію ключа та інтервал часу між генерацією та його використання в сумі більший, ніж період використання ключа  $K_i$  в системі, то зміна періоду використання ключа може інтерпретуватися як протидія засобів захисту атакам підміни ключа на цьому, першому, кроці відповідної атаки. В існуючих реалізаціях системи масової інформації зміна ключа  $K_i$  здійснюється у відповідності з певним правилом, наприклад, при зміні абонентом персонального номера телефона. У випадку



де  $\alpha_i$  – ідентифікатор успішності кроку  $x_{ij}$  атаки  $a_i$ ,  $\beta_i$  – ідентифікатор неуспішності кроку  $x_j$  атаки  $a_i$ . Ідентифікатори приймають значення, що дорівнює 1, якщо результат реалізації кроку відповідає успішному його завершенню, а в протилежному випадку відповідний ідентифікатор приймає значення, що дорівнює нулю. Таким чином, ймовірність  $P_{ij}(x_{ij})$  означає відношення кількості успішних дій атаки на цьому кроці до загальної кількості дій, які виконуються в процесі реалізації цієї ж атаки, що відповідає класичному визначенню ймовірності виникнення тієї чи іншої події. Прийmemo, що ймовірність викривання атаки на кожному окремому кроці її реалізації є незалежною величиною. Очевидно, що таке припущення дещо спрощує задачу, але з огляду на те, що модель, в рамках якої реалізуються процеси виявлення атак є інформаційною, то результати аналізу даних, що накопичуються в  $I(u_i)$ , можуть представлятися у вигляді дискретних незалежних величин. Якщо прийняти, що такі величини між собою не зв'язані, то наведене вище припущення не призведе до значних похибок. Завдяки такому припущенню, кожен рядок із співвідношення (5) можна просумувати:

$$P_i(C_i(a_i)) = \sum_{j=1}^n P_{ij}(x_{ij}).$$

В цьому випадку можна розрахувати ймовірність досягнення цілі кожною атакою.

Різні атаки призводять до різних цілей, кожна з яких допускає певну інтерпретацію зміни величини рівня безпеки системи. Наприклад, атаки порушення конфіденційності послуги зв'язку не призводять до безпосередньої відмови системи у наданні відповідної послуги. Більше того, в рамках системи масової інформації можуть виникати трафіки, які не потребують протидії атакам, що направлені на порушення конфіденційності передачі даних. Вимога до забезпечення необхідного рівня конфіденційності може залежати від абонентів та характеру даних, що передаються. Аналогічна ситуація має місце і у випадку атаки направленої на



несанкціоноване використання чужих ресурсів, які в системі можуть являти собою плату за надання послуг. Це може мати місце, коли величина втрачених ресурсів не перебільшує заданого порогового значення.

Як уже зазначалося, необхідно визначити інтегральний параметр величини безпеки функціонування системи масової інформації. Очевидно, що він може бути представлений, як деяка функція цілей атак, які діють на систему протягом певного часу:

$$R(W) = F \{ P_1 [ C_1 (a_1) ], \dots, P_m [ C_m (a_m) ] \}.$$

При побудові можливого варіанта явної форми цієї функції необхідно сформувавати для відповідних операцій допустиму інтерпретацію, яка була б узгоджена з імовірнісною природою аргументів. Таке узгодження є можливим, якщо функція  $F$  являє собою логічний вираз, що сформований з кон'юнкцій і диз'юнкцій. В цьому випадку ймовірності можуть відповідно перемножуватися й додаватися, а сама логічна зв'язка інтерпретується, як ймовірність отримання значення одиниці в результаті її виконання. Завдяки використанню параметра  $R(W)$ , можна визначити величину безпеки функціонування системи зв'язку на кожному кроці функціонування системи  $W$ . Це означає, що величина  $R(W)$  може використовуватися в ролі критерію для ініціації процесів, що опосередковано чи безпосередньо впливають на можливість успішної реалізації атаки. Наприклад, може змінюватися ключ шифрування, час актуальності ключа і т.д. Величина  $R(W)$  в процесі функціонування системи може збільшуватися чи зменшуватися і таким чином частота ініціації моніторингу атак моделлю загроз буде адаптуватися до інтенсивності їх здійснення.

Процеси прогнозування моментів виникнення атак, виникнення модифікацій відомих атак чи нових атак та процес оцінки впливу атаки на об'єкт в конкретній версії реалізації моделі загроз розглядатися не будуть. В цьому випадку вплив атаки на об'єкт розглядається не тільки з точки зору зміни величини  $R(W)$ , а насамперед з точки зору зміни параметрів, що характеризують

якість надання послуг. Наприклад, одинична дія атаки при порушенні конфіденційності зв'язку може несуттєво вплинути на  $R(W)$ , але, в окремому випадку, може суттєво вплинути на показники якості послуг.

## Розробка алгоритмів протидії виявленим атакам

Протидія виявленим атакам зі сторони системи захисту є важливим етапом функціонування засобів захисту. Оскільки така система захисту подається у вигляді інформаційної моделі, то відповідна протидія буде реалізовуватися процесами, що діють в інформаційній моделі  $I(z_i)$  та ініціюються процесами виявлення атак  $V_i(U_i, e_i)$  з моделі загроз  $I(u_i)$ . Перш за все відзначимо, що ЗМІ, особливо мобільні ЗМІ, обслуговуються комп'ютерними системами, на яких реалізуються регістри HLR, VLR та інші системи, такі як центр аутентифікації, центр експлуатації та обслуговування й інші. В склад ЗМІ входять шлюзи, через які ЗМІ можуть підключатися до комп'ютерної мережі чи інших зовнішніх систем. Тому відносно ЗМІ можливі атаки на відповідні комп'ютерні системи, які відомі в теорії захисту комп'ютерних мереж. В нашому випадку такі атаки, особливо якщо вони реалізуються через мережу Internet, розглядатися не будуть. Основну увагу зосередимо на атаках, що породжуються в мережах телекомунікаційної системи. Відносно згаданих атак будемо вважати, що відповідні комп'ютерні системи захищаються традиційними для комп'ютерних мереж засобами.

Як уже зазначалось, система захисту може протидіяти атакам такими способами:

- безпосередньо протидіяти атаці, що виявлена в системі масової інформації і діє в певний момент часу;
- протидіяти опосередковано шляхом зміни параметрів засобів захисту чи параметрів загроз у випадку інтенсифікації дії атак та інтенсифікації їх ініціацій відносно до системи;

- здійснювати протидію на основі результатів прогнозування атак, така протидія є випереджувальною і полягає у модифікації системи захисту;
- протидіяти атакам, яких реально на момент відповідної протидії може небути, що обумовлює підвищення рівня безпеки системи масової інформації.

Кожний спосіб протидії буде реалізовуватися окремими процесами моделі загроз та процесами аналізу величини функції  $R(W)$ .

В рамках цього підходу, процес, що розглядається як базовий фактор, що визначає функціонування моделі, відрізняється від алгоритму функціонування кількома особливостями. Перша особливість характерна тим, що:

- в алгоритмі визначено всі функціональні залежності, що в ньому використовуються і являють собою послідовності чітко визначених перетворень, які складають методи аналізу даних;
- в процесі, в рамках різних кроків його реалізації, використовуються різні взаємозв'язки лише між вхідними і вихідними параметрами, які можуть описуватися таблично, логічними чи аналітичними залежностями, при цьому, у випадку повторної ініціації процесу, окремі кроки його реалізації можуть використовувати інші типи взаємозв'язків, відносно попередньої реалізації.

Друга особливість має такі ознаки:

- в одному і тому ж процесі  $V_i(z_i)$ , при різних його реалізаціях на окремих, однакових кроках, можуть використовуватися різні параметри в ролі параметрів-аргументів;
- в алгоритмах параметри-аргументи та параметри-функції визначаються днозначно і, при різних ініціаціях алгоритму, вони не змінюються.

Наступна відмінність полягає у тому, що процес може повторюватись однією і тією ж ініціалізацією, в кожній з яких відбуваються модифікації процесу, ціллю яких є адаптація результатів функціонування процесу до обмежень, що описуються

різними цілями, та адаптацією до інших відмінностей, які стосуються окремих деталей процесу.

Реалізацію процесів протидії атакам будемо розглядати окремо для кожного із способів протидії. Оскільки відповідні способи реалізації протидії можуть використовуватись в рамках різних засобів захисту і, відповідно, в рамках різних моделей засобу захисту, то будемо таким чином формувати процеси, щоб останні були придатними для протидії атакам, що мають відношення до  $Z_{sh}$ ,  $Z_{do}$  і  $Z_{mo}$ . Відмінності кожного із способів протидії, що обумовлюються різними типами засобів захисту, будемо враховувати і аналізувати в рамках одного процесу. Розглянемо формування процесу протидії, який здійснює протидію атаці, що безпосередньо діє на об'єкт в момент її виявлення  $V_i(u_i, b)$ .

Ініціатором процесу  $V_i(u_i, b_i)$  є процес з моделі  $I(u_i)$ , який розпізнає діючу атаку. Засоби захисту, для формування процесів протидії, використовують параметри, що описують відповідний засіб.

Наприклад, засіб захисту:

$$Z_{sh} = \{D[d(\omega), d(k_i)], \delta t_i(k_i), \varphi(\omega, k_i), \Psi(k_i)\}$$

може використовувати параметри, які описують різні аспекти атак для розкриття ключа шифрування. Один з проявів такої атаки являє собою спробу нелегальної реєстрації. В рамках існуючої системи такої спробі здійснюється протидія, яка полягає у блокуванні відповідного MS. Крім блокування нелегальної станції NMS, засоби захисту фіксують персональні параметри відповідної MS. У випадку повторної, успішної реєстрації, з точки зору використання ключа ідентифікації  $K_i$ , засоби захисту аналізують наявність в інформаційній моделі  $I(z_i)$  послуги, що обслуговує відповідну MS, на основі якої здійснюється розблокування відповідної станції. Якщо такої послуги не було надано відповідній MS, то реєстрація станції переводиться в категорію псевдореєстрацій, а остання, незалежно від того, чи була вона розпізнана як легальна, розгля-

дається, як станція типу NMS. В цьому полягає безпосередня протидія атаці зі сторони процесу  $V_i(z_i, b)$ .

Розглянемо атаку на ключі шифрування даних. Як відомо, для шифрування тексту, що передається з MS, використовуються поточні шифри, суть яких полягає в тому, що ключ формується у вигляді потоку  $K_i = \xi_1 \dots \xi_m$  і використовується для шифрування потоку явного тексту  $\omega_i = \omega_{i_1}, \dots, \omega_{i_m}$ . В загальному випадку потоковий алгоритм формування ключа записується у вигляді:

$$\xi_i = f_i(k, \omega_1, \dots, \omega_{i-1}).$$

Елемент ключа  $\zeta_i$  використовується для шифрування  $\omega_i$ , в результаті чого отримуємо  $y_i = (e(\Sigma_i)(\omega_i))$ . Таким чином, при шифруванні явного тексту  $\omega_1, \dots, \omega_m$  по черзі обраховується послідовність  $\Sigma_1 y_1 \Sigma_2 y_2 \dots \Sigma_m y_m$ . В явному вигляді функція  $f_i$  записується у вигляді лінійного рекурсивного співвідношення.

$$\xi_{i+m} = \sum_{j=0}^{m-1} C_j \zeta_{i+j} \bmod 2, \quad (6)$$

де  $C_0, \dots, C_{m-1} \in Z_2$ . В процесі шифрування виконується формування послідовного значення ключа шляхом виконання таких дій:

- вибирається  $\zeta_i$  в ролі поточного біта потоку;
- здійснюється зсув кожного з елементів  $\zeta_2 \dots \zeta_m$  на один біт вліво;
- вираховується нове значення  $\xi_m$  у відповідності із співвідношенням:

$$\xi_i = \sum_{j=0}^{m-1} C_j \zeta_{j+1}.$$

Описана послідовність відповідає роботі лінійного регістру зсуву з зворотним зв'язком, схема якого зображена на рис. 12.

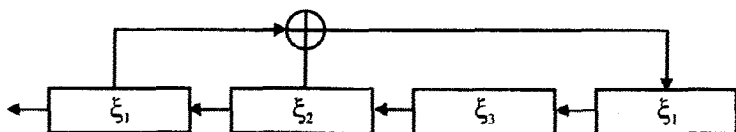


Рис. 12. Лінійний реєстр зсуву з зворотним зв'язком

Можлива атака на шифр такого типу використовує те, що відповідна криптосистема є лінійною. Якщо припустити, що атакуючому відомий відкритий текст і текст зашифрований та відоме значення  $m$ , то співвідношення (6) можна подати у вигляді системи лінійних рівнянь з  $m$  невідомими, яка запишеться у вигляді:

$$(\xi_{m+1}, \xi_{m+2}, \dots, \xi_{2m}) = (C_0, C_1, \dots, C_{m-1}) \begin{pmatrix} \xi_1 \xi_2 \dots \xi_m \\ \xi_1 \xi_2 \dots \xi_{m+1} \\ \vdots \\ \xi_m \xi_{m-1} \dots \xi_{2m-1} \end{pmatrix}.$$

Якщо матриця у цьому співвідношенні є зворотною по модулю 2, то отримаємо розв'язок:

$$(C_0, C_1, \dots, C_{m-1}) = (\xi_{m+1}, \xi_{m+2}, \dots, \xi_{2m}) \begin{pmatrix} \xi_1 \xi_2 \dots \xi_m \\ \xi_1 \xi_2 \dots \xi_{m+1} \\ \vdots \\ \xi_m \xi_{m-1} \dots \xi_{2m-1} \end{pmatrix}^{-1}.$$

Наведений вище алгоритм атаки на ключ не здійснюється в режимі реального часу, а реалізується у вигляді пасивного етапу атаки. На пасивні етапи атаки система захисту не може протидіяти безпосередньо.

В рамках цього підходу існує можливість здійснювати опосереднену протидію, яка може полягати у наступному. При блокуванні NMS в рамках моделі  $I(z_i)$  реєструється вся інформація про NMS, наприклад, тип MS, регіон, в якому викрита NMS, створюється образ абонента, якому легально належить заблокована MS. Цей образ описується такими параметрами:

— інтенсивністю атак на даний MS;

- даними про втрати MS, що формуються на основі відповідних повідомлень абонентів;
- інтенсивністю використання послуг ЗМІ певним абонентом та їх характером;
- мірою мобільності цього абонента;
- персональними вимогами абонента до бажаної міри безпеки передачі даних і т.д.

Вся ця інформація реєструється в рамках  $I(z_i)$ , і вона у відповідності з встановленими критеріями та алгоритмами її обробки аналізується. Для прийняття рішень з підвищення рівня безпеки певного абонента необхідно сформулювати критерії оцінки біжучого рівня безпеки. При цьому критерій, який можна визначити на основі встановленого або прийнятого способу вимірювання рівня безпеки, не завжди є обґрунтованим з точки зору затрат на реалізацію захисту. Справа у тому, що розширення засобів безпеки чи розширення їх можливостей потребують відповідних затрат. Такі затрати повинні покриватися за рахунок коштів абонентів. В цьому випадку рівень безпеки надання послуг може бути залежним від оплати, яку цей абонент може забезпечувати для надання відповідної можливості використання підвищеного рівня безпеки. На сьогодні в рамках систем ЗМІ індивідуальна орієнтація систем масової інформації на окремого абонента не використовується достатньою мірою. Завдяки створенню інформаційних засобів захисту така орієнтація технічних параметрів може розвиватися в необхідній мірі.

Розглянемо інші моделі захисту інформації в ЗМІ. До таких моделей належать модель захисту від несанкціонованого доступу:

$$Z_{do} = f_i \{ \chi, \eta, \tau, \lambda \},$$

та модель захисту від моніторингу

$$Z_{mo} = F_i \{ G_p, G_m, G_n, y_i^* \}.$$

Модель захисту ЗМІ від несанкціонованого доступу  $Z_{do}$  використовує в якості аргументів параметри, що відрізняються від

параметрів моделі захисту  $Z_{sh}$ . Модель  $Z_{sh}$  в більшій мірі орієнтована на опис алгоритмів шифрування і, відповідно, параметри описують можливості самого шифру. З точки зору технічної реалізації доступу, що має місце в ЗМІ, такий доступ реалізується на основі використання алгоритмів шифрування та протоколів доступу. Незважаючи на це,  $Z_{do}$  відрізняється від  $Z_{sh}$  тим, що в рамках  $Z_{do}$  використовуються, в першу чергу, параметри загального характеру, або організаційні параметри. Наприклад, параметр, що характеризує можливість отримувати додаткову інформацію про засоби захисту завдяки використанню послуги WAP, параметр, що характеризує додаткові умови надання послуг та інші. Параметри такого типу не можуть використовуватися поза рамками інформаційної моделі, оскільки вони мають значною мірою якісний характер. Тому основною задачею, що розв'язується в рамках моделі  $Z_{do}$ , є задача оцінювання цих параметрів таким чином, щоб можна було говорити про кількісні величини цих параметрів.

Розглянемо більш детально параметр  $\chi$ , який характеризує міру реалізації відновлення явного тексту повідомлення, що зашифрований потоковим алгоритмом типу АЗ. Відомо, що всі криптосистеми (криптоалгоритми) є зворотними. З точки зору захисту інформації, зворотність криптоалгоритму є обов'язковою. При несанкціонованому дешифруванні тексту, що зашифрований поточним шифром, процес дешифрування складається з таких етапів:

- визначення періоду ключа  $m$ ;
- визначення ключа шифрування  $k$ .

Для визначення періоду ключа використовуються методи, що ґрунтуються на визначенні індекса збігання, який визначається у відповідності із співвідношенням:

$$I_c = \sum_{i=1}^N \left[ \frac{F_i(F_i - 1)}{N(N - 1)} \right],$$



де  $F_i$  – частота використання  $i$ -тої букви в послідовності шифротексту. Індекс збігання послідовності  $a_1, \dots, a_N$  дорівнює ймовірності  $P_a(a_j = a_{j^*})$ , збігання букв цієї послідовності на випадково вибраних місцях  $j$  і  $j^*$  з  $N$  місць, де  $j \neq j^*$ . Для розв'язку задачі дешифрування повідомлення можуть використовуватися різні методи:

- метод протягування ймовірного слова;
- метод читання по колонках;
- метод дешифрування з використанням взаємного індекса збігання;
- метод Сімпсона та інші методи.

Наприклад, в методі протягування ймовірного слова вибираються дві послідовності відомого шифротексту довжиною  $m$ . Припускаємо, що вибране слово є початком відкритого тексту, та знаходимо перші  $\xi_1, \xi_2, \dots, \xi_t$  підстановки ключа  $K_i$ . Рівняння  $\xi(a) = b$  при відомих  $a$  і  $b$  однозначно розв'язується відносно  $\xi$  з  $K_i$ . Правильність вгадування ймовірного слова  $a'_1, a'_2, \dots, a'_t$  перевіряється на змістовність розшифрованого тексту:

$$\xi_1^{-1}(b_{1+t}), \dots, \xi_m^{-1}(b_{t+m}).$$

Якщо послідовність цих букв являє собою випадковий текст, то вибирається наступне ймовірне слово для опробування. Пошук зчитуваного слова продовжується до того часу, поки для перших  $m$  букв таке слово не буде відшуканим. З наведеного опису виходить, що процес дешифрування може мати різну довжину і ця довжина залежить від ймовірності вибору читаного слова з шифротексту. Ймовірність вибору читаного слова з шифротексту на першому кроці чи на наступних кроках визначається алгоритмом потокового шифрування. Тому введений параметр  $\chi$  являє собою характеристику алгоритму шифрування, яка інтегрально характеризує необхідну кількість кроків вибору слів з шифротексту, щоб можна було розкрити ключ  $K_i$ . В цьому сенсі в нашій роботі й інтерпретується параметр міри зворотності алгоритму АЗ. Очевидно, що

цей параметр не може бути обрахований детермінованими методами, а формується на основі апріорних даних про спроби розшифрування ключа та даних про кількість успішних спроб розшифрування зашифрованого тексту.

Розглянемо більш детально параметр  $\eta$ , який визначає додаткові умови використання послуг системи масової інформації. Такий параметр визначається наступним чином. Кожна з додаткових умов, що стосується окремого абонента, оцінюється певною величиною вартості відповідної умови. Якщо окрему умову позначити буквою  $\delta_i$ , то  $\alpha_i \delta_i$  буде означати величину або вартість умови  $\delta_i$ . Тоді параметр  $\eta$  будемо визначати, як суму вартості всіх умов:

$$\eta = \sum_{i=1}^n \alpha_i \delta_i (MS_i).$$

Величина  $\eta$  в процесі експлуатації системи та станцій MS може змінюватися, що реєструється в  $I(z_i)$ , яка вміщує фрагмент, що описує  $Z_{do}$ .

Використання параметра  $\eta$  для реалізації протидії атакам може полягати у наступному. Нехай в рамках  $I(z_i)$  виявилось, що інтенсивність атак на MS, що характеризується певним образом абонента, зростає. Тоді аналізується характер зміни параметра  $\eta$ . Характер змін параметра може описуватися швидкістю його зміни, величиною зміни чи мірою рівномірності таких змін. В залежності від цього вибирається складова, що спричиняє в найбільшій мірі такі зміни. Прикладом таких складових можуть слугувати такі параметри:

- частота зміни номера абонента;
- періодичність оплат послуг зв'язку;
- номенклатура використовуваних послуг;
- частота виникнення критичних ситуацій (втрати мобільної станції з різних причин);

— параметри сеансів зв'язку (середня тривалість однієї трансакції) і т.д.

Наведені вище приклади додаткових умов експлуатації MS носять якісний характер з точки зору їх зв'язку з рівнем безпеки. Тому залежності між величинами параметрів, що характеризують відповідні умови, та рівнем безпеки встановлюється на рівні апіорних даних та на основі досвіду експлуатації ЗМІ. Найчастіше такі зв'язки описуються логічними функціями, розширеними пороговим аналізом біжучих значень окремих параметрів. Крім зв'язків між параметрами  $\delta_i$  і їх впливом на рівень безпеки системи, між окремими параметрами також можуть існувати зв'язки. Такі зв'язки встановлюються на основі апіорних даних, що формуються в результаті реєстрації відповідних  $\delta_i$  та на основі аналізу причин, що обумовлюють зміни значень відповідних параметрів.

Розглянемо параметр  $\lambda$ , який характеризує можливість отримання додаткової інформації про абонентів та інші особливості системи масової інформації, яка може бути використана для організації атаки на ЗМІ зі сторони небезпеки. Відомо, що перед всякою реалізацією безпосередньої несанкціонованої дії на той або інший об'єкт, здійснюється пошук інформації про відповідний об'єкт, яка є необхідною для реалізації фрагмента атаки, що безпосередньо на цей об'єкт діє. Очевидно, що чим менше даних про об'єкт, тим менше шансів, що реалізація атаки буде успішною. Тому перед здійсненням активної фази атаки необхідно реалізувати розвідку, або пошук даних про об'єкт атаки. Такий пошук даних є можливим, якщо інформація про функціонування об'єкта атаки може бути отримана в результаті тих чи інших дій.

Можливість отримувати ту чи іншу інформацію про об'єкт атаки залежить від номенклатури послуг, які надає система. Тому параметр  $\lambda$  будемо розглядати, як сукупність певних можливостей отримання інформації про систему в різних режимах її роботи. Способи отримання такої інформації можуть бути легальними і нелегальними. Очевидно, що розширення номенклатури послуг

супроводжується розширенням інформації про систему, яка ці послуги надає. Нехай такою послугою є послуга з надання зв'язку з Web-сервером. Така послуга надається в рамках використання WAP-протоколів. Згідно з форумом WAP, для використання служб безпеки при реалізації такої послуги в архітектуру WAP можна інтегрувати протокол безпеки транспортного рівня в безпроводних мережах WTLS. Впровадження такого протоколу в процедуру надання відповідної послуги є одним із методів протидії атакам, що на початкових фазах орієнтовані на отримання інформації про абонентів. Можливості такої протидії атакам розвідки даних ґрунтуються на наступному. Протокол WTLS може надавати різні рівні захисту. Новим, відносно GSM, в цьому випадку, є забезпечення безпеки обміну між двома одноранговими об'єктами, а не тільки між мобільною та базовою станціями. Цей протокол ґрунтується на механізмі TLS, який є протоколом захищених сокетів. Для використання WTLS встановлюється безпечний сеанс зв'язку. Першим етапом є ініціація сеансу зв'язку. Параметрами, які при цьому використовуються, є адреса джерела, порт джерела ініціатора зв'язку, адреса призначення, порт призначення. Крім того, ініціатор пропонує ключі обміну, набір шифрів, методи компресії. Одноранговий об'єкт передає у відповідь параметри режиму, порядкові номери, цикл оновлення ключів, ідентифікатор сеансу зв'язку, вибраний набір шифрів та метод компресії. Атаки на протоколи WAP є подібними на атаки, що використовуються в комп'ютерних мережах на протоколи з метою отримання додаткової інформації про потенційні об'єкти активних атак. Параметр  $\lambda$  являє собою сукупність даних, які характеризують інформацію та способи її отримання при використанні в рамках ЗМІ послуг, що подібну інформацію використовують. Цей параметр, як і параметр  $\eta$ , має якісний характер.

## **Загальна організація функціонування інформаційної технології системи захисту засобів масової інформації**

В рамках існуючої системи масової інформації використовуються засоби захисту, що мають цілеспрямований характер відносно процесів, які відбуваються в системі упродовж її функціонування. Додаткові компоненти засобів орієнтовані на розширення функцій системи із забезпеченню її безпечного функціонування шляхом реєстрації, аналізу та вимірювання додаткових параметрів безпеки, які об'єднуються в рамках моделей засобів захисту та інформаційних моделей системи захисту в цілому. Оскільки система масової інформації за своєю природою є системою розподіленою, то і засоби захисту є розподіленими, і не завжди атаки, що діють на локальні фрагменти системи масової інформації, повною мірою аналізуються в рамках цілої системи. Наприклад, протидія типовій атаці на несанкціоновану реєстрацію MS в системі масової інформації, у випадку її виявлення, полягає у блокуванні відповідної MS і реєстрації цього факту у відповідних реєстрах, що являють собою бази даних. В рамках цього підходу запропоновано розширення кількості параметрів, що організовані в інформаційні моделі системи безпеки, які дозволяють більш повно використовувати дані про всі атаки, що реалізуються в рамках системи масової інформації.

Оскільки розширення засобів здійснюється в рамках відповідної інформаційної технології, то завдяки цьому виникає можливість використовувати якісну інформацію для аналізу біжучого стану безпеки системи, якісну інформацію для прийняття рішень із здійснення протидії атакам. Принциповою особливістю, яка має практичний характер і ґрунтується на використанні моделей захисту, моделей загроз та інформаційних моделей системи захисту в цілому, є можливість здійснювати опосереднену протидію на атаки, що реалізуються небезпеками відносно системи масової інформації. Пасивна протидія призводить до підвищення рівня захисту, що існує в системі масової інформації.

Розширення можливостей системи захисту ЗМІ необхідне ще й для того, щоб в рамках відповідної системи можна було розв'язувати задачі персоніфікації необхідного рівня захисту. Це забезпечить можливість оптимізувати затрати на створення нових систем захисту в ЗМІ та при розширенні існуючих засобів захисту. Для того, щоб проілюструвати в цілому можливості, які створюють інформаційні компоненти в рамках реалізації інформаційної технології захисту, розглянемо узагальнену структурну схему організації системи захисту ЗМІ, розширену запропонованими засобами захисту та методами їх використання. Загальна структурна схема організації системи захисту наведена на рис. 13. Оскільки система масової інформації є розподіленою, то і відповідна система захисту також розподілена. Компоненти, що розширюють відповідну систему захисту, не потребують спеціально виділених компонент в рамках структури системи зв'язку, а можуть реалізовуватися як розширення або доповнення до існуючих компонент.

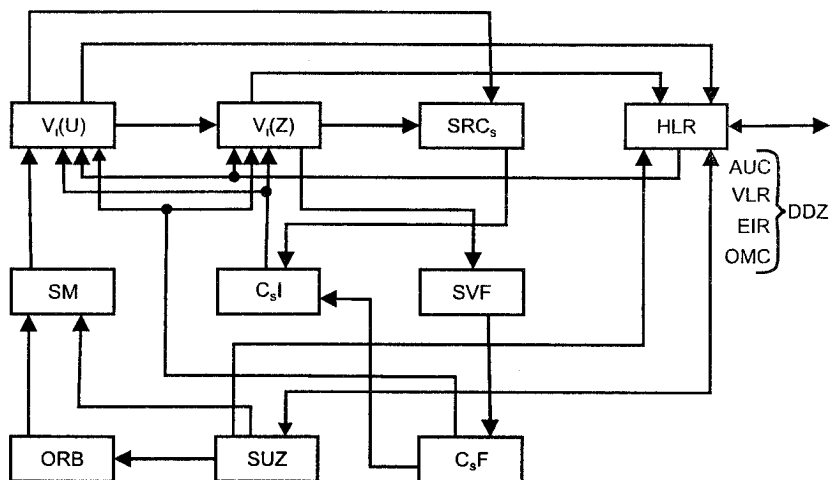


Рис. 13. Структурна схема загальної організації системи захисту

На рисунку прийнято такі позначення:

$V_i(U)$  – моделі загроз;

$V_i(Z)$  – моделі елементів захисту;

SRC<sub>s</sub> – модуль системи розширення словника C<sub>s</sub>;  
HLR – реєстр вихідного положення;  
SM – система моніторингу атак;  
DDZ – додаткові дані по захисту системи зв'язку;  
C<sub>s</sub>I – семантичний словник, що описує інтерпретації параметрів, які використовуються в системі захисту;  
C<sub>s</sub>F – семантичний словник, що описує функціональні зв'язки між параметрами;  
SVF – система встановлення функціональних залежностей між параметрами, якими розширюється C<sub>s</sub>F;  
ORB – система оцінки рівня безпеки об'єкта, що захищається;  
SUZ – модуль управління системою захисту.

Виходячи з наведеної структурної схеми, можна стверджувати, що запропонована система захисту являє собою програмно реалізоване розширення функціональних можливостей реєстра HLR при умові, що цей реєстр зв'язаний з центром аутентифікації AUC, реєстром місцезнаходження абонентів VLR та реєстром розпізнавання обладнання EIR, а також центром експлуатації і обслуговування OMC. Всі необхідні зв'язки HLR, крім зв'язку з реєстром AUC, в рамках структури ЗМІ реалізуються через контролер базових станцій BTS, тому існує принципова можливість отримувати системою захисту необхідну інформації в рамках існуючої системи. Цього достатньо для проведення дослідних випробувань відповідної системи. При подальшому розвитку системи захисту можуть реалізовуватись безпосередні зв'язки між системою захисту та наведеними вище модулями системи GSM, які реалізуються у вигляді додаткових інтерфейсів відповідних модулів.

Розглянемо спосіб функціонування системи захисту на загальному рівні. Алгоритм функціонування системи (алгоритм A(z)) зображено на рис. 14.

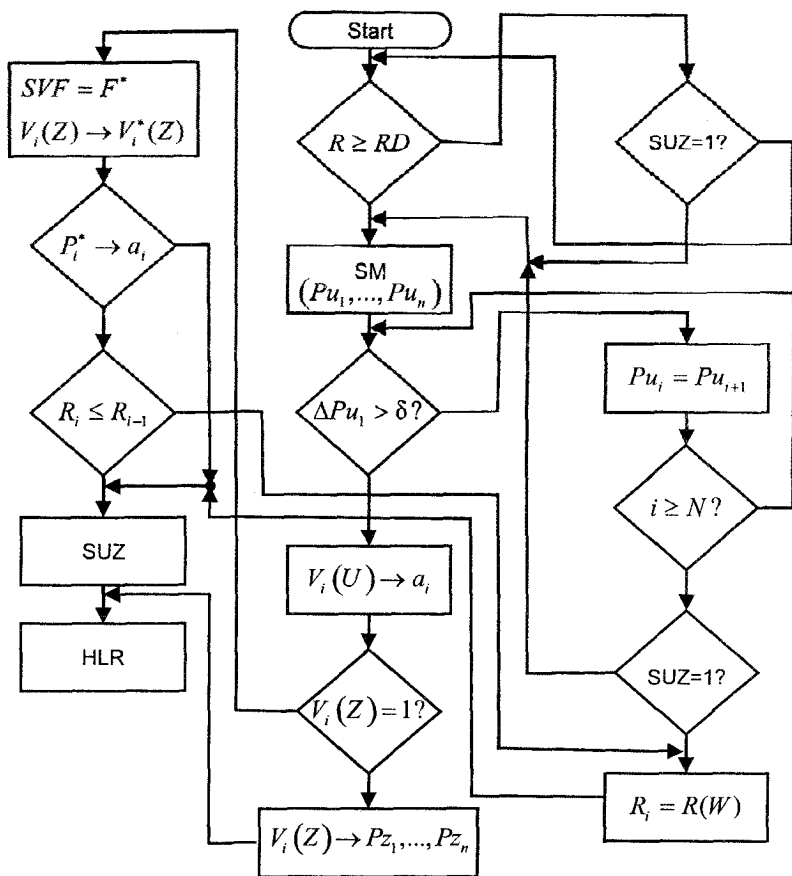


Рис. 14. Структурна схема алгоритму функціонування розширення системи захисту ЗМІ

Насамперед визначається рівень безпеки функціонування системи. Це здійснюється на основі використання моделі обчислення рівня ризику та на основі даних про порушення параметрів безпеки в системі  $R_i(W)$ . Якщо рівень ризику біжучого стану ЗМІ більший, ніж допустимий рівень ризику  $R_i(W) \geq R_{\zeta}(W)D$ , то управління передається на блок, що реалізує алгоритми моніторингу параметрів системи, які пов'язані з загрозами. Ініціація системи безпеки може здійснюватись незалежно від рівня ризику порушення безпеки в



системі масової інформації, а також й на основі ініціації останньої модулем управління SUZ, який, в свою чергу, може використовувати для такої ініціації інформацію з реєстра HLR.

В процесі моніторингу, який управляється модулем SM, а реалізується в рамках інформаційної моделі  $I(U)$ , шляхом ініціації відповідного процесу здійснюється розпізнавання факту наявності атаки  $a_i$ . Таке розпізнавання, у найпростішому випадку, полягає в контролі біжучих значень параметрів загроз, які описані і визначаються інформаційною моделлю загроз. Послідовність вибору тих чи інших параметрів моделі загроз здійснюється модулем моніторингу SM. Це обумовлено тим, що в залежності від біжучої інформації, яка може поступити з HLR в SUZ, може виникнути необхідність у зміні пріоритетів аналізу параметрів моделі загроз  $I(U)$ .

Після виявлення безпосередньо діючої атаки або при виявленні факту інтенсифікації атак відповідний процес моделі загроз  $V_i(U)$  ініціює відповідний процес протидії атаці  $V_i(Z)$ , яка може бути опосередкованою. Якщо такий процес закінчив своє функціонування, то відповідна інформація передається в реєстр HLR. Якщо необхідного процесу в  $I(Z)$  немає, то управління передається до засобів формування необхідного процесу, що знаходяться в моделі  $I(Z_i)$ . До таких засобів належить, в першу чергу, модуль формування нових взаємозв'язків між параметрами. Відсутність необхідного процесу може обумовлюватися відсутністю фрагмента в послідовностях дій, що реалізують відповідні процеси. В окремих діях відбувається перетворення значень одних параметрів у значення інших параметрів у відповідності з функціями взаємозв'язків між параметрами. Після цього формується новий процес. Якщо він відрізняється від існуючих процесів лише відсутністю однієї операції, що відповідає функції перетворення, то цей процес ініціюється і здійснює формування протидії безпосередній атаці чи формування протидії збільшенню інтенсивності атак певного типу.

Може виникнути ситуація, коли на початковому етапі функціонування алгоритму  $A(Z)$  рівень ризику, на якому перебуває система  $i$ , в першу чергу об'єкти, що захищаються, є допустимим. Тоді управління передається в модуль управління системою SUZ і перевіряється, чи система управління не вимагає ініціювати роботу алгоритму  $A(Z)$ . Якщо SUZ таку вимогу виставляє, то управління передається на модуль моніторингу SM. В процесі аналізу параметрів загроз  $P_{ui}$ , може виявитися, що черговий параметр знаходиться в допустимих межах. В цьому випадку здійснюється перехід до наступного параметра, якщо не всі параметри проаналізовано. Якщо проаналізовано всі параметри, то управління передається в модуль SUZ, який може продовжити роботу системи захисту незалежно від біжучого стану рівня ризику або обчислити біжуче значення величини ризику роботи з системою масової інформації, передати дані в реєстр HLR і черговий раз розпочати роботу із ініціативи реєстра HLR.

Засоби захисту від моніторингу радіоканалів досить тісно пов'язані з апаратною реалізацією та засобами управління апаратурою, яка використовується в мобільних системах. У зв'язку з цим дослідження методів підвищення захисту на основі модифікації методів управління чи на основі модифікації самих засобів тісно пов'язані з проектуванням, дослідженням та виготовленням відповідних апаратних засобів, що являє собою в більшій мірі область, яка стосується фізичної реалізації каналів зв'язку та відповідної апаратури управління ними. Тому в рамках інформаційної технології ці методи не розглядаються з точки зору розв'язку задач підвищення безпеки мобільної системи. Інформаційні аспекти безпеки, в частині цих засобів, можуть обмежуватися тільки реєстрацією змін режимів роботи апаратних засобів, що можна пов'язати з безпекою роботи ЗМІ. Ця інформація може використовуватися в рамках розроблених інформаційних компонент з метою підвищення вірогідності рішень, що приймаються в процесі функціонування розроблених розширень системи захисту масової інформації.

Розглянемо більш детально реалізацію блоків, що стосується розширення словника  $C_s$  – модуль  $SRC_s$  та блоку, що стосується формування нових функціональних зв'язків – блок SVF. Завдяки блоку SVF, в рамках інформаційної моделі  $I(Z_i)$  стає можливим породження нових процесів  $V_i^*(Z)$ .

Породження нового процесу, з технічної точки зору, являє собою створення послідовності перетворень параметрів, що використовуються в інформаційній моделі системи захисту. Ініціатором породження процесу є процес моделі загроз, однією з його цілей функціонування є розпізнавання типу атаки. Метою для процесів, що функціонують в моделях засобів захисту, є протидія атакам, яка полягає у ліквідації самої атаки, якщо остання проявляється у вигляді певних дій або полягає у нейтралізації дії атаки на об'єкт захисту. Для прикладу, обмежимося другим випадком, оскільки проти більшості атак, що діють в ЗМІ, неможливо здійснювати безпосередню протидію. В цьому випадку кожна атака  $a_i \in A$  описується значеннями параметрів окремих загроз, що існують в об'єкті, які використовує відповідна атака, та описується зв'язками між параметрами, що характеризують засоби захисту. Крім того, цілі атаки описують порогові значення параметрів моделі захисту, при яких відповідна атака виявиться нейтралізованою. Таким чином, процес  $V_i(Z_i)$ , що відповідає реалізації протидії чи реалізації нейтралізації атаки, полягає у виконанні такої послідовності змін значень параметрів, яка призведе до зміни значень параметрів описаних в цілі процесу реалізації атаки, при яких атака виявиться нейтралізованою. Оскільки в рамках системи масової інформації можна говорити про наявність залежностей між параметрами, що описують функціонування ЗМІ, то має місце можливість побудови відповідної послідовності взаємних перетворень значень параметрів, між якими існує локальний зв'язок. В цьому випадку виконання процесу протидії, або процесу захисту  $V_i(Z_i)$ , полягає в тому, що, починаючи від значень параметрів, які описані в цілі функціонування процесу атаки, шляхом виконання перетворень

цих значень у відповідності з типом зв'язку між парою параметрів, в рамках процесу проводяться зміни їх біжучих значень. Такі зміни здійснюються послідовно від кінцевого параметра процесу до початкового параметра процесу, на вході якого задано параметри загроз, які також підлягають змінам. Якщо на деякому кроці виконання процесу має місце функціональний зв'язок в аналітичній формі, то на цьому кроці обраховане нове значення параметра мусить потрапляти в діапазон допустимих значень, який визначено в рамках інформаційної моделі системи захисту  $I(Z)$ .

Може існувати ситуація, коли в рамках моделі захисту  $I(Z_i)$  не існує детального опису процесу  $V_i(z_i)$ , який би пов'язував вхідні параметри, тоді параметри моделі загроз з відповідними параметрами цілі атаки і, відповідно, цілями процесу протидії атаці, що можна записати в загальному вигляді таким чином:

$$V_i(z_i) = P(U) \rightarrow P_k(z) \rightarrow \dots \rightarrow P_l(z) \rightarrow \dots \rightarrow P_j[C(a_i)].$$

При реалізації процесу  $V_i(z_i)$  кожна із стрілок замінюється функцією зв'язку між черговими параметрами, наприклад:  $P_l(z)\varphi P_j(z)$ . Процес  $V_i^*(z_i)$  мусить бути породженим, якщо в послідовності типу:

$$V_i(z_i) = \left\{ \begin{array}{l} P_{i-1}(z_i) = \varphi_1 [P_i[C(a_i)]], P_{i-2}(z) = \\ = \varphi_2 [P_{i-2}(z)], \dots, P_i(z) = \varphi_m [P_{i-m-1}(z)] \end{array} \right\},$$

немає хоча б одного функціонального зв'язку. В цьому випадку можливі такі ситуації:

- в інформаційній моделі існує необхідний функціональний зв'язок, але він не використовується в цьому процесі;
- в інформаційній моделі  $I(z_i)$  не існує функціонального зв'язку, який необхідно використати в цьому процесі протидії.

В першому випадку породження  $V_i^*(z_i)$  здійснюється шляхом внесення необхідного функціонального співвідношення у відповідне місце процесу  $V_i(z_i)$ . Це місце вибирається таким чином, щоб

вся послідовність функціональних перетворень була узгоджена за типами параметрів. Така узгодженість означає, що параметри, які послідовно пов'язані між собою рядом функціональних зв'язків, повинні становити безперервну послідовність процесу. В другому випадку, коли необхідного функціонального зв'язку в інформаційній моделі немає, в модулі SVF реалізується формування відповідного зв'язку. Суть такого формування полягає у наступному. Якщо два параметри, між якими необхідно встановити функціональний зв'язок, являють собою множини дискретних значень, то один із способів встановлення такого зв'язку полягає у визначенні деякого третього параметра, який умовно називається синхронізуючим параметром. Наприклад, досить часто таким синхронізуючим параметром є параметр часу. В інших випадках формуються апроксимуючі функції, що задовольняють додаткові умови відповідного зв'язку.

## ВИСНОВКИ

В монографії розв'язано актуальну науково-технічну задачу розробки інформаційної технології систем захисту даних в електронних засобах масової інформації, що передаються по мобільній системі, на основі використання моделей засобів захисту та моделей загроз. При цьому отримано такі основні результати.

Розроблено та обґрунтовано способи побудови моделі системи захисту у вигляді функціональних залежностей, що визначають основні параметри, від яких залежить рівень захисту інформації, завдяки чому стало можливим дослідити вплив кожного з параметрів на рівень захисту.

Запропоновано нові уявлення про загрози, що існують в системі масової інформації і використовуються при реалізації різного типу атак, завдяки чому стало можливим сформулювати нові способи виявлення активних та пасивних атак.

Встановлено та формалізовано основні компоненти інформаційної моделі систем масової інформації, що являють собою семантичні словники різної функціональної орієнтації, правила формування нових інформаційних описів, правила виводу розширень інтерпретаційних описів окремих компонент словників, завдяки чому стало можливим будувати інформаційні моделі компонент системи захисту даних.

Розроблено інформаційні моделі загроз та інформаційні моделі засобів захисту на основі синтезу формального опису функціональних моделей загроз та моделей засобів захисту, що дозволило встановити інформаційні взаємозв'язки між параметрами відповідних моделей, оскільки аналітичні залежності між ними описувати досить складно.

Розроблено методи виявлення атак на інформацію, що передається в рамках системи масової інформації, методи протидії атакам пасивного та активного типу, що діють на систему масової інформації безпосередньо та опосередковано, що дозволяє підвищити рівень захисту послуг, які надаються електронними засобами масової інформації.

Розроблено структуру системи захисту даних, яка включає в себе моделі засобів захисту, моделі загроз та інші компоненти, що використовуються для ініціації процесів виявлення атак та протидії атакам несанкціонованого доступу до ресурсів; несанкціонованого відбору інформації, що передається мобільними системами та іншим видам атак на електронні засоби масової інформації.

## CONCLUSIONS

Important and actual scientific and technical problem of developing the information technology system of data protection in electronic means of mass media which are transmitted over a mobile system had been solved using the models of protection means and models of security threats. The following results were obtained.

Methods of constructing the models of protection system in the form of functional correlations that determine the main parameters which influence the level of information protection had been worked out and grounded, so it became possible to investigate the impact of each parameter on the level of protection.

New understandings of the threats that exist in mass media system and are used for different types of attacks were proposed, so now it becomes possible to form the new methods of the active and passive attacks identifying.

Basic components of the information model of mass media system, that are semantic dictionaries of different functional orientation by the origin, rules of the new information description formation, rules of the output of the interpretation descriptions extension of the individual vocabulary components had been worked out, so now it becomes possible to build the information models of the data protection component system.

Information models of security threats and information models of means of protection based on the synthesis of a formal description of the functional models of security threats and models of protection means which allowed to detect the informational correlations between the parameters of the appropriate models were worked out because the analytical correlations between them was too difficult to describe.

Methods of detecting attacks on the information, transmitted in the framework of mass media system, methods of counteraction to attacks of the passive and active type which act on the system of mass media information directly and indirectly what allows to improve the level of the protection services provided by means of electronic mass media had been worked out.



The structure of data protection, which includes the models of protection means, models of security threat and other components used to initiate detection of attacks and counteraction to attacks of unauthorized access to the resources; unauthorized selection of information transmitted by mobile systems and other types of attacks by electronic means of mass media had been worked out.

## СПИСОК ДЖЕРЕЛ

1. Любарский Ю. Я. Интеллектуальные информационные системы / Ю. Я. Любарский. – М. : Наука, 1990. – 227 с.
2. Юбін О. Г. Основи інформатики / О. Г. Юбін. – Хмельницький : ТУП, 1997. – 95 с.
3. Антипов И. Н. Основы информатики и вычислительной техники / И. Н. Антипов. – М. : Высшая школа, 1991. – 246 с.
4. Каныгин Ю. М. Основы теоретической информатики / Ю. М. Каныгин, Г. И. Калитич. – К. : Наук. думка, 1990. – 232 с.
5. Кукин В. И. Информатика: организация и управления / В. И. Кукин. – М. : Экономика, 1991. – 175 с.
6. Цымбал В. П. Информатика и индустрия информации / В. П. Цымбал. – К. : Высшая школа, 1989. – 158 с.
7. Колесник В. Д. Введения в теорию информации / В. Д. Колесник, Г. Ш. Полтырев. – Л. : ЛПУ, 1980. – 163 с.
8. Кузьмин И. В. Основы теории информации и кодирования / И. В. Кузьмин, В. А. Кедрус. – К. : Вища школа, 1986. — 238 с.
9. Казарин Л. С. Теория кодирования / Л. С. Казарин. – Ярославль : ЯрГУ, 1987. – 61 с.
10. Когновицкий О. С. Основы циклических кодов / О. С. Когновицкий. – Ленинград : ЛЭИС, 1990. – 62 с.
11. Кузьмин И. В. Кодирования и декодирование в информационных системах / И. В. Кузьмин. – К. : Высшая школа, 1985. – 190 с.
12. Татарин В. Я. Прикладна теорія інформації і кодування у волоконно-оптичних лініях зв'язку / В. Я. Татарин. – Л. : НУЛП, 2005. – 36 с.
13. Цымбал В. П. Теория информации и кодирование / В. П. Цымбал. – К. : Высшая школа, 1992. – 263 с.
14. Кон Е. Л. Избыточное кодирование в системах телемеханики и передачи данных / Е. Л. Кон. – Пермь, 1986. – 74 с.
15. Кричевский Р. Е. Сжатие и поиск информации / Р. Е. Кричевский. – М. : Радио и связь, 1989. – 168 с.

16. Алгоритмы и структуры систем обработки информации : сб. науч. тр. – Тула : ТПИ, 1989. – 122 с.
17. Лосев В. В. Поиск и декодирование сложных дискретных сигналов / В. В. Лосев. – М. : Радио и связь, 1988. – 225 с.
18. Марков А. А. Введения в теорию кодирования / А. А. Марков. – М. : Наука, 1982. – 192 с.
19. Прокис Джон Дж. Цифровая связь / Джон Дж. Прокис. – М. : Радио и связь, 2000. – 797 с.
20. Харатишвили Н. Г. Цифровое кодирование с предсказанием непрерывных сигналов / Н. Г. Харатишвили. – М. : Радио и связь, 1986. – 140 с.
21. Шпак Н. О. Економічна оцінка розробки і застосування програмного забезпечення в системах телекомунікації / Н. О. Шпак. – Л. : НУЛП, 2003. – 12 с.
22. Стенлов В. К. Проектування телекомунікаційних мереж / В. К. Стенлов, Л. Н. Беркман. – К. : Техніка, 2002. – 792 с.
23. Згуровский М. З. Микроволновые устройства телекоммуникационных систем : у 2-х томах / М. З. Згуровский, М. Е. Ильченко, С. А. Кравчук. – К. : Політехніка, 2003.
24. Babak Y. P. Microwave Technologies in Telecommunications systems / Y. P. Babak, T. N. Narytnik, S. A. Kravchuk. – K. : Техніка, 2002. – 272 с.
25. Крук Б. И. Телекоммуникационные системы и сети: учебное пособие. В 3 томах. Том 1. Современные технологии / Б. И. Крук, В. Н. Попантонопуло, В. П. Шувалов. – М. : Горячая линия, 2003. – 643 с.
26. Волгин Л. И. Непрерывная логика. Теория и применения / Л. И. Волгин, В. И. Левин. – Талин : АН, 1990. – 211 с.
27. Нагорный Н. М. Вопросы математической логики и теории алгоритмов / Н. М. Нагорный. – М. : ВЦ АН СССР, 1988. – 38 с.
28. Гастев Ю. А. Гомоморфизмы и модели. Логико-алгебраические аспекты моделирования / Ю. А. Гастев. – М. : Наука, 1975. – 151 с.
29. Григория Р. Ш. Свободные алгебры неклассических логик / Р. Ш. Григория. – Тбилиси : АН ГССР, 1987. – 110 с.

30. Девис, Мартин Прикладной нестандартный анализ / Мартин Девис. – М. : Мир 1980. – 236 с.
31. Закревский А. Д. Логические уравнения / А. Д. Закревский. – Минск : Наука и техника, 1975. – 95 с.
32. Заславский И. Д. Симметрическая конструктивная логика / И. Д. Заславский. – Ереван : Изд-во АН АССР, 1978. – 281 с.
33. Кирий В. Г. Логико-вероятностные методы и средства идентификации и прогнозирования бинарных систем / В. Г. Кирий. – Иркутск : Изд-во Иркутского университета, 1987. – 112 с.
34. Косовский Н. К. Элементы математической логики и ее приложения к теории субрекурсивных алгоритмов / Н. К. Косовский. – Л. : Изд-во ЛГУ, 1981. – 192 с.
35. Левин В. И. Бесконечнозначная логика в задачах кибернетики / В. И. Левин. – М. : Радио и связь, 1982. – 176 с.
36. Левин В. И. Динамика логических устройств и систем / В. И. Левин. – М. : Энергия, 1980. – 224 с.
37. Марков А. А. Элементы математической логики / А. А. Марков. – М. : МГУ, 1984. – 74 с.
38. Мендельсон Э. Введения в математическую логику / Э. Мендельсон. – М. : Наука, 1984. – 319 с.
39. Донской В. И. Дискретная математика / В. И. Донской. – Симферополь : «СОНАТ», 2000. – 354 с.
40. Плоткин Б. И. Универсальная алгебра, алгебраическая логика и базы данных / Б. И. Плоткин. – М. : Наука, 1991. – 448 с.
41. Сайфуллаев Н. М. Логический анализ понятия количества / Н. М. Сайфуллаев. – Душанбэ : АН ТаджССР, 1989. – 133 с.
42. Справочная книга по математической логике / под ред. Дж. Барейса. – М. : Наука, 1983.
43. Теребилов О. Ф. Логика математического мышления / О. Ф. Теребилов. – Л. : Изд-во ЛГУ, 1987. – 191 с.
44. Успенский В. А. Вводный курс в математическую логику / В. А. Успенский, Н. К. Верещагин, В. Е. Плиско. – М. : Изд-во МГУ, 1991. – 136 с.
45. Мышкис А. Д. Элементы теории математических моделей / А. Д. Мышкис. – М. : Наука, 1994.

46. Колмогоров А. Н. Математическая логика. Дополнительные главы / А. Н. Колмогоров, А. Г. Драгалин. – М. : МГУ, 1982. – 118 с.
47. Математические методы управления и обработки информации : междунар. вед. сб. – М. : МФТИ, 1983. – 169 с.
48. Математическое моделирование процессов управления и обработки информации : междунар. вед. сб. – М. : МИФИ, 1993. – 203 с.
49. Лавренюк С. П. Курс функціональних рівнянь / С. П. Лавренюк. – Львів : ВНТЛ, 1997.
50. Цыпкин Я. З. Информационная теория идентификации / Я. З. Цыпкин. – М. : Наука, 1995. – 336 с.
51. Зеленский К. Х. Компьютерные методы прикладной метаматики / К. Х. Зеленский, В. Н. Игнатенко, А. П. Коц. – Киев. : Дизайн-В, 1999. – 352 с.
52. Ершов Ю. А. Математическая логика / Ю. А. Ершов, Е. А. Палютин. – М. : Наука, 1987. – 336 с.
53. Самарский А. А. Математическое моделирование: Идеи. Методы. Примеры / А. А. Самарский, А. П. Михайлов. – М. : Наука, 1997. – 316 с.
54. Астанина Н. П. Математическая логика / Н. П. Астанина. – ЯГПИ, 1990. – 73 с.
55. Капітонова Ю. В. Основи дискретної математики / Ю. В. Капітонова, С. Л. Кривий, О. А. Летичевский, Г. М. Луцький, М. К. Печорін. – К. : Наукова думка, 2002. – 570 с.
56. Белоусов А. И. Дискретная математика / А. И. Белоусов, С. Б. Ткачев. – М. : МГТУ им. Н. Э. Баумана, 2001. – 743 с.
57. Конаненко С. И. Прикладная математическая логика / С. И. Конаненко. – Днепропетровск : ДНИТ, 1988.
58. Математическое и информационное моделирование : сборн. ст. – Тюмень : ТГУ, 1996. – 96 с.
59. Кук Д. Компьютерная математика / Д. Кук, Г. Бейз. – М. : Мир, 1990. – 383 с.
60. Гринченко Т. А. Машинный интеллект и новые информационные технологии / Т. А. Гринченко, А. А. Стогний. – К. : Манускрипт, 1993. – 168 с.

61. Глушков В. А. Алгебра. Языки. Программирование / В. А. Глушков. – К. : Наукова думка, 1989. – 376 с.
62. Киндлер Е. Языки моделирования / Е. Киндлер. – М. : Энергоатомиздой, 1985. – 288 с.
63. Шенфилд Дж. Математическая логика / Дж. Шенфилд. – М. : Наука, 1975. – 528 с.
64. Асосков А. В. Поточные шифры / А. В. Асосков, М. А. Иванов, А. А. Мирский, А. В. Рузин, А. В. Сланин, А. Н. Тютвин. – М. : КУДИЦ-ОБРАЗ, 2003. – 334 с.
65. Зензин О. С. AES – стандарт криптографической защиты. Конечные поля / О. С. Зензин, М. А. Иванов. – М. : КУДИЦ-ОБРАЗ, 2003. – 176 с.
66. Иванов М. А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей / М. А. Иванов, И. В. Чугунков. – М. : КУДИЦ-ОБРАЗ, 2003. – 240 с.
67. Осмоловский С. А. Стохастические методы передачи данных / С. А. Осмоловский. – М. : Радио и связь, 1991.
68. Червенчук В. Д. Логические функции, таблицы решений и аксиоматическое моделирование / В. Д. Червенчук. – Омск : ОмПИ, 1989. – 80 с.
69. Грушо А. А. Теоретические основы защиты информации / А. А. Грушо, Е. Е. Тимонина. – М. : Яхтсмен, 1996. – 187 с.
70. Шрейдер Ю. А. Системы и модели / Ю. А. Шрейдер, А. А. Шаров. – М. : Радио и связь, 1982. – 152 с.
71. Математическое моделирование сложных технических систем. – М. : МГТУ, 1997. – 94 с.
72. Мамиконов А. Г. Принятие решений и информации / А. Г. Мамиконов. – М. : Наука, 1983. – 183 с.
73. Математическое моделирование процессов управления и обработки информации. – Межвед. сб. М. : МИФИ, 1993. – 203 с.
74. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. – М. : Издательство ТРИУМФ, 2002. – 816 с.
75. Вербіцький О. В. Вступ до криптології / О. В. Вербіцький. – Львів : ВНТЛ, 1998. – 247 с.

76. Бернет С. Официальное руководство RSA Security / С. Бернет, С. Пэйн. – М. : Бином-Пресс, 2002. – 384 с.
77. Романец Ю. В. Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шальгин. – М. : Радио и связь, 1999. – 328 с.
78. Нечаев В. И. Элементы криптографии. Основы теории защиты информации / В. И. Нечаев. – М. : Высшая школа, 1999. – 109 с.
79. Романовский И. В. Дискретный анализ / И. В. Романовский. – СПб. : Невский диалект, 2002. – 240 с.
80. Алферов А. П. Основы криптологии / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмын, А. В. Черемушкин. – М. : Гелиос АРВ, 2001. – 480 с.
81. Задірака В. Методи захисту фінансової інформації / В. Задірака, О. Олексюк. – К. : Вища школа, 2000. – 460 с.
82. Баричев С. Г. Основы современной криптографии / С. Г. Баричев, В. В. Гончаров, Р. Е. Серов. – М. : Горячая линия-Телеком, 2001. – 120 с.
83. Жельников В. Криптография от папируса до компьютера / В. Жельников. – М. : АБФ., 1997. – 336 с.
84. Коутинхо С. Введение в теорию чисел. Алгоритм RSA / С. Коутинхо. – М. : Постмаркет, 2001. – 328 с.
85. Тапскотт Д. Электронное цифровое общество / Д. Тапскотт. – М. : Рефа-бук, 1999. – 432 с.
86. Домаев А. В. Программирование алгоритмов защиты информации / А. В. Домаев, М. М. Грунтович, В. О. Попов, Д. И. Правиков, И. В. Прокофьев, А. Ю. Щербаков. – М. : Нолидж, 2002. – 416 с.
87. Романенко А. Г. Моделирование информационных систем / А. Г. Романенко. – М. : МГИАИ, 1988. – 83 с.
88. Мышкис А. Д. Элементы теории математических моделей / А. Д. Мышкис. – М. : Наука, 1994.
89. Дифдж У. Новое направление в криптографии / У. Дифдж, Э. Хеллмен. – ТИИЭР : IT-22, 1976.
90. Шеннон К. Э. Теория связи в секретных системах / К. Э. Шеннон // Работы по теории информации и кибернетике. – М. : ИЛ, 1963.

91. Лидл Р. Конечные поля / Р. Лидл, Г. Нидеррайтер. – М. : Мир, 1988. – т. 1. – 425 с.
92. Яблонский С. В. Введение в дискретную математику / С. В. Яблонский. – М. : Наука, 1986. – 384 с.
93. Булос Дж. Вычислимость и логика / Дж. Булос, Р. Джеффри. – М. : Мир, 1994. – 396 с.
94. Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях / М. А. Иванов. – М. : КУДИЦ-ОБРАЗ, 2001. – 368 с.
95. Домамаев А. В. Программирование алгоритмов защиты информации / А. В. Домамаев, В. О. Попов, Д. И. Правиков, И. В. Прокофьев, А. Ю. Щербаков. – М. : Нолидж, 2000. – 288 с.
96. Фильчаков П. Ф. Справочник по высшей математике / П. Ф. Фильчаков. – К. : Наукова думка, 1974. – 743 с.
97. Грэхем Р. Паташник О. Конкретная математика / Р. Грэхем, Д. Кнут. – М. : Мир, 1998. – 703 с.
98. Максимов С. А. Прикладные задачи: учебное пособие / С. А. Максимов; (Владимир, гос. ун-т). – Владимир, 1997. – 190 с.
99. Закиров З. Г. Сотовая связь стандарта GSM / З. Г. Закиров, А. Ф. Надеев, Р. Р. Файзуллин. – М. : Эко-Трендз, 2004. – 204 с.
100. Черноруцкий И. Г. Методы принятия решений / И. Г. Черноруцкий. – СПб. : БХВ-Петербург, 2005. – 416 с.
101. Заренин Ю. Г. Корректирующие коды для передачи и обработки информации / Ю. Г. Заренин. – К. : Техника, 1965. – 170 с.
102. Притуляк Я. Г. Моделі загроз в телекомунікаційних системах / Я. Г. Притуляк, І. М. Лях // Моделювання та інформаційні технології : зб. наук. пр. (ІПМЕ НАН України). – К., 2005. – Вип. 29. – С. 100–105.
103. Притуляк Я. Г. Аналіз систем зв'язку мобільного телефону / Я. Г. Притуляк, І. М. Лях // Моделювання та інформаційні технології : зб. наук. пр. (ІПМЕ НАН України). – К., 2005. – Вип. 30. – С. 88–91.
104. Дурняк Б. В. Методи опису залежностей між параметрами інформаційних моделей систем захисту / Б. В. Дурняк,



- І. М. Лях // Моделювання та інформаційні технології : зб. наук. пр. (ІПМЕ НАН України). – К., 2005. – Вип. 34. – С. 43–46.
105. Лях І. М. Аналіз параметрів захисту інформації в системах зв'язку / І. М. Лях // Моделювання та інформаційні технології : зб. наук. пр. (ІПМЕ НАН України). – К., 2005. – Вип. 35. – С. 30–33.
106. Пригуляк Я. Г. Аналіз складових засобів захисту інформації в системах зв'язку / Я. Г. Пригуляк, І. М. Лях // Зб. наук. пр. (ІПМЕ НАН України). – К., 2005. – Вип. 28. – С. 80–84.
107. Лях І. М. Теоретичні основи захисту даних в телекомунікаційних системах / І. М. Лях // Зб. наук. пр. (ІПМЕ НАН України). – К., 2005. – Вип. 29. – С. 88–92.
108. Дурняк Б. В. Алгоритми протидії деяким атакам в системах зв'язку / Б. В. Дурняк, І. М. Лях // Зб. наук. пр. (ІПМЕ НАН України). – К., 2005. – Вип. 30. – С. 59–63.
109. Дурняк Б. В. Інформаційні засоби захисту даних в телекомунікаційних системах / Б. В. Дурняк, І. М. Лях // Зб. наук. пр. (ІПМЕ НАН України). – К., 2005. – Вип. 31. – С. 65–69.
110. Дурняк Б. В. Параметри засобів захисту в телекомунікаційних системах / Б. В. Дурняк, І. М. Лях // Моделювання та інформаційні технології : зб. наук. пр. (ІПМЕ НАН України). – К., 2007. – Вип. 43. – С. 169–171.
111. Дурняк Б. В. Синтез моделей захисту з інформаційними моделями / Б. В. Дурняк, І. М. Лях // Зб. наук. пр. (ІПМЕ НАН України). – К., 2007. – Вип. 44. – С. 178–182.

Наукове видання

Дурняк Богдан Васильович

Лях Ігор Михайлович

**ЗАХИСТ ДАНИХ В ЕЛЕКТРОННИХ ЗАСОБАХ  
МАСОВОЇ ІНФОРМАЦІЇ**

Монографія

Художнє оформлення та верстка *В. І. Сабат*

Редактор *Н. П. Шимечко*

Свідоцтво про внесення до Державного реєстру  
ДК № 3050 від 11.12.2007 р.

Підписано до друку 01.03.12. Формат 60×84/16

Папір офсетний. Гарнітура «Times».

Умов. друк. арк. 9,07. Обл.-вид. арк. 11,7.

Друк офсетний. Наклад 500 примірників.

Зам. № 155.

Видавництво Української академії друкарства

79020, Львів, вул. Підголюско, 19

Віддруковано в НВЕД Української академії друкарства

79008, м. Львів, пл. Митна, 1