МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ
ЖИТОМИРСЬКИЙ ВІЙСЬКОВИЙ ІНСТИТУТ ІМЕНІ С.П. КОРОЛЬОВА

ПІЛЬКЕВИЧ І.А.
ЛОБАНЧИКОВА Н.М.
МОЛОДЕЦЬКА К.В.

ЗАХИСТ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ УПРАВЛІННЯ

НАВЧАЛЬНИЙ ПОСІБНИК

Житомир
Вид-во ЖДУ ім. І. Франка
2015

УДК 681.51:004.056
ББК 32.965+32.973.202 я73
З 75

Рекомендовано до друку вченою радою Державного університету телекомунікацій (протокол № 3 від 29 жовтня 2014 року).

Рецензенти:

Ю.О. Подчашинський – завідувач кафедри комп'ютеризованих систем управління та автоматики Житомирського державного технологічного університету, д.т.н., доцент

В.М. Котенко – завідувач кафедри безпеки інформаційних і комунікаційних систем Житомирського військового інституту ім. С.П. Корольова, к.т.н., доцент

З 75 Захист інформації в автоматизованих системах управління [Текст]: навч. посібник/ Уклад. І.А. Пількевич, Н.М. Лобанчикова, К.В. Молодецька. – Житомир: Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.

У навчальному посібнику розглядаються сучасні напрямки забезпечення захисту інформації в автоматизованих системах управління. Представлено теоретичні основи та понятійних апарат безпеки інформаційних систем та технологій. Розглянуто питання вразливості, організаційно-правового забезпечення захисту інформації. Викладаються технічні, криптографічні, програмні моделі, методи, засоби та технологій побудови сучасних систем захисту інформації. Виклад матеріалу з прикладним спрямуванням допоможе студентам освоїти матеріал дисципліни "Захист інформації в автоматизованих системах управління" з метою набуття необхідних знань, вмінь та компетенцій. Навчальний посібник призначений для студентів, що навчаються за напрямом 6.050201 "Системна інженерія".

Укладачі: доктор технічних наук, професор **І.А. Пількевич**; кандидат технічних наук, доцент **Н.М. Лобанчикова**; кандидат технічних наук, доцент **К. В. Молодецька**.

ББК 32.817

ЗМІСТ

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АСУ – автоматизовані системи управління
БД – база даних
ІКС – інформаційно-комунікаційна система
ІС – інформаційна система
ДПБ – дискреційна політика безпеки
КІ – карти ідентифікації
КЗЗ – комплекс засобів захисту
КНОІ – канал несанкціонованого отримання інформації
МПБ – мандатна політика безпеки
НСД – несанкціонований доступ
ОС – операційна система
ПБ – політика безпеки
ПВЧ – псевдовипадкові числа
ПЗ – програмне забезпечення
ПЗП – постійний запам’ятовуючий пристрій
РПБ – рольова політика безпеки
СВК – система з відкритим ключем
СЗІ – система захисту інформації
СКБД – система керування базами даних

ВСТУП

На сучасному етапі розвитку науки і техніки захист інформації перетворюється на одну з найактуальніших задач внаслідок надзвичайно широкого розповсюдження як автоматизованих систем обробки інформації, так і розширення локальних та глобальних комп'ютерних мереж, якими передаються величезні об'єми інформації державного, військового, комерційного, приватного характеру. Важливим завданням є широке впровадження інформаційних технологій у різні сфери людської діяльності в Україні: стрімке зростання обігу пластикових карток, введення електронних паспортів і медичних карт, студентських квитків та залікових книжок. Все більше державних установ і приватних підприємств переходять на електронний документообіг, який вимагає юридичної чинності підпису фізичної або юридичної особи. Розповсюдження таких технологій вимагає захисту інформації. Усі ці та багато інших задач покликані вирішувати різноманітні методи, засоби і технології захисту інформації.

Мета навчальної дисципліни закласти термінологічний фундамент, навчити студентів правильно проводити аналіз загроз інформаційній безпеці, основним методам, принципам, алгоритмам захисту інформації в АСУ з урахуванням сучасного стану і прогнозу розвитку методів, систем та засобів здійснення загроз зі сторони потенційних порушників.

Завданнями дисципліни є ознайомити студентів з основними уявленнями про основні загрози інформаційної безпеки АСУ, навчити їх самостійно обирати та використовувати сучасний методи та засоби захисту інформації, виконувати оцінку якості функціонування системи захисту інформації в АСУ.

У результаті вивчення навчальної дисципліни студент повинен ***знати*****:** загальне поняття та характеристики інформації, загальні вимоги до захисту інформації в АСУ; поняття та основні складові інформаційної безпеки; існуючі моделі загроз та порушника безпеки інформації в АСУ, причини порушення безпеки; класифікацію засобів забезпечення безпеки в АСУ, організаційні та технічні заходи забезпечення захисту інформації; принципи захисту інформації від несанкціонованого доступу в АСУ, методи аутентифікації та ідентифікації користувачів АСУ, методи контролю доступу; криптографічні методи захисту

інформації, їх класифікація, особливості застосування; поняття електронного цифрового підпису, особливості розподілу ключів в АСУ; організаційні принципи побудови систем захисту інформації, особливості їх реалізації, методи побудови захищених АСУ; поняття політики безпеки, класифікація політик безпеки, особливості реалізації в АСУ; основні поняття стеганографії як науки про приховання передачі даних; методи та засоби оцінки ефективності СЗІ АСУ; ***вміти*:** виконувати організацію технічного захисту інформації в серверних приміщеннях; реалізовувати організацію безпеки даних на рівні сумісного використання; проводити реалізацію алгоритмів шифрування та дешифрування даних; визначати структуру системи захисту інформації АСУ, розраховувати міцність захисту інформації; виконувати адміністрування СКБД MS SQL Server; проводити багатокритеріальний вибір варіанту системи захисту інформації в АСУ; проводити розрахунок інтегральних показників ефективності системи захисту інформації АСУ.

Вибір засобів захисту інформації в автоматизованих системах – складна задача, при розв'язанні якої потрібно враховувати всі можливі дії щодо порушення роботи інформаційної системи, вартість реалізації різних заходів та засобів захисту і наявність всіх зацікавлених сторін. Сучасна наука має в своєму розпорядженні методи та інформаційні технології, що дозволяють вибрати таку сукупність засобів захисту, яка забезпечить максимізацію міри безпеки інформації при даних витратах або мінімізацію витрат при заданому рівні безпеки інформації.

У навчальному посібнику викладені теоретичні та практичні аспекти захисту інформації в АСУ. Викладаються технічні, криптографічні, програмні моделі, методи, засоби та технологій побудови сучасних систем захисту інформації. Виклад матеріалу з прикладним спрямуванням допоможе студентам освоїти матеріал дисципліни "Захист інформації в автоматизованих системах управління" з метою набуття необхідних знань, вмінь та компетенцій. Навчальний посібник призначений для студентів, що навчаються за напрямом 6.050201 "Системна інженерія".

При підготовці навчального посібника використано досвід та напрацювання авторів в галузях інформаційної безпеки та автоматики та управління, математичного моделювання та прогнозування, а також результати численних досліджень провідних вчених сьогодення, навчально-методичні та наукові видання професіоналів Житомирського військового інституту імені С.П. Корольова.

РОЗДІЛ 1. ПОНЯТТЯ ІНФОРМАЦІЇ, КОМПЛЕКС ДЕРЖАВНИХ СТАНДАРТІВ УКРАЇНИ

СКЛАД ЗМІСТОВНОГО МОДУЛЯ

Лекція 1. Поняття інформації, комплекс державних стандартів України
1.1. Інформація, її види і властивості.
1.2. Форми представлення інформації в АСУ.
1.3. Особливості інформації.
1.4. Сучасний стан питання захисту інформації.
1.5. Нормативно-правове забезпечення захисту інформації в АСУ.
Контрольні питання
Література для самопідготовки
Лекція 2. Загрози безпеки інформації в АСУ
2.1. Джерела загроз інформаційної безпеки.
2.2. Системна класифікація і загальний аналіз загроз безпеки інформації.
Контрольні питання
Література для самопідготовки
Лекція 3. Основні моделі теорії захисту інформації в АСУ
3.1. Моделі загроз і потенційного порушника.
3.2. Причини порушення безпеки.
Контрольні питання
Література для самопідготовки
Лекція 4. Організаційно-технічні заходи забезпечення захисту інформації в АСУ
4.1. Напрями забезпечення безпеки інформації.
4.2. Основні види технічних каналів і джерел витоку інформації.
4.3. Способи запобігання витоку інформації по технічним каналам.
Контрольні питання
Література для самопідготовки
Питання, що опрацьовуються студентами самостійно

ЛЕКЦІЯ 1. ПОНЯТТЯ ІНФОРМАЦІЇ, КОМПЛЕКС ДЕРЖАВНИХ СТАНДАРТІВ УКРАЇНИ

1.1. Інформація, її види і властивості.
1.2. Форми представлення інформації в АСУ.
1.3. Особливості інформації.
1.4. Сучасний стан питання захисту інформації.
1.5. Нормативно-правове забезпечення захисту інформації в АСУ.

1.1. Інформація, її види і властивості

В умовах широкого застосування обчислювальної техніки і засобів обміну інформацією поширюються можливості її просочення та несанкціонованого доступу до неї зі злочинною метою. Особливо уразливими сьогодні залишаються незахищені системи зв'язку, в тому числі обчислювальні мережі. Інформація, циркулююча в них, може бути незаконно змінена, викрадена або знищена. Останнім часом у засобах масової інформації з'явилося безліч сенсаційних повідомлень про факти злочинних впливів на автоматизовані системи обробки, зберігання і передачі інформації, особливо в банківській діяльності.

За деякими даними, в промислово розвинених країнах середній збиток від одного злочину в сфері комп'ютерної інформації близький до 450 тис. дол., а щорічні сумарні втрати в США і Західній Європі, за даними, що наводять Гайкович В. та Прешин А., досягають 100 млрд. і 35 млрд. доларів відповідно. В останні десятиріччя зберігалася стійка тенденція до зростання збитків, пов'язаних з злочинністю в сфері комп'ютерної інформації. В пресі та літературі наводиться багато подібних прикладів.

Комерційним і фінансовим установам доводиться реалізовувати широкий набір заходів, щоб захистити себе від таких злочинів. Наслідки недооцінки питань безпеки можуть виявитися вельми сумними. Досить згадати про великі суми, викрадені за допомогою підроблених авізо. На жаль, досвід західних фірм дає небагато підстав сподіватися, що цей перелік не буде продовжений у майбутньому в нашій країні. Тому питанням інформаційної безпеки приділяється все більше уваги.

З метою протидії злочинам у сфері комп'ютерної інформації або зменшення збитків від них необхідно грамотно вибирати заходи і засоби забезпечення захисту інформації від просочування та несанкціонованого доступу до неї. Необхідно знати також основні законодавчі положення в цій області, організаційні, програмно-технічні та інші заходи забезпечення безпеки інформації.

Актуальність даної проблеми пов'язана із зростанням можливостей обчислювальної техніки. Розвиток засобів, методів і форм автоматизації процесів обробки інформації і масове застосування персональних комп'ютерів роблять інформацію більш уразливою. У всіх аспектах забезпечення захисту інформації основним елементом є аналіз можливих дій щодо порушення роботи автоматизованих систем.

Основними чинниками, які сприяють підвищенню її уразливості, є:

– збільшення обсягів інформації, що накопичується, зберігається та обробляється за допомогою комп'ютерів;

– зосередження в базах даних інформації різного призначення і різної приналежності;

– розширення кола користувачів, що мають безпосередній доступ до ресурсів обчислювальної системи та масивів даних;

– ускладнення режимів роботи технічних засобів обчислювальних систем;

– обмін інформацією в локальних та глобальних мережах, в тому числі на великих відстанях.

Поняття «інформація» сьогодні вживається досить широко і різнобічно. Важко знайти таку область знань, де б воно не використовувалося. До середини XX ст. **інформація** трактувалась які відомості, які передаються людьми усним, письмовим або іншим способом. Після появи електронно-обчислювальним машин дещо змінилося трактування поняття інформації. Там під **інформацією за Шеноном** (ентропійний підхід, американський математик Д.Є. Шенон) почали розуміти зменшення міри невизначеності знання про який-небудь об'єкт, систему, процес або явище, як зміну невизначеності стану самого об'єкта, системи, явища, процесу.

В цей час з'являється і загальнонаукове трактування поняття **інформації**, як зміни обсягу та структури знання сприймання системи. Тут, сприймальна система розуміється не лише як сама людина або її похідні (колектив, суспільство), але й будь-яка система, наприклад, біологічна клітина, що є носієм генетичної інформації.

Згідно ISO/IEC 17799:2000, **інформація** – це майно (або активи), яке, подібно до інших важливих ділових активів, має цінність для організації, отже, має бути захищене відповідним чином.

Згідно Закону України «Про інформацію», **інформація** – це документовані або публічно оголошені відомості про події та явища, що відбуваються в суспільстві, державі та навколишньому природному середовищі.

Відомо, що інформація може мати різну форму, включаючи дані, які закладені в комп'ютерах, записки, досьє, формули, креслення, діаграми, моделі продукції і прототипи, дисертації, судові документи й ін. Інформація характеризується життєвим циклом, який можна представити такими складовими (рис.1.1):

– *одержання інформації* – це набуття, придбання, накопичення відповідно до чинного законодавства України документованої або публічно оголошуваної інформації громадянами, юридичними особами або державою;

– *обробка інформації* – вся сукупність операцій (збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрація), що здійснюються за допомогою технічних і програмних засобів, включаючи обмін по каналах передачі даних;

– *використання інформації* – це задоволення інформаційних потреб громадян, юридичних осіб і держави;

– *зберігання інформації* – це забезпечення належного стану інформації та її матеріальних носіїв;

– *знищення*;

– *оновлення* – формування інформації в джерелі інформації.

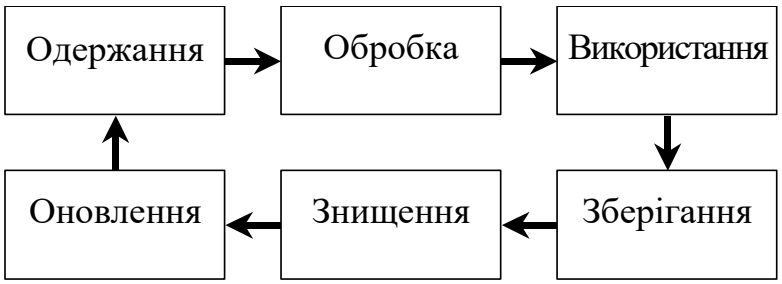

Рис. 1.1. Життєвий цикл інформації

Разом з терміном «інформація» вживається термін «**дані**». Від інформації дані відрізняються конкретною формою подань і є певною підмножиною, визначеною метою та завданнями збору й обробки інформації. Наприклад, дані про співробітників якої-небудь організації у вигляді формалізованих облікових карток кадрового підрозділу містять лише певний перелік необхідних відомостей, на відміну від величезної кількості відомостей, що характеризують кожну конкретну людину.

Можна виділити **неструктуровану** та **структуровану** форми представлення даних. Прикладом неструктурованих форми є зв'язний текст, графічні дані у вигляді фотографій, малюнків та інших неструктурованих зображень. Прикладами структурованих даних є анкети, таблиці, графічні дані у вигляді креслень, схем, діаграм.

Інформація завжди була, є і буде найважливішим із комунікативних ресурсів. Відомий біржовий гравець Натан Ротшильд говорив: «**Хто володіє інформацією, той володіє світом**».

Як і всякий продукт, інформація має споживачів, які потребують її, і тому володіє визначеними споживчими якостями. Також інформація має своїх власників або виробників.

1.2. Форми представлення інформації в АСУ

На світовому ринку інформації прийнято розрізняти наступні **основні сектори**, які також характерні й для України:

а) сектор ділової інформації;
б) сектор юридичної (нормативної) інформації;
в) сектор інформації для фахівців;
г) сектор соціально-побутової (сервісної) інформації;
д) сектор технічних і програмних засобів.

Підприємцеві, в тому числі і соціально-культурної сфери, потрібна інформація із всіх секторів, але успіх його діяльності визначається насамперед своєчасним використанням ділової (фахової) інформації. Сучасний інформаційний ринок даних можна розділити на кілька основних секторів (рис.1.2).

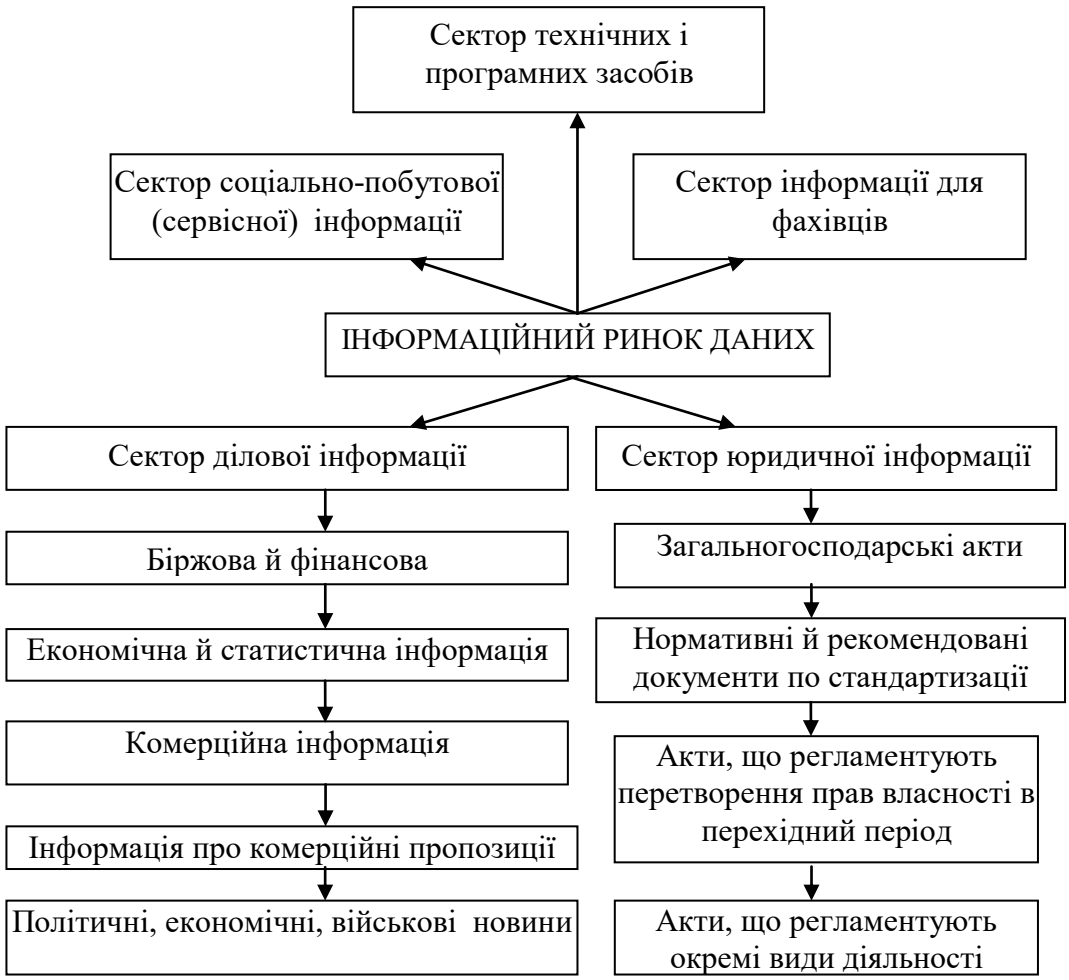

Рис. 1.2. Сучасний інформаційний ринок даних

Постійно зростаюча складність і динамічність виробничих, економічних і соціально-економічних систем, великі розміри цих систем, складність їх зв'язків і взаємозв'язків, колосальні обсяги обчислювальних робіт при плануванні, прогнозуванні і прийнятті управлінських рішень створюють підстави для широкого впровадження інформаційних технологій в практику повсякденного життя фахівців різних сфер діяльності. Інформаційні технології сьогодні представлені великою різноманітністю як по інтелектуальному і системотехнічному складу, так і за областями застосування і організаційними формами функціонування. При цьому в різних сферах діяльності є місце і простим, і складним інформаційним системам.

Прийняті рішення повинні ґрунтуватися на достовірній, поточній і прогнозованій інформації, аналізі всіх факторів, що роблять вплив на рішення, з урахуванням передбачення його можливих наслідків.

Керівники зобов'язані постійно й всебічно вивчати інформацію, що надходить для підготовки й прийняття на її основі управлінських рішень, які необхідно погоджувати на всіх рівнях внутрішньофірмової ієрархічної піраміди керування. У процесі управлінської діяльності інформація стала більш важливим ресурсом, ніж матеріальні, енергетичні, трудові та фінансові ресурси.

Для проведення якісного аналізу наявних інформаційних ресурсів дамо визначення поняттю «**інформаційні ресурси**». Відповідно ЗУ «Про інформацію»: «До інформаційних ресурсів України входить вся належна їй інформація, незалежно від змісту, форм, часу і місця створення».

За змістом інформація поділяється на такі види:

– інформація про фізичну особу;
– інформація довідково-енциклопедичного характеру;
– інформація про стан довкілля (екологічна інформація);
– інформація про товар (роботу, послугу);
– науково-технічна інформація;
– податкова інформація;
– правова інформація;
– статистична інформація;
– соціологічна інформація;
– інші види інформації.

Згідно ДСТУ 3396.2-97 «Захист інформації. Технічний захист інформації. Терміни та визначення» визначається:

інформація з обмеженим доступом – інформація, право доступу до якої обмежено встановленими правовими нормами і (чи) правилами;

таємна інформація – інформація з обмеженим доступом, яка містить відомості, що становлять державну або іншу передбачену законом таємницю;

конфіденційна інформація – інформація з обмеженим доступом, якою володіють, користуються чи розпоряджаються окремі фізичні чи юридичні особи або держава і порядок доступу до якої встановлюється ними.

Інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація. До *інформації з обмеженим доступом* не можуть бути віднесені такі відомості:

1) про стан довкілля, якість харчових продуктів і предметів побуту;

2) про аварії, катастрофи, небезпечні природні явища та інші надзвичайні ситуації, що сталися або можуть статися і загрожують безпеці людей;

3) про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти і культури населення;

4) про факти порушення прав і свобод людини і громадянина;

5) про незаконні дії органів державної влади, органів місцевого самоврядування, їх посадових та службових осіб;

6) інші відомості, доступ до яких не може бути обмежено відповідно до законів та міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України.

Залежно від ступеня секретності інформації встановлюються такі форми допуску до державної таємниці:

а) форма 1 – для роботи з секретною інформацією, що має ступені секретності «особливої важливості», «цілком таємно» та «таємно»;

б) форма 2 – для роботи з секретною інформацією, що має ступені секретності «цілком таємно» та «таємно»;

в) форма 3 – для роботи з секретною інформацією, що має ступінь секретності «таємно».

Діють такі терміни дії допусків: для форми 1 – 5 років; для форми 2 – 7 років (абзац сьомий частини першої статті 22 із змінами, внесеними згідно із Законом N 2432-VI (2432-17) від 06.07.2010); для форми 3 – 10 років (абзац восьмий частини першої статті 22 із змінами, внесеними згідно із Законом N 2432-VI (2432-17) від 06.07.2010).

1.3. Особливості інформації

Особливості інформації:

– нематеріальність (не має маси, енергії, тощо);

– передається та зберігається на матеріальних носіях (книги, диски, флешки, папір та ін.);

– будь-який матеріальний об'єкт містить інформацію про самого себе або інший об'єкт.

Інформації притаманні такі властивості:

1. *Інформація, якщо вона міститься на матеріальному носієві, доступна людині*.

2. *Інформація має цінність*. Цінність інформації визначається мірою її корисності для власника. Володіння дійсною (достовірною) інформацією дає її власникові певні переваги. Інформація, що спотворено передає дійсність (недостовірна) інформація, може завдати власникові значного матеріального та морального збитку. Якщо інформація викривлена зумисне, то її називають дезінформацією.

3. *Цінність інформації змінюється в часі*. Як правило цінність інформації з часом зменшується. Залежність визначається таким виразом:

$$C(t) = C_0 e^{-2,3t/\tau},$$

де C_0 – цінність інформації в момент її виникнення (здобуття); t – час від моменту виникнення інформації до моменту визначення її вартості; τ – час від моменту виникнення інформації до моменту її старіння.

4. *Інформація купується і продається*. Інформацію доцільно розглядати як товар, що має певну цінну. Ціна як цінність інформації, пов'язана з користю інформації для конкретних людей, організацій, держав. Інформація може бути коштовною для її власника, але не становити цінність для інших. В цьому випадку інформація не може бути товаром. Інформація може бути отримана трьома шляхами: проведення наукових досліджень; купівлею інформації; протиправним здобуттям інформації.

5. *Складність об'єктивної оцінки кількості інформації*. Існує кілька підходів до виміру кількості інформації:

– ентропійний підхід (кількість інформації оцінюється зменшенням в одержувача невизначеності (ентропії) вибору або зменшення очікування подій після здобуття інформації);

– тезаурус ний підхід (запропонований Ю.А. Шрейдером). Тезарусний підхід заснований на розумінні інформації як знань. Кількість інформації, здобутої людиною з повідомлення, можливо оцінити мірою зміни її знань);

– практичний підхід (на практиці кількість інформації вимірюють за об'ємом – сторінки, біти, байти).

У результаті копіювання без зміни інформаційних параметрів носія кількість інформації не змінюється, а ціна знижується.

1.4. Сучасний стан питання захисту інформації

Широкомасштабне використання обчислювальної техніки, збільшення обсягів інформації і розширення кола користувачів телекомунікаційних та інших територіально-розподілених АС обробки інформації приводять до якісно нових можливостей несанкціонованого доступу до інформації, що обробляється. Тому питання безпеки інформації – є важливою частиною процесу впровадження нових інформаційних технологій в усі сфери життя суспільства.

Під *інформаційною безпекою* будемо розуміти такий стан певної системи, за якого вона, з одного боку здатна протистояти дестабілізуючій дії зовнішніх і

внутрішніх інформаційних загроз, а з другого – її функціонування не становить інформаційної загрози для елементів самої системи і зовнішнього середовища.

Безпека інформації – захищеність інформації від факторів, що представляють загрозу для її конфіденційності (розголошення), цілісності (спотворення) та доступності.

Під захистом інформації будемо розуміти діяльність із запобігання просочуванню інформації, що захищається, несанкціонованих умисних впливів на інформацію, що захищається.

Тобто, **захист інформації** – це сукупність методів, засобів, організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи АС та осіб, які користуються інформацією.

Основними проблемами захисту інформації в комунікаційних мережах є:

1) запобігання витоку, розкрадання, втрати, перекручування, підробки інформації;
2) запобігання загроз безпеки особистості, суспільства, держави;
3) запобігання несанкціонованих дій по знищенню, модифікації, перекручуванню, копіюванню, блокуванню інформації;
4) запобігання інших форм незаконного втручання в інформаційні ресурси й інформаційні системи; забезпечення правового режиму документованої інформації як об'єкта власності;
5) захист конституційних прав громадян на збереження особистої таємниці і конфіденційності персональних даних, що є в інформаційних системах;
6) збереження державної таємниці, конфіденційності документованої інформації відповідно до законодавства;
7) гарантія прав суб'єктів в інформаційних процесах і при розробці, виробництві і застосуванні інформаційних систем, технологій і засобів їхнього забезпечення.

Останнім часом використовується декілька понять для визначення безпеки інформації в інформаційних системах. Таким чином визначимо поняття:

Інформаційно-телекомунікаційна система – організаційно-технічна система, яка виконує функції інформаційної системи, тобто такої організаційно-технічної системи, що реалізує певну технологію обробки інформації, та (або) телекомунікаційної системи – технічної системи, що реалізує певну технологію передавання даних шляхом їх кодування у формі фізичних сигналів. Є різні тлумачення терміну «автоматизована система».

Ми дотримуватимемося визначення з НД ТЗІ 1.1-003-99: *автоматизована система* (АС) – це організаційно-технічна система (рис. 1.3), що реалізує інформаційну технологію і поєднує у собі: обчислювальну систему; фізичне середовище; персонал; інформацію, яка обробляється.

Термін *доступність* вживають не лише, коли йдеться про інформаційні ресурси, але й до ІКС у цілому, до її компонентів або окремих ресурсів.

Наприклад, коректно говорити про доступність сервера, сегмента мережі, служби електронної пошти тощо.

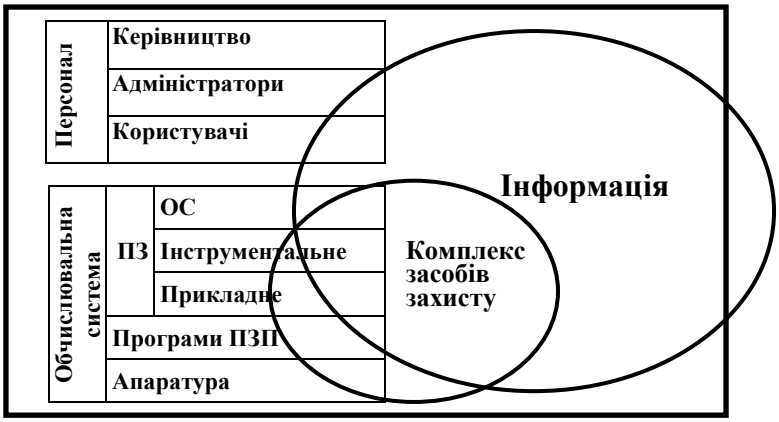

Рис. 1.3. Структура автоматизованої системи

Тепер визначимо, що може спричинити порушення безпеки інформації та проти чого, власне, застосовують заходи захисту інформації.

Несприятливий вплив – вплив, що призводить до зменшення цінності інформаційних ресурсів.

Загроза – будь-які обставини чи події, що можуть спричинити порушення політики безпеки інформації та (або) нанесення збитку ІКС. Тобто загроза – це будь-який потенційно можливий несприятливий вплив.

Атака – це спроба реалізації загрози. Якщо атака є успішною (здійснено подолання засобів захисту), це називають *проникненням*. Наслідком успішної атаки є порушення безпеки інформації в системі, яке називають *компрометацією*. Слід звернути увагу на те, що за комплексного підходу до захисту інформації розглядаються не лише впливи, спрямовані на інформаційні ресурси, але й будь-які впливи, що можуть завдати шкоди ІКС. Це твердження про необхідність захисту не самої інформації, а насамперед технології її оброблення вже узагальнили.

Уразливість системи – нездатність системи протистояти реалізації певної загрози або ж сукупності загроз.

Вади захисту – сукупність причин, умов і обставин, наявність яких може призвести до порушення нормального функціонування системи або політики безпеки інформації. Здебільшого під вадами захисту розуміють особливості побудови програмних (а іноді й апаратних) засобів захисту, що за певних обставин спричиняють їхню нездатність протистояти загрозам і виконувати свої функції. Тобто вади захисту є окремим випадком уразливості системи.

У літературі іноді використовують інше тлумачення цих термінів. Наприклад, часто замість терміну загроза вживають термін атака. Однак потрібно розрізняти атаку, яка є дією, тобто спробою реалізувати певну загрозу, та загрозу, яка робить потенційно можливим здійснення несприятливого впливу. Атака – це здебільшого цілеспрямований вплив, як правило, умисний. Загрози можуть бути випадковими,

хоча втрати від цього не стають меншими. Тому захищати інформацію потрібно також від загроз, а не лише від атак.

Порушник – фізична особа (необов'язково користувач системи), яка порушує політику безпеки системи. Іноді використовують термін *зловмисник*, чим наголошують умисність здійсненого ним порушення, тоді як порушник може здійснювати порушення ненавмисно (наприклад, через необережність або недостатню обізнаність). Часто вживаний термін *хакер* є доволі неоднозначним, тому ми не використовуватимемо його як синонім терміну порушник.

Захищена комп'ютерна система – комп'ютерна система, що здатна забезпечувати захист оброблюваної інформації від визначених загроз. Цей термін частіше вживають до обчислювальних систем або їхніх складових (програмних продуктів, окремих програмно-апаратних пристроїв). Іноді його застосовують до ІКС, але слід розуміти, що будь-яка сучасна ІКС має бути захищеною (навіть домашній комп'ютер із одним користувачем). Інакше її використання дуже швидко призведе до втрат інформації.

Спостережність – властивість ІКС, що дає змогу фіксувати діяльність користувачів і процесів, використання пасивних об'єктів, а також однозначно встановлювати ідентифікатори причетних до певних подій користувачів і процесів із метою запобігання порушенню політики безпеки і (або) забезпеченню відповідальності за певні дії. Це дуже важлива властивість обчислювальних систем та ІКС, яка досягається реалізацією засобів реєстрації або аудита.

Під *захистом інформації в ІКС* розуміють діяльність, спрямовану на забезпечення безпеки оброблюваної в ІКС інформації й ІКС у цілому, що дає змогу запобігти реалізації загроз або унеможливити її, та зменшити ймовірність завдання збитків від реалізації загроз.

Захист інформації в ІКС полягає у створенні системи технічних (інженерних, програмно-апаратних) і нетехнічних (правових, організаційних) заходів та в підтримці її роботоздатного стану.

Систему таких заходів називають комплексною системою захисту інформації. Відтак *комплексна система захисту інформації* (КСЗІ) – це сукупність організаційних, інженерних і програмно-апаратних засобів, що забезпечують захист інформації в ІКС.

Отже, захист інформації в ІКС формально зводиться до створення і супроводу КСЗІ. Слід зазначити, що навіть домашній комп'ютер з одним користувачем має якусь КСЗІ, щоправда, недокументовану. Нічого дивного, адже операційна система обов'язково має засоби контролю цілісності компонентів самої ОС і файлової системи. Швидше за все, користувач установив антивірусний засіб і хоча б зрідка оновлює його бази даних (або просто видаляє застарілу програму і встановлює нову). Час від часу він робить резервні копії своїх найцінніших файлів. Зрештою, якщо користувач має вихід в Інтернет, він мусить вживати додаткових заходів безпеки.

Потрібно добре знати про те, що підключення до Інтернету є найкритичнішим із міркувань безпеки системи. Якщо без такого підключення користувач може працювати роками, не застосовуючи специфічних заходів безпеки, то з виходом в Інтернет йому, фактично, необхідно створити КСЗІ. Крім антивірусного ПЗ до складу цієї системи мають входити настроєні певним чином засоби між мережної фільтрації (наприклад, персональний брандмауер), реєстрації подій, а, можливо, і виявлення вторгнень. Потрібно також періодично вживати заходів, на кшталт оновлення програмного забезпечення, встановлення виправлень, оновлення антивірусних баз тощо.

Що стосується ІКС, які використовують у державних органах і установах, підприємствах різної форми власності, то для них створення КСЗІ є життєво необхідним. У багатьох випадках обов'язковість створення КСЗІ визначається чинним законодавством.

До цього ми розглядали систему як ціле, хоча й згадували окремі її складові та ресурси. Далі ми розглядатимемо окремі підсистеми і об'єкти системи, а також їх взаємодію.

Комплекс засобів захисту (КЗЗ) – сукупність програмно-апаратних засобів, що забезпечують реалізацію політики безпеки інформації. Тобто КЗЗ є складовою обчислювальної системи (рис. 1.3). КЗЗ може бути локалізованим у системі у вигляді одного чи кількох апаратних і програмних компонентів, а може бути розпорошеним по різноманітних програмних засобах. Безперечно, перший варіант має суттєві переваги, проте другий – також іноді використовують у достатньо надійних, перевірених часом рішеннях (наприклад, саме такий вигляд має архітектура КЗЗ ОС UNIX).

Об'єкт системи – це елемент ресурсів обчислювальної системи, який знаходиться під керуванням КЗЗ і характеризується визначеними атрибутами й поводженням. Розрізняють такі види об'єктів: пасивні об'єкти; об'єкти-користувачі; об'єкти-процеси. Об'єкти-користувачі й об'єкти-процеси є активними об'єктами. Активні об'єкти можуть виконувати дії над пасивними об'єктами.

У більшості зарубіжних стандартів, зокрема й у сучасному міжнародному стандарті ISO 15408, пасивні об'єкти називають *об'єктами*, а активні об'єкти – суб'єктами. Потрібно розуміти, що, як правило, *суб'єкт* – це об'єкт-процес, який діє від імені певного об'єкта-користувача.

Об'єкт-користувач – це подання фізичного користувача в обчислювальній системі, яке утворюється під час його входження в систему і характеризується своїм контекстом (обліковий запис, псевдонім, ідентифікаційний код, повноваження тощо).

Об'єкт-процес – задача, процес, потік, що виконується в поточний момент (абстракція програми, що виконується) і повністю характеризується своїм контекстом (стан регістрів, адресний простір, повноваження тощо).

З міркувань безпеки інформації в ІКС виняткове значення має спроможність об'єктів взаємодіяти. Для цього використовують поняття доступу.

Доступ – це взаємодія двох об’єктів обчислювальної системи, коли один із них (той, що здійснює доступ) виконує дії над іншим (тим, до якого здійснюється доступ). Результатом такого доступу є зміна стану системи (наприклад, запуск програми на виконання) і (або) утворення інформаційного потоку від одного об’єкта до іншого (наприклад, читання або записування інформації). У випадку, коли утворюється інформаційний потік, кажуть, що здійснюється доступ до інформації. Для забезпечення захисту інформації доступ до об’єктів, які містять інформацію, що підлягає захисту, слід здійснювати з дотриманням визначених правил.

Правила розмежування доступу (ПРД) – складова політики безпеки, що регламентує правила доступу користувачів і процесів до пасивних об’єктів.

Несанкціонований доступ (НСД) – доступ, який здійснюють з порушенням політики безпеки, тобто з порушенням ПРД. Цей термін є найбільш уживаним, переважно до систем, в яких обробляють таємну інформацію, тому його винесено в назви деяких нормативних документів системи технічного захисту інформації (НД ТЗІ). Разом із тим навіть у цих документах зазначено, що захист інформації не обмежується захистом від НСД.

Адекватність – це показник реально гарантованого рівня безпеки, що відображає ступінь ефективності та надійності реалізованих засобів захисту та їхніх відповідностей поставленим задачам.

1.5. Нормативно-правове забезпечення захисту інформації в АСУ

Розглянемо інформаційний перелік документів Фонду нормативних документів у сфері технічного та криптографічного захисту інформації.

Частина 1. Нормативні документи системи технічного захисту інформації.

1. Загальні питання організації та функціонування системи технічного захисту інформації

Закони України:

Закон України «Про Державну службу спеціального зв’язку та захисту інформації України».

Закон України «Про інформацію».

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».

Закон України «Про державну таємницю».

Закон України «Про захист персональних даних».

Закон України «Про доступ до публічної інформації».

Закон України «Про основи національної безпеки України».

Укази, постанови, розпорядження Верховної Ради України, Президента України, Кабінету Міністрів України, накази Адміністрації Держспецзв’язку:

Положення про технічний захист інформації в Україні. Указ Президента України від 27.09.1999 № 1229.

Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України. Указ Президента України від 30.06.2011 № 717/2011.

Концепція технічного захисту інформації в Україні. Постанова КМ України від 08.10.1997 № 1126.

Про деякі питання захисту інформації, охорона якої забезпечується державою. Постанова КМ України від 13.03.2002 № 281.

Положення про порядок розроблення, прийняття, перегляду та скасування міжвідомчих нормативних документів системи технічного захисту інформації. Наказ Адміністрації Держспецзв'язку від 22.03.2007 № 36, зареєстрований в Міністерстві юстиції України 04.04.2007 за № 312/13579.

Державні стандарти України, нормативні документи системи ТЗІ, стандарти та нормативні документи колишнього СРСР:

ДСТУ 3396 0-96 Захист інформації. Технічний захист інформації. Основні положення.

ДСТУ 3396 1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.

ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення.

ДСТУ 1.5:2003 Правила побудови, викладання, оформлення та вимоги до змісту нормативних документів.

НД ТЗІ 1.6-002-03. Правила побудови, викладення, оформлення та позначення нормативних документів системи технічного захисту інформації.

2. Вимоги до захисту інформації**.**

Накази Адміністрації Держспецзв'язку, нормативні документи системи ТЗІ:

Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок (ТР ЕОТ-95).

Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок. (ТР ТЗІ – ПЕМВН-95).

НД ТЗІ 2.5-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації функціональних послуг захисту.

НД ТЗІ 2.5-002-99 Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації гарантій захисту.

НД ТЗІ 2.5-003-99 Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації довірчих оцінок коректності реалізації захисту.

НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу (зі зміною № 1).

НД ТЗІ 2.5-008-02 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу “2”.

НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу.

НД ТЗІ 2.7-002-99 Методичні вказівки з використання засобів копіювально-розмножувальної техніки.

НД ТЗІ 2.7-008-08 Захист інформації на об’єктах інформаційної діяльності. Вимоги та рекомендації із забезпечення захисту мовної інформації від витоку акустичним та віброакустичним каналами. Методичні вказівки.

НД ТЗІ Р-001-2000 Засоби активного захисту мовної інформації з акустичними та віброакустичним джерелами випромінювання. Класифікація та загальні технічні вимоги. Рекомендації.

Контрольні питання

1. Назвіть чинники, які сприяють підвищенню уразливості інформації.
2. Визначте поняття «інформація», «захист інформації».
3. Перерахуйте складові життєвого циклу інформації.
4. Які дані відносяться до структурованих?
5. Які дані відносяться до неструктурованих?
6. Перерахуйте особливості інформації.
7. Назвіть властивості інформації.
8. Дайте визначення поняттям «інформація з обмеженим доступом», «таємна інформація», «конфіденційна інформація».
9. Які дані не можуть бути віднесені до інформації з обмеженим доступом?

Література для самопідготовки

1. Бобунов А.І. Захист інформації в автоматизованих системах / Бобунов А.І., Шестаков В.І. Захист інформації в автоматизованих системах: Навчальний посібник. – Житомир: ЖВІРЕ, 2004. – С. 7–11.
2. Антонюк А.О. Основи захисту інформації в автоматизованих системах управління / Антонюк А.О. – Київ: Видавничий дім "КМ академія", 2003. – С. 7–33.
3. Малюк А.А. Введение в защиту информации в автоматизированных системах / Малюк А.А., Пазизин С.В., Погожин Н.С. – М.: Горячая линия-Телеком, 2001. – С. 12–43.
4. Завгородний В.И. Комплексная защита информации в компьютерных системах: учебное пособие / Завгородний В.И. . – М.: Логос; ПБОЮЛ Н.А. Егоров, 2001. – С. 8–13, С. 29–36

ЛЕКЦІЯ 2. ЗАГРОЗИ БЕЗПЕКИ ІНФОРМАЦІЇ В АСУ

2.1. Джерела загроз інформаційної безпеки.
2.2. Системна класифікація і загальний аналіз загроз безпеки інформації.

2.1. Джерела загроз інформаційної безпеки

Поняття загрози інформації є основним в теорії і практиці ЗІ. Аналіз загроз є початковим і одним з основних етапів при розробці СЗІ і проводиться на основі моделі загроз. Він має виявити можливі загрози інформації, а також показати, з якого боку і в якій точці АСУ слід чекати атаки.

Модель загроз – це абстрактний формалізований або неформалізований опис методів і способів здійснення загроз. Нижче розглянуто формальний опис основних класів загроз інформації, каналів доступу та послуг, реалізація яких дозволяє їм протистояти.

Під *загрозами* слід розуміти шляхи реалізації дій, що вважаються небезпечними. Наприклад, загроза знімання інформації і перехоплення випромінювання з дисплею може привести до втрати таємності або конфіденційності, загроза пожежі може привести до порушення цілісності та доступності інформації, загроза розриву каналу передачі інформації може реалізувати втрату доступності.

Існує багато підходів щодо класифікації загроз, проте, як здається, найбільш придатною для аналізу є визначення та класифікація загроз за результатом їх дії на інформацію, а точніше, на її основні (фундаментальні) властивості – конфіденційність, цілісність, доступність, спостереженість.

Тоді з цієї точки зору в АСУ розрізняються наступні класи загроз інформації:

1) порушення конфіденційності;
2) порушення цілісності;
3) порушення доступності або відмова в обслуговуванні;
4) порушення спостереженості або керованості.

Нова інформація від фахівців з безпеки з AV-Test свідчить, що в минулому році кількість випадків виявлення шкідливого ПЗ зросла на 72% порівняно з

2013 р. У загальній складності антивірусами AV-Test було виявлено 143 млн подібних випадків.

Причому це абсолютно нові шкідливі програми, які раніше не потрапляли на очі тим, хто забезпечує комп'ютерну безпеку. Таким чином, можна зробити висновок, що кіберзлочинці стають розумнішими і амбітними – компанія Sony відчула це, як ніхто інший. Схожий спалах був зафіксований і іншими фірмами, наприклад Malwarebytes і Kaspersky.

Легкість, з якою хакери можуть перебудовувати шматочки коду і створювати нову загрозу, означає, що антивірусним компаніям стало ще складніше йти в ногу з постійно еволюціонуючими потенційними небезпеками. Лідерство серед країн, відповідальних за поширення спаму, займає США – ця країна перебувала на вершині спамерського античарту, а всього на неї припадає 9,2% спаму. Крім США, в п'ятірці лідерів В'єтнам (7,2%), Аргентина (5,9%), Іспанія (5,8%) і Німеччина (5,6%).

У різного роду публікаціях, присвячених проблемам безпеки інформації, наводилося досить багато фактів несанкціонованого доступу до інформації, що захищалася, і інших зловмисних дій, що мали місце. Причому, за оцінками фахівців, до 85% випадків несанкціонованих проникнень в АСУ взагалі залишаються нерозкритими. З урахуванням введеного фахівцями Стенфордского інституту (США) коефіцієнта розкриття загальне число несанкціонованого проникнення в ПЕОМ урядових установ цієї країни складає більше 450 в рік, а загальний збиток – більше 200 млн. доларів. Аналогічна картина спостерігається і в комерційних системах, де щорічно реєструється близько 400 випадків розкрадання інформації.

Значне місце серед злочинів проти АСУ займають напади на системи і саботаж. Так, у Німеччині нерідкі випадки вандалізму (вибухи, руйнування, виведення із ладу сполучних кабелів, систем кондиціонування і тому подібне). Більше 40 терористичних актів на обчислювальні центри щорічно реєструється в Італії. Широке поширення отримали злочини, пов'язані з порушенням технологічного процесу автоматизованої обробки інформації, причому такі злочини завдають ще більшого збитку.

Особливо широкий розмах отримали злочини в АСУ, обслуговуючих банківські установи і установи торгівлі. За оцінками фахівців, в США, наприклад, збитки від несанкціонованого проникнення тільки в ці АСУ оцінюються в десятки мільйонів доларів.

Своєрідне джерело загроз безпеки інформації представляють спеціальні шкідливі програми, що таємно (приховано) і навмисно впроваджувані в різні функціональні програмні системи. Вказані програми після одного або декількох запусків роблять передбачені при їх створенні деструктивні дії, руйнуючи програмне забезпечення АС, дані, що обробляються, зберігаються або передаються, виводячи з ладу апаратуру і навіть чинячи небезпечну психофізіологічну дію на оператора. На тепер відомі декілька різновидів

шкідливих програм, основними з яких є електронні віруси, «комп'ютерні черв'яки» і «троянські коні».

Електронні віруси – це такі шкідливі програми, які не лише здійснюють несанкціоновані дії, але мають здатність до саморозмноження, через що представляють особливу небезпеку для обчислювальних мереж. Відомо декілька визначень програм-вірусів, що підкреслює їх різноманітність. Проте найбільшу популярність здобуло визначення, дане доктором Фредеріком Козном: «*комп'ютерний вірус* є програмою, яка здатна заражати інші програми, модифікуючи їх так, щоб вони включали копію вірусу (чи його різновид)». Процес життя і розмноження електронного (комп'ютерного) вірусу багато в чому схожий з аналогічними процесами усім нам знайомого біологічного вірусу, що підкреслюється спільністю їх назв.

До «комп'ютерних черв'яків» віднесені шкідливі програми, подібні по своїй дії електронним вірусам. «*Черв'як*» – це програма, яка поширюється в системах і мережах по лініях зв'язку Як і віруси «комп'ютерні черв'яки» заражають інші програми, проте на відміну від вірусів вони не мають програми-носія. Для розмноження «черв'як» зазвичай використовує додатковий вхід в операційну систему, який створюється для зручності її «відладки» і який нерідко забувають прибрати після закінчення «відладки».

Раніше інших з'явилися і використовувалися в зловмисних цілях шкідливі програми, що дістали назву «троянських коней».

Відомості про них відносяться ще до 70-их рр., причому найбільш поширеною несанкціонованою процедурою було зчитування інформації з областей запам'ятовуючого пристрою, що виділяються законним користувачам. «*Троянський кінь*» – це програма, яка призводить до несподіваних (зазвичай небажаним) дій на систему. Відмінною характеристикою «троянського коня» є те, що користувач звертається до цієї програми, вважаючи її корисною. Такі програми мають можливість розкрити, змінити або знищити файли даних і програм. «Троянські коні» зустрічаються в програмах широкого використання (обслуговування мережі, електронна пошта та ін.).

Вже огляду шкідливих програм досить, щоб переконатися у великій небезпеці їх як джерел загроз безпеки інформації в сучасних автоматизованих системах. Таким чином, при обробці інформації засобами обчислювальної техніки виникає велика кількість загроз як прямого несанкціонованого доступу до інформації, що захищається, так і непрямого її отримання коштами технічної розвідки. Упродовж усього періоду регулярного використання обчислювальної техніки для вирішення практичних завдань робилися спроби класифікувати джерела загроз безпеки інформації і самі загрози з метою подальшої стандартизації засобів і методів, вживаних для захисту інформації.

У відомій монографії Л. Дж. Хоффмана «Сучасні методи захисту інформації" було виділено 5 груп різних загроз: розкрадання носіїв, запам'ятовування або копіювання інформації, несанкціоноване підключення до апаратури,

несанкціонований доступ до ресурсів ЕОМ, перехоплення побічних випромінювань і наведень. У книзі "Захист інформації в персональних ЕОМ" [2] зроблена спроба класифікації загроз по джерелу можливої небезпеки (людина, апаратура і програма).

До групи загроз, в реалізації яких основну роль відіграє людина, віднесені: розкрадання носіїв, читання інформації з екрану, читання інформації з роздруків; до групи, де основним засобом виступає апаратура: підключення до пристроїв, перехоплення випромінювань; до групи, де основний засіб – це програма: несанкціонований програмний доступ, програмне дешифрування зашифрованих даних, програмне копіювання інформації з носіїв.

Аналогічний підхід пропонується і групою авторів навчальних посібників по захисту інформації від несанкціонованого доступу. Ними виділено три класи загроз: природні (стихійні лиха, магнітні бурі, радіоактивне випромінювання і наведення), технічні (відключення або коливання напруги мережі електроживлення, відмови і збої апаратно-програмних засобів, електромагнітні випромінювання і наведення, витоки через канали зв'язку), створені людьми, причому в останньому випадку розрізняють неумисні і умисні дії різних категорій осіб.

Ще один вид джерел загроз безпеки інформації, пов'язаний з її розкраданням, досить детально класифікований в монографії С.П. Расторгуева «Програмні методи захисту інформації в комп'ютерах і мережах». Автор виділяє чотири способи розкрадання інформації:

1. по каналам побічних електромагнітних випромінювань;
2. за допомогою негласного копіювання, причому виділено два різновиди копіювання:

- «ручне» (виведення інформації на друк або на екран оператором)
- «вірусне» (виведення інформації за допомогою вбудованої в ЕОМ радіозакладки);

3. розкрадання носіїв інформації;
4. розкрадання персональної ЕОМ.

Класифікують за відношенням джерела загрози до АС (зовнішні і внутрішні загрози), по виду джерела загрози:

а) *фізичні* – відбивають фізичні дії на систему;

б) *логічні* – засоби, за допомогою яких людина дістає доступ до логічної інформації системи;

в) *комунікаційні* – відносяться до процесів передачі даних по лініях зв'язку;

г) *людські* – є найважче контрольованими і безпосередньо пов'язаними з фізичними і логічними загрозами), по мірі злого наміру (випадкові і умисні) тощо.

Умисні загрози, у свою чергу, можуть бути підрозділені на *активні* (несанкціонована модифікація даних або програм) і *пасивні* (несанкціоноване копіювання даних або програм).

Цікавою є класифікація загроз безпеки інформації за способами їх можливої негативної дії. Така класифікація підтримується переважною більшістю фахівців в області захисту інформації і передбачає підрозділ загроз на інформаційні, програмно-математичні, фізичні і організаційні.

Інформаційні загрози реалізуються у вигляді:

а) порушення адресності і своєчасності інформаційного обміну;

б) протизаконного збору і використання інформації;

в) здійснення несанкціонованого доступу до інформаційних ресурсів і їх протиправного використання;

г) розкрадання інформаційних ресурсів з банків і баз даних;

д) порушення технології обробки інформації.

Програмно-математичні загрози реалізуються у вигляді:

1) впровадження в апаратні і програмні вироби компонентів, що реалізовують функції, не описані в документації на ці вироби;

2) розробки і поширення програм, що порушують нормальне функціонування інформаційних систем або їх систем захисту інформації.

Фізичні загрози реалізуються у виді:

– знищення, ушкодження, радіоелектронного пригнічення або руйнування засобів і систем обробки інформації, телекомунікації і зв'язку;

– знищення, ушкодження, руйнування або розкрадання машинних і інших носіїв інформації;

– розкрадання програмних або апаратних ключів і засобів криптографічного захисту інформації;

– перехоплення інформації в технічних каналах зв'язку і телекомунікаційних системах;

– впровадження електронних пристроїв перехоплення інформації в технічні засоби зв'язку і телекомунікаційні системи, а також в службові приміщення;

– дії на парольно-ключові системи захисту засобів обробки і передачі інформації.

Організаційні загрози реалізуються у вигляді:

- невиконання вимог законодавства в інформаційній сфері;
- протиправної закупівлі недосконалих або застарілих інформаційних технологій, засобів інформатизації, телекомунікації і зв'язку.

На закінчення відмітимо, що в результаті реалізації загроз безпеки інформації може бути нанесений серйозний збиток життєво важливим інтересам країни в політичній, економічній, оборонній і інших сферах діяльності держави, причинний соціально-економічний збиток суспільству і окремим громадянам.

Реалізація загроз може утруднити прийняття найважливіших політичних, економічних і інших рішень, підірвати державний авторитет країни на міжнародній арені, порушити баланс інтересів особи, суспільства і держави, дискредитувати органи державної влади і управління, порушити функціонування

системи державного управління, кредитно-фінансової і банківської сфери, а також систем управління військами і зброєю, об’єктами підвищеної небезпеки.

Наслідком реалізації загроз може стати істотний економічний збиток в різних сферах громадського життя і у сфері бізнесу, зниження темпів науково-технічного розвитку країни, підривання оборонного потенціалу.

2.2. Системна класифікація і загальний аналіз загроз безпеки інформації

Із вищевикладеного зрозуміло, що дотепер відома велика кількість різнопланових загроз безпеки інформації різного походження. Різними авторами пропонується цілий ряд підходів до їх класифікації. При цьому в якості критеріїв ділення безлічі загроз на класи використовуються види породжуваних небезпек, міра злого наміру, джерела прояву загроз і так далі. Усе різноманіття пропонованих класифікацій за допомогою підходів, запропонованих В.А. Герасименко, на основі методів системного аналізу може бути зведено до деякої системної класифікації, приведеної в табл. 2.1.

Таблиця 2.1

Системна класифікація загроз безпеки інформації

Параметри класифікації	**Значення параметрів**	**Зміст значення параметра**
1. Види	1.1. Фізична цілісність	Знищення (спотворення)
	1.2. Логічна структура	Спотворення структури
	1.3. Зміст	Несанкціонована модифікація
	1.4. Конфіденційність	Несанкціоноване отримання
	1.5. Право власності	Привласнення чужого права
2. Природа походження	2.1. Випадкова	Відмови, збої, помилки, стихійні лиха, побічні впливи
	2.2. Навмисна	Зловмисні дії людей
3. Передумови появи	3.1. Об’єктивні	Кількісна недостатність елементів системи, якісна недостатність елементів системи
	3.2. Суб’єктивні	Розвідка іноземних держав, промислове шпигунство, карні елементи, недобросовісні співробітники
4. Джерела загроз	4.1. Люди	Сторонні особи, користувачі, персонал
	4.2. Технічні пристрої	Реєстрації, передачі, збереження, переробки, видачі
	4.3. Моделі, алгоритми, програми	Загального призначення, прикладні, допоміжні
	4.4. Технологічні схеми обробки	Ручні, інтерактивні, внутрішньо машинні, мережеві
	4.5. Зовнішнє середовище	Стан атмосфери, стороні шуми, побічні сигнали

1 *Види загроз*. Цей параметр є основним, таким, що визначає цільову спрямованість захисту інформації.

2. *Походження загроз*. У таблиці виділено два значення цього параметра: випадкове і умисне. Під випадковим розуміється таке походження загроз, яке обумовлюється спонтанними і незалежними від волі людей обставинами, що виникають в АСУ в процесі її функціонування. Найбільш відомими подіями цього плану є відмови, збої, помилки, стихійні лиха і побічні впливи. Суть перерахованих подій (окрім стихійних лих, суть яких ясна) визначається таким чином:

відмова – це порушення працездатності якого-небудь елементу системи, що призводить до неможливості виконання ним основних своїх функцій;

збій – це тимчасове порушення працездатності якого-небудь елементу системи, слідством чого може бути неправильне виконання ним у цей момент своїй функції;

помилка – це неправильне (разове або систематичне) виконання елементом однієї або декількох функцій, що відбувається внаслідок специфічного (постійного або тимчасового) його стану,

побічний вплив – це негативна дія на систему в цілому або окремі це елементи, що робиться якими-небудь явищами, що відбуваються усередині системи або в зовнішньому середовищі.

Умисне походження загрози обумовлюється зловмисними діями людей.

3. Передумови появи загроз. У таблиці приведено два можливі різновиди передумов: об’єктивні (кількісна або якісна недостатність елементів системи) і суб’єктивні (діяльність розвідки іноземних держав, промислове шпигунство, діяльність карних елементів, дії недобросовісних співробітників системи).

Перераховані різновиди передумов інтерпретуються таким чином:

кількісна недостатність – фізична нестача одного або декількох елементів системи, що викликає порушення технологічного процесу обробки даних і перевантаження наявних елементів;

якісна недостатність – недосконаліть конструкції (організації) елементів системи, через що можуть з’являтися можливості випадкової або умисної негативної дії на інформацію, що обробляється або зберігається;

діяльність розвідки іноземних держав – спеціально організована діяльність державних органів, професійно орієнтованих на добування необхідної інформації усіма доступними способами і засобами.

До основних видів розвідки відносяться *агентурна* (несанкціонована діяльність професійних розвідників, завербованих агентів і так званих «доброзичливців») і *технічна*, що включає *радіорозвідку* (перехоплення радіоелектронними засобами інформації, циркулюючої в телекомунікаційних каналах), *радіотехнічну* розвідку (реєстрацію спецзасобами електромагнітних випромінювань технічних систем) і *космічну* розвідку (використання космічних кораблів і штучних супутників Землі для спостереження за територією, її фотографування, реєстрації радіосигналів і отримання корисної інформації будь-якими іншими доступними способами);

промислове шпигунство – негласна діяльність організації (це представників) по добуванню інформації, що спеціально охороняється від несанкціонованого її витоку або розкрадання, з метою створення для себе сприятливих умов і отримання максимальних вигод (недобросовісна конкуренція);

зловмисні дії карних елементів – розкрадання інформації або комп'ютерних програм в цілях наживи;

дії недобросовісних співробітників – розкрадання (копіювання) або знищення інформаційних масивів і програм за егоїстичними або корисливими мотивами, а також в результаті недотримання встановленого порядку роботи з інформацією.

4. *Джерела загроз*. Під джерелом загроз розуміється безпосередній її генератор або носій. Таким джерелом можуть бути люди, технічні засоби, моделі (алгоритми), програми, зовнішнє середовище

Спробуємо тепер, спираючись на приведену системну класифікацію загроз безпеки інформації, визначити повну множину загроз, потенційно можливих в сучасних автоматизованих системах. При цьому ми повинні врахувати не лише усі відомі (що раніше проявлялися) загрози, але і такі загрози, які раніше не проявлялися, але потенційно можуть виникнути при нинішніх концепціях архітектурної побудови АС і технологічних схем обробки інформації.

Класифікуємо усі можливі канали несанкціонованого отримання інформації (КНОІ) за двома критеріями: необхідності доступу (фізичного або логічного) до елементів АС для реалізації того або іншого КНОІ і залежності появи КНОІ від стану АС.

За першим критерієм КНОІ можуть бути розділені на ті, що не вимагають доступу, тобто що дозволяють отримувати необхідну інформацію дистанційно (наприклад, шляхом візуального спостереження через вікна приміщень АС) і що вимагають доступу в приміщення АС У свою чергу, КНОІ, скористатися якими можна тільки отримавши доступ в приміщення АС, діляться на сліди, що не залишають, в АС (наприклад, візуальний перегляд зображень на екранах моніторів або документів на паперових носіях) і на КНОІ, використання яких залишає ті або інші сліди (наприклад, розкрадання документів або машинних носіїв інформації).

За другим критерієм КНОІ діляться на потенційно існуючі незалежно від стану АС (наприклад, викрадати носії інформації можна незалежно від того, в робочому стані знаходяться засоби АС або ні) і існуючі тільки в робочому стані АС (наприклад, побічні електромагнітні випромінювання і наведення).

Відповідно до викладеного класифікаційна структура КНОІ може бути представлена наступною таблицею (табл. 2.2)

Приведемо орієнтовний перелік каналів несанкціонованого отримання інформації виділених нами класів

Таблиця 2.2

Класифікаційна структура каналів несанкціонованого отримання інформації

Залежність від доступу до елементів системи	Відношення до обробки інформації	
	Проявляється без відношення до обробки	Проявляється в процесі обробки
Не потребують доступу	1-й клас Загальнодоступні постійні	2-й клас Загальнодоступні функціональні
Потребують доступу без зміни елементів системи	3-й клас Вузькодоступні постійні без залишення слідів	4-й Вузькодоступні функціональні без залишення слідів
Потребують доступу із зміною елементів системи	5-й клас Вузькодоступні спеціальні із залишенням слідів	6-й клас Вузькодоступні функціональні із залишенням слідів

КНОІ 1-го класу – канали, що проявляються безвідносно до обробки інформації і без доступу зловмисника до елементів системи, Сюди може бути віднесене підслуховування розмов, а також провокація на розмови осіб, що мають відношення до АС, і використання зловмисником візуальних, оптичних і акустичних засобів. Цей канал може проявитися і шляхом розкрадання носіїв інформації у момент їх знаходження за межами приміщення, де розташована АС.

КНОІ 2-го класу – канали, що проявляються в процесі обробки інформації без доступу зловмисника до елементів АС. Сюди можуть бути віднесені електромагнітні випромінювання різних пристроїв ЕОМ, апаратури і ліній зв'язку, паразитні наведення в ланцюгах живлення, телефонних мережах, системах теплопостачання, вентиляції і каналізації, шинах заземлення, підключення до інформаційно-обчислювальної мережі генераторів перешкод і реєструючої апаратури. До цього ж класу може бути віднесений огляд відходів виробництва, що потрапляють за межі контрольованої зони.

КНОІ 3-го класу – канали, що проявляються безвідносно до обробки інформації з доступом зловмисника до елементів АС, але без зміни останніх. До них відносяться всілякі види копіювання носіїв інформації і документів, а також розкрадання виробничих відходів

КНОІ 4-го класу – канали, що проявляються в процесі обробки інформації з доступом зловмисника до елементів АС, але без зміни останніх. Сюди може бути віднесене запам'ятовування і копіювання інформації в процесі обробки, використання програмних пасток, недоліків мов програмування і операційних систем, а також ураженості програмного забезпечення шкідливими закладками, маскування під зареєстрованого користувача.

КНОІ 5-го класу – канали, що проявляються безвідносно до обробки інформації з доступом зловмисника до елементів АС і зі зміною останніх. Серед цих каналів: підміна і розкрадання носіїв інформації і апаратури, включення в програми блоків типу «троянський кінь», «комп'ютерний черв'як» і тому подібне,

читання залишкової інформації, що міститься в пам’яті, після виконання санкціонованих запитів.

КНОІ 6-го класу – канали, що проявляються в процесі обробки інформації з доступом зловмисника до елементів АС і зі зміною останніх. Сюди може бути віднесене незаконне підключення до апаратури і ліній зв’язку, а також зняття інформації на шинах живлення різних елементів АС.

Контрольні питання

1. Визначте поняття «модель загроз», «електронні віруси».
2. У якому вигляді реалізують інформаційні загрози.
3. У якому вигляді реалізують програмно-математичні загрози?
4. У якому вигляді реалізуються фізичні загрози?
5. У якому вигляді реалізуються організаційні загрози?
6. Назвіть параметри класифікації загроз безпеки інформації.
7. Дайте визначення поняттям «комп’ютерні віруси», «троянський кінь».
8. Назвіть орієнтований перелік каналів несанкціонованого отримання інформації.

Література для самопідготовки

1. Бобунов А.І. Захист інформації в автоматизованих системах / Бобунов А.І., Шестаков В.І. Захист інформації в автоматизованих системах: Навчальний посібник. – Житомир: ЖВІРЕ, 2004. – С. 18–22.
2. Малюк А.А. Введение в защиту информации в автоматизированных системах / Малюк А.А., Пазизин С.В., Погожин Н.С. – М.: Горячая линия-Телеком, 2001. – С. 15-22.
3. Завгородний В.И. Комплексная защита информации в компьютерных системах: учебное пособие / Завгородний В.И. . – М.: Логос; ПБОЮЛ Н.А. Егоров, 2001. – С. 16–19.

ЛЕКЦІЯ 3. ОСНОВНІ МОДЕЛІ ТЕОРІЇ ЗАХИСТУ ІНФОРМАЦІЇ В АСУ

3.1. Моделі загроз і потенційного порушника.
3.2. Причини порушення безпеки.

3.1. Моделі загроз і потенційного порушника

Захист інформації повинен забезпечуватись на всіх її стадіях життєвого циклу в АС, на всіх технологічних етапах обробки інформації та в усіх режимах функціонування АС.

Основними завданнями захисту можуть бути:

1) організація і координація робіт із захисту інформації, яка обробляється та передається засобами АС;

2) визначення, класифікація ресурсів АС, що підлягають захисту;

3) забезпечення визначених конфіденційності, цілісності, доступності інформації під час створення та експлуатації АС, недопущення витоку інформації з обмеженим доступом (ІзОД) та втрати її матеріальних носіїв;

4) створення механізму та умов оперативного реагування на загрози для безпеки інформації;

5) ефективне попередження, своєчасне виявлення та знешкодження загроз для ресурсів АС, причин та умов, які спричиняють або можуть привести до порушення її функціонування;

6) організація служби захисту інформації;

7) організація та впровадження системи допуску особового складу (користувачів) до роботи з інформацією, яка потребує захисту;

8) керування засобами захисту інформації, керування доступом користувачів до ресурсів АС, контроль за їхньою роботою з боку персоналу служби захисту інформації, оперативне сповіщення про спроби НСД до ресурсів АС;

9) створення умов для максимально можливого відшкодування та локалізації збитків, що завдаються неправомірними та несанкціонованими діями порушників, зменшення негативного впливу наслідків порушення безпеки на функціонування АС;

10) забезпечення режиму секретності під час обробки секретної інформації;

11) розробка організаційно-розпорядчої і робочої документації, що визначає вимоги і порядок захисту та обробки ІзОД;

12) організація обліку, зберігання, обігу інформації, яка потребує захисту, та її матеріальних носіїв;

13) реєстрація, збір, зберігання, обробка даних про всі події в системі, які мають відношення до безпеки інформації;

14) здійснення контролю за забезпеченням захисту ІзОД та за збереженням її матеріальних носіїв.

Модель загроз складається для конкретної АС та повинна враховувати особливості функціонування, склад АС, технологію обробки інформації та ін. Мають бути визначені основні види загроз для безпеки інформації, які можуть бути реалізовані стосовно АС і повинні враховуватись у моделі загроз (загрози об'єктивної природи, випадкові та навмисні загрози суб'єктивної природи).

Необхідно визначити перелік суттєвих загроз, класифікувати їх за результатом впливу на інформацію та описати методи і способи їхнього здійснення. Перелік загроз має бути максимально повним і деталізованим. Для кожної з загроз необхідно визначити:

а) на порушення яких властивостей інформації або АС вона спрямована (рекомендується користуватись чотирма основними градаціями – порушення конфіденційності, цілісності, доступності інформації, а також порушення спостереженості та керованості АС);

б) джерела виникнення (які суб'єкти АС або суб'єкти, зовнішні по відношенню до неї, можуть ініціювати загрозу);

в) можливі способи здійснення загроз.

Модель потенційного порушника. Розглянемо тепер модель порушника. Згідно з ЗУ порушник – це користувач, який здійснює НСД до інформації.

Оскільки під порушником розуміється людина, то цілком зрозуміло,що створення його формалізованої моделі – дуже складне завдання. Тому, звичайно, мова може йти тільки про неформальну або описову модель порушника. Отже, нижче подається опис можливого для даного класу ІСБ порушника.

Порушник – це особа, яка може отримати доступ до роботи звключеними до складу АС засобами. Вона може помилково, унаслідок необізнаності, цілеспрямовано, свідомо чи несвідомо, використовуючи різні можливості, методи та засоби, здійснити спробу виконати операції, які призвели або можуть призвести до порушення властивостей інформації, що визначені політикою безпеки.

Зрозуміло, що в кожному конкретному випадку для кожного об'єкта визначаються імовірні загрози і моделі потенційних порушників – «провідників» цих загроз, включаючи можливі сценарії їх здійснення. Цей етап дуже складний, оскільки від служби безпеки вимагається для кожного об'єкта вибрати з кількох можливих типів один, на який і буде орієнтована ІСБ, що проектується.

Модель порушника – це абстрактний формалізований або неформалізований опис порушника.

Модель порушника відображає його практичні та потенційні можливості, апріорні знання, час та місце дії тощо.

При розробці моделі порушника визначаються:

– припущення щодо категорії осіб, до яких може належати порушник;

– припущення щодо мотивів дій порушника (цілей, які він має);

– припущення щодо рівня кваліфікації та обізнаності порушника і його технічної оснащеності (щодо методів та засобів, які використовуються при здійсненні порушень);

– обмеження та припущення щодо характеру можливих дій порушників (за часом та місцем дії та інші).

Припускається, що за своїм рівнем порушник – це фахівець вищої кваліфікації, який має повну інформацію про систему. Зазвичай розглядаються 5 типів порушників. Спочатку їх поділяють на дві групи: зовнішні і внутрішні порушники. Серед *зовнішніх* порушників виділяють такі:

а) добре озброєна й оснащена силова група, що діє і ззовні швидко і напролом;

б) поодинокий порушник, що не має допуску на об’єкт і намагається діяти потайки й обережно, оскільки він усвідомлює, що сили реагування мають над ним переваги.

Серед потенційних *внутрішніх* порушників можна відзначити:

а) допоміжний персонал об’єкта, що допущений на об’єкт, але недопущений до життєво важливого центру (ЖВЦ) АСУ;

б) основний персонал, що допущений до ЖВЦ (найбільш небезпечний тип порушників);

в) співробітників служби безпеки, які часто формально і не допущені до ЖВЦ, але реально мають достатньо широкі можливості для збору необхідної інформації і вчинення акції.

Має також розглядатися можливість змови між порушниками різних типів, що ще більше ускладнює задачу формалізації моделей порушника. Але слід відзначити, що такий поділ є дуже загальним, а також не всі групи мають важливе значення для всіх АС.

Серед внутрішніх порушників можна виділити такі *категорії персоналу*:

1) користувачі (оператори) системи;

2) персонал, що обслуговує технічні засоби (інженери, техніки);

3) співробітники відділів розробки та супроводження ПЗ (прикладні та системні програмісти)

4) технічний персонал, що обслуговує будівлю (прибиральниці, електрики, сантехніки та інші співробітники, що мають доступ до будівлі та приміщення, де розташовані компоненти АС);

5) співробітники служби безпеки;

6) керівники різних рівнів та посадової ієрархії.

Сторонні особи, що можуть бути порушниками:

а) клієнти (представники організацій, громадяни);

б) відвідувачі (запрошені з якого-небудь приводу);

в) представники організацій, що займаються забезпеченням життєдіяльності організації (енерго-, водо-, теплопостачання і т. д.);

г) представники конкуруючих організацій (іноземних служб) або особи, що діють за їхнім завданням;

д) особи, які випадково або навмисно порушили пропускний режим (не маючи на меті порушити безпеку);

е) будь-які особи за межами контрольованої зони.

Можна виділити також три основні мотиви порушень: безвідповідальність, самоствердження та з корисною метою.

При порушеннях, викликаних *безвідповідальністю*, користувач цілеспрямовано або випадково здійснює руйнівні дії, які не пов’язані, проте, зі злим умислом. У більшості випадків – це наслідок некомпетентності або недбалості. Деякі користувачі вважають одержання доступу до системних наборів даних значним успіхом, затіваючи свого роду гру "*користувач проти системи*" заради самоствердження або у власних очах, або в очах колег.

Порушення безпеки АС може бути викликане *корисливим* інтересом користувача системи. У цьому випадку він буде цілеспрямовано намагатися перебороти систему захисту для доступу до інформації в АС. Навіть якщо АС має засоби, що роблять таке проникнення надзвичайно складним, цілком захистити її від проникнення практично неможливо.

Усіх порушників можна класифікувати *за рівнем знань про АС*:

1) знає функціональні особливості АС, основні закономірності формування в ній масивів даних і потоків запитів до них, уміє користуватися штатними засобами;

2) має високий рівень знань і досвід роботи з технічними засобами системи і їх обслуговуванням;

3) має високий рівень знань у галузі програмування й обчислювальної техніки, проектування й експлуатації автоматизованих інформаційних систем;

4) знає структуру, функції і механізм дії засобів захисту, їх сильні і слабкі сторони.

За рівнем можливостей (методами та засобами, що використовуються):

1) застосовує суто агентурні методи отримання відомостей;

2) застосовує пасивні засоби (технічні засоби перехоплення без модифікації компонент системи);

3) використовує тільки штатні засоби та недоліки системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні магнітні носії інформації, які можуть бути потайки пронесені через пости охорони;

4) застосовує методи та засоби активного впливу (модифікація та підключення додаткових технічних засобів, підключення до каналів передавання даних, впровадження програмних закладок та використання спеціальних інструментальних та технологічних програм).

За часом дії:

- у процесі функціонування (під час роботи компонент системи);
- у період неактивності системи (у неробочий час, під час планових перерв у її роботі, перерв для обслуговування і ремонтів і т.д.);
- як у процесі функціонування, так і в період неактивності компонент системи.

За місцем дії:

- без доступу на контрольовану територію організації;
- з контрольованої території без доступу до будівель та споруд;
- усередині приміщень, але без доступу до технічних засобів;
- з робочих місць кінцевих користувачів (операторів);
- з доступом у зону даних (баз даних, архівів тощо);
- з доступом у зону управління засобами забезпечення безпеки.

Враховуються також наступні обмеження і припущення про характер дій можливих порушників:

✓ робота з підбору кадрів і спеціальні заходи ускладнюють можливість створення коаліцій порушників, тобто об'єднання (змови)і цілеспрямованих дій з подолання системи захисту двох і більше порушників;

✓ порушник, плануючи спробу НСД, приховує свої несанкціоновані дії від інших співробітників;

✓ НСД може бути наслідком помилок користувачів, системних адміністраторів, а також хиб прийнятої технології обробки інформації тощо.

Визначення конкретних характеристик можливих порушників є значною мірою суб'єктивним. Модель порушника, що побудована з урахуванням особливостей конкретної предметної галузі і технології обробки інформації, може бути подана перелічуванням кількох варіантів його образу. Кожний вид порушника має бути схарактеризований згідно з класифікаціями, наведеними вище. Всі значення характеристик мають бути оцінені (наприклад, за 5-бальною системою) і зведені до відповідних форм.

Однак при формуванні моделі порушника на її виході обов'язково повинні бути визначені: імовірність реалізації загрози, своєчасність виявлення і відомості про порушення. Слід звернути увагу на те, що всі злочини, зокрема і комп'ютерні,здійснюються людиною. Користувачі АС є її складовою, необхідним елементом. З іншого ж боку, вони є основною причиною і рушійною силою порушень і злочинів. Отже, питання безпеки захищених АС фактично є питанням людських відносин та людської поведінки.

На підставі викладеного для вибору вихідної моделі поводження потенційного порушника доцільний диференційований підхід. Оскільки кваліфікація

порушника - поняття досить відносне і наближене, можна взяти за основу чотири класи безпеки:

1-й клас – для захисту життєво важливої інформації, витік, руйнування або модифікація якої можуть призвести до втрат для користувача. Міцність розрахована на порушника – професіонала.

2-й клас – використовується для захисту важливої інформації при роботі декількох користувачів, що мають доступ до різних масивів даних або формуючих свої файли, недоступні іншим користувачам. Міцність розрахована на порушника високого класу, але непрофесіонала.

3-й клас рекомендується для захисту щодо важливої інформації, постійний НСД до якої шляхом її нагромадження може привести до витоку і більш важливої інформації. Міцність захисту при цьому повинна бути розрахована на відносно кваліфікованого порушника – непрофесіонала.

4-й клас рекомендується для захисту іншої інформації, що не представляє інтересу для серйозних порушників. Однак його необхідність диктується дотриманням технологічної дисципліни обліку й обробки інформації службового користування з метою захисту від НСД.

Реалізація перерахованих рівнів безпеки повинна забезпечуватися набором відповідних засобів захисту, що перекривають визначену кількість можливих каналів НСД відповідно до очікуваного класу потенційних порушників. Рівень безпеки захисту усередині класу забезпечується кількісною оцінкою міцності окремих засобів захисту й оцінкою міцності контуру захисту від навмисних засобів захисту й оцінкою міцності контуру захисту від навмисного НСД.

3.2. Причини порушення безпеки

Сформована практика дослідження випадків порушення безпеки, що приділяє основну увагу методам і засобам подолання захисту, має істотний недолік – відштовхуючись від дій зловмисника, вона фактично являє собою лише аналіз технології подолання засобів захисту і не дозволяє виявити недоліки засобів забезпечення безпеки [9].

Крім того, подібний підхід відразу розділяє усі випадки порушення безпеки на навмисні, що класифікуються за способами подолання захисту, і ненавмисні, зумовлені помилками, закладеними б самій АС при її розробці та експлуатації. Однак, здається цілком прийнятною і дуже прагматична точка зору – важливі сам факт порушення безпеки і ті заходи, яких необхідно вживати для запобігання таким порушенням, а їхня навмисність не має значення. З цього погляду можливість успішних дій зловмисника, як і передумови випадкових порушень, визначена властивостями самої АС – її архітектурою, реалізацією та адмініструванням.

Це означає, що в основі кожного факту порушення безпеки АС лежить відповідна вада засобів захисту, то зумовлює успішне здійснення атаки. Аналіз

випадків порушення безпеки повинен ґрунтуватися не стільки на дослідженні методів, використовуваних порушником, скільки на виявленні властивостей АС, що дають змогу йому здійснити свої дії. Інакше кажучи, що стало причиною успішного здійснення порушення безпеки в тому чи іншому випадку?

Аналіз і статистика показують, що всі випадки порушення безпеки АС відбуваються з однієї або кількох наступних причин. Наведені причини порушення безпеки зручно подати у вигляді схеми (рис. 3.1).

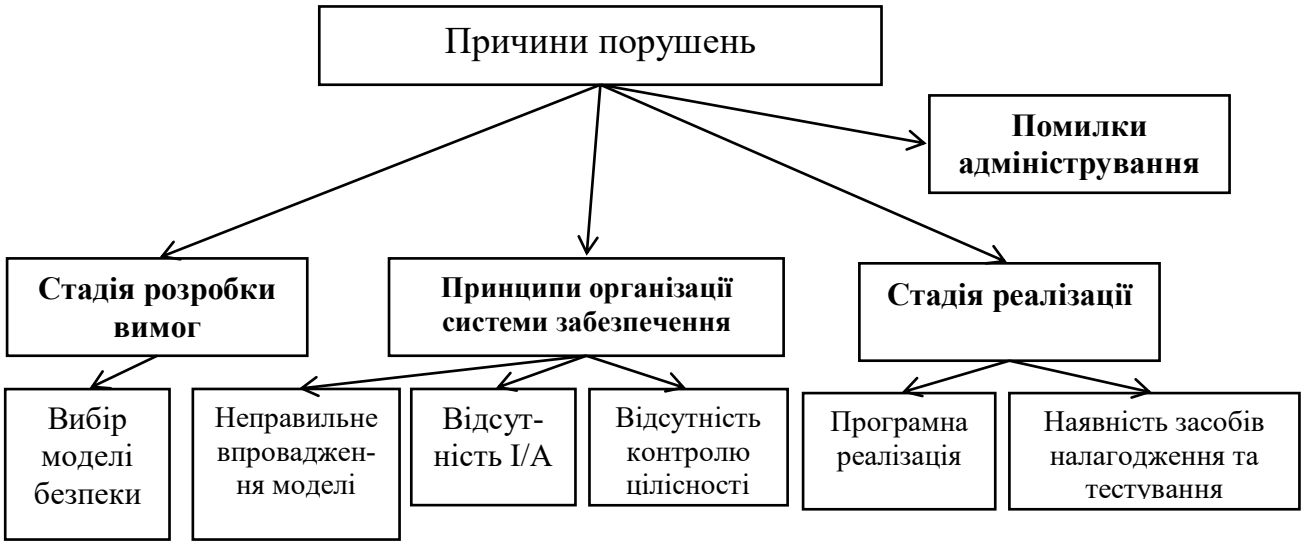

Рис. 3.1. Причини порушення безпеки

1. *Вибір моделі безпеки, що не відповідає призначенню чи архітектурі АС*. Модель безпеки повинна відповідати вимогам безпеки, запропонованим для АС. Сьогодні спостерігається певна невідповідність між моделями безпеки та архітектурою АС. Фактично формальні моделі безпеки існують тільки у вигляді теорії, а розробники АС змушені піддавати їх певній інтерпретації, щоб пристосувати до конкретної АС. При цьому доводиться йти на певні компроміси, і може виявитися, що модель безпеки в ході реалізації була істотно спотворена. Це означає, що при виборі моделі безпеки не можна не враховувати специфіки архітектури, інакше, незважаючи на всі переваги моделі, гарантованого нею рівня безпеки досягти не вдасться.

2. *Неправильне впровадження моделі безпеки*. Незважаючи на цілком адекватний вибір моделі безпеки, її реалізація і застосування до архітектури конкретно ОС через властивості самої моделі чи ОС були проведені невдало. Це означає, що в ході реалізації були втрачені всі теоретичні досягнення, отримані при формальному доведенні безпеки моделі. Звичайно неправильне впровадження моделі безпеки в систему виражається в недостатньому обмеженні доступу до найбільш важливих для безпеки систем служб і об’єктів, а також введенні різних винятків з передбачених моделлю правил розмежування доступу типу привілейованих процесів, утиліт і т. д.

3. *Відсутність ідентифікації і/або аутентифікації суб'єктів і об'єктів*. У багатьох сучасних ОС ідентифікація та аутентифікації суб'єктів і об'єктів взаємодії знаходяться на дуже примітивному рівні – суб'єкт (зловмисник) може порівняно легко видати себе за іншого суб'єкта і скористатися його повноваженнями доступу до інформації.

4. *Відсутність контролю цілісності засобів забезпечення безпеки*. У багатьох ОС контролю цілісності самих механізмів, що реалізують функції захисту, приділяється слабка увага. Багато систем допускають прозору для служб безпеки підміну компонентів. З погляду безпеки таке становище є неприпустимим.

5. *Помилки, яких припустилися в ході програмної реалізації засобів забезпечення безпеки*. Ця група причин порушення безпеки буде існувати доти, доки не з'являться технології програмування, що гарантують виробництво безпомилкових програм. Оскільки, як відомо, програми завжди мають помилки, то, очевидно, такі технології не з'являться взагалі, і помилки такого роду будуть виникати завжди.

6. *Наявність засобів налагодження і тестування в кінцевих продуктах*. Багато розробників залишають у комерційних продуктах так звані «люки», «діри», налагоджувальні можливості тощо. Причини, з яких це відбувається, цілком зрозумілі – програмні продукти стають усе складнішими, і налагодити їх у лабораторних умовах просто неможливо. Отже, для визначення причин збоїв і помилок уже в процесі експлуатації розробникам доводиться залишати у своїх продуктах можливості для налагодження і діагностики в ході експлуатації.

7. *Помилки адміністрування*. Наявність найсучасніших засобів захисту не гарантує від можливих порушень безпеки, тому що в безпеці будь-якої системи завжди присутній людський фактор – адміністратор, який керує засобами забезпечення безпеки, може зробити помилку, і всі зусилля розробників будуть зведені нанівець. Помилки адміністрування є досить поширеною причиною порушень безпеки, але часто списуються на помилки розробників засобів захисту.

Контрольні питання

1. Перерахуйте основні завдання захисту інформації.
2. Які особливості створення моделі загроз?
3. Які особливості створення моделі порушника?
4. Кого виділяють серед потенційних зовнішніх порушників?
5. Кого виділяють серед потенційних внутрішніх порушників?
6. Яка послідовність дій можливих порушників?
7. Назвіть причини порушення безпеки.

Література для самопідготовки

1. Бобунов А.І. Захист інформації в автоматизованих системах / Бобунов А.І., Шестаков В.І. Захист інформації в автоматизованих системах: Навчальний посібник. – Житомир: ЖВІРЕ, 2004. – С. 28–43.
2. Антонюк А.О. Основи захисту інформації в автоматизованих системах управління / Антонюк А.О. – Київ: Видавничий дім "КМ академія", 2003. – С.70–76.
3. Малюк А.А. Введение в защиту информации в автоматизированных системах / Малюк А.А., Пазизин С.В., Погожин Н.С. – М.: Горячая линия-Телеком. 2001. – С. 22–23.

ЛЕКЦІЯ 4. ОРГАНІЗАЦІЙНО-ТЕХНІЧНІ ЗАХОДИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСУ

4.1. Напрями забезпечення безпеки інформації.
4.2. Основні види технічних каналів і джерел витоку інформації.
4.3. Способи запобігання витоку інформації по технічним каналам.

4.1. Напрями забезпечення безпеки інформації

Напрями забезпечення безпеки взагалі розглядаються як нормативно-правові категорії, що визначають комплексні міри захисту інформації на державному рівні, на рівні підприємства й організації, на рівні окремої особи.

З урахуванням сформованої практики забезпечення інформаційної безпеки виділяють наступні напрямки захисту інформації (рис. 4.1):

Рис. 4.1. Основні напрямки забезпечення безпеки інформації

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

– *організаційний захист* – це регламентація виробничої діяльності й взаємин виконавців на нормативно-правовій основі, що виключає або послаблює нанесення якого-небудь збитку виконавцям;

– *інженерно-технічний захист* – це використання різних технічних засобів, що перешкоджають завданню збитків комерційної діяльності.

Як відомо, право – це сукупність загальнообов'язкових правил і норм поведінки, установлених або санкціонованих державою відносно певних сфер життя й діяльності державних органів, підприємств (організацій) і населення (окремої особистості).

Правовий захист інформації як ресурс, визнаний на міжнародному та державному рівні, визначається міждержавними договорами, конвенціями, деклараціями й реалізується патентами, авторським правом і ліцензіями на їхній захист. На державному рівні правовий захист регулюється державними й відомчими актами (рис. 4.2).

Рис. 4.2. Характеристика правового захисту інформації

У нашій країні такими правилами (актами, нормами) є Конституція, закони України, цивільне, адміністративне, карне право, викладені у відповідних кодексах. Що стосується відомчих нормативних актів, то вони визначаються

наказами, порадниками, положеннями й інструкціями, видаваними відомствами, організаціями й підприємствами, що діють у рамках певних структур.

Питання правового режиму інформації з обмеженим доступом реалізуються у законі про державну таємницю. Інформація становить *службову або комерційну таємницю* у випадку, коли інформація має дійсну або потенційну комерційну цінність у силу невідомості її третім особам, до неї немає вільного доступу на законній підставі й власник інформації вживає заходів до охорони її конфіденційності. Відомості, які не можуть становити службову або комерційну таємницю, визначаються законом і іншими правовими актами.

Створюючи систему інформаційної безпеки, необхідно чітко розуміти, що без правового забезпечення захисту інформації будь-які наступні претензії з вашої сторони до несумлінного співробітника, клієнтові, конкурентові й посадовій особі виявляться просто необґрунтованими.

Якщо перелік відомостей конфіденційного характеру не доведений вчасно до кожного співробітника (природно, якщо він допущений по посадових обов'язках) у письмовому вигляді, то співробітник, що вкрав важливу інформацію в порушення встановленого порядку роботи з нею, швидше за все розведе руками: звідки мені це знати? У цьому випадку ніякі інстанції, аж до судових, не зможуть Вам допомогти.

Правові норми забезпечення безпеки й захисту інформації на конкретному підприємстві (фірмі, організації) відбиваються в сукупності установчих, організаційних і функціональних документів.

Вимоги забезпечення безпеки й захисту інформації відбиваються в Уставі (установчому договорі) у вигляді наступних положень:

- підприємство має право визначати склад, обсяг і порядок захисту відомостей конфіденційного характеру, вимагати від своїх співробітників забезпечення їхньої схоронності й захисту від внутрішніх і зовнішніх загроз;
- підприємство зобов'язане забезпечити схоронність конфіденційної інформації.

Такі вимоги надають право адміністрації підприємства:

– створювати організаційні структури по захисту конфіденційної інформації;

– видавати нормативні й розпорядницькі документи, що визначають порядок виділення відомостей конфіденційного характеру й механізми їхнього захисту;

– включати вимоги по захисту інформації в договори по всіх видах господарської діяльності;

– вимагати захисту інтересів підприємства з боку державних і судових інстанцій;

– розпоряджатися інформацією, що є власністю підприємства, з метою витягу вигоди й недопущення економічного збитку колективу підприємства й власникові засобів виробництва;

– розробити «Перелік відомостей конфіденційної інформації». Вимоги правової забезпеченості захисту інформації передбачаються в колективному договорі.

Колективний договір повинен містити наступні вимоги.

Розділ «Предмет договору». Адміністрація підприємства (у тому числі й адміністрація самостійних підрозділів) ЗОБОВ'ЯЗУЄТЬСЯ забезпечити розробку й здійснення заходів щодо визначення й захисту конфіденційної інформації. Трудовий колектив приймає на себе зобов'язання по дотриманню встановлених на підприємстві вимог по захисту конфіденційної інформації. Адміністрація зобов'язана врахувати вимоги захисту конфіденційної інформації в правилах внутрішнього розпорядку.

Розділ «Кадри. Забезпечення дисципліни праці». Адміністрація зобов'язується: порушників вимог по захисту комерційної таємниці залучати до адміністративної й кримінальної відповідальності відповідно до діючого законодавства. Правила внутрішнього трудового розпорядку для робітників та службовців підприємства доцільно доповнити наступними вимогами.

Розділ «Порядок прийому й звільнення робітників та службовців»:

1. При надходженні робітника або службовця на роботу або переводу його у встановленому порядку на іншу роботу, пов'язану з конфіденційною інформацією підприємства, а також при звільненні адміністрація зобов'язана проінструктувати працівника або службовця за правилами збереження комерційної таємниці з оформленням письмового зобов'язання про її нерозголошення.

2. Адміністрація підприємства вправі приймати рішення про відсторонення від робіт осіб, які порушують установлені вимоги по захисту конфіденційної інформації.

Розділ «Основні обов'язки робітників та службовців». Робітники та службовці зобов'язані дотримувати вимог нормативних документів по захисту конфіденційної інформації підприємства.

Розділ «Основні обов'язки адміністрації». Адміністрація підприємства, керівники підрозділів зобов'язані:

а) забезпечити строге збереження конфіденційної інформації, постійно здійснювати організаторську й виховно-профілактичну роботу, спрямовану на захист секретів підприємства;

б) включити в посадові інструкції й положення обов'язку по збереженню конфіденційної інформації;

в) неухильно виконувати вимоги Уставу, колективного договору, трудових договорів, правил внутрішнього трудового розпорядку й інших організаційних і господарських документів у частині забезпечення економічної й інформаційної безпеки.

Зобов'язання конкретного співробітника, робітника або службовця в частині захисту інформації обов'язково повинні бути обговорені в трудовому договорі (контракті). Відповідно до кодексу законів про працю КЗП при заключенні

трудового договору працівник зобов’язується виконувати певні вимоги, що діють на даному підприємстві. Незалежно від форми укладання договору (усний або письмового) підпис трудящого на наказі про прийом на роботу підтверджує його згода з умовами договору.

Вимоги по захисту конфіденційної інформації можуть бути обговорені в тексті договору, якщо договір укладається в письмовій формі. Якщо ж договір укладається в усній формі, то діють вимоги по захисту інформації, що випливають із нормативно-правових документів підприємства. При заключенні трудового договору й оформленні наказу про прийом на роботу нового співробітника робиться оцінка про інформованість його з порядком захисту інформації підприємства. Це створює необхідний елемент включення даної особи в механізм забезпечення інформаційної безпеки.

Використання договорів про нерозголошення таємниці – зовсім не самостійний захід для її захисту. Не слід думати, що після підписання такої угоди з новим співробітником таємниця буде збережена. Це тільки попередження співробітникові, що в справу вступає система заходів щодо захисту інформації, і правова основа до того, щоб припинити його невірні або протиправні дії. Далі завдання - не допустити втрати комерційних секретів. Реалізація правових норм і актів, орієнтованих на захист інформації на організаційному рівні, опирається на ті або інші організаційно-правові форми, до числа яких ставляться дотримання конфіденційності робіт і дій, договори (угоди) і різні форми обов’язкового права.

Конфіденційність – це форма звертання з відомостями, що становлять комерційну таємницю, на основі організаційних заходів, що виключають неправомірне оволодіння такими відомостями. *Договори* – це угоди сторін (двох і більше осіб) про встановлення, зміну або припинення взаємних зобов’язань. *Зобов’язання* – цивільні правовідносини, у силу якого одна сторона (боржник) зобов’язана зробити на користь іншої сторони певні дії (рис. 4.3).

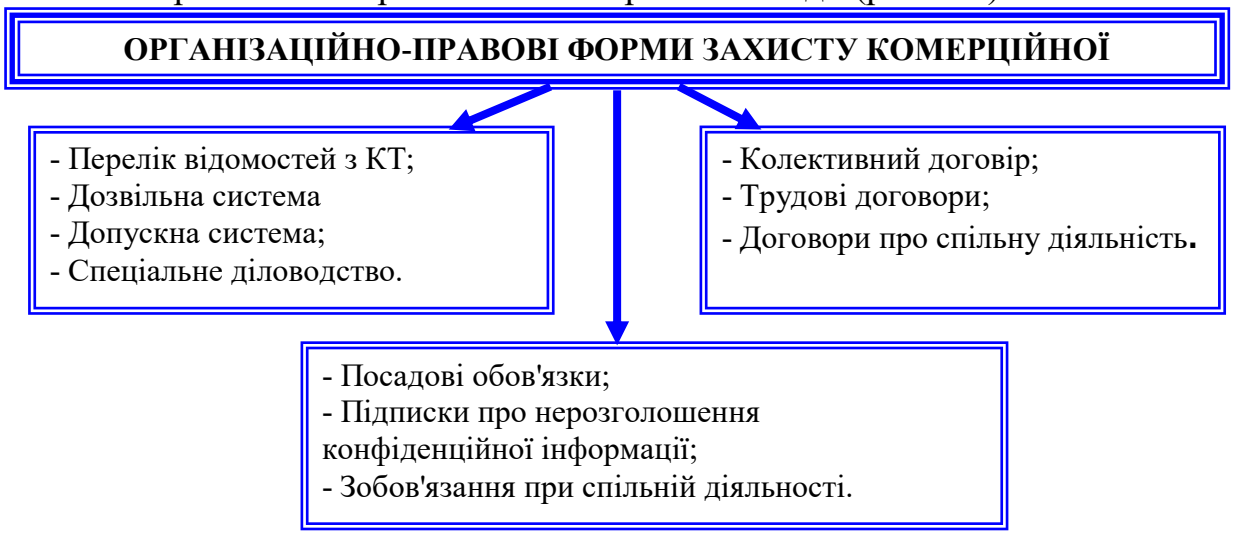

Рис. 4.3. Організаційно-правові форми захисту комерційної інформації

Аналіз законодавства, що регулює діяльність суб'єктів у сфері інформаційної безпеки, показує наявність певних недоліків. Існуючі правові норми розкидані по різних нормативних актах, що видавався в різний час, у різних умовах і на різних рівнях. Чинне законодавство не систематизоване, що створює більші труднощі в його використанні на практиці.

4.2. Основні види технічних каналів і джерел витоку інформації

При обробці інформації в АСУ можливий її витік по так званих побічних технічних каналах. Під *технічним каналом* витоку інформації розуміється сукупність фізичних полів, що несуть конфіденційну інформацію, конструктивних елементів, що взаємодіють з ними, і технічних засобів зловмисника для реєстрації поля і зняття інформації. Конфіденційна інформація в такому технічному каналі представлена у вигляді сигналів (акустичних, віброакустичних, електричних, електромагнітних), які дістали назву *небезпечних сигналів*.

Виходячи із цього визначення, залежно від фізичної природи виникаючих полів і типу конструктивних елементів, що взаємодіють з ними, можуть бути виділені наступні види технічних каналів витоку:

1. *акустичним* канал;
2. *віброакустичний* канал, пов'язаний з роботою оргтехніки, електромеханічного периферійного і зв'язного устаткування, яка супроводжується взаємними переміщеннями механічних деталей, що викликає появу в навколишньому просторі і в елементах конструкцій будівель акустичних і вібраційних коливань, що несуть (у разі їх відповідності тим або іншим символам оброблюваного конфіденційного тексту) відповідну небезпечну інформацію;
3. *канал дротяного і радіозв'язку*;
4. *електромагнітний канал*;
5. *оптичний канал*;
6. *вторинні джерела електроживлення* основних технічних засобів, в яких циркулює конфіденційна інформація, : канал, пов'язаний з дією електричних, магнітних і акустичних полів небезпечного сигналу на допоміжні технічні засоби і системи (засоби, не призначені для обробки конфіденційної інформації);
7. *ланцюги заземлення*;
8. *канал, пов'язаний з взаємовпливом ланцюгів*, по яких передається конфіденційна інформація, і ланцюгів допоміжних технічних засобів і систем, що мають вихід за межі контрольованої зони об'єкту (фактично цей канал визначається наявністю ефекту індуктивного і ємності зв'язку будь-яких неекранованих провідників);
9. *побічні електромагнітні випромінювання і наведення* (ПЕВН), що виникають під час роботи основних технічних засобів АС.

Канал ПЕВН через свою стабільність і неявну форму отримання інформації є одним їх основних каналів, по якому технічні розвідки прагнуть отримати ті або інші закриті відомості. Як відомо, усім ПЕОМ властива проблема випромінювання високочастотної електромагнітної енергії, яка може бути перехоплена. Електромагнітні випромінювання випускаються принтерами, графічними пристроями і каналами зв'язку мереж ПЕОМ Сигнали від ПЕОМ наводяться в лініях електроживлення і зовнішніх дротяних лініях.

Слід зазначити, що у міру вдосконалення техніки роль окремих каналів витоку змінюється. Причому спостерігаються спроби зловмисників створювати і використовувати нові канали витоку інформації. Саме тому важливим є визначення джерел витоку інформації і можливостей її знімання, які є у потенційного зловмисника.

Практично в кожній АСУ існують два об'єкти, які можуть створювати небезпечні сигнали і сприяти їх поширенню, тобто служити джерелом витоку інформації. До них відносяться *технічні засоби*, в яких обробляється конфіденційна інформація, а також *людина*, в мові якого може міститися конфіденційна інформація (мова у вигляді акустичних сигналів), доступна зловмисникові після акустичного каналу або по каналу дротяної і радіозв'язку при використанні певних технічних засобів.

З попереднього викладу видно, що усі технічні засоби АС діляться на дві групи: основні технічні засоби і допоміжні. До *основних технічних засобів* можуть бути віднесені персональні комп'ютери з периферійним устаткуванням, мережі ПЕОМ; телефонні апарати міської АТС; телефонні апарати місцевої АТС; радіотелефони, мобільні і стільникові телефони; селекторний зв'язок; телефакс; засоби розмноження документів.

Допоміжні технічні засоби і системи – це радіоапаратура (телевізор, магнітофон, відеоапаратура, радіоприймач); радіотрансляційний гучномовець; датчики охоронної і пожежної сигналізації з відповідними каналами збору і обробки інформації; табельне електроустаткування приміщень; кондиціонери.

Приведений перелік основних технічних засобів складений з урахуванням того факту, що конфіденційна інформація обробляється в першу чергу саме цими засобами. При цьому, як видно, ми не згадуємо спеціальні засоби і системи захисту інформації, висока ефективність застосування яких не припускає розгляду їх як можливих джерел витоку інформації.

Розглянемо тепер деякі технічні можливості зловмисника з урахуванням класифікації джерел інформації, наведеної вище.

На підставі обробки даних з експлуатації прослуховуючих пристроїв великими фірмами (2010 рік) були зроблені наступні висновки: для зняття інформації найчастіше використовується електромагнітний канал (61%) з впровадженням на об'єкт «жучків», потім телефонний канал (15%) і далі провідні канали та диктофони (13%). Акустичний канал із застосуванням спрямованих мікрофонів, вібраційний і електромережеві канали використовуються рідко.

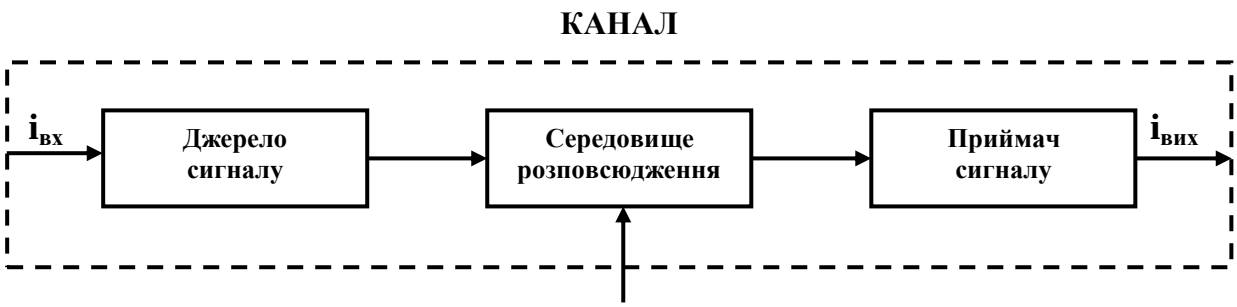

Рис. 4.4. Типова структура каналу передачі інформації

Контроль акустичної інформації. Якщо джерелом інформації є мова людини, то для несанкціонованого зняття інформації можуть застосовуватися як різні види мікрофонів, так і технічні засоби, що використовують дротяну і радіозв'язок.

Гостронаправлені мікрофони, електронні стетоскопи, лазерні детектори і записуючі диктофони можуть бути використані для безпосереднього слухового контролю і запису конфіденційних розмов. При цьому за допомогою спеціальних технічних засобів, таких, наприклад, як аналоговий процесор обробки мовних сигналів, можна значно поліпшити якість знімання інформації, підвищити комфортність прослуховування зашумлених мовних сигналів.

За допомогою таких засобів, як використання радіоканалу і застосування ліній електроживлення для передачі звукової інформації, можливий так званий електронний контроль мови. У першому випадку для акустичного контролю приміщень використовуються мініатюрні радіопередавачі, що встановлюються зазвичай в місцях, на які людина рідко звертає увагу. Зустрічаються мікропередавачі, закамуфльовані під звичайні предмети, присутність яких не викликає підозри: запальничка, сірникова коробка, попільничка, настільний письмовий прилад, авторучка, калькулятор і тому подібне.

Широко відомі і мініатюрні кишенькові передавачі, що носяться зловмисником з собою. В деяких випадках радіопередавальні пристрої встановлюються капітально під час будівництва або ремонту в стіни приміщень або в їх облицювання. Режим роботи мікропередавачів може бути *неперервним* і *з контрольованим часом включення*.

У другому випадку звукова інформація за допомогою спеціальних технічних засобів передається за межі приміщення по лініях електроживлення. Сигнал від передавача до приймача передається по ланцюгах електроживлення в ультразвуковому діапазоні частот. При цьому дальність дії системи «передавач-приймач» обмежується однією трансформаторною розв'язкою лінії електроживлення.

При уявній простоті поводження з радіомікрофонами (включення, установка) необхідно враховувати, що самому факту їх застосування передує велика, складна і добре спланована робота. Вона включає визначення приміщень, що цікавлять, попередній вибір місця установки, підбір виконавців і розміщення приймальної фіксуючої апаратури.

Контроль інформації технічними засобами в каналах телефонного зв'язку. Слід зазначити, що канали телефонного зв'язку є найуразливішими. Прослуховування розмов в приміщеннях, а також телефонних розмов може бути здійснено наступними методами:

1) безпосереднє підключення до телефонної лінії (у простому випадку застосовується трубка ремонтника-телефоніста, що підключається до лінії в розподільній коробці, де виробляється розводка кабелів);

2) негальванічне підключення до телефонної лінії (з використанням ефекту електромагнітної індукції можна з дроту, що йде близько і паралельно телефонному дроту, отримати сигнали і прослухати телефонну розмову);

3) використання мікропередавача з живленням від телефонної лінії (в даному випадку підслуховуючий пристрій у вигляді радіопередавача підключається в розрив телефонної лінії в будь-якому місці від апарату до АТС);

4) прослуховування приміщень за допомогою кодового мікрофонного підсилювача (цей спосіб є одним з найскладніших і дорожчих, оскільки вимагає спеціального пристрою, який має бути вбудований в телефонний апарат);

5) прослуховування приміщень за допомогою мікрофону телефонного апарату (елементи конструкції і електронної схеми телефонного апарату є хорошим провідником високочастотних електричних сигналів, тому, якщо до телефонної мережі підключити високочастотний генератор, то звукові сигнали, перетворюючись в мікрофоні в електричні сигнали звукової частоти, модулюватимуть високочастотний сигнал, що поступає від генератора, який надалі може бути прийнятий приймачем, підключеним до тієї ж телефонної лінії);

6) прослуховування приміщень з використанням телефонних апаратів, що містять електромагнітний дзвінок (дія акустичних коливань призводить до появи в електричному ланцюзі дзвінка модульованого струму, амплітуда якого достатня для прийому пристроєм обробки сигналу, підключеного зловмисником до телефонної лінії);

7) прослуховування телефонних розмов, що ведуться по радіотелефонах без застосування засобів захисту;

8) перехоплення факсимільних повідомлень.

Контроль інформації, що обробляється засобами обчислювальної техніки. Сучасний рівень розвитку електроніки і радіотехніки дозволяє виготовити пристрої перехоплення інформації, що виділяється з ПЕВН працюючого комп'ютера, у тому числі через незахищені ланцюги живлення і заземлення, і забезпечити скритність їх роботи.

Застосування цих пристроїв дозволяє фіксувати циркулюючу в комп'ютері інформацію на відстані до декількох сотень метрів. Існуючі системи знімання інформації враховують особливості структури сигналів в каналі зв'язку, адресні сигнали, особливості інформації, що при сукупному аналізі істотно допомагає рішенню проблем промислового шпигунства.

У разі перехоплення інформації за допомогою використання ПЕВН окрім хорошої технічної оснащеності зловмисник повинен ще мати певні алгоритмічні (аналітичними) можливості. Сюди відноситься розробка алгоритмів попередньої обробки сигналів, що приймаються, складаються з сукупності корисних сигналів і перешкод, з метою виділення сигналів, що несуть інформацію. Така робота вимагає знання техніки, уміння працювати з алгоритмами, хорошого знання суті питання (проблеми), до якого відноситься перехоплювана інформація.

4.3. Способи запобігання витоку інформації по технічним каналам

До основних способів запобігання просочуванню інформації по технічних каналах можна віднести організаційні заходи і використання різних технічних засобів захисту. Причому ефективний захист досягається при комплексному застосуванні названих підходів.

Усі вживані технічні засоби використовуються або для виявлення знімання інформації, або для його запобігання. Нині виділяють три напрями реалізації вказаних завдань:

а) виявлення активних, засобів негласного знімання акустичної інформації (радіомікрофонів, мікрофонів з передачею інформації по ланцюгах електромережі змінного струму, радіотрансляційних і іншим дротяним мережам, телефонних передавачів з передачею інформації по радіоканалу, радіостетоскопів і тому подібне);

б) постійний або періодичний контроль завантаження радіодіапазону (радіомоніторинг), виявлення і аналіз нових випромінювань, потенційних і спеціально організованих радіоканалів просочування інформації (наприклад, цифрових радіозакладних пристроїв або пристроїв з накопиченням і наступною передачею);

в) проведення спеціальних досліджень систем обробки конфіденційної інформації з метою визначення каналів витоку, рівня захищеності інформації і наступної реалізації заходів по забезпеченню виконання вимог по захисту інформації.

Розглянемо детальніше вживані тут технічні рішення.

Захист від витоку інформації по акустичному каналу. Слід відразу відмітити, що виявлення наявності акустичного контролю за допомогою гостронаправлених мікрофонів, електронних стетоскопів і лазерних детекторів досить ускладнене. Тому в цілях захисту частіше використовуються засоби запобігання зніманню інформації. До них відносяться генератори аудіоперешкод, які виробляють шумовий сигнал-перешкоду з амплітудою, що змінюється, і частотою і можуть бути портативними (кишеньковими), настільними і стаціонарними.

До більш менш ефективних засобів виявлення відносяться тільки прилади, що дозволяють встановити факт використання записуючих диктофонів. Принцип роботи подібних пристроїв базується або на реєстрації магнітних полів

працюючого електродвигуна диктофона, або на реєстрації полів струмів підмагнічування і стирання. Сучасні цифрові диктофони не мають електродвигуна, так що виявити їх практично неможливо.

Для захисту від контролю акустичної інформації у виняткових випадках використовуються спеціальні прозорі захисні кабіни, що гарантують захист від будь-яких видів прослуховування. Матеріалом для таких кабін і внутрішніх меблів служить прозорий пластик. Подібні кабіни використовуються як найбільш ефективний засіб захисту від прослуховування в посольствах провідних країн світу.

Істотно ширше спектр технічних засобів, призначених для виявлення спеціальних пристроїв електронного контролю мови. За принципом роботи їх можна розділити на дві групи:

– *апаратуру пошуку* і контролю по електромагнітному випромінюванню, яка використовується тільки для виявлення працюючих електронних пристроїв зняття інформації, випромінюючих радіохвилі (детектори випромінювання, приймачі, сканери, аналізатори спектру, частотоміри, селективні мікровольтметри, а також автоматизовані програмно-апаратні комплекси, які виконують функції радіомоніторингу);

– *апаратуру пасивного виявлення*, яка застосовується для виявлення технічних засобів знімання інформації незалежно від режиму їх роботи (нелінійні локатори, ендоскопи, дефектоскопи, металошукачі, тепловізори і тому подібне).

Апаратура пасивного виявлення дозволяє виявити технічні засоби знімання інформації навіть, якщо вони в даний момент не функціонують. Принцип їх роботи ґрунтується на виявленні аномальних особливостей в приміщеннях і конструкціях будівель. Наприклад, за допомогою нелінійних локаторів може бути виявлена присутність напівпровідникових приладів, за допомогою ендоскопів, дефектоскопів, металошукачів зміни в традиційній структурі конструкцій приміщень і будівель, а за допомогою тепловізорів аномалії в температурі.

Захист інформації в каналах зв'язку. До технічних засобів захисту інформації в каналах зв'язку можна віднести прилади, що встановлюють факт підключення до телефонних каналів підслуховуючих пристроїв, спектральні аналізатори каналів зв'язку і пристрою захисту конфіденційних розмов по телефонних каналах. Сучасні спектральні аналізатори каналів зв'язку, як правило, є комбінованими приладами, вирішальними також завдання радіомоніторингу.

У мовних системах зв'язку відомі два основні методи закриття мовних сигналів, що розділяються за способом передачі по каналах зв'язку: аналогове скремблювання і дискретизація мови з наступним шифруванням. Під *скремблюванням* розуміється зміна характеристик мовного сигналу таким чином, що отриманий модульований сигнал, маючи властивості нерозбірливості і невпізнання, займає таку ж смугу частот, як і початковий відкритий мовний сигнал.

У *системах дискретизації* мовні компоненти за допомогою аналого-цифрового перетворювача перетворяться в цифровий потік даних, який змішується по певному алгоритму з псевдовипадковою послідовністю, що виробляється ключовим генератором по одному з криптографічних алгоритмів, і отримане таким чином закрите мовне повідомлення передається за допомогою модему в канал зв'язку. На приймальному кінці виробляється перетворення в зворотному порядку з целіт отримання відкритого мовного сигналу.

Захист інформації від витоку по каналу ПЕВН. Для захисту інформації від витоку за рахунок ПЕВН застосовується пасивний, активний і комбінований методи. *Пасивний захист* полягає в зниженні рівнів випромінювання до величин, співрозмірних з природними шумами, за допомогою спеціальної елементної бази і конструктивного доопрацювання техніки, оброблювальної конфіденційну інформацію.

Існують різні способи реалізації цього методу. Одне з найпростіших технічних рішень полягає в тому, щоб помістити усе устаткування в безпечне і екрануюче радіовипромінювання середовище. Це застосовується для малогабаритної апаратури, дозволяючи зберігати її вартість на прийнятному рівні. Для великих систем екранування цілих залів і навіть будівель може бути надзвичайно дорогим, тому проблеми забезпечення електронного захисту для них розглядаються на стадії проектування.

Наприклад, для систем зв'язку визначаються вимоги безпеки окремих компонентів кожної секції усієї системи. Розробник може зажадати екранування окремих пристроїв системи за допомогою металевого захисного покриття або використовувати стандартні екрановані корпуси для блоків апаратури. Там. де екранування компонентів недоцільне, передбачається достатня ізоляція ліній даних і живлення за рахунок різних поєднань фільтрів, пристроїв пригнічення сигналу, низько імпедансного заземлення.

Допустимі рівні випромінювань апаратури і міри захисту інформації регламентуються спеціальними стандартами. У США, наприклад, а також у ряді інших західних країн в цих цілях прийнятий стандарт «Tempest» (Transcient Electromagnetic Pulse Emanations Standart) Існує повний і ослаблений варіанти цього стандарту. У США останній введений в дію в 1990 р. Повний стандарт використовується для захисту секретної інформації міністерства оборони і дипломатичної служби, а ослаблений для захисту «чутливої» інформації банків, фірм і інших організацій.

Останніми роками спостерігається стійке зростання виробництва і продажів за кордоном устаткування, що відповідає вимогам стандарту «Tempest». Цьому сприяє усе більш широке його застосування на комерційному ринку. Вартість устаткування, що відповідає цьому стандарту, як правило, в 3-5 разів вище за вартість відповідного незахищеного варіанту.

Активний захист припускає приховання інформаційних сигналів за рахунок шумової або загороджувальної перешкоди за допомогою спеціальних генераторів

шуму. *Активне радіотехнічне маскування* полягає у формуванні і випромінюванні маскуючого сигналу в безпосередній близькості від маскованої системи. В даному випадку розрізняють енергетичний і неенергетичний методи активного радіотехнічного маскування.

При *енергетичному маскуванні* виходить широкосмуговий шумовий сигнал з рівнем, що істотно перевищує в усьому частотному діапазоні рівень випромінювання системи. Одночасно відбувається наведення шумових коливань в ланцюгах, що відходять. Енергетичне маскування може бути реалізоване тільки у разі, якщо рівень випромінювань істотно менше встановленого існуючими стандартами на електромагнітну сумісність і медичними вимогами. Інакше пристрій маскування або створюватиме перешкоди різним радіопристроям, розташованим поблизу від системи, що захищається, або його не можна буде використовувати з медичних міркувань.

Неенергетичний метод активного радіотехнічного маскування (статистичний) полягає в зміні імовірнісної структури сигналу, який може бути прийнятий приймачем зловмисника. Для такої зміни сигналу потрібний спеціальний пристрій, який може вбудовуватися безпосередньо в систему або розміщуватися поруч. Рівень випромінюваного цим пристроєм маскуючого сигналу не перевершує рівня інформативного випромінювання системи, тому подібні пристрої не створюють відчутних перешкод для інших електронних приладів, що знаходяться поруч, а також безпечні для здоров’я оператора системи.

Комбінований захист – це зниження рівнів випромінювання до заданих значень з одночасним використанням і пасивного, і активного захисту.

Контрольні питання

1. Перерахуйте напрями забезпечення безпеки інформації.
2. Перерахуйте складові правового захисту інформації.
3. Які особливості укладання трудового договору.
4. Перерахуйте складові організаційно-правового захисту інформації.
5. Назвіть основні види технічних каналів і джерел витоку інформації.
6. Назвіть складові структуру каналу передачі інформації.
7. Якими методами може бути здійснено прослуховування розмов в приміщеннях?

Література для самопідготовки

1. Бобунов А.І. Захист інформації в автоматизованих системах / Бобунов А.І., Шестаков В.І. Захист інформації в автоматизованих системах: Навчальний посібник. – Житомир: ЖВІРЕ, 2004. – С. 55–64.
2. Малюк А.А. Введение в защиту информации в автоматизированных системах / Малюк А.А., Пазизин С.В., Погожин Н.С. – М.: Горячая линия-Телеком, 2001. – С. 70–76.
3. Завгородний В.И. Комплексная защита информации в компьютерных системах: учебное пособие / Завгородний В.И. . – М.: Логос; ПБОЮЛ

Питання, що опрацьовуються студентами самостійно

1. Виникнення і історія розвитку задачі ЗІ в АСУ
2. Основні підходи до розробки нормативно-правового забезпечення захист інформації в АСУ
3. Система стандартизації в області ЗІ
4. Класифікація шляхів витоку інформації та загроз.
5. Аналіз підходів до формування множини загроз інформації в АСУ
6. Методи визначення вимог до системи захисту інформації.
7. Функції і задачі захисту інформації.

РОЗДІЛ 2. МЕТОДИ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ В АСУ

СКЛАД ЗМІСТОВНОГО МОДУЛЯ

Лекція 5. Захист інформації від несанкціонованого доступу
5.1. Принципи захисту інформації від несанкціонованого доступу.
5.2. Методи ідентифікації і аутентифікації користувачів.
Контрольні питання
Література для самопідготовки
Лекція 6. Криптографічні методи захисту інформації в АСУ
6.1. Основні відомості із криптології.
6.2. Загальна класифікація алгоритмів шифрування.
6.3. Методи перестановки і заміни.
6.4. Реалізація алгоритмів шифрування.
Контрольні питання
Література для самопідготовки
Лекція 7. Системи шифрування із відкритим ключем
7.1. Основні відомості про системи шифрування із відкритим ключем. Алгоритм RSA.
7.2. Алгоритм Діффі-Хеллмана.
7.3 Алгоритм Ель-Гамаля.
Контрольні питання
Література для самопідготовки
Лекція 8. Цифровий підпис
8.1. Електронний підпис.
8.2. Хеш-функції та вимоги до них.
8.3. Керування ключами.
Контрольні питання
Література для самопідготовки
Питання, що опрацьовуються студентами самостійно

ЛЕКЦІЯ 5. ЗАХИСТ ІНФОРМАЦІЇ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

5.1. Принципи захисту інформації від несанкціонованого доступу.
5.2. Методи ідентифікації і аутентифікації користувачів.

5.1. Принципи ЗІ від НСД

Узагальнений алгоритм підготовки і реалізації несанкціонованого доступу, як правило, включає наступні етапи (рисунок 1).

1. Ретельний аналіз структури і принципів функціонування комп'ютерної мережі, що атакується, з метою пошуку уразливостей системи захисту її ресурсів.
2. Аналіз знайдених слабостей і розробка найбільш діючих способів подолання системи інформаційно-комп'ютерної безпеки.
3. Виконання підготовлених атак і оцінка отриманих результатів.
4. При невідповідності отриманих результатів необхідний ретельний аналіз процесу виконання атак і перехід до першого кроку для уточнення способів їхньої реалізації.

Рис. 5.1. Алгоритм підготовки і реалізації несанкціонованого доступу в сучасних АСУ

Представлений алгоритм припускає поетапну процедуру реалізації впливів на комп'ютерну систему, що атакується. Для атаки важливо визначити лише її слабку ланку. Така ланка може бути виявлена в усьому, що зв'язано з інформаційно-комп'ютерною безпекою: у політиці безпеки, засобах захисту, реалізаціях програмного й апаратного забезпечення, керуванні системою. Можуть використовуватися також дефекти, що на перший погляд не мають

безпосереднього відношення до забезпечення безпеки, наприклад, дефекти прикладного програмного забезпечення.

Закриття каналів несанкціонованого отримання інформації повинне починатися з контролю доступу користувачів до ресурсів АС. Завдання це вирішується на основі ряду засадничих принципів.

ПРИНЦИП ОБГРУНТОВАНОСТІ ДОСТУПУ. Цей принцип полягає в обов'язковому виконанні двох основних умов: користувач повинен мати достатню "форму допуску" для отримання інформації потрібного ним рівня конфіденційності, і ця інформація потрібна йому для виконання його виробничих функцій. Помітимо тут, що у сфері автоматизованої обробки інформації користувачами можуть виступати активні програми і процеси, а також носії інформації різної міри укрупненості. Тоді система доступу припускає визначення для усіх користувачів відповідного програмно-апаратного середовища або інформаційних і програмних ресурсів, які будуть ним доступні для конкретних операцій.

ПРИНЦИП ДОСТАТНЬОЇ ГЛИБИНИ КОНТРОЛЮ ДОСТУПУ. Засоби захисту інформації повинні включати механізми контролю доступу до усіх видів інформаційних і програмних ресурсів АС, які відповідно до принципу обґрунтованості доступу слід розділяти між користувачами.

ПРИНЦИП РОЗМЕЖУВАННЯ ПОТОКІВ ІНФОРМАЦІЇ. Для попередження порушення безпеки інформації, яке, наприклад, може мати місце при записі секретної інформації на несекретні носії і в несекретні файли, її передачі програмам і процесам, не призначеним для обробки секретної інформації, а також при передачі секретної інформації по незахищених каналах і лініях зв'язку, необхідно здійснювати відповідне розмежування потоків інформації.

ПРИНЦИП ЧИСТОТИ ПОВТОРНО ВИКОРИСТОВУВАНИХ РЕСУРСІВ. Цей принцип полягає в очищенні ресурсів, що містять конфіденційну інформацію, при їх видаленні або звільненні користувачем до перерозподілу цих ресурсів іншим користувачам.

ПРИНЦИП ПЕРСОНАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ Кожен користувач повинен нести персональну відповідальність за свою діяльність в системі, включаючи будь-які операції з конфіденційною інформацією і можливі порушення це захисту, тобто які-небудь випадкові або умисні дії, які приводять або можуть привести до несанкціонованого ознайомлення з конфіденційною інформацією, її спотворенню або знищенню, або роблять таку інформацію недоступною для законних користувачів.

ПРИНЦИП ЦІЛІСНОСТІ ЗАСОБІВ ЗАХИСТУ Цей принцип має на увазі, що засоби захисту інформації в АС повинні точно виконувати свої функції відповідно до перерахованих принципів і бути ізольованими від користувачів, а для свого супроводу повинні включати спеціальний захищений інтерфейс для засобів контролю, сигналізації про спроби порушення захисту дії на процеси в системі

Реалізація перерахованих принципів здійснюється за допомогою так званого «монітора звернень», контролюючого будь-які запити до даних або програм з боку користувачів (чи їх програм) по встановлених для них видах доступу до цих даних і програм. Схемний такий монітор представляється у вигляді, показаному на рис. 5.2.

Рис. 5.2. Структура монітора звернень

Практичне створення монітора звернень, як видно з приведеного малюнка, припускає розробку конкретних правил розмежування доступу у вигляді так званої моделі захисту інформації. Історично моделі захисту інформації виникли з робіт по теорії захисту операційних систем (ОС). Перша спроба використання такої моделі була зроблена при розробці захищеної ОС ADEPT-50 за замовленням міністерства оборони США.

Поведінка цієї моделі описується наступними простими правилами:

а) користувачеві дозволений доступ в систему, якщо він входить в множину відомих системі користувачів,

б) користувачеві дозволений доступ до терміналу, якщо він входить в підмножину користувачів, закріплених за цим терміналом;

в) користувачеві дозволений доступ до файлу, якщо: рівень конфіденційності користувача не нижчий за рівень конфіденційності файлу; прикладна область файлу включається в прикладну область завдання користувача; режим доступу завдання користувача включає режим доступу до файлу; користувач входить в підмножину допущених до файлу користувачів.

У моделі Хартсона [1] як основні характеристики використовується множина так званого п'ятивимірного «простору безпеки», рис.5.3

- встановлених повноважень;
- користувачів;
- операцій;
- ресурсів;
- станів.

Область безпечних станів системи представляється у вигляді декартового добутку перерахованих вимірів. Кожен запит на доступ представляється підпростором чотиривимірної проекції простору безпеки. Запити отримують право на доступ у тому випадку, коли вони повністю поміщені у відповідні підпростори.

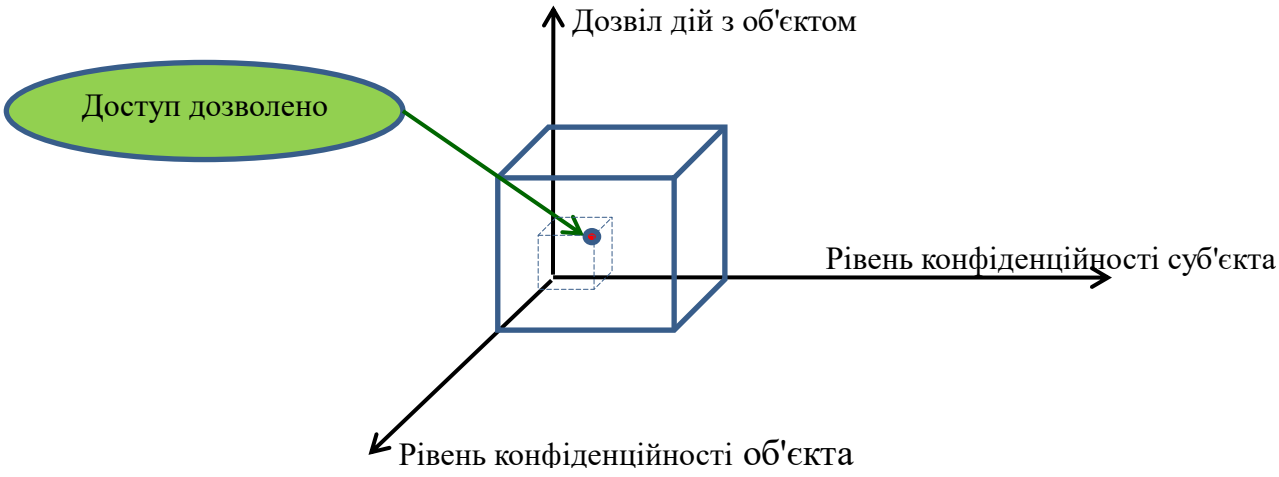

Рис. 5.3. Модель Хартсона

Одна з перших фундаментальних моделей захисту була розроблена Лемпсоном і потім вдосконалена Грехемом і Деннінгом, рис.5.4. Основу їх моделі складає ***матриця (таблиця) доступу A***, в якій:

1) стовпці $O_1, O_2, ..., O_n$ представляють собою об'єкти доступу;

2) рядки $S_1, S_2, ..., S_m$ це суб'єкти доступу;

3) елемент таблиці $A\left[S_i, O_j\right]$ містить список видів доступу $T_1, T_2, ..., T_k$, який визначає привілеї суб'єкта S_i по відношенню до об'єкту O_j.

	O_1,	O_2	...	O_j,		O_n
S_1	R	R,W		E		R
S_2	R,N	-		R		E
...						
Si	R	-		-		R
…						
S_m	RW	-		E		E

Рис. 5.4.

Ця модель припускає, що усі спроби доступу до об'єктів перехоплюються і перевіряються спеціальним процесом, що управляє. Таким чином, суб'єкт S_i

отримає доступ T_k, що ініціюється ним, до об’єкту O_j тільки у разі, якщо елемент матриці $A\left[S_i, O_j\right]$ має значення T_k.

Наведені моделі можуть використовуватися як для захисту ОС, так і для захисту баз даних (БД). Враховуючи, що такі єдині моделі, як показує практика, значно ускладнюють розгляд питань безпеки, рядом авторів були зроблені спроби розробки спеціальних моделей захисту БД.

Розглянуті вище моделі захисту інформації відносяться до класу матричних і набули найбільшого поширення внаслідок того, що вони служать не лише для цілей аналізу логічного функціонування системи, але і успішно піддаються реалізації в конкретних програмах.

Правило розмежування доступу полягає в такому: особа допускається до роботи з документом лише в тому випадку, якщо рівень допуску суб'єкта доступу дорівнює або вищий за рівень конфіденційності документа, а в наборі категорій, присвоєних даному суб'єктові доступу, містяться всі категорії, визначені для даного документа. У ІС всі права суб'єкта доступу фіксуються в його мандаті. Суб'єкт повинен мати набір мандатів для доступу до всіх необхідних йому об’єктів. Мандатне управління дозволяє спростити процес регулювання доступу, оскільки під час створення нового об'єкта достатньо створити його позначку. Проте при такому управлінні доводиться завищувати конфіденційність інформації через неможливість детального розмежування доступу. Найбільшого поширення набула багаторівнева модель захисту Белла-Ла Падула, рис.5.5.

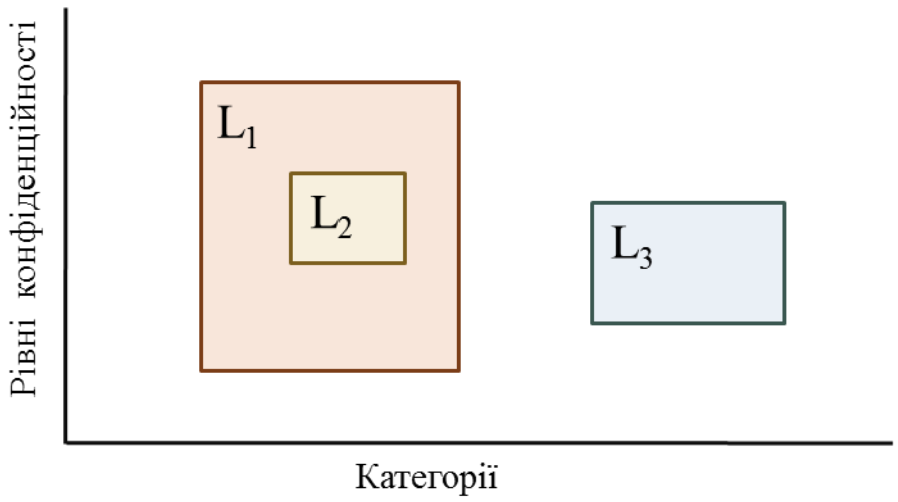

Рис.5.5. Модель Белла-Ла Падула

Основою цієї моделі є поняття рівня конфіденційності (форми допуску) і категорії (прикладної області) суб'єкта і об'єкта доступу. На підставі присвоєних кожному суб'єктові й об'єкту доступу конкретних рівнів і категорій у моделі визначаються їхні рівні безпеки, а потім встановлюється їх взаємодія. При цьому в моделі приймається, що один рівень безпеки домінує над іншим тоді й лише

тоді, коли відповідний йому рівень конфіденційності більший або дорівнює рівню конфіденційності іншого, а множина категорій включає відповідну множину іншого. Рівні конфіденційності є впорядкованими, тоді як рівні безпеки впорядковані частково**,** тому деякі суб'єкти й об'єкти можуть бути непорівнянні.

Оскільки програми в цих моделях виступають в правилах доступу як суб’єктів, то вони можуть, при необхідності, розширювати права конкретних користувачів. Наприклад, програма може мати права на сортування файлу, читання якого користувачеві заборонене.

Іншим видом моделей є багаторівневі моделі. Вони відрізняються від матричних моделей декількома аспектами. По-перше, ці моделі розглядають управління доступом не у рамках тих, що задаються деяким адміністратором прав, а у рамках представлення усієї системи так, щоб дані однієї категорії або області не були доступні користувачам іншої категорії. По-друге, багаторівневі моделі розглядають не лише сам факт доступу до інформації, але також і потоки інформації усередині системи.

Підводячи підсумок розгляду двох класів моделей захисту інформації, відмітимо, що перевага матричних моделей полягає в легкості представлення широкого спектру правил забезпечення безпеки інформації. Основний же недолік цих моделей полягає у відсутності контролю за потоками інформації. Зі свого боку, головним недоліком багаторівневих моделей є неможливість управління доступом до конкретних об’єктів на основі обліку індивідуальних особливостей кожного з суб’єктів. Отже, обидва підходи як би припускають пошук різних компромісів між ефективністю, гнучкістю і безпекою. Очевидно, що оптимальне рішення питань безпеки повинне вироблятися із застосуванням обох видів моделей захисту.

5.2. Методи ідентифікації і аутентифікації користувачів

Реалізація конкретних моделей захисту від несанкціонованого доступу повинна спиратися на відповідні адміністративні (процедурні) заходи і технічні засоби, спрямовані в першу чергу на ідентифікацію і аутентифікацію користувачів автоматизованої системи.

Ідентифікація користувачів АС полягає у встановленні і закріпленні за кожним з них унікального ідентифікатора у вигляді номера, шифру, коду тощо. Це пов’язано із тим, що традиційний ідентифікатор виду прізвище-ім’я-по батькові не завжди може бути використаний в конкретній АС. Для цілей ідентифікації в різних автоматизованих системах широко, наприклад, застосовуються так званий персональний ідентифікаційний номер (PIN), соціальний безпечний номер (SSN), особистий номер, код безпеки тощо [14]. Такі ідентифікатори використовуються при побудові різних систем розмежування доступу і захисту інформації.

Аутентифікація полягає в перевірці достовірності користувача за пред'явленим їм ідентифікатору, наприклад, при вході в систему. Така перевірка повинна виключати фальсифікацію користувачів в системі і їх компрометацію. Без перевірки достовірності втрачається сенс в самій ідентифікації користувачів і застосуванні засобів розмежування доступу, побудованих на базі особистих ідентифікаторів. Відсутність надійних засобів перевірки достовірності користувачів може істотно утруднити реалізацію принципу персональної відповідальності, про який говорилося вище.

Перевірка достовірності (аутентифікація) може проводитися різними методами і засобами, рис.5.6. Нині в автоматизованих системах використовуються три основні способи аутентифікації за наступними ознаками:

1) паролю або особистому ідентифікуючому номеру (користувач «знає»);

2) деякому предмету, який є у користувача (користувач «має»);

3) яким-небудь фізіологічним ознакам, властивим конкретним особам (користувач «є»).

Рис.5.6. Способи аутентифікації

Перший спосіб реалізують програмні засоби аутентифікації, що вживаються в більшості операційних систем, систем управління базами даних, моніторів телеобробки, мережевих пакетів. Суть цього способу полягає в тому, що кожному зареєстрованому користувачеві видається персональний пароль, який він повинен тримати в таємниці і вводити в автоматизовану систему при кожному зверненні до неї. Спеціальна програма порівнює введений пароль з еталоном, що зберігається в пам'яті, і при збігу паролів запит користувача приймається до виконання.

Простота цього способу очевидна, але очевидні також і його явні недоліки: пароль може бути підібраний перебором можливих комбінацій, а майстерний зловмисник може проникнути в ту область пам'яті, де зберігаються еталонні

паролі. Наприклад, в ОС RSX-11 M, що застосовувалася свого часу в банківській сфері, в стандартній конфігурації були відсутні засоби шифрування паролів у файлі рахунків користувачів. В процесі завантаження цією ОС можна було легко проглянути паролі усіх користувачів. Безпечніші системи здійснюють зберігання списків паролів в зашифрованому виді. В той же час перехоплення навіть зашифрованого пароля дозволяє при його використанні дістати несанкціонований доступ до видаленої ПЕОМ.

До заходів підвищення безпеки парольних систем аутентифікації, окрім згаданого зберігання списків паролів в зашифрованому виді, може бути віднесене скорочення термінів дії паролів аж до застосування паролів одноразового використання. Останнім часом для цілей аутентифікації широко використовується так званий метод «запит-відповідь», яка дозволяє не лише аутентифікувати користувача, але і дає можливість користувачеві здійснювати аутентифікацію системи, з якою він працює. Це має принципове значення при роботі в мережі, оскільки використання підставної ПЕОМ, ОС або програми є одним з шляхів несанкціонованого отримання повідомлень або паролів законних користувачів. Слід зазначити, що необхідність такої взаємної аутентифікації підтверджена міжнародним стандартом по взаємодії відкритих систем.

Різновидом першого способу аутентифікації є і так зване пізнання в діалоговому режимі, здійснюване за наступною схемою. У файлах механізмів захисту завчасно створюються записи, що персоніфікують, що містять, користувача дані (дата народження, зростання, вага, імена і дати народження рівних і близьких і тому подібне) або досить великий і впорядкований набір паролів. При зверненні користувача програма захисту пропонує йому назвати деякі дані з наявного запису, які порівнюються з тими, що зберігаються у файлі. За результатами порівняння приймається рішення про допуск. Для підвищення надійності пізнання прошені у користувача дані можуть вибиратися кожного разу різні.

Як предмет, наявний у користувача (другий спосіб аутентифікації), застосовуються так звані карти ідентифікації (КІ), на які наносяться дані, що персоніфікують користувача: персональний ідентифікаційний номер, спеціальний шифр або код тощо. Ці дані заносяться на картку в зашифрованому виді, причому ключ шифрування може бути додатковим ідентифікуючим параметром, оскільки він може бути відомий тільки користувачеві, вводиться ним кожного разу при зверненні до системи і знищується відразу ж після використання.

Інформація, що знаходиться на карті, може бути записана і зчитана різними способами або комбінацією декількох способів Наприклад, КІ поміщається в зчитувачі, джерело світла освітлює мікрокристалічну точкову матрицю, встановлену на карті. Оскільки тільки неполяризовані елементи матриці будуть прозорі для світла, то буде прочитаний відповідний код, що містить інформацію про конкретного користувача.

Ще одним типом КІ є *інформаційна картка* з нанесеними особливим способом із застосуванням фосфору на її поверхню декількома рядами знаків, букв тощо. Зчитування даних з пристрою в цьому випадку є двома електродами, один з яких прозорий.

Картка поміщається між електродами, і при подачі на них напруга електрони, що збуджуються між ізолюючим шаром (основою картки) і шаром фосфору, викликають світіння останнього. Таким чином, інформаційні знаки можуть бути лічені тільки спеціальним способом, що виключає візуальне розпізнавання інформації.

Іншим типом КІ є *електронна ідентифікуюча карта*, побудована на інтегральній мікросхемі. У цієї карти на короткій стороні друкованої плати розташовуються котушки індуктивності, через які передається електроживлення на плату і здійснюється обмін кодованою інформацією з пристроєм, що пізнає. Інтегральна схема містить арифметичний блок, а також постійне і оперативне пристрої, що запам'ятовують.

На поверхню карти може також наноситися покриття, що дозволяє бачити зображення або текст тільки в інфрачервоному або ультрафіолетовому діапазоні. Над текстом або зображенням можна розмістити рідкокристалічну матрицю, прозору тільки при певній орієнтації кристалів.

Найбільше поширення серед пристроїв аутентифікації за типом «користувач має» отримали *індивідуальні магнітні карти*. Популярність таких пристроїв пояснюється універсальністю їх застосування (не лише в автоматизованих системах), відносно низькою вартістю і високою точністю, вони легко комплектуються з терміналом і персональною ПЕОМ. Оскільки зчитувачі цих пристроїв ідентифікують не особу, а магнітну карту, то вони комплектуються спеціальною, часто цифровою клавіатурою для введення власником карти свого шифру, пароля. Для захисту карт від несанкціонованого зчитування і підробки, як і в попередніх випадках, застосовуються спеціальні фізичні і криптографічні методи.

Для пізнання компонентів обробки даних, тобто ПЕОМ, ОС, програм функціональної обробки, масивів даних (таке пізнання особливе актуально при роботі в мережі ПЕОМ) використовуються спеціальні апаратні блоки-приставки, що є пристроями, що генерують індивідуальні сигнали. В цілях попередження перехоплення цих сигналів і наступного їх зловмисного використання вони можуть передаватися в зашифрованому виді, причому періодично може мінятися не лише ключ шифрування, але і використовуваний спосіб (алгоритм) криптографічного перетворення.

Усього зростаючого значення останнім часом починають набувати системи розпізнання користувачів *за фізіологічними ознаками*. Тільки при такому підході дійсно встановлюється, що користувач, що претендує на доступ до терміналу, саме той, за кого себе видає. При використанні цього класу засобів аутентифікації виникає проблема «соціальної прийнятності»: процедура аутентифікації не

повинна принижувати людську гідність, створювати дискомфорт, просто бути занадто морочливою і займати багато часу.

Існує досить фізіологічних ознак, що однозначно вказують на конкретну людину, рис. 5.7. До них відносяться: відбитки ніг і рук, зуби, ферменти, динаміка дихання, риси обличчя і так далі. Для аутентифікації термінальних користувачів автоматизованих систем найбільш прийнятними вважаються відбитки пальців, геометрія руки, голос, особистий підпис.

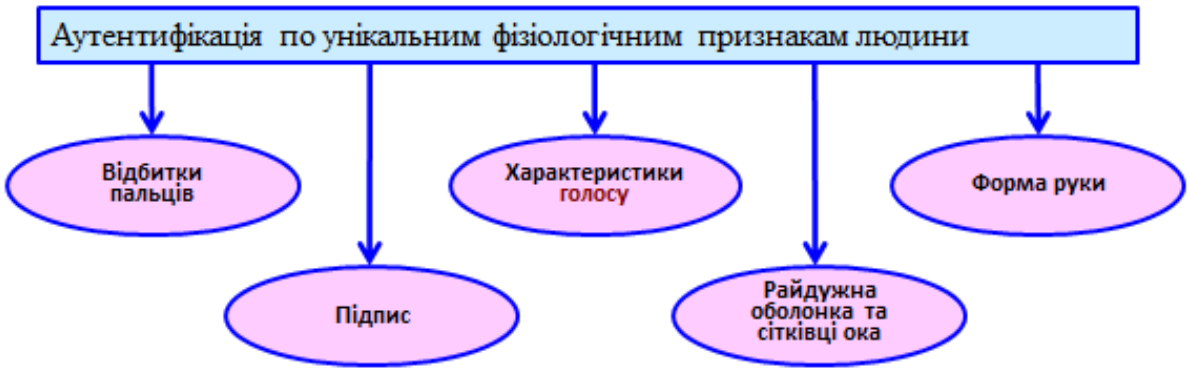

Рис.5.7.

Аутентифікація за відбитками пальців. Встановлення особи по відбитках пальців – старий і перевірений прийом. Нині існують два можливі способи використання цього прийому для аутентифікації термінального користувача:

– безпосереднє порівняння зображень відбитків пальців, отриманих за допомогою оптичних пристроїв, з відбитками з архіву;

– порівняння характерних деталей відбитку в цифровому виді, які отримують в процесі сканування зображень відбитку.

На сьогодні розроблені спеціальні чутливі матеріали, що забезпечують отримання відбитків без використання фарби, засновані на здатності речовин змінювати свої відбивні характеристики залежно від температури предметів, що прикладаються.

При безпосередньому порівнянні зображень відбитків пристрій аутентифікації визначає оптичне співвідношення двох зображень і виробляє сигнал, що визначає міру збігу відбитків. Порівняння відбитків зазвичай виконується безпосередньо на місці установки пристрою. Передача зображення відбитку по каналах зв'язку не застосовується із-за її складності, високої вартості і необхідності додаткового захисту цих каналів.

Великого поширення набув спосіб, побудований на порівнянні деталей відбитків (метод співвідношення борозенок на відбитках). При цьому користувач вводить з клавіатури ідентифікуючу інформацію, по якій пристрій аутентифікації проводить пошук необхідного списку деталей відбитку в архіві. Після цього він поміщає палець на оптичне віконце пристрою, і починається процес сканування, в результаті якого обчислюються координати 12 точок, що визначають відносне розташування борозенок відбитку. Об'єм інформації при цьому складає близько

100 байт на відбиток. Порівняння виробляється в ЕОМ по спеціальних алгоритмах. Недоліком цього способу, проте, являється те, що практично неможливо забезпечити точне центрування і стабільну пластичність пальця, тому неможливо отримати і точне положення борозенок, внаслідок чого оцінка відповідності має імовірнісний характер.

Одним з прикладів пристрою аутентифікації по відбитках пальців може служити американська система Fingerprint [15] Ця система складається з центральною пристрої управління і пристроїв для зняття відбитків пальців. Користувач вводить свій ідентифікуючий номер, поміщає палець в спеціальну щілину, і пристрій виробляє оптичне сканування шкіри. До складу пристрою входять лазерна оптична система, апаратура обробки сигналів і мікропроцесор з програмами побудови "образу" відбитку пальця. Рельєф шкіри прочитується пристроєм майже безпомилково. Для занесення еталону відбитку одного пальця вимагається від 3 до 5 хвилин, необхідний об’єм пам’яті 256 байт.

Аутентифікація за формою кисті руки. Принцип дії таких пристроїв аутентифікації заснований на тому, що на руку випробовуваному направляють яскраве світло і аналізують освітленість чутливих елементів, яка залежить від довжини пальців, закругленості їх кінчиків і прозорості шкіри. Вихідна інформація від кожного фоторезистора перетвориться в цифровий код. Ідентифікуюча інформація може зберігатися централізований в головній ПЕОМ. Перевагою подібних систем є велике число аналізованих параметрів, що зменшує вірогідність помилки.

Аутентифікація за допомогою автоматичного аналізу підпису. Відомо, що почерк кожної людини строго індивідуальний, ще більше індивідуальний його підпис. Вона стає надзвичайно стилізованою і з часом набуває характеру умовного рефлексу. Нині існують два принципово різних способу аналізу підпису: візуальне сканування і дослідження динамічних характеристик руху руки при виконанні підпису (прискорення, швидкості, тиски, тривалість пауз) Вважається, що другий спосіб прийнятніший, оскільки очевидно, що два підписи однієї і тієї ж людини не можуть бути абсолютно ідентичними. З іншого боку, маючи оригінал підпису, можна навчитися повторювати її практично точно.

При другому способі аутентифікації передбачається застосування спеціальних вимірювальних авторучок з датчиками, чутливими до вказаних вище динамічних характеристик руху. Ці параметри унікальні для кожної людини, їх неможливо підробити. У авторучку вбудований двомірний датчик прискорення, що дозволяє вимірювати характеристики на площини, а також датчик тиску, фіксувальний параметри вертикальної сили. Існують два способи порівняння результатів вимірів. Перший заснований на порівнянні амплітуд прискорення кожні 5..10 мс. Необхідна пам’ять в цьому випадку – 2 кБайта Другий спосіб заснований на обчисленні середніх величин повного часу написання, проміжків «мовчання», швидкості і прискорення по осях *X* і *Y* та середньої сили по осі *Z*. Необхідна пам’ять для зберігання одного еталонного векторів цьому випадку складає 200

байт. Фахівці вважають, що системами встановлення достовірності підпису при меншій вартості і більше соціальною прийнятністю не поступається по надійності пристроям, що звіряють відбитки пальців.

Аутентифікація по характеру голосу. На думку ряду фахівців, найбільш надійними засобами аутентифікації користувачів є засоби верифікації по голосах. Це напрям дуже перспективно тому, що для аутентифікації можуть бути використані телефонні канали зв'язку, а алгоритм пізнання може бути реалізований в центральній ПЕОМ Можна виділити три основні напрями реалізації цього способу аутентифікації:

– *аналіз короткочасних сегментів мови* (тривалістю до 20 мс) – вибирається серія коротких фрагментів, обробляється, складається статистичний образ, який і порівнюється з еталоном;

– *контурний аналіз мови* – з фрагмента мови виділяється декілька характеристик, наприклад, висота тону, для них визначається характеристична функція, яка порівнюється з еталонною;

– *статистична оцінка голосу* – мова повинна звучати достатньо довго (близько 12 с), упродовж усього цього періоду збирається інформація про декілька параметрів голосу, на основі якої створюється цифровий образ і порівнюється з еталоном.

Слова, які вимовляє користувач, вибираються за принципом найбільшої різноманітності звуків і заздалегідь виводяться на екран дисплея у випадковій послідовності, що виключає підробки, у тому числі використання магнітофонного запису.

Основними характеристиками пристроїв аутентифікації є: частота помилкового заперечення законного користувача;

1) частота помилкового визнання стороннього;
2) середній час напрацювання на відмову;
3) число обслуговуваних користувачів;
4) вартість;
5) об'єм інформації, циркулюючої між зчитувачем і блоком порівняння;
6) прийнятність з боку користувачів.

Дослідження і випробування пристроїв аутентифікації різних типів показали, що частота помилкового заперечення дещо перевищує частоту помилкового визнання і складає величину, що не перевищує 1–2%. Так, вітчизняний пристрій аутентифікації по підпису має частоту помилкового заперечення, приблизно рівну частоті помилкового визнання і що становить близько 0,5%.

Головним висновком, що виходить з досвіду створення пристроїв аутентифікації, є те, що отримання високої точності пізнання користувача можливо тільки при поєднанні різних методів.

Необхідно відмітити, що усі розглянуті методи аутентифікації у разі не підтвердження достовірності повинні здійснювати тимчасову затримку перед обслуговуванням наступного запиту. Це необхідно для зниження загрози підбору

ідентифікуючих ознак (особливо паролів) в автоматичному режимі. При цьому усі спроби неуспіхів діставання доступу повинні реєструватися в цілях забезпечення ефективного нагляду (контролю) за безпекою системи.

Контрольні питання

1. Алгоритм підготовки і реалізації несанкціонованого доступу в сучасних АСУ.
2. Назвіть основні принципи захисту інформації від НСД.
3. Структура монітора звернень.
4. Основні характеристики моделі Хартсона?
5. У чому суть мандатної моделі?
6. Основні характеристики моделі Белла-Ла Падула.
7. Дайте визначення поняттям «ідентифікація», «аутентифікація».
8. Назвіть методи аутентифікації по унікальним фізіологічним признакам людини.

Література для самопідготовки

1. Бобунов А.І. Захист інформації в автоматизованих системах / Бобунов А.І., Шестаков В.І. Захист інформації в автоматизованих системах: Навчальний посібник. – Житомир: ЖВІРЕ, 2004. – С. 55–64.
2. Антонюк А.О. Основи захисту інформації в автоматизованих системах управління / Антонюк А.О. – Київ: Видавничий дім "КМ академія", 2003. – 38–57.
3. Малюк А.А. Введение в защиту информации в автоматизированных системах / Малюк А.А., Пазизин С.В., Погожин Н.С. – М.: Горячая линия-Телеком, 2001. – С. 53–85.
4. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа / Щеглов А.Ю. – СПб: Наука и техника.

ЛЕКЦІЯ 6. КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ В АСУ

6.1. Основні відомості із криптології.
6.2. Загальна класифікація алгоритмів шифрування.
6.3. Методи перестановки і заміни.
6.4. Реалізація алгоритмів шифрування.

6.1. Основні відомості із криптології

Виключно важливим механізмом ЗІ є криптографія. Оскільки цей складний і широкий розділ математики вимагає окремого детального вивчення, тут подамо лише основні відомості з криптології.

Проблема захисту інформації шляхом її перетворення, що виключає її прочитання сторонньою особою, хвилювала людський розум з давніх часів. Історія криптографії – ровесниця історії людської писемності. Більш того, спочатку писемність сама по собі була криптографічною системою, тому що в древніх суспільствах нею володіли тільки обрані. Із поширенням писемності криптографія стала формуватися як самостійна наука. Перші криптосистеми зустрічаються вже на початку нашої ери. Так, Цезар у своїй переписці використовував уже більш-менш систематичний шифр, що одержав його ім’я. Бурхливий розвиток криптографічні системи одержали в роки Першої і Другої світових воєн. Починаючи з післявоєнного часу і по нинішній день поява обчислювальних засобів прискорила розробку й удосконалення криптографічних методів.

Чому проблема використання криптографічних методів у АСУ стала в даний момент особливо актуальною? З одного боку, розширилося використання комп’ютерних мереж, зокрема глобальної мережі Internet, по яких передаються великі обсяги інформації державного, військового, комерційного і приватного характеру, що не допускає можливість доступу до неї сторонніх осіб. З іншого боку, поява потужних комп’ютерів, технологій мережевих і нейронних обчислень

уможливила дискредитацію криптографічних систем, для яких ще недавно розкриття вважалося практично неможливим.

Проблемою захисту інформації шляхом її перетворення займається *криптологія* (kryptos – таємний, logos – наука). Криптологія поділяється на два напрямки: криптографію і криптоаналіз. Цілі цих напрямків прямо протилежні.

Криптографія займається пошуком і дослідженням математичних методів перетворення інформації. Сфера ж інтересів *криптоаналізу* – дослідження можливості розшифрування інформації без знання ключів.

Сучасна криптографія включає чотири великих розділи:

1. Симетричні криптосистеми.
2. Криптосистеми з відкритим ключем.
3. Системи електронного підпису.
4. Керування ключами.

З основних напрямків використання криптографічних методів відзначимо передачу інформаційними каналами зв'язку (наприклад, електронна пошта), встановлення дійсності переданих повідомлень, збереження інформації (документів, баз даних) на носіях у зашифрованому вигляді. Наведемо деякі найбільш уживані терміни криптографії.

Як інформацію, що підлягає шифруванню і дешифруванню, розглядають тексти, побудовані на деякому алфавіті.

Алфавіт – скінченна множина використовуваних для кодування інформації знаків.

Текст – упорядкований набір з елементів алфавіту.

Шифрування – процес перетворення: вихідний текст, що має також назву відкритого тексту, заміняється шифрованим текстом.

Дешифрування – зворотний шифруванню процес. На основі ключа шифрований текст перетворюється у вихідний.

Ключ – інформація, яка необхідна для безперешкодного шифрування і дешифрування.

Криптографічна система являє собою сімейство перетворень відкритого тексту. Члени цього сімейства індексуються, чи позначаються символом к; параметр k є ключем. Простір K – це набір можливих значень ключа. Звичайно ключ являє собою послідовний ряд символів з алфавіту.

Криптосистеми поділяються на симетричні і з відкритим ключем. У *симетричних системах* і для шифрування, і для дешифрування використовується той самий ключ.

У *системах з відкритим ключем* (СВК) використовуються два ключі – відкритий і закритий, котрі математично зв'язані один з одним. Інформація шифрується за допомогою відкритого ключа, що доступний усім бажаючим, а розшифровується за допомогою закритого ключа, відомого тільки одержувачу повідомлення.

Терміни «*розподіл ключів*» і «*керування ключами*» стосуються процесів системи обробки інформації, змістом яких є складання і розподіл ключів між користувачами.

Електронним (цифровим) підписом називається приєднане до тексту його криптографічне перетворення, що дозволяє при одержанні тексту іншим користувачем перевірити авторство і дійсність повідомлення.

Криптостійкістю називається характеристика шифру, що визначає його стійкість до дешифрування без знання ключа (тобто криптоаналізу). Є декілька показників криптостійкості, серед яких:

1. Кількість усіх можливих ключів.
2. Середній час, необхідний для криптоаналізу.

Перетворення тексту визначається відповідним алгоритмом і значенням параметра *k*. Ефективність шифрування з метою захисту інформації залежить від збереження таємниці ключа і криптостійкості ключа.

Абстрактно *систему засекреченого зв'язку* можна описати як безліч відображень безлічі відкритих повідомлень у безліч закритих. Вибір конкретного типу перетворення визначається ключем шифрування (або розшифрування). Відображення повинні мати властивість взаємооднозначності, тобто при розшифруванні повинен виходити єдиний результат, що збігається з первісним відкритим повідомленням (рис. 6.1)

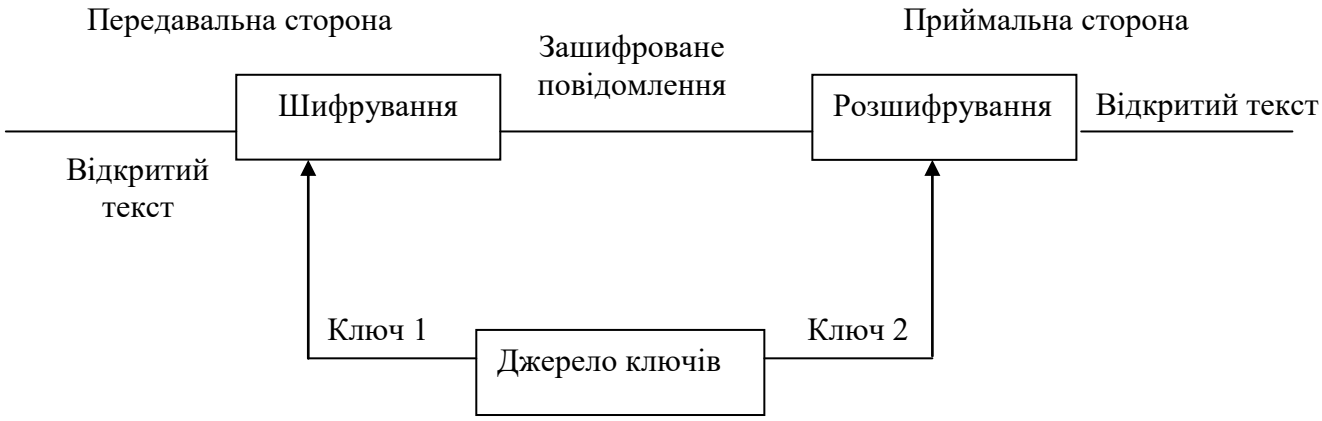

Рис. 6.1. Загальна структура системи засекреченого зв'язку

Ключі шифрування й розшифрування можуть у загальному випадку бути різними, хоча для простоти міркувань припустимо, що вони ідентичні. Множина, з якої вибираються ключі, називається *ключовим простором.* Сукупність процесів шифрування, множини відкритих повідомлень, множини можливих закритих повідомлень і ключового простору називається *алгоритмом шифрування*. Сукупність процесів розшифрування, множини можливих закритих повідомлень, множини відкритих повідомлень і ключового простору називається *алгоритмом розшифрування*.

Роботу системи засекреченого зв'язку можна описати в такий спосіб:

1. Із ключового простору вибирається ключ шифрування K і відправляється по надійному каналу передачі.

2. До відкритого повідомлення C, призначеного для передачі, застосовують конкретне перетворення F_k, обумовлене ключем K, для одержання зашифрованого повідомлення M: $M = F_k(C)$.

3. Отримане зашифроване повідомлення M пересилають по каналу передачі даних.

4. На приймаючій стороні до отриманого повідомлення M застосовують конкретне перетворення D_k, обумовлене із усіх можливих перетворень ключем K, для одержання відкритого повідомлення C: $C = D_k(M)$.

Розглянемо *основні вимоги до криптосистем*. Процес криптографічного закриття даних може здійснюватися як програмно, так і апаратно. *Апаратна реалізація* відрізняється істотно більшою вартістю, однак вона має і переваги: висока продуктивність, простота, захищеність тощо. *Програмна реалізація* більш практична, допускає певну гнучкість у використанні.

Для сучасних криптографічних систем захисту інформації сформульовані такі загально прийняті вимоги:

1) зашифроване повідомлення має піддаватися читанню тільки за наявності ключа;

2) число операцій, необхідних для визначення використаного ключа шифрування за фрагментом шифрованого повідомлення і відповідного йому відкритого тексту, повинно бути не меншим від загального числа можливих ключів;

3) число операцій, необхідних для розшифровування інформації шляхом перебору різних ключів, повинно мати строгу нижню оцінку і виходити за межі можливостей сучасних комп'ютерів (з урахуванням можливості використання мережевих обчислень);

4) знання алгоритму шифрування не повинно впливати на надійність захисту;

5) незначна зміна ключа повинна приводити до істотної зміни вигляду зашифрованого повідомлення;

6) структурні елементи алгоритму шифрування повинні бути незмінними;

7) додаткові біти, що вводяться в повідомлення в процесі шифрування. повинні бути цілком і надійно сховані в шифрованому тексті;

8) довжина шифрованого тексту повинна бути рівною довжині вихідного тексту;

9) не повинно бути простих і легко встановлюваних залежностей між ключами, послідовно використовуваними в процесі шифрування;

10) будь-який ключ з множини можливих повинен забезпечувати надійний захист інформації;

11) алгоритм повинен допускати як програмну, так і апаратну реалізацію, при цьому зміна довжини ключа не повинна вести до якісного погіршення алгоритму шифрування.

6.2. Загальна класифікація алгоритмів шифрування

В основі криптографічних алгоритмів лежать математичні перетворення, що дозволяють домогтися високої практичної стійкості більшості алгоритмів. Було доведено, що в криптографії існують тільки два основні типи перетворень – заміни й перестановки, усі інші є лише комбінацією цих двох типів. Таким чином, є криптографічні алгоритми, побудовані на основі заміни, перестановки й об'єднання цих двох перетворень.

У перестановочних шифрах символи відкритого тексту змінюють своє місце розташування. З іншого боку, у шифрах заміни один символ відкритого тексту заміщається символом зашифрованого тексту.

У класичній криптографії розрізняють чотири типи шифрів заміни:

- *шифри простої заміни (моноалфавітні шифри).* Один символ відкритого тексту заміняється одним символом зашифрованого тексту;
- *шифри складної заміни.* Один символ відкритого тексту заміняється одним або декількома символами зашифрованого тексту, наприклад: "А" може бути замінений "З" або "РО4Е";
- *шифри блокової заміни.* Один блок символів відкритого тексту заміняється блоком закритого тексту, наприклад: "АВС" може бути замінений "СРТ" або "КАР";
- *поліалфавітні шифри заміни,* у яких до відкритого тексту застосовуються кілька шифрів простої заміни.

Класична криптографія, зокрема теорія зв'язку, у секретних системах, заснована К. Шеноном, виходила з того, що ключі, використовувані відповідно для шифрування й розшифрування, є секретними й однаковими, і передача їх повинна здійснюватися по надійному каналу обміну ключової інформації. Подібні алгоритми були названі *симетричними*, тому що шифрування й розшифрування відбувається на однакових ключах.

Однак розвиток теорії побудови алгоритмів шифрування з відкритими ключами, родоначальниками якої стали У. Діффі й М. Хеллман, поклала початок повсюдному використанню *асиметричних* алгоритмів шифрування, у яких ключі шифрування й розшифрування різні залежно від застосування один із ключів буде відкритим, тобто загальнодоступним, а іншої необхідно зберігати в секреті. Різновидом таких криптосистем є системи електронних цифрових підписів, таємного електронного голосування, захисту від нав'язування неправильних повідомлень, електронного жеребкування й ряд інших криптосистем.

Через деякий час симетричні алгоритми були розділені на два більші класи – *блокові* й *потокові*. У перших відкритий текст розбивається на блоки підходящої довжини, і кожний блок шифрується. У потокових алгоритмах кожний символ відкритого тексту зашифровується незалежно від інших і розшифровується в такий же спосіб. Інакше кажучи, перетворення кожного символу відкритого тексту міняється від одного символу до іншого, у той час як для блокових

алгоритмів у рамках шифрування блоку використовується одне й теж криптографічне перетворення.

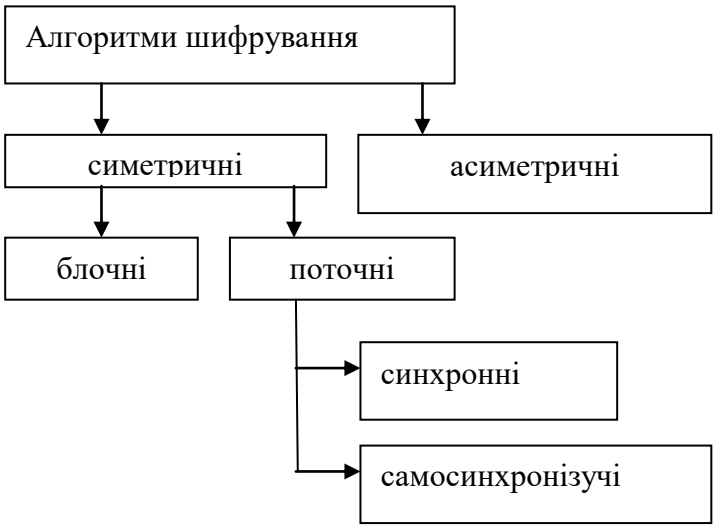

Рис. 6.2. Класифікація алгоритмів шифрування

Головна ідея, втілена в алгоритмах потокового шифрування полягає у виробітку на основі секретного ключа послідовності символів із вхідного алфавіту, з яким працює алгоритм шифрування. Це можуть бути як, наприклад, символи англійської мови, так і цифри десяткової системи вирахування, при цьому вхідний текст перетвориться відповідно до обраного алфавіту. Слід урахувати, що така послідовність має довжину, яка дорівнює відкритому тексту. Її іноді називають *гамою*.

Шифрування й розшифрування може, наприклад, здійснюватися шляхом модульного додавання символу відкритого тексту із символом гами. Стійкість потокових алгоритмів шифрування залежить від того, наскільки вироблена гама буде мати властивість рівноймовірності появи чергового символу.

Потокові алгоритми мають високу швидкість шифрування, однак при їхнім *програмному* використанні виникають певні труднощі, що звужує область їх практичного застосування.

Слід зазначити, що в останні роки на базі вдосконалювання електронних технологій з'явилися нові теоретичні розробки в області *квантової криптографії*, заснованої на принципах невизначеності Гейзенберга.

Усе різноманіття існуючих криптографічних методів можна звести до таких класів перетворень рис. 6.3.

Перестановки – метод криптографічного перетворення, що полягає в перестановці символів вихідного тексту за більш чи менш складним правилом. Використовується, як правило, в сполученні з іншими методами.

Системи підстановок – найбільш простий вид перетворень, що полягає в заміні символів вихідного тексту на інші (того ж алфавіту) за більш чи менш складним правилом. Для забезпечення високої криптостійкості потрібне використання великих ключів.

Рис. 6.3. Класифікація симетричних криптосистем

Гамування є криптографічним перетворенням, яке широко використовується. Принцип шифрування гамуванням полягає в генерації гами шифру за допомогою датчика псевдовипадкових чисел і накладенні отриманої гами на відкриті дані (наприклад, використовуючи додавання за модулем 2).

Широко використовується *блокове* шифрування, яке являє собою послідовність (з можливим повторенням і чергуванням) основних методів перетворення, що застосовуються до блоку (частини) тексту, який шифрується. Блокові шифри на практиці зустрічаються частіше, ніж «чисті» перетворення того чи іншого класу, через їх більш високу криптостійкість. Російський і американський стандарти шифрування базуються саме на цьому класі шифрів.

Хоч би якими складними і надійними були криптографічні системи, їх слабке місце при практичній реалізації – проблема розподілу ключів. Для того щоб був можливий обмін конфіденційною інформацією між двома суб'єктами ІС, ключ повинен бути згенерований одним із них, а потім якимось чином знову ж у конфіденційному порядку переданий іншому. Тобто у загальному випадку для передачі ключа знову ж потрібне використання якоїсь криптосистеми.

6.3. Методи перестановки і заміни

Нехай потрібно зашифрувати наступне повідомлення (відкритий текст):

DEAR DAD SEND MORE MONEY AS SOON AS POSSIBLE TOM

«Дорогий тато. Якомога швидше прийшли ще грошей. Том.»

Один зі способів шифрування – *проста заміна*, при якій кожна буква відкритого тексту заміняється на якусь букву алфавіту (можливо, на ту ж саму). Для цього відправник повідомлення повинен знати, на яку букву в шифротексті слід замінити кожну букву відкритого тексту. Часто це робиться шляхом відомості потрібних відповідностей букв у вигляді двох алфавітів, наприклад так, як показано нижче.

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

Шифрограма отримується шляхом заміни кожної букви відкритого тексту на записану безпосередньо під нею букву шифрувального алфавіту.

ESBM EBE

HGSBPS PSDE AFMS AFDSY BP PFFD BP HFPPKLGS QFA

Дві алфавітні послідовності, що використовуються в процесі шифрування, називаються, відповідно, відкритим і шифрувальним компонентом системи. Щоб одержувач шифрограми міг відновити відкритий текст і прочитати повідомлення, йому необхідно мати копію вищенаведеної таблиці. Дешифрувальник повторює у зворотному порядку всі дії шифрувальника, розкриваючи тим самим зміст повідомлення.

У вищенаведеному прикладі використовувався алгоритм побуквеної заміни. Цей метод називається простий, або моноалфавітної заміною. Ключ до даного шифру складається з таблиці, що містить відкритий і шифрувальний алфавіти, у якій вказується, на яку букву в шифротексті слід замінити букву відкритого тексту. У такій криптографічній системі передбачається, що алгоритм шифрування загальновідомий, тоді як ключ доступний тільки відправникові й одержувачеві відповідних повідомлень.

У відкритому алфавіті букви розташовані в їх звичайній послідовності; такий алфавіт називається прямій стандартною послідовністю. Шифрувальний же алфавіт у нашому прикладах складається з 26 букв латинського алфавіту, певним чином переставлених з використанням ключового слова BLUESTOCKING (букв. «синя панчоха»). Після ключового слова (ключової фрази) ключ далі записується з опущенням усіх тих букв, що вже з’явилися в цім слові (або в першому слові цієї фрази), а потім уписуються букви, що залишаються, алфавіту у звичайному порядку, знову ж з опущенням усіх букв, що раніше з’явилися. Так, якщо в якості ключової ми використовуємо фразу UNITED STATES OF AMERICA, те шифрувальний алфавіт буде виглядати в такий спосіб:

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

За допомогою ключового слова (фрази) при шифруванні можна перемішати будь-яку алфавітну послідовність. Використання ключових слів полегшує відновлення відкритого й шифрувального компонента системи, оскільки при цьому необхідно запам’ятати тільки відповідне ключове слово (фразу). Немає необхідності записувати (або розгадувати) які б то ні було таблиці: якщо пам’ятати ключове слово, то алфавітну послідовність завжди можна відновити по пам’яті.

У вищенаведеній шифрограмі між словами збережені пробіли, однак шифровку можна зробити більш захищеною (або, як говорять криптографи, стійкою, або стійкою до злому; шифр уважається тим більше стійким, чим довше він не піддається розкриттю) шляхом видалення міжслівних пробілів з остаточного шифротекста. Згідно з практикою, шифротекст прийнято ділити на групи з п’яти букв кожна. (Колись телеграфні компанії при стягненні плати кожну

групу з п’яти букв уважали як одне слово відкритого тексту.) Якщо забрати пробіли між словами, то нашу шифрограму можна було б записати так:

ESBME BEMGS BPSPS DEAFM SAFDS YBPPF FDBPH FPPKL GSQFA

Іншим найважливішим шифрувальним алгоритмом є *перестановка*. У шифрі перестановки всі букви відкритого тексту залишаються без змін, але переставляються згідно із заздалегідь визначеним правилом. Тут також може використовуватися ключ, керуючий процедурою шифрування. Так, використовуючи в якості ключа слово PANAMA, ми могли б зашифрувати вищезгаданий відкритий текст у такий спосіб.

Ключ	P A N A M A
Числова послідовність	6 1 5 2 4 3
Блок перестановки	D E A R D A
	D P L E A S
	E S E N D M
	O N E Y A S
	S O O N A S
	P O S S I B
	L E T O M
Шифрограмма	EPSNO OEREN YNSOA SMSSB
	DADAA IMALE EOSTD DEOSP L

У цьому прикладі ключове слово використане для одержання шифрувальної числової послідовності шляхом нумерації букв ключового слова (відносно один одного) у порядку їх проходження ліворуч праворуч у стандартному алфавіті. Далі під числовою послідовністю в рядках, рівних по довжині ключовому слову, записаний відкритий текст. У процесі шифрування текст виписується вже по окремих стовпцях у порядку, обумовленому даної числовою послідовністю.

Цей метод перестановки називається перестановкою стовпців, але можна обрати й інші «маршрути» перестановки, наприклад виписувати шифротекст випливаючи по діагоналі (ліворуч праворуч або праворуч ліворуч, або ж чергуючи лівий і правий напрямку) або по спіралі тощо. Крім того, букви шифротексту можуть записуватися у вигляді різних геометричних фігур або будь-якими іншими способами. Один з них полягає в подвійному шифруванні шляхом повторної перестановки стовпців. При цьому й у першому, і в другому блоках перестановки може бути використане те саме ключове слово, хоча краще використовувати різні ключові слова. Такий шифр, що називається подвійний перестановкою, одержав широке поширення в XX ст.

6.4. Реалізація алгоритмів шифрування

Проблема реалізації методів захисту включає два аспекти:

1) розробку засобів, що реалізують криптографічні алгоритми;
2) методику використання цих засобів.

Будь-який криптографічний метод може бути реалізовано трьома методами: програмним, апаратним, або програмно-апаратним.

Перед тем, як перейти безпосередньо до розгляду переваг і недоліків перерахованих типів реалізації, сформулюємо загальні вимоги до реалізації криптографічних алгоритмів. Сучасні алгоритми шифрування повинні задовольняти наступним умовам:

– повинні бути адаптовані до новітньої програмно-апаратної бази (наприклад, алгоритми блокового шифрування в програмній реалізації повинні бути адаптовані до операцій з 64-розрядними числами);

– обсяг ключа повинен відповідати сучасним методам і засобам дешифрування зашифрованих повідомлень;

– операції шифрування й розшифрування повинні, по можливості, бути простими, щоб задовольняти сучасним вимогам до швидкісних характеристик;

– не повинні допускати появи постійно зростаючого числа помилок;

– повинні зводити до мінімуму обсяг повідомлення в ході виконання операцій шифрування.

Програмна реалізація

Можливість програмної реалізації обумовлена тим, що всі методи криптографічного перетворення формальні й можуть бути представлені у вигляді кінцевої алгоритмічної процедури.

До переваг програмної реалізації можна віднести її гнучкість і транспортованість. Інакше кажучи, програма, написана під одну операційну систему, може бути модифікована під будь-який тип операційної системи. Крім того, обновити програмне забезпечення можна з меншими часовими й фінансовими витратами. До того ж багато сучасних досягнень в області криптографічних протоколів недоступні для реалізації у вигляді апаратних засобів.

До недоліків програмних засобів криптографічного захисту слід віднести можливості втручання в дію алгоритмів шифрування й одержання доступу до ключової інформації, що зберігається в загальнодоступній пам’яті. Ці операції звичайно виконуються за допомогою простого набору програмних інструментів. Так, наприклад, у багатьох операційних системах здійснюється аварійний дамп пам’яті на жорсткий диск, при цьому в пам’яті можуть перебувати ключі, знайти які не важко буде. Таким чином, слабка фізична захищеність програмних засобів є одним з основних недоліків подібних методів реалізації алгоритмів шифрування.

Апаратна реалізація

При апаратній реалізації всі процедури шифрування й дешифрування виконуються спеціальними електронними схемами. При цьому неодмінним компонентом усіх апаратно реалізованих методів є гамування. Це пояснюється тим, що метод гамування поєднує в собі високу криптостійкість і простоту реалізації.

Найбільше часто в якості генератора використовується широко відомий регістр зсуву зі зворотними зв'язками (лінійними або нелінійними). Мінімальний період породжуючої послідовності рівний 2^n – 1 біт. Для підвищення якості генерованої послідовності можна передбачити спеціальний блок керування роботою регістру зсуву. Таке керування може, наприклад, полягати в тому, що після шифрування певного обсягу інформації вміст регістру зрушення циклічно змінюється.

Інша можливість поліпшення якості гамування полягає у використанні нелінійних зворотних зв'язків. При цьому поліпшення досягається не за рахунок збільшення довжини гами, а за рахунок ускладнення закону її формування. Перелічимо переваги апаратних засобів.

По-перше, апаратна реалізація має кращі швидкісні характеристики, ніж програмно реалізовані алгоритми шифрування. Використання спеціальних чіпів, адаптованих до реалізації на них процедур шифрування й розшифрування приводить до того, що, на відміну від процесів загального призначення вони дозволяють оптимізувати багато математичних операцій, застосовувані в алгоритмах шифрування.

По-друге, апаратні засоби захисту інформації мають незрівнянно більшу захищеність як від побічних електромагнітних випромінювань виникаючих у ході роботи апаратури, так і від безпосереднього фізичного впливу на пристрій, де здійснюються операції шифрування й зберігання ключової інформації. Сучасні мікросхеми, на яких реалізуються алгоритми шифрування й здійснюється зберігання ключової інформації, здатні успішно протистояти будь-яким спробам фізичного впливу – у випадку виявлення несанкціонованого доступу до мікросхеми вона саморуйнується.

По-третє, апаратні засоби більш зручні в експлуатації, тому що дозволяють здійснювати операції шифрування й розшифрування для користувача в прозорому режимі; крім того, їх легко інсталювати.

По-четверте, враховуючи різноманіття варіантів застосування засобів криптографічного захисту інформації, апаратні засоби повсюдно використовуються для захисту телефонних переговорів, відправленню факсимільних повідомлень і інших видів передачі інформації, де неможливо використовувати програмні засоби.

Програмно-апаратна реалізація

Останнім часом стали з'являтися комбіновані засоби шифрування, т.зв. програмно-апаратні засоби. У цьому випадку в комп'ютері використовується

своєрідний «криптографічний співпроцесор» – обчислювальний пристрій, орієнтоване на виконання криптографічних операцій (додаванні по модулю, зрушення і т.д.). Міняючи програмне забезпечення для такого пристрою, можна вибрати той або інший метод шифрування.

Основними функціями, покладеними на апаратну частину програмно – апаратного комплексу криптографічного захисту інформації, звичайно є генерація ключової інформації і її зберігання в пристроях, захищених від несанкціонованого доступу з боку зловмисника. Крім того, за допомогою методик такого типу можна здійснювати аутентифікацію користувачів за допомогою паролів (статичних або динамічно змінюваних, які можуть зберігатися на різних носіях ключової інформації), або на основі унікальних для кожного користувача біометричних характеристик. Пристрій зчитування подібних відомостей можуть входити до складу програмно – апаратної реалізації засобів захисту інформації.

Контрольні питання

1. Визначте поняття «криптографія», «криптологія», «стеганографія», «шифротекст», «криптограф», «криптоаналіз», «ключ», «криптостійкість».
2. Назвіть розділи сучасної криптографії.
3. Яка відмінність симетричних та асиметричних криптографічних систем?
4. Назвіть основні вимоги до криптографічних систем.
5. Назвіть типи шифрів заміни.
6. Поясність сутність методів заміни та перестановки?
7. Класифікація алгоритмів шифрування.

Література для самопідготовки

1. Бобунов А.І. Захист інформації в автоматизованих системах / Бобунов А.І., Шестаков В.І. Захист інформації в автоматизованих системах: Навчальний посібник. – Житомир: ЖВІРЕ, 2004. – С. 120–141.
2. Антонюк А.О. Основи захисту інформації в автоматизованих системах управління / Антонюк А.О. – Київ: Видавничий дім "КМ академія", 2003.– С. 108–126.
3. Малюк А.А. Введение в защиту информации в автоматизированных системах / Малюк А.А., Пазизин С.В., Погожин Н.С. – М.: Горячая линия-Телеком, 2001. – С. 52–77.
4. Завгородний В.И. Комплексная защита информации в компьютерных системах: учебное пособие / Завгородний В.И. . – М.: Логос; ПБОЮЛ Н.А. Егоров, 2001. – С. 133–138.

ЛЕКЦІЯ 7. СИСТЕМИ ШИФРУВАННЯ ІЗ ВІДКРИТИМ КЛЮЧЕМ

7.1. Основні відомості про системи шифрування із відкритим ключем. Алгоритм RSA.

7.2. Алгоритм Діффі-Хеллмана.

7.3 Алгоритм Ель-Гамаля.

7.1. Основні відомості про системи шифрування із відкритим ключем. Алгоритм RSA

Хоч би якими складними і надійними були криптографічні системи, їх слабке місце при практичній реалізації – це проблема розподілу ключів. Для того щоб був можливий обмін конфіденційною інформацією між двома суб'єктами АСУ, ключ повинен бути згенерований одним із них, а потім якимось чином знову ж у конфіденційному порядку переданий іншому. Тобто, у загальному випадку для передачі ключа знову ж потрібне використання якоїсь криптосистеми.

Для вирішення цієї проблеми на основі результатів, отриманих класичною і сучасною алгеброю, були запропоновані СВК.

Суть їх полягає в тому, що кожним адресатом АСУ генеруються два ключі, зв'язані між собою за певним правилом. Один ключ є відкритим, а інший – закритим. *Відкритий* ключ публікується і доступний кожному, хто бажає послати повідомлення адресату. *Секретний* ключ зберігається в таємниці.

Вихідний текст шифрується відкритим ключем адресата і передається йому. Зашифрований текст у принципі не може бути розшифрований тим же відкритим ключем. Дешифрування повідомлення можливе тільки з використанням закритого ключа, що відомий тільки самому адресату.

Криптографічні системи з відкритим ключем використовують так звані необоротні чи однобічні функції, що мають таку властивість: при заданому значенні x відносно просто обчислити значення $f(x)$, однак якщо $y = f(x)$, то немає простого шляху для обчислення значення x.

Вимоги до СВК:

1. Перетворення вихідного тексту має бути необоротним і виключати його відновлення на основі відкритого ключа.

2. Визначення закритого ключа на основі відкритого також повинне бути неможливим на сучасному технологічному рівні. При цьому бажана точна нижня оцінка складності (кількості операцій) розкриття шифру.

Алгоритми шифрування з відкритим ключем набули значного поширення в сучасних АС. Так, алгоритм RSA став світовим стандартом де-факто для відкритих систем. Взагалі ж усі запропоновані сьогодні криптосистеми з відкритим ключем спираються на один з таких типів необоротних перетворень:

1. Розкладання великих чисел на прості множники.

2. Обчислення логарифма в скінченному полі.

3. Обчислення коренів алгебраїчних рівнянь.

Тут же слід зазначити, що алгоритми криптосистеми СВК можна використовувати за трьома призначеннями.

1) як самостійні засоби захисту переданих і збережених даних;

2) як засоби для розподілу ключів. Алгоритми СВК більш трудомісткі, ніж традиційні криптосистеми, тому часто на практиці раціонально за допомогою СВК розподіляти ключі, обсяги яких як інформації незначні. А потім за допомогою звичайних алгоритмів здійснювати обмін великими інформаційними потоками.

3) як засоби аутентифікації користувачів.

Нижче розглядаються найбільш розповсюджені системи з відкритим ключем. Незважаючи на досить велике число різних СВК, найбільш популярний ***криптосистема RSA***, розроблена в 1977 році, яка отримала назву на честь її розробникыв: Рона Рівеста, Аді Шаміра і Леонарда Адлемана. Алгоритм RSA використовується в банківських комп'ютерних мережах, особливо для роботи з віддаленими клієнтами (обслуговування кредитних карток).

Розглянемо математичні результати, що покладені в основу цього алгоритму.

Теорема 1. (Мала теорема Ферма.) Якщо p – просте число, то $x^{p-1} = 1 \pmod p$ для будь-якого x, простого відносно p, і $x^p = x \pmod p$ для будь-якого x.

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

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

Теорема 2. Якщо $n = pq$ (p і q – відмінні одне від одного простічисла), то

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

Теорема 3. Якщо $n = pq$ (p і q – відмінні одне від одного простічисла) і x – просте відносно p і q, то

$$x^{\varphi(n)} = 1(\mathrm{mod}\, n).$$

Наслідок. Якщо $n = pq$ (p і q – відмінні одне від одного простічисла) і e просте відносно $\varphi(n)$, то відображення

$$E(e,n): x \to x^e (\mathrm{mod}\, n)$$

є взаємно однозначним на алфавіті Z_n.

Користувач i вибирає пару різних простих p_i і q_i – і розраховує пари цілих (e_i, d_i), що є простими відносно $\varphi(n_i)$, де $n_i = p_i q_i$. Довідкова таблиця містить публічні ключі $\{(e_i, n_i)\}$.

Користувач i зашифровує текст N при передачі його користувачеві j, застосовуючи до n відображення $E(d_i, n_i)$:

$$N \to E(d_i, n_i) N = N'.$$

Користувач j робить дешифрування N', застосовуючи $E(e_i, n_i)$:

$$N' \to E(e_i, n_i) N' = E(e_i, n_i) N = N.$$

Очевидно, для того щоб знайти інверсію $E(d_i, n_i)$ стосовно $E(e_i, n_i)$,потрібно знати множники $n = p_i q_i$. Час виконання найкращих з відомих алгоритмів розкладання при $n=10^{100}$ на сьогоднішній день виходить за межі сучасних технологічних можливостей.

Розглянемо приклад, що ілюструє застосування алгоритмуRSA. Нехай необхідно зашифрувати повідомлення "CAB". Будемо використовувати маленькі числа (на практиці застосовуються набагато більші).

1. Виберемо $p = 3$ і $q = 11$.

2. Визначимо $n = 3 \cdot 11 = 33$.

3. Знайдемо $(p-1)(q-1) = 20$. Отже, як d, взаємно просте з 20, наприклад, виберемо $d = 3$.

4. Виберемо число e. Як таке число може бути взяте будь-яке число, для якого задовольняється співвідношення $(e \cdot 3)(\mathrm{mod}\, 20) = 1$, наприклад 7.

5. Представимо повідомлення, яке потрібно шифрувати, як послідовність цілих чисел за допомогою відображення: A→1, B→2, C→3. Тоді повідомлення набуває вигляду (3, 1, 2). Зашифруємо повідомлення за допомогою ключа $\{7, 33\}$.

$ШТ1 = (3^7)(\mathrm{mod}\, 33) = 2187(\mathrm{mod}\, 33) = 9;$

$ШТ2 = (1^7)(\mathrm{mod}\, 33) = 1(\mathrm{mod}\, 33) = 1;$

$ШТ3 = (2^7)(\mathrm{mod}\, 33) = 128(\mathrm{mod}\, 33) = 29.$

6. Розшифруємо отримане зашифроване повідомлення *(9, 1, 29)* на основі закритого ключа $\{3, 33\}$. Отримаємо вихідний текст:

$$BT1 = \left(9^3\right)\left(\mathrm{mod}\,33\right) = 729\left(\mathrm{mod}\,33\right) = 3;$$

$$BT2 = \left(1^3\right)\left(\mathrm{mod}\,33\right) = 1\left(\mathrm{mod}\,33\right) = 1;$$

$$BT3 = \left(29^3\right)\left(\mathrm{mod}\,33\right) = 24389\left(\mathrm{mod}\,33\right) = 2.$$

7.2. Алгоритм Діффі-Хеллмана

Перша публікація даного алгоритму з'явилася в 70-х рр. XX ст. в статті Діффі і Хеллмана, в якій вводилися основні поняття криптографії з відкритим ключем. Алгоритм Діффі-Хеллмана не застосовується для шифрування повідомлень або формування електронного підпису. Його призначення – у розподілі ключів. Він дозволяє двом або більше користувачам обмінятися без посередників ключем, який може бути використаний потім для симетричного шифрування.

Це була перша криптосистема, яка дозволяла захищати інформацію без використання секретних ключів, переданих по захищених каналах. Схема відкритого розподілу ключів, запропонована Діффі і Хеллманом, здійснила справжню революцію в світі шифрування, так як знімала основну проблему класичної криптографії – проблему розподілу ключів.

Алгоритм заснований на складності обчислень дискретних логарифмів. У цьому алгоритмі, як і в багатьох інших алгоритмах з відкритим ключем, обчислення проводяться за модулем деякого великого простого числа *P*. Спочатку спеціальним чином підбирається деяке натуральне число *A*, менше *P*. Якщо ми хочемо зашифрувати значення *X*, то обчислюємо:

$$Y = A^X \bmod P.$$

Причому, маючи *X*, обчислити *Y* легко. Зворотнє завдання обчислення *X* з *Y* є досить складним. Експонента *X* називається *дискретним логарифмом Y*. Таким чином, знаючи про складність обчислення дискретного логарифма, число *Y* можна відкрито передавати будь-яким каналом зв'язку, так як при великому модулі *P* вихідне значення X підібрати буде практично неможливо. На цьому математичному факті заснований алгоритм Діффі-Хеллмана для формування ключа.

Формування загального ключа

Нехай два користувачі, яких умовно назвемо користувач 1 і користувач 2, бажають сформувати спільний ключ для алгоритму симетричного шифрування. Спочатку вони повинні вибрати велике просте число P_i деяке спеціальне число *A*, *1 <A <P-1*, таке, що всі числа з інтервалу [*1, 2, ..., P-1*] можуть бути представлені як різні степені *A mod P*. Ці числа мають бути відомі всім абонентам системи і можуть вибиратися відкрито. Це будуть так звані *загальні параметри*.

Потім перший користувач вибирає число X_1 *(X 1 <P)*, яке бажано формувати за допомогою датчика випадкових чисел. Це буде закритий ключ першого

користувача, і він повинен триматися в секреті. На основі закритого ключа користувач 1 обчислює число:

$$Y_1 = A^{X_1} \bmod P,$$

яке він посилає другому абоненту.

Аналогічно робить і другий користувач, генеруючи X_2 і обчислюючи:

$$Y_2 = A^{X_2} \bmod P.$$

Це значення користувач 2 відправляє першому користувачу. Після цього у користувачів повинна бути інформація, зазначена в табл. 7.1.

Таблиця 7.1

	Загальні параметри	Відкритий ключ	Закритий ключ
Користувач 1	*P, A*	Y_1	X_1
Користувач 2		Y_2	X_2

З чисел Y_1 і Y_2, а також своїх закритих ключів кожен з абонентів може сформувати загальний секретний ключ Z для сеансу симетричного шифрування. Ось як це має зробити перший користувач:

$$Z = \left(Y_2\right)^{X_1} \bmod P.$$

Ніхто інший окрім користувача 1 цього зробити не може, так як число X_1 секретне. Другий користувач може отримати те ж саме число Z, використовуючи свій закритий ключ і відкритий ключ свого абонента у такий спосіб:

$$Z = \left(Y_1\right)^{X_2} \bmod P.$$

Якщо весь протокол формування загального секретного ключа виконаний вірно, значення Z у одного і другого абонента повинні вийти однаковими. Причому, що найважливіше, противник, не знаючи секретних чисел X_1 і X_2, не зможе обчислити число Z. Не знаючи X_1 і X_2, зловмисник може спробувати вирахувати Z, використовуючи тільки передавані відкрито P, A, Y_1 і Y_2.

Безпека формування загального ключа в алгоритмі Діффі-Хеллмана випливає з того факту, що, хоча відносно легко обчислити експоненти по модулю простого числа, дуже важко обчислити дискретні логарифми. Для великих простих чисел розміром сотні і тисячі біт завдання вважається невирішеним, оскільки вимагає колосальних витрат обчислювальних ресурсів.

Користувачі 1 і 2 можуть використовувати значення Z в якості секретного ключа для шифрування і розшифрування даних. Таким же чином будь-яка пара абонентів може обчислити секретний ключ, відомий тільки їм.

Приклад обчислень за алгоритмом. Нехай два абоненти, бажаючі обмінюватися через Інтернет зашифрованими повідомленнями, вирішили сформувати секретний ключ для чергового сеансу зв’язку. Нехай вони мають такі загальні параметри:

$$P = 11,\ A = 7.$$

Кожен абонент вибирає секретне число X і обчислює відповідне йому відкрите число Y. Нехай обрані

$$X_1 = 3, X_2 = 9.$$

Обчислюємо:

$$Y_1 = 7^3 \bmod 11 = 2,$$
$$Y_2 = 7^9 \bmod 11 = 8.$$

Потім користувачі обмінюються відкритими ключами Y_1 і Y_2. Після цього кожен з користувачів може обчислити загальний секретний ключ:

користувач 1: $Z = 8^3 \bmod 11 = 6$;

користувач 2: $Z = 2^9 \bmod 11 = 6$.

Тепер вони мають загальний ключ 6, який не передавався по каналу зв'язку.

Питання практичного використання алгоритму Діффі-Хеллмана

Для того, щоб алгоритм Діффі-Хеллмана працював правильно, тобто обидва користувачі, що беруть участь в протоколі, отримували одне і те ж число Z, необхідно правильним чином вибрати число A, використовуване в обчисленнях. Число A повинно володіти наступним властивістю: всі числа виду $A \bmod P$, $A^2 \bmod P$, $A^3 \bmod P$,... , $A^{P-1} \bmod P$ повинні бути різними і складатися з цілих позитивних значень в діапазоні від 1 до $P-1$ з деякими перестановками. Тільки в цьому випадку для будь-якого цілого $Y < P$ і значення A можна знайти єдину експоненту X, таку, що:

$$Y = A^X \bmod P, \text{ де } 0 <= X <= (P - 1).$$

При довільно заданому P завдання вибору параметра A може виявитися складним завданням, пов'язаної з розкладанням на прості множники числа $P-1$. На практиці можна використовувати наступний підхід, рекомендований фахівцями. Просте число P вибирається таким, щоб виконувалась рівність $P = 2q + 1$, де q – це також просте число. Тоді в якості A можна взяти будь-яке число, для якого справедливі нерівності:

$$1 < A < P-1 \text{ і } A^q \bmod P \neq -1.$$

На підбір відповідних параметрів A і P необхідно деякий час, однак це звичайно не критично для системи зв'язку і не уповільнює її роботу. Ці параметри є загальними для цілої групи користувачів. Вони, зазвичай, вибираються один раз при створенні спільноти користувачів, які хочуть використовувати протокол Діффі-Хеллмана і не змінюються в процесі роботи. А значення закритих ключів рекомендується кожен раз міняти і вибирати їх за допомогою генераторів псевдовипадкових чисел.

Слід зауважити, що даний алгоритм, як і всі алгоритми асиметричного шифрування, уразливий для атак типу «man-in-the-middle» («людина в середині»). Якщо супротивник має можливість не тільки перехоплювати повідомлення, але і замінювати їх іншими, він може перехопити відкриті ключі учасників, створити свою пару відкритого та закритого ключа і послати кожному з учасників свій відкритий ключ. Після цього кожен учасник обчислить ключ, який буде спільним з супротивником, а не з іншим учасником.

7.3. Алгоритм Ель-Гамаля

Асиметричний алгоритм, запропонований в 1985 р. Ель-Гамалем (T. ElGamal), універсальний. Він може бути використаний для вирішення всіх трьох основних завдань: для шифрування даних, для формування цифрового підпису і для узгодження спільного ключа. Крім того, можливі модифікації алгоритму для схем перевірки пароля, доказу ідентичності повідомлення й інші варіанти. Безпека цього алгоритму, так само як і алгоритму Діффі-Хеллмана, заснована на труднощі обчислення дискретних логарифмів. Цей алгоритм фактично використовує схему Діффі-Хеллмана, щоб сформувати загальний секретний ключ для абонентів, що передають один одному повідомлення, і потім повідомлення шифрується шляхом множення його на цей ключ.

І в разі шифрування, і в разі формування цифрового підпису кожному користувачеві необхідно згенерувати пару ключів. Для цього, так само як і в схемі Діффі-Хеллмана, обираються деяке велике просте число P і число A, такі, що різні степені A представляють собою різні числа по модулю P. Числа P і A можуть передаватися у відкритому вигляді і бути загальними для всіх абонентів мережі.

Потім кожен абонент групи вибирає своє секретне число X_i, $1<X_i<P-1$, і обчислює відповідне йому відкрите число $Y_i : Y_i = A^{X_i} \bmod P$. Таким чином, кожен користувач може згенерувати закритий ключ X_i і відкритий ключ Y_i. Інформація про необхідні параметри системи зведена в наступну табл. 7.2.

Таблиця 7.2

	Загальні параметри	Відкритий ключ	Закритий ключ
Користувач 1	P, A	Y_1	X_1
...		...	...
Користувач і		Y_i	X_i

Шифрування

Тепер розглянемо, яким чином проводиться шифрування даних. Повідомлення, призначене для шифрування, повинне бути презентовано у вигляді одного числа або набору чисел, кожне з яких менше P. Нехай користувач 1 хоче передати користувачеві 2 повідомлення m. У цьому випадку послідовність дій наступна.

Перший користувач вибирає випадкове число k, взаємно просте з $P-1$, і обчислює числа:

$$r = A^k \bmod P,\ e = mY_2^k \bmod P.$$

де Y_2 – відкритий ключ користувача 2; число k тримається в секреті.

Пари чисел (r, e), що є шифротекстом, передається другому користувачеві. Другий користувач, одержавши (r, e), для розшифрування повідомлення обчислює:

$$m = e \cdot r^{P-1-X_2} \bmod P.$$

де X_2 – закритий ключ користувача 2.

У результаті він одержує вихідне повідомлення *m*. Якщо зловмисник довідається або перехопить *P, A, Y_2, r, e*, то він не зможе по них розкрити *m*. Це пов'язано з тим, що супротивник не знає параметр *k*, обраний першим користувачем для шифрування повідомлення m. Обчислити яким-небудь чином число *k* практично неможливо, тому що це завдання дискретного логарифмування.

Отже, зловмисник не може обчислити й значення *m*, тому що *m* було помножено на невідоме йому число. Супротивник також не може відтворити дії законного одержувача повідомлення (другого абонента), тому що йому не відомий закритий ключ X_2 (обчислення X_2 на основі Y_2 – також завдання дискретного логарифмування).

За аналогічним алгоритмом може проводитися й узгодження ключа, що використовується для симетричного шифрування більших обсягів даних. Більш того, алгоритм Ель-Гамаля на практиці доцільно використовувати саме для узгодження загального ключа сесії, а не прямого шифрування більших повідомлень. Це пов'язано з тим, що в алгоритмі використовуються операції зведення в ступінь і множення по великому модулю. Так само, як і в алгоритмах RSA і Діффі-Хеллмана, операції проводяться над більшими, що складаються із декількох сотень або тисяч біт, числами. Тому шифрування більших повідомлень проводиться вкрай повільно.

Приклад шифрування. Нехай два абоненти, що обмінюються через Інтернет зашифрованими повідомленнями, мають наступні загальні параметри:

$$P = 11, A = 7.$$

Крім того, користувачі 1 і 2 мають пари закритих і відкритих ключів.

Користувач 1: закритий ключ $X_1 = 3$, відкритий ключ $Y_1 = 7^3 \bmod 11 = 2$,

Користувач 2: закритий ключ $X_2 = 9$, відкритий ключ $Y_2 = 7^9 \bmod 11 = 8$.

Перший абонент хоче передати другому повідомлення. Для цього перший абонент запитує із центру розподілу ключів відкритий ключ другого абонента $Y_2 = 8$. Тепер він може зашифрувати своє повідомлення, яке в числовому вигляді нехай має значення $m=9$.

Перший абонент обирає випадкове число *k*, наприклад $k = 7$. Число *k* повинне бути взаємно простим з $P-1$. Значення $k = 7$ не має спільних дільників з $P-1=10$, отже, воно підходить. Перший абонент шифрує своє повідомлення за формулами:

$$r = A^k \bmod P = 7^7 \bmod 11=6;$$

$$e = m\, Y_2^{\,k} \bmod P = 9 * 8^7 \bmod 11 = 7.$$

Пара чисел (6,7) буде представляти собою шифротекст і передається другому користувачеві. Другий користувач, одержавши (6,7) і використовуючи свій закритий ключ $X_2 = 9$ для розшифрування повідомлення, обчислює:

$$m = e \cdot r^{P-1-X_2} \bmod P = 7 \cdot 6^{11-1-9} \bmod 11 = 7 \cdot 6^1 \bmod 11 = 9.$$

У результаті він дійсно одержує вихідне повідомлення *m*.

Контрольні питання

1. Визначте поняття «відкритий ключ», «секретний ключ».
2. Криптосистема RSA.
3. Поясніть сутність алгоритму Діффі-Хеллмана?
4. Яка процедура формування загального ключа?

Література для самопідготовки

1. Бобунов А.І. Захист інформації в автоматизованих системах / Бобунов А.І., Шестаков В.І. Захист інформації в автоматизованих системах: Навчальний посібник. – Житомир: ЖВІРЕ, 2004. – С. 120–141.
2. Малюк А.А. Введение в защиту информации в автоматизированных системах / Малюк А.А., Пазизин С.В., Погожин Н.С. – М.: Горячая линия-Телеком, 2001. – С. 72-83.
3. Завгородний В.И. Комплексная защита информации в компьютерных системах: учебное пособие / Завгородний В.И. . – М.: Логос; ПБОЮЛ Н.А. Егоров, 2001. - С. 151–154.
4. Хорошко В.О. Методы и средства защиты информации / Хорошко В.О., Чекатов И. О. – Киев: ГУИКТ.– С. 336–428.

ЛЕКЦІЯ 8. ЦИФРОВИЙ ПІДПИС

8.1. Електронний підпис.
8.2. Хеш-функції та вимоги до них.
8.3. Керування ключами.

8.1. Електронний підпис

У чому полягає проблема автентифікації даних? Наприкінці звичайного листа чи документа виконавець чи відповідальна особа звичайно ставить свій підпис. Подібна дія звичайно має дві мети. По-перше, одержувач має можливість переконатися в істинності листа, звіривши підпис із наявним у нього зразком. По-друге, особистий підпис є юридичним гарантом авторства документа. Останній аспект особливо важливий при підписанні різного роду торгівельних угод, складанні доручень, зобов'язань тощо.

Якщо підробити підпис людини на папері дуже непросто, а встановити авторство підпису сучасними криміналістичними методами – це технічна деталь, то з підписом електронним все зовсім інакше. Підробити ланцюжок бітів, просто його скопіювавши, чи непомітно внести нелегальні виправлення в документ зможе будь-який користувач.

Із значним поширенням у сучасному світі електронних форм документів (у тому числі і конфіденційних) і засобів їхньої обробки особливо актуальною стала проблема встановлення дійсності й авторства безпаперової документації. Вже було показано, що з всіх переваг сучасних систем шифрування вони не дозволяють забезпечити автентифікацію даних. Тому засоби аутентифікації повинні використовуватися в комплексі із криптографічними алгоритмами.

Електронний підпис – це дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації підписувача цих даних.

Електронний цифровий підпис – вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис

накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа.

Нехай є два користувачі – Олександр і Борис. Від яких порушень і дій зловмисника повинна захищати система автентифікації?

Відмова (ренегатство). Олександр заявляє, що він не надсилав повідомлення Борисові, хоча насправді він усе-таки надсилав. Для виключення цього порушення використовується електронний (чи цифровий) підпис.

Модифікація (переробка). Борис змінює повідомлення і стверджує, що дане (змінене) повідомлення послав йому Олександр.

Підробка. Борис формує повідомлення і стверджує, що дане (змінене) повідомлення послав йому Олександр.

Активне перехоплення. Володимир перехоплює повідомлення між Олександром і Борисом з метою прихованої модифікації. Для захисту від модифікації, підробки і маскування використовуються цифрові сигнатури.

Маскування (імітація). Володимир посилає Борисові повідомлення від імені Олександра. У цьому випадку для захисту також використовується електронний підпис.

Повтор. Володимир повторює повідомлення, яке Олександр посилав раніше Борисові. Незважаючи на те, що вживаються різноманітні заходи захисту від повторів, саме на цей метод припадає більшість випадків незаконного зняття і витрати грошей у системах електронних платежів.

Найбільш дієвим методом від повторів є:

1) використання імітовставок,
2) облік вхідних повідомлень.

Іноді немає необхідності зашифровувати передане повідомлення, але потрібно його скріпити електронним підписом. У цьому випадку текст шифрується закритим ключем відправника й отриманий ланцюжок символів прикріплюється до документа. Одержувач за допомогою відкритого ключа відправника розшифровує підпис і звіряє його з текстом.

8.2. Хеш-функції та вимоги до них

Хеш-функцією називається однобічна функція, призначена для одержання *дайджесту* або «відбитків пальців» файлу, повідомлення або деякого блоку даних.

Хеш-код створюється функцією H:

$$h = H(M),$$

де M – це повідомленням довільної довжини; h – хеш-код фіксованої довжини.

Розглянемо вимоги, яким повинна відповідати хеш-функція для того, щоб вона могла використовуватися в якості аутентифікатора повідомлення. Розглянемо дуже простий приклад хеш-функції. Потім проаналізуємо кілька підходів до побудови хеш-функцій.

Хеш-функція *H*, яка використовується для аутентифікації повідомлень, повинна мати наступні властивості:

1. Хеш-функція *H* повинна застосовуватися до блоку даних будь-якої довжини.

2. Хеш-функція H створює вихід фіксованої довжини.

3. *H (M)* відносно легко (за поліноміальний час) обчислюється для будь-якого значення *M*.

4. Для будь-якого даного значення хеш-коду *h* розрахунково неможливо знайти *M* таке, що *H (M) = h*.

5. Для будь-якого даного x обчислювально неможливо знайти $y \neq x$, що *H (y) = H (x)*.

6. Обчислювально неможливо знайти довільну пару (*x*, *y*) таку, що *H (y) = H (x)*.

Перші три властивості вимагають, щоб хеш-функція створювала хеш-код для будь-якого повідомлення. Четверта властивість визначає вимога однобічності хеш-функції: легко створити хеш-код по даному повідомленню, але неможливо відновити повідомлення по даному хеш-коду. Ця властивість важлива, якщо аутентифікація з використанням хеш-функції включає секретне значення. Саме секретне значення може не посилати, проте, якщо хеш-функція не є однобічною, супротивник може легко розкрити секретне значення в такий спосіб.

При перехопленні передачі атакуючий одержує повідомлення *M* і хеш-код $C = H\ (S_{AB} \| M)$. Якщо атакуючий може інвертувати хеш-функцію, то він може одержати $S_{AB} \| M = H^{1}\ (C)$. Тому, що атакуючий тепер знає M і $S_{AB} \| M$, одержати S_{AB} зовсім просто.

П’ята властивість гарантує, що неможливо знайти інше повідомлення, чиє значення хеш-функції збігалося б зі значенням хеш-функції даного повідомлення. Це запобігає підробці аутентифікатора при використанні зашифрованого хеш-коду. У цьому випадку супротивник може читати повідомлення й створити його хеш-код. Але тому що супротивник не володіє секретним ключем, він не має можливості змінити повідомлення так, щоб одержувач цього не виявив.

Якщо дана властивість не виконується, атакуючий має можливість виконати наступну послідовність дій: перехопити повідомлення і його зашифрований хеш-код, обчислити хеш-код повідомлення, створити альтернативне повідомлення з тим самим хеш-кодом, замінити вихідне повідомлення на підроблене. Оскільки хеш-коди цих повідомлень збігаються, одержувач не виявить підміни.

Хеш-функція, яка задовольняє першим п’яти властивостям, називається *простою або слабкою хеш-функцією*. Якщо, крім того, виконується шоста властивість, то така функція називається *сильною хеш-функцією*. Шоста властивість захищає проти класу атак, відомих як атака «*день народження*».

Стандарт цифрового підпису DSS

У багатьох країнах сьогодні існують стандарти на електронний (цифровий) підпис. *Стандарт цифрового підпису DSS* (*DigitalSignature Standard* – DSS) був

прийнятий в США в 1991 р. й переглянутий в 1994 р. В основі стандарту лежить алгоритм *DSA* (*DigitalSignatureAlgorithm*), що і є варіацією підпису Ель-Гамаля. В алгоритмі використовується односпрямована хеш-функція *H(m)*. У якості хеш-алгоритму стандарт DSS передбачає використання алгоритму SHA-1.

Розглянемо сам алгоритм генерації ЕЦП. Спочатку для групи абонентів вибираються три загальні (несекретних) параметра *p*, *q* і *a*:

1) Параметр *p* повинен бути простим числом довжиною від 512 до 1024 біт.

2) q – просте число довжиною 160 біт; між *p* і *q* повинне виконуватися співвідношення $p = bq + 1$ для деякого цілого *b*. Старші біти в *p* і *q* повинні бути рівні одиниці (таким чином $2^{159} < q < 2^{160}$).

3) число *a* задовольняє нерівності $1 < a < p-1$ і є коренем рівняння $a^q mod\ p = 1$.

Знаючи ці числа, кожний абонент системи випадково вибирає число *x*, що задовольняє нерівності $0 < x < q$, і обчислює:

$$y = a^x mod\ p.$$

Число *x* буде секретним ключем користувача, а число *y* – відкритим ключем. Обчислити *y* по відомому *x* досить просто. Однак, маючи відкритий ключ *y*, обчислювально неможливо визначити *x*, який є дискретним логарифмом *y* за основою *a*.

Передбачається, що відкриті ключі всіх користувачів вказуються в деякому несекретному, але «сертифікованому» довіднику, який повинен бути в усіх, хто збирається перевіряти підписи. На цьому етап вибору параметрів закінчується і абоненти готові до того, щоб формувати й перевіряти підписи.

Нехай є повідомлення *m*, яке один з користувачів бажає підписати. Для генерації підпису користувач повинен виконати наступні дії:

1. Обчислити значення хеш-функції $h = H(m)$ для повідомлення *m*. Значення хеш-функції повинне бути в межах $0 < h < q$.
2. Потім згенерувати випадкове число k, $0 < k < q$.
3. Обчислити $r = (a^k\ mod\ p)\ mod\ q$.
4. Визначити $s = [k^{-1}(H(m) + x * r)]\ mod\ q$.

У результаті користувач одержить для повідомлення m підпис, що складається з пари чисел (*r*,*s*). Повідомлення разом з підписом може бути послане будь-якому іншому абонентові системи. Перевірити підпис можна в такий спосіб:

1. Обчислити значення хеш-функції $h = H(m)$ для повідомлення m.
2. Перевірити виконання нерівностей $0 < r < q$, $0 < s < q$.
3. Обчислити $w = s^{-1}\ mod\ q$;

$$u_1 = [H(m) * w]\ mod\ q;$$
$$u_2 = r * w\ mod\ q;$$
$$v = [(a^{u1} * y^{u2})\ mod\ p]\ mod\ q.$$

4. Перевірити виконання рівності $v = r$. Якщо $v = r$, то підпис уважається справжнім, інакше підпис уважається недійсним.

У силу складності обчислення дискретних логарифмів зловмисник не може відновити *k* з *r* або *x* з *s*, а отже, не може підробити підпис. По тій же самій

причині автор повідомлення не зможе відмовитися від свого підпису, тому що ніхто крім нього не знає закритого ключа *x*.

8.3. Керування ключами

Крім вибору придатної для конкретної АСУ криптографічної системи, важлива проблема – це керування ключами. Якою б складною і надійною не була сама криптосистема, вона базується на використанні ключів. Якщо для забезпечення конфіденційного обміну інформацією між двома користувачами процес обміну ключами тривіальний, то в АСУ, де кількість користувачів становить десятки і сотні, керування ключами – серйозна проблема.

Під *ключовою інформацією* розуміється сукупність усіх діючих у АСУ ключів. Якщо не забезпечене досить надійне керування ключовою інформацією, то, заволодівши нею, зловмисник одержує необмежений доступ до всієї інформації.

Керування ключами – інформаційний процес, що включає три елементи:

– генерацію ключів;
– накопичення ключів;
– розподіл ключів.

Розглянемо, як вони мають реалізуватися для того, щоб забезпечити безпеку ключової інформації в АСУ. На самому початку було сказано, що не варто використовувати невипадкові ключі з метою легкості їх запам’ятовування. У серйозних АСУ використовуються спеціальні апаратні і програмні методи генерації випадкових ключів. Як правило, використовують датчики псевдовипадкових чисел (ПВЧ). Однак ступінь випадковості їхньої генерації має бути досить високим. Ідеальними генераторами є пристрої на основі «натуральних» випадкових процесів. Наприклад, з’явилися серійні зразки генерації ключів на основі білого радіошуму. Іншим випадковим математичним об’єктом є десяткові знаки ірраціональних чисел, наприклад π чи e, що обчислюються за допомогою стандартних математичних методів.

У АСУ із середніми вимогами захищеності цілком прийнятні програмні генератори ключів, що обчислюють ПВЧ як складну функцію від поточного часу і/або числа, введеного користувачем.

Під *накопиченням ключів* розуміється організація їхнього збереження, обліку і видалення. Оскільки ключ є найпривабливішим для зловмисника об’єктом, що відкриває йому шлях до конфіденційної інформації, то питанням накопичення ключів варто приділяти особливу увагу.

Секретні ключі ніколи не повинні записуватися в явному вигляді на носій, що може бути зчитаний чи скопійований.

У досить складній АСУ один користувач може працювати з великим обсягом ключової інформації, й іноді навіть виникає необхідність організації міні-баз даних з ключовою інформацією. Такі бази даних відповідають за прийняття, збереження, облік, і видалення використовуваних ключів.

Отже, кожна інформація про використовування ключів повинна зберігатися в зашифрованому вигляді. Ключі, що зашифровують ключову інформацію, називаються *майстер-ключами*. Бажано, щоб майстри-ключі кожен користувач знав напам'ять і не зберігав їх узагалі на яких-небудь матеріальних носіях.

Дуже важливою умовою безпеки інформації є періодичне відновлення ключової інформації в ІС. При цьому перепризначуватися повинні як звичайні ключі, так і майстри-ключі. В особливо відповідальних АСУ відновлення ключової інформації бажано робити щодня.

Питання відновлення ключової інформації пов'язане і з третім елементом керування ключами – розподілом ключів. *Розподіл ключів* – найвідповідальніший процес у керуванні ключами. До нього висуваються дві вимоги:

1. Оперативність і точність розподілу.

2. Таємність ключів, що розподіляються.

Останнім часом помітне зрушення у бік використання криптосистем з відкритим ключем, у яких проблема розподілу ключів відпадає. Проте розподіл ключової інформації в АСУ вимагає нових ефективних рішень.

Розподіл ключів між користувачами реалізується двома різними підходами:

1. Шляхом *створення одного чи кількох центрів розподілу ключів*. Недолік такого підходу полягає в тому, що в центрі розподілу відомо, кому і які ключі призначені, і це дозволяє читати всі повідомлення, що циркулюють у АСУ. Можливі зловживання істотно впливають на захист.

2. *Прямий обмін ключами* між користувачами АСУ. У цьому випадку проблема полягає в тому, щоб надійно засвідчити дійсність суб'єктів

В обох випадках повинна бути гарантована *дійсність сеансу зв'язку*. Це можна забезпечити двома способами:

1) *механізм запиту-відповіді*, що полягає в такому. Якщо користувач А бажає бути впевненим, що повідомлення, які він одержує від В, не є помилковим, він включає в повідомлення, що посилається для В, непередбачений елемент (запит). При відповіді користувач В повинен виконати певну операцію над цим елементом (наприклад, додати 1). Це неможливо здійснити заздалегідь, тому що невідомо, яке випадкове число прийде в запиті. Після одержання відповіді з результатами дій користувач А може бути впевнений, що сеанс є справжнім. Недоліком цього методу є можливість встановлення, хоча і складної, закономірності між запитом і відповіддю.

2) *механізм оцінки часу* («часовий штемпель»). Він передбачає фіксацію часу для кожного повідомлення. У цьому випадку кожен користувач ІС може знати, наскільки «старим» є повідомлення, що надійшло.

В обох випадках варто використовувати шифрування, щоб бути впевненим, що відповідь надіслана не зловмисником і штемпель оцінки часу не змінений. При використанні оцінок часу постає проблема припустимого часового інтервалу затримки для підтвердження дійсності сеансу. Адже повідомлення з «часовим штемпелем» у принципі не може бути передане миттєво. Крім цього, комп'ютерні

годинники одержувача і відправника не можуть бути абсолютно синхронізовані. Яке запізнення «штемпеля» вважати підозрілим?

Тому в реальних АСУ, наприклад, системах оплати кредитних карток, використовується саме другий механізм встановлення дійсності і захисту від підробок. Використовуваний інтервал становить від однієї до декількох хвилин. Велика кількість відомих способів крадіжки електронних грошей базується на «вклинюванні» у цей проміжок з підробленими запитами на зняття грошей. Для обміну ключами можна використовувати криптосистеми з відкритим ключем, застосовуючи той же алгоритм RSA.

Як узагальнення сказаного про розподіл ключів варто наголосити, що завдання керування ключами зводиться до пошуку такого протоколу розподілу ключів, який забезпечував би:

– можливість відмови від центру розподілу ключів;
– взаємне підтвердження дійсності учасників сеансу;
– підтвердження вірогідності сеансу механізмом запиту-відповіді, використання для цього програмних чи апаратних засобів;
– використання при обміні ключами мінімального числа повідомлень.

Які проблеми та перспективи мають криптографічні системи? Однією з важливих практичних проблем є шифрування великих повідомлень і потоків даних. Ця проблема з’явилася відносно нещодавно з появою засобів мультимедіа і мереж з високою пропускною здатністю, що забезпечують передачу мультимедійних даних.

Дотепер говорилося про захист повідомлень. При цьому під ними малася на увазі скоріше деяка текстова чи символічна інформація. Однак, у сучасних АСУ застосовуються технології, що вимагають передачі істотно великих обсягів даних. Серед таких технологій:

– факсимільна, відео- і мовний зв’язок;
– голосова пошта;
– системи відеоконференцій.

Якщо порівнювати обсяги переданої інформації різних типів, то можна сказати, що обсяг текстової інформації є найменшим, обсяг звукової – у 2-3 рази більший, графічної – на порядок більший, відео – майже на два порядки.

Оскільки передача оцифрованої звукової, графічної і відеоінформації в багатьох випадках вимагає конфіденційності, то виникає проблема шифрування величезних інформаційних масивів. Для інтерактивних систем типу телеконференцій, ведення аудіо- чи відеозв’язку таке шифрування повинне здійснюватися в реальному масштабі часу і по можливості бути «прозорим» для користувачів.

Це немислимо без використання сучасних технологій шифрування. Найбільш розповсюдженим є потокове шифрування даних. Якщо в описаних раніше криптосистемах передбачалося, що на вході мається певне кінцеве повідомлення,

до якого і застосовується криптографічний алгоритм, то в системах із потоковим шифруванням принцип інший.

Система захисту не чекає, коли закінчиться передане повідомлення, а відразу ж здійснює його шифрування і передачу. Найбільш очевидним є побітове додавання вхідної послідовності (повідомлення) з деяким нескінченним чи періодичним ключем, одержуваним, наприклад, від генератора ПВЧ. Прикладом стандарту потокового шифрування є RC4, розроблений Рівестом. Однак технічні подробиці цього алгоритму тримаються в таємниці.

Іншим, іноді більш ефективним методом потокового шифрування є шифрування блоками. Тобто накопичується фіксований обсяг інформації (блок), а потім перетворений деяким криптографічним методом передається в канал зв'язку. Як було неодноразово відзначено, проблема розподілу ключів є найбільш гострою у великих ІС. Частково ця проблема вирішується (а точніше, знімається) за рахунок використання відкритих ключів. Але найбільш надійні криптосистеми з відкритим ключем типу RSA досить трудомісткі, а для шифрування мультимедійних даних і зовсім не придатні.

Оригінальні рішення проблеми «блукаючих ключів» активно розробляються фахівцями. ці системи є певним компромісом між системами з відкритими ключами і звичайними алгоритмами, для яких потрібна наявність того самого ключа у відправника й одержувача.

Ідея методу досить проста. Після того, як ключ використовується в одному сеансі, за деяким правилом він змінюється іншим. Це правило має бути відомим і відправнику, і одержувачу. Знаючи правило, після одержання чергового повідомлення одержувач теж змінює ключ. Якщо правило зміни ключів акуратно дотримується і відправником, і одержувачем, то в кожен момент часу вони мають однаковий ключ. Постійна зміна ключа ускладнює розкриття інформації зловмисником.

Основне завдання в реалізації цього методу – вибір ефективного правила зміни ключів. Найбільш простий шлях – генерування випадкового списку ключів. Зміна ключів здійснюється в порядку списку. Однак очевидно, що список доведеться якимось чином передавати.

Інший варіант — використання математичних алгоритмів, що ґрунтуються на так званих перебірних послідовностях. На множині ключів шляхом однієї і тієї ж операції над елементом отримуємо інший елемент. Послідовність цих операцій дозволяє переходити від одного елемента до іншого, поки не буде перебрана вся множина.

Найбільш доступним є використання полів Галуа. За рахунок піднесення до степеня породжуючого елемента можна послідовно переходити від одного числа до іншого. Ці числа приймаються як ключі. Ключовою інформацією в даному випадку є вихідний елемент, що перед початком зв'язку повинен бути відомий і відправнику, й одержувачу. Надійність таких методів повинна бути забезпечена з урахуванням знання зловмисником використовуваного правила зміни ключів.

Цікавим і перспективним завданням є реалізація методу «блукаючих ключів» не для двох абонентів, а для досить великої мережі, коли повідомлення пересилаються між усіма учасниками.

Три види (шифрування, кодування і стиснення інформації) перетворення інформації використовуються в різних цілях (табл. 8.1).

Таблиця 8.1

Види перетворень інформації

Вид перетворення	Мета	Зміна обсягу інформації після перетворення
Шифрування	Передача конфіденційної інформації; забезпечення автентифікації і захисту від навмисних змін	Звичайно не змінюється, збільшується лише в цифрових сигнатурах і підписах
Перешкодостійкість	Захист від спотворення перешкодами в каналах зв'язку	Збільшується
Стиснення (компресія)	Скорочення обсягу переданих чи збережених даних	Зменшується

Як видно, ці три види перетворення інформації частково доповнюють один одного і їхнє комплексне застосування допоможе ефективно використовувати канали зв'язку для надійного захисту змінюваної інформації. Особливо цікавим видасться можливість об'єднання методів кодування і шифрування. Можна стверджувати, що по суті кодування – це елементарне шифрування, а шифрування – це елементарне перешкодостійке кодування.

Інша можливість – комбінування алгоритмів шифрування і стиснення інформації. Завдання стиснення полягає в тому, щоб перетворити повідомлення в межах того самого алфавіту таким чином, щоб його довжина (кількість букв алфавіту) стала меншою, але при цьому повідомлення можна було б відновити без використання якоїсь додаткової інформації. Найбільш популярні алгоритми стиснення – RLE, коди Хаффмана, алгоритм Лемпеля-Зіва. Для стиснення графічної і відеоінформації використовуються алгоритми JPEG і MPEG.

Головне достоїнство алгоритмів стиснення з погляду криптографії полягає в тому, що вони змінюють статистику вхідного тексту убік її вирівнювання. Так, у звичайному тексті, стиснутому за допомогою ефективного алгоритму, всі символи мають однакові частотні характеристики, і навіть використання простих систем шифрування зробить текст недоступним для криптоаналізу.

Розробка і реалізація таких універсальних методів – перспектива сучасних АСУ. Проблема реалізації методів захисту інформації має два аспекти:

1) розробку засобів, що реалізують криптографічні алгоритми,
2) методику використання цих засобів.

Кожний з розглянутих криптографічних методів може бути реалізований програмним або апаратним способом. Можливість програмної реалізації

зумовлюється тим, що всі методи криптографічного перетворення формальні і можуть бути представлені у вигляді кінцевої алгоритмічної процедури.

При апаратній реалізації всі процедури шифрування і дешифрування виконуються спеціальними електронними схемами. Найбільшого поширення набули модулі, що реалізують комбіновані методи. При цьому неодмінним компонентом усіх апаратно реалізованих методів є гамування. Це пояснюється тим, що метод гамування вдало поєднує високу криптостійкість і простоту реалізації.

Найчастіше як генератор використовується широко відомий регістр зсуву зі зворотними зв'язками (лінійними чи нелінійними). Мінімальний період породжуваної послідовності дорівнює 2^n-1 біт. Для підвищення якості генерованої послідовності можна передбачити спеціальний блок керування роботою регістра зсуву. Таке керування може полягати, наприклад, у тому, що після шифрування певного обсягу інформації вміст регістра зсуву циклічно змінюється.

Інша можливість поліпшення якості гамування полягає у використанні нелінійних зворотних зв'язків. при цьому поліпшення досягається не за рахунок збільшення довжини гами, а за рахунок ускладнення закону її формування, що істотно ускладнює криптоаналіз.

Основним достоїнством програмних методів реалізації захисту є їх гнучкість, тобто можливість швидкої зміни алгоритмів шифрування. Основним же недоліком програмної реалізації є істотно менша швидкодія в порівнянні з апаратними засобами (приблизно в 10 разів).

Останнім часом стали з'являтися комбіновані засоби шифрування, так звані програмно-апаратні засоби. У цьому випадку в комп'ютері використовується своєрідний «криптографічний співпроцесор» – обчислювальний пристрій, орієнтований на виконання криптографічних операцій (додавання за модулем, зсув тощо). Змінюючи програмне забезпечення для такого пристрою, можна вибрати той чи інший метод шифрування. Такий метод поєднує переваги програмних і апаратних методів.

Таким чином, вибір типу реалізації криптозахисту для конкретної АСУ істотною мірою залежить від її особливостей і повинен спиратися на всебічний аналіз вимог, що висуваються до СЗІ. Вибір для конкретних АСУ повинен базуватися на глибинному аналізі слабких і сильних сторін тих чи інших методів захисту. Обґрунтований вибір тієї чи іншої СЗІ взагалі ж повинен спиратися на якісь критерії ефективності. На жаль, дотепер не розроблено придатних методик оцінювання ефективності криптографічних систем.

Найбільш простий критерій такої ефективності – імовірність розкриття ключа або потужність множини ключів. По суті це те ж саме, що і криптостійкість. Для її чисельної оцінки можна використовувати також і складність розкриття шифру шляхом перебору всіх ключів.

Однак цей критерій не враховує інших важливих вимог до криптосистем:

1) неможливість розкриття чи осмисленої модифікації інформації на основі аналізу її структури;

2) досконалість використовуваних протоколів захисту;

3) мінімальний обсяг використовуваної ключової інформації;

4) мінімальна складність реалізації (у кількості машинних операцій), її вартість;

5) висока оперативність.

Отже, бажаним є використання деяких інтегральних показників, що враховують усі зазначені фактори.

Для обліку вартості, трудомісткості й обсягу ключової інформації можна використовувати питомі показники – відношення зазначених параметрів до потужності множини ключів шифру. Часто більш ефективним при виборі й оцінці криптографічної системи є використання експертних оцінок і імітаційне моделювання.

У будь-якому випадку обраний комплекс криптографічних методів повинен поєднувати як зручність, гнучкість і оперативність використання, так і надійний захист від зловмисників циркулюючої в АСУ інформації.

Контрольні питання

1. Визначте поняття «електронний цифровий підпис», «хеш-функція».
2. Назвіть найбільш дієві методи від повторів.
3. Назвіть вимоги, яким повинна відповідати хеш-функція?
4. Розкрийте сутність стандарт цифрового підпису DSS.
5. Дайте визначення поняттям «відмова від авторства», «модифікація даних».

Література для самопідготовки

1. Малюк А.А. Введение в защиту информации в автоматизированных системах / Малюк А.А., Пазизин С.В., Погожин Н.С. – М.: Горячая линия-Телеком, 2001. – С. 131-136.
2. Завгородний В.И. Комплексная защита информации в компьютерных системах: учебное пособие / Завгородний В.И. . – М.: Логос; ПБОЮЛ Н.А. Егоров, 2001. - С. 72–77.

Питання, що опрацьовуються студентами самостійно:

1. Потокові системи шифрування та генератори псевдовипадкових чисел
2. Шифрування, перешкодостійке кодування та алгоритми стиснення інформації
3. Надійність шифрів
4. Протоколи розподілу ключів
5. Теоретичні аспекти створення і використання криптографічних протоколів

РОЗДІЛ 3. ПОБУДОВА І ОРГАНІЗАЦІЯ ФУНКЦІОНУВАННЯ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ В АСУ

СКЛАД ЗМІСТОВНОГО МОДУЛЯ

Лекція 9. Аспекти створення захищених АСУ
9.1. Організаційні принципи побудови СЗІ.
9.2. Методи побудови захищених АСУ.
Контрольні питання
Література для самопідготовки
Лекція 10. Політика безпеки
10.1. Поняття політики безпеки.
10.2. Види політик безпеки.
10.3. Організація секретного діловодства.
Контрольні питання
Література для самопідготовки
Лекція 11. Стеганографія як наука про приховання передачі даних
11.1. Поняття стеганографії. Вимоги до стегосистем.
11.2. Додатки стеганографії.
11.3. Стеганографічні методи захисту інформації.
Контрольні питання
Література для самопідготовки
Лекція 12. Особливості захисту інформації в базах даних
12.1. Загрози в БД.
12.2. Реалізація системи захисту в MS SQL Server.
Контрольні питання
Література для самопідготовки
Лекція 13. Оцінка ефективності СЗІ в АСУ
13.1. Моделювання комплексних СЗІ.
13.2. Підходи до оцінки ефективності комплексних СЗІ.
Контрольні питання
Література для самопідготовки
Питання, що опрацьовуються студентами самостійно

ЛЕКЦІЯ 9. АСПЕКТИ СТВОРЕННЯ ЗАХИЩЕНИХ АСУ

9.1. Організаційні принципи побудови СЗІ.
9.2. Методи побудови захищених АСУ.

9.1. Організаційні принципи побудови СЗІ

Нагадаємо найбільш загальні якісні риси проблеми захисту інформації, які були наведені вище. Отже, вона характеризується:

– невизначеністю, яка, в свою чергу, зумовлена наявністю «людського фактора», оскільки невідомо, хто, коли, де і яким чином може порушити безпеку об’єкта захисту;

– неможливістю створення ідеальної СЗІ, тобто може йтися тільки про той або інший ступінь забезпечення безпеки об’єктів захисту;

– використанням при організації захисту вимог мінімальності

– ризику та мінімальності можливих витрат;

– необхідністю організації захисту від усіх і всього.

Аналіз цих рис, а також широкого спектру можливих загроз інформації дає можливість сформулювати найбільш загальні принципи створення захищених АСУ, тобто принципи, якими доцільно керуватися при розробці і втіленні в життя СЗІ для певного класу АСУ. Їх зручно подавати у вигляді двох груп: організаційні принципи та принципи реалізації СЗІ.

Організаційні принципи побудови СЗІ. Серед організаційних принципів відзначимо такі:

1. Принцип *законності*, тобто додержання всіх законодавчих та нормативних актів, які мають відношення до забезпечення інформаційної безпеки. Важко переоцінити важливість цього принципу. Хоча додержуватися його дуже непросто, особливо зважаючи на недосконалість та відставання від життя нашого відповідного законодавства.

2. Принцип *персональної відповідальності*, відповідно до якого кожен співробітник підприємства, фірми або їхній партнер несе персональну відповідальність за збереження режиму безпеки в рамках своїх повноважень. СЗІ має будуватися таким чином, щоб при будь-яких порушеннях було чітко відоме

або хоча б мінімізоване коло осіб, що мають відношення до порушень. Це не тільки полегшує процес розслідування порушень, а також є ефективним засобом сумлінного виконання службових обов'язків і утримання потенційних ЗЛ від несанкціонованих дій.

3. Принцип *обмеження повноважень*, який має відношення як до персоналу, так і до засобів захисту та обробки інформації;

4. Принцип *взаємодії та співпраці усіх служб* АСУ, спрямований на створення в АСУ сприятливої внутрішньої та зовнішньої атмосфери безпеки. Внутрішня атмосфера безпеки досягається довірчими відносинами між співробітниками служби безпеки та персоналом, допоміжними заходами та стимулюванням, у тому числі і матеріальним.

Принципи реалізації СЗІ. Реалізація СЗІ базується на принципах: системності та комплексності; централізованого управління СЗІ; неможливості обминути захисні засоби; рівноміцності і рівнопотужності рубежів захисту; ешелонованості оборони; неможливості переходу до безпечного стану; мінімальних привілеїв; розподілу обов'язків; простоти, гнучкості та керованості; захисту засобів СЗІ; неперервності захисту; розумної достатності; відкритості алгоритмів та засобів захисту; економічної ефективності СЗІ.

Коротко пояснимо зміст наведених принципів.

Системність та комплексність включають необхідність урахування усіх елементів, умов і чинників, які є взаємозалежні, взаємодіють і змінюються в часі, а також є істотно значимі для розуміння і вирішення проблеми забезпечення безпеки АС. При створенні системи захисту необхідно враховувати всі слабкі, найбільш вразливі місця системи обробки інформації, а також характер, можливі об'єкти і напрямки атак на систему з боку порушників (особливо висококваліфікованих зловмисників), шляхи проникнення в АСУ і НСД до інформації.

У розпорядженні фахівців з комп'ютерної безпеки є широкий спектр заходів, методів і засобів захисту комп'ютерних систем. Їх комплексне використання передбачає узгоджене застосування різнорідних засобів при побудові цілісної СЗ, що перекриває всі відомі методи реалізації загроз і не містить слабких місць на стиках окремих її компонентів.

Централізоване управління СЗІ необхідно планувати внаслідок наявності у будь-якій АСУ цілого комплексу різнорідних технічних і нетехнічних заходів і засобів захисту АСУ. Крім того, централізоване управління дозволяє відстежувати виконання прийнятої політики безпеки.

Неможливість обминути захисні засоби полягає в тому, що внаслідок якісного та надійного інформаційного обстеження АС повинна бути впевненість у відсутності різного роду «обхідних шляхів» захисних засобів.

Рівноміцність і рівнопотужність рубежів захисту передбачають виявлення в рубежах захисту незахищених (або слабозахищених) ділянок і планування посилення найслабкішої ланки, а також однакового відносного рівня захищеності

кожного рубежу захисту – більш потужний захист там, де більша загроза, і менш потужний у протилежному випадку. Крім того, рівноміцність передбачає найбільш ефективний розподіл захисних ресурсів по рубежах.

Ешелонованість оборони означає, що не слід покладатися на один захисний рубіж, яким би надійним він не здавався. За засобами фізичного захисту повинні слідувати програмно-технічні засоби, за ідентифікацією та автентифікацією – управління доступом тощо. Засоби захисту на рівні ОС повинні забезпечувати одну з найбільш укріплених ліній оборони, оскільки ОС – це саме та частина комп'ютерної системи, яка керує використанням усіх її ресурсів. Зовнішній захист повинен забезпечуватися фізичними, організаційними і правовими засобами.

Неможливість переходу до безпечного стану передбачає що за будь-яких обставин, в тому числі і нештатних, захисний засіб або виконує свої функції. або повністю блокує доступ. Такий стан має бути подібним до наступного: якщо в фортеці механізм під'ємного мосту ламається, то міст має залишатися в піднятому стані.

Принцип мінімальних привілеїв наказує виділяти персоналу тільки ті права доступу, які необхідні йому для виконання службових обов'язків, зменшуючи тим самим збитки від випадкових або навмисних некоректних дій персоналу.

Принцип розподілу обов'язків передбачає такий розподіл ролей і відповідальності, щоб лише одна людина не могла порушити критично важливий для організації процес або створити пролом у захисті на замовлення зловмисника. Зокрема, його реалізація може попередити зловмисні або некваліфіковані дії персоналу.

Простота означає, що механізми захисту повинні бути інтуїтивно зрозумілі і прості у використанні. Застосування засобів захисту не повинно бути пов'язане зі знанням спеціальних мов або виконанням дій, що вимагають значних додаткових трудовитрат при звичній роботі законних користувачів, а також не повинно вимагати від користувача виконання рутинних малозрозумілих йому операцій (наприклад, запровадження декількох паролів та імен тощо). Крім того, простота дає формально або неформально доводити коректність захисту.

Майже завжди вжиті заходи і встановлені засоби захисту, особливо в початковий період їхньої експлуатації, можуть забезпечувати як надмірний, так і недостатній рівень захисту. Природно, що для забезпечення можливості варіювання рівня захищеності засоби захисту повинні мати певну *гнучкість*.

Особливо важливою ця властивість є в тих випадках, коли встановлення засобів захисту необхідно здійснювати на працюючій системі, не порушуючи процесу її нормального функціонування. Крім того, зовнішні умови і вимоги з часом змінюються. В таких ситуаціях властивість гнучкості може врятувати власників АС від необхідності вжиття кардинальних заходів для повної заміни засобів захисту на нові. *Керованість* дозволяє перевіряти узгодженість конфігурацій різних компонентів і здійснювати централізоване адміністрування.

Принцип захисту засобів СЗІ вимагає, щоб будь-який захисний захід або засіб був, у свою чергу, забезпечений захистом. При цьому в основі принципу повинні лежати правила: «захист від усіх», «все, що незрозуміле – небезпечне», «довіряй, але перевіряй».

Неперервність захисту означає, що захист інформації – це не разовий захід і навіть не певна сукупність проведених заходів і встановленого засобу захисту, а безперервний цілеспрямований процес, що передбачає вжиття відповідних заходів на всіх етапах життєвого циклу АСУ, починаючи з ранніх стадій проектування, а не тільки на етапі її експлуатації. Розробка СЗ повинна вестися паралельно з розробкою самої АС. Це дозволить врахувати вимоги безпеки при проектуванні архітектури і, у кінцевому рахунку, дозволить створити більш ефективну (як за затратами ресурсів, так і за невразливістю) захищену систему.

Більшості фізичних і технічних засобів захисту для ефективного виконання своїх функцій необхідна постійна організаційна (адміністративна) підтримка (своєчасна зміна і забезпечення правильного збереження і застосування імен, паролів, ключів шифрування, перевизначення повноважень тощо). Перерви в роботі засобів захисту можуть бути використані ЗЛ для аналізу застосованих методів і засобів захисту, для впровадження спеціальних програмних і апаратних «закладок» та інших засобів подолання СЗІ після відновлення її функціонування.

Розумна достатність передбачає, що створити абсолютно неперебороню СЗІ принципово неможливо – при достатній кількості часу і засобів можна перебороти будь-який захист. Однак високоефективна СЗІ коштує дорого, використовує при роботі суттєву частину потужності і ресурсів КС і може створювати істотні додаткові незручності користувачам. Отже, СЗІ має бути організована ефективно, тобто обсяг застосованих заходів повинен бути розумним і відповідати існуючим загрозам.

Відкритість алгоритмів та засобів захисту полягає в тому, що застосовані для організації захисту методи, алгоритми та інші засоби не обов'язково мають бути засекреченими. Наприклад, відкритість алгоритму роботи СЗІ не повинна давати можливість подолати її (навіть його автору). Як показує досвід, засекреченість розробок із захисту аж ніяк не підвищує рівень захищеності системи, а іноді навіть провокує підвищену увагу до неї, фактично підвищуючи ризик подолання СЗІ.

Економічна ефективність СЗІ означає, що слід вести мову тільки про деякий прийнятний рівень безпеки. Він має досягатися мінімумом витрат, тобто важливо правильно обрати той достатній рівень захисту, при якому поточні економічні витрати, ризик і розмір можливих майбутніх витрат були б прийнятними.

9.2. Методи побудови захищених АСУ

Методи побудови захищених АСУ умовно можна розділити на 2 групи:

1) що стосуються довільного ПЗ АСУ: ієрархічний метод розробки; дослідження коректності і верифікація;

2) специфічні тільки для систем захисту (теорія безпечних систем).

Спочатку розглянемо *ієрархічний метод розробки ПЗ АСУ*. Відповідно до принципу абстракції при проектуванні АС розробники можуть іти щонайменше двома шляхами: від апаратури «вгору» – до віртуальної машини, яку являє собою АС, чи від віртуальної машини «униз» – до реального устаткування. Це і є два основні методи проектування – метод знизу вгору і метод зверху вниз. Інші методи по своїй суті зводяться до цих двох чи є їх комбінацією.

Метод знизу вгору передбачає початок проектування з основного апаратного устаткування системи. При проектуванні модулі розбиваються на ряд шарів, причому нульовий шар віртуальної системи утворює апаратура. Шари, що реалізують одну чи кілька необхідних властивостей, додаються послідовно, поки не буде отримана бажана віртуальна машина.

До недоліків методу проектування знизу вгору відносять:

– необхідність із самого початку приймати рішення про вибір способу реалізації компонентів АСУ – за допомогою апаратури, мікропрограм чи програм, який зробити дуже важко;

– можливість проектування АСУ тільки після розробки апаратури;

– розбіжність між реальною АСУ і визначеною в технічному завданні.

При використанні *методу зверху вниз (ієрархічний метод)* виходять від віртуальної машини, що представляє АСУ, з необхідними властивостями і послідовно розробляють шари віртуальної системи апаратури. У цьому випадку проектування відбувається в такій послідовності. Визначається рівень абстракції опису компонентів АСУ вищого шару. Далі систематично проводиться аналіз того, чи достатньо визначені компоненти, щоб можна було їх реалізувати, використовуючи деякі примітивні поняття.

Якщо ні, то кожна функція кожного компонента представляється функціями компонентів наступного шару, якому відповідає більш низький рівень абстракції, і знову проводиться аналіз на можливість їхньої реалізації. В ієрархічному методі доцільно використовувати структурний принцип і принцип модульного проектування.

Структурний принцип має фундаментальне значення і є основою більшості реалізацій. Відповідно до цього принципу, для побудови ПЗ вимагаються тільки три основні конструкції:

а) функціональний блок;

б) конструкція узагальненого циклу;

в) конструкція ухвалення двійкового рішення.

Функціональний блок можна представити як окремий обчислювальний оператор чи як будь-яку іншу реальну послідовність обчислень з єдиним входом і єдиним виходом, як у підпрограмі. Організація циклу в літературі часто згадується як елемент DO-WHILE. Конструкція ухвалення двійкового рішення називається IF-THEN-ELSE.

Зауважимо, що ці конструкції можуть самі розглядатися як функціональні блоки, оскільки вони мають тільки один вхід і однин вихід. Таким чином, можна ввести перетворення операції циклу у функціональний блок і в подальшому розглядати всякий такий оператор циклу еквівалентом (трохи більш складного) функціонального блоку.

Аналогічно можна ввести перетворення конструкції ухвалення рішення до функціонального блоку. Нарешті, можна привести будь-яку послідовність функціональних елементів до одного функціонального елемента. У той же час зворотна послідовність перетворень може бути використана в процесі проектування програми за спадною, тобто виходячи з єдиного функціонального блоку, що поступово розкладається в структуру основних елементів.

Принцип модульного проектування полягає в поділі програм на функціонально самостійні частини (модулі), що забезпечують замінність, кодифікацію, видалення і доповнення складових. Переваги використання модульного принципу такі:

– спрощується налагодження програм, тому що обмежений доступ до модуля й однозначність його зовнішнього прояву виключають вплив помилок в інших, зв’язаних з ним, модулях на його функціонування;

– забезпечується можливість організації спільної роботи великих колективів розробників, тому що кожен програміст має справу з незалежною бід інших частиною програми;

– підвищується якість програми, тому що відносно малий розмір модулів і, як наслідок, невелика складність їх дають змогу провести більш повну перевірку програми.

Іншою проблемою є *дослідження коректності реалізації і верифікація АСУ*. Під поняттям *коректності* чи правильності розуміється відповідність об’єкта, що перевіряється, певному еталонному об’єкту чи сукупності формалізованих еталонних характеристик і правил. Коректність ПЗ при розробці найбільш повно визначається ступенем відповідності висунутим до неї формалізованим вимогам програмної специфікації.

У специфікаціях відбивається сукупність еталонних характеристик, властивостей і умов, яким повинна відповідати програма. Основну частину специфікації складають функціональні критерії і характеристики. Вихідною програмною специфікацією, якій повинна відповідати програма, є технічне завдання.

У разі відсутності такої цілком формалізованої специфікації вимог, як технічне завдання, якому повинна відповідати АСУ і результати її

функціонування, іноді використовуються неформалізовані представлення розробника чи користувача-замовника програм. Однак поняття коректності програм стосовно запитів користувача чи замовника пов'язане з невизначеністю самого еталона, якому повинна відповідати АС. Для складних програм завжди існує ризик знайти їхню некоректність (на думку користувача чи замовника) при формальній коректності щодо специфікацій унаслідок неточності самих специфікацій.

Традиційний погляд на специфікацію висот полягає у тому, що вона являє собою документ, написаний природною мовою, що є інтерфейсом між замовником і виготовлювачем. Хоча підготовці документа передує деяка взаємодія, він виступає як «точка відліку» для виготовлення програм.

Таким чином, можна зробити висновок про те, що створення сукупності взаємопов'язаних несуперечливих специфікацій є необхідною базою для забезпечення коректності проектованої програми. При цьому специфікації повинні:

– бути формальними;
– дозволяти перевіряти несуперечність і повноту вимог замовника;
– бути основою для подальшого формалізованого проектування ОС.

Існує кілька підходів до визначення специфікацій вимог.

Специфікація як опис. Замовник видає специфікацію, щоб виробники могли постачати йому той виріб, що він бажає, тому замовник бачить цей документ головним чином як опис системи, яку він бажав би мати. У принципі, в описі має бути зазначено, що повинна і що не повинна робити система. На практиці звичайно по замовчуванню передбачається, що система повинна робити те, що уточнюється в специфікації, і не повинна робити нічого іншого. У цьому полягає головна проблема з описовою стороною специфікації. Передбачається, що замовник завжди точно знає все, що система повинна і не повинна робити. Більше того, надалі передбачається, що замовник цілком переніс ці знання в специфікований документ.

Специфікація як розпорядження. Виробник дивиться на специфікацію як на набір складових, що підлягають збиранню, щоб розв'язати проблему замовника. Такий директивний підхід обумовлюється не тільки труднощами створення описового документа (як зазначалося вище), а й відомостями, що навмисно чи ненавмисно розширюють чи обмежують волю виробника.

Договірна методологія. У рамках «опис замовника – розпорядження виробнику» специфікація розглядається як формальний поділ між сторонами. Що стосується замовника, то він обумовлює мінімально прийнятне, тоді як виробник – максимально необхідне. Договір розробляється і приймається при зародженні системи і закінчуються після тестування системи, коли замовник приймає систему, яка відповідає його мінімальним вимогам. Під час виготовлення системи в принципі не передбачається ніяких взаємодій, навіть якщо виробник

підозрює, що система не зовсім відповідає тому, що замовник бажав бачити насправді.

Специфікація як модель. Сучасні більш строгі уявлення про специфікацію трактують її як модель системи. За умови, що покладена в основу моделі семантика достатньою мірою обґрунтована, така специфікація забезпечує чітке формулювання вимог.

Відповідні моделі підходять також для автоматизованого контролю цілісності й іншого прогнозного аналізу, що, зокрема, забезпечить припинення розробки системи, у принципі не здатної задовольнити вимоги. Моделі як опис системи мають такі відмітні риси порівняно з іншими способами формального опису:

1) добре сполучення спадного і висхідного підходів до їхньої розробки з можливістю вибору абстрактного опису;
2) можливість опису рівнобіжної, розподіленої і циклічної роботи;
3) можливість вибору різних формалізованих апаратів для опису систем.

Основна перевага використання формальної моделі полягає в можливості дослідження з її допомогою особливостей системи, що моделюється. Докладаючи в основу формального методу розробки математичну модель і потім досліджуючи модель, можна виявити такі грані поводження системи, що в іншому разі не були б очевидні до більш пізніх стадій.

Оскільки цільовим об'єктом проектування є АС, то модель може описувати або саму АС, або її поводження, тобто зовнішні прояви функціонування АС. Модель, що описує поводження АС у порівнянні з моделлю АС, має одну важливу перевагу – вона може бути перевірена й оцінена як виконавцями, так і замовниками, оскільки замовники не знають, як повинна працювати АС, але зате вони уявляють, що вона повинна робити. У результаті такого моделювання може бути перевірена коректність специфікацій щодо вихідної постановки задачі, тобто ТЗ. Крім того, критерії правильності вважаються достатніми за умови, що специфікація являє собою вичерпний опис «зовнішнього» поводження об’єкта в усіх можливих (чи запланованих) ситуаціях його використання.

Як було відзначено вище, при розробці АС, особливо її компонентів, що представляють СЗІ, для забезпечення високих гарантій відсутності несправностей і наступного доказу того, що система функціонує відповідно до вимог ТЗ, використовуються формальні підходи до її проектування.

Формальне проектування алгоритмів базується, в основному, на мовах алгоритмічних логік, що включають вислови наступного вигляду:

$$Q\{S\}R,$$

що читається в такий спосіб: «якщо до виконання оператора S була виконана умова Q, то після нього буде R». Тут Q називається передумовою, а R – постумовою. Ці умови були винайдені практично одночасно Р.У. Флойдом (1967 р.), С.А.Р. Хоаром (1969 р.) і вченими польської логічної школи (А. Сальвіцький та ін., 1970 р.). Як передумова, так і постумова є предикатами.

Розгляд програм як деяких «перетворювачів предикатів» дає змогу прямо визначити зв'язок між початковими і кінцевими станами без яких-небудь посилань на проміжні стани, що можуть виникнути під час виконання програми.

Перевага представлення алгоритму у вигляді перетворювача предикатів полягає в тому, що воно дає можливість:

- аналізувати алгоритми як математичні об'єкти;
- дати формальний опис алгоритму, що дозволяє інтелектуально охопити алгоритм;
- синтезувати алгоритми за представленими специфіками;
- провести формальне верифікування алгоритму, тобто довести коректність його реалізації.

Методологія формальної розробки і доведення коректності в даний час добре розроблена і викладена в цілому ряді робіт. Коротко викладемо суть цих методів:

- розробка алгоритму проводиться методом послідовної декомпозиції, з розбивкою загальної задачі, розв'язуваної алгоритмом, на ряд дрібніших підзадач;
- критерієм деталізації підзадач є можливість їхньої реалізації за допомогою однієї конструкції чи розгалуження циклу;
- розбивка загальної задачі на підзадачі передбачає формулювання перед- і постумов для кожної підзадачі з метою їхнього коректного проектування і подальшої верифікації.

Для проведення коректності алгоритму (верифікація) формулюється математична теорема $Q\{S\}R$, що потім доводиться. Доведення теореми про коректність прийнято розбивати на дві частини. Одна частина служить для проведення того, що розглянутий алгоритм може завершити роботу (проводиться аналіз усіх циклів). В іншій частині доводиться коректність постумови в припущенні, що алгоритм завершує роботу.

Дуже важливим напрямком є **теорія довірених безпечних систем (ТСВ).** Поняття «довірене обчислювальне середовище» (trusted computing base - TCB) з'явилося у закордонній практиці забезпечення інформаційної безпеки досить давно. Зміст характеристики «довірена» можна пояснити в такий спосіб.

Дискретна природа характеристики «безпечний» (у тому сенсі, що аби щось є безпечним, цілком задовольняючи ряд пропонованих вимог, або не є, якщо одна чи кілька вимог не виконані) у сполученні з твердженням «ніщо не буває безпечним на сто відсотків» підштовхують до того, щоб увести більш гнучкий термін, який дає можливість оцінювати те, наскільки розроблена захищена АС відповідає очікуванням замовників. У цьому відношенні характеристика «довірений» більш адекватно відбиває ситуацію, де оцінка, виражена цією характеристикою (безпечний чи довірений), ґрунтується не на думці розробників, а на сукупності факторів, включаючи думку незалежної експертизи, досвід попереднього співробітництва з розробниками, і в остаточному підсумку, є прерогативою замовника, а не розробника.

Довірене обчислювальне середовище (ТСВ) включає сукупність усіх компонентів і механізмів захищеної АС, що відповідають за реалізацію політики безпеки. Всі інші частини АС, а також її замовник покладаються на те, що ТСВ конкретно реалізує задану політику безпеки навіть у тому випадку, якщо окремі модулі чи підсистеми АС розроблені висококваліфікованими ЗЛ для того, щоб втрутитися у функціонування ТСВ і порушити підтримувану нею політику безпеки.

Мінімальний набір компонентів, що утворюють довірене обчислювальне середовище, забезпечує такі функціональні можливості:

- взаємодію з апаратним забезпеченням АС;
- захист пам'яті;
- функції файлового виведення-введення-висновку;
- керування процесами.

Доповнення і модернізація існуючих компонентів АС з урахуванням вимог безпеки можуть призвести до ускладнення процесів супроводу і документування. З іншого боку, реалізація всіх перелічених функціональних можливостей у рамках централізованого довіреного обчислювального середовища в повному обсязі може викликати розростання розмірів ТСВ і, як наслідок, ускладнення доведення конкретності реалізації політики безпеки. Так, операції з файлами можуть бути реалізовані в ТВС у деякому обмеженому обсязі, достатньому для підтримки політики безпеки, а розширене введення-виведення у такому випадку реалізується в тій частині АС, що перебуває за межами ТСВ. Крім того, необхідність упровадження пов'язаних з безпекою функцій у багато компонентів АС, які реалізовані в різних модулях АС, призводить до того, що захисні функції розподіляються по всій АС, викликаючи аналогічну проблему.

Контрольні питання

1. Визначте поняття «керованість», «неперервність захисту».
2. Сформулюйте найбільш загальні принципи створення захищених АСУ.
3. В чому полягає сутність принципу персональної відповідальності?
4. Поясніть зміст принципів системність та комплексність.
5. В чому полягає сутність принципу розподілу обов'язків?
6. Назвіть методи побудови захищених АСУ.

Література для самопідготовки

1. Антонюк А.О. Основи захисту інформації в автоматизованих системах управління / Антонюк А.О. – Київ: Видавничий дім "КМ академія", 2003. – С.141–172.
2. Хоффман Л. Современные методы защиты информации / Хоффман Л. – пер. с англ. / Под ред. В.А. Герасименко. – М.: Сов. Радио, 1980. – С. 142–189.

ЛЕКЦІЯ 10. ПОЛІТИКА БЕЗПЕКИ

10.1. Поняття політики безпеки.

10.2. Види політик безпеки.

10.3. Організація секретного діловодства.

10.1. Поняття політики безпеки

Фундаментальним поняттям захисту інформації є політика безпеки (ПБ), або політика захисту. Важливість цього поняття важко переоцінити – існують ситуації, коли правильно сформульована політика є чи не єдиним механізмом захисту від НСД.

З ПБ пов’язується поняття оптимальності рішень з організації та підтримки системи захисту. Іноді вдається досягти загальноприйнятного розуміння оптимальності прийнятого рішення і навіть довести його існування. Однак, коли розв’язок багатоальтернативний, то загальноприйнятного розуміння оптимальності немає, а в тих випадках, коли розглядається питання про оптимальний у якомусь сенсі розв’язок, то його існування, частіше за все, вдається довести лише в окремих задачах [7].

Подібна ситуація існує і в задачах захисту інформації, оскільки неоднозначним є рішення про те, що система захищена. Крім того, система захисту не самоціль, а має лише підпорядковане значення і має виконувати підпорядковану функцію порівняно з головною метою обчислювального процесу. Наведемо приклади.

Приклад 1. Нехай два відділи в деякій організації ведуть розробки двох проблем. Кожний з відділів користується своїми базами даних, у тому числі і для збору інформації про вирішення проблем. Припустимо, що серед множин задач першого і другого відділів виявилися однакові. На жаль, звичайний офіцер служби безпеки, що дозволяє чи забороняє доступ до баз, не в змозі встановити, що в двох базах накопичується інформація з вирішення одного і того ж завдання. Розглянемо різні рішення офіцера щодо забезпечення безпеки інформації.

1. Якщо він дозволить доступ відділів до баз один одного, то співробітники одного з них, взявши інформацію з іншої бази чи зі своєї, анонімно, і тому безкарно, зможуть продати інформацію, тому що немає персональної відповідальності (неможливо встановити, хто саме продав інформацію з даної бази). При цьому безкарність іноді може навіть стимулювати злочин.

2. Якщо він не дозволить доступ відділів до баз один одного, то виникає небезпека збитків через недоступність інформації (одні вирішили завдання, а інші – ні; тоді завдання іншого відділу виявиться невирішеним, через що можливі великі збитки для фірми, тому що відповідну проблему могли вирішити конкуренти).

Очевидно, що в обох випадках досягається зменшення однієї небезпеки за рахунок зростання іншої.

Приклад 2. Нехай у БД збирається інформація про здоров'я приватних осіб, яка у більшості країн вважається конфіденційною. БД потрібна, тому що ця інформація дозволяє ефективно робити діагностику. Якщо доступ до цієї бази з точки зору захисту інформації сильно обмежений, то в такій БД не буде користі для лікарів, які ставлять діагнози, і не буде користі від самої бази. Якщо доступ відкрити, то можливий витік конфіденційної інформації, за який через суд може бути поданий позов. Яким має бути оптимальне рішення?

Результатом рішення в наведених прикладах та інших аналогічних задачах є вибір правил розподілу і збереження інформації, а також поводження з інформацією, що й називається політикою безпеки.

Під поняттям *ПБ інформації* розуміється організована сукупність документованих керівних рішень, спрямованих на захист інформації й асоційованих з нею ресурсів системи. ПБ викладає систему поглядів, основних принципів, практичних рекомендацій і вимог, що закладаються в основу реалізованого в системі комплексу заходів із захисту інформації.

Формування ПБ є дуже складним аналітичним процесом, який важко формалізувати. Існують різні типи конкретних політик, причому деякі з них передбачають достатньо високий рівень формалізації. Більше того, існують точні доказові методи оцінки ПБ.

Дотримання ПБ має забезпечити виконання того компромісу між альтернативами, який вибрали власники цінної інформації для її захисту. Вочевидь, будучи результатом компромісу, ПБ ніколи не задовольнить усі сторони, що беруть участь у взаємодії з інформацією, що захищається. У той же час вибір ПБ це кінцеве вирішення проблеми: що добре і що погано при роботі з цінною інформацією. Після прийняття такого рішення можна будувати захист, тобто систему підтримки виконання правил ПБ. Таким чином, побудована система захисту інформації добра, якщо вона надійно підтримує виконання правил ПБ. Навпаки, система захисту інформації погана, якщо вона ненадійно підтримує ПБ.

Таке вирішення проблеми захищеності інформації і проблеми побудови системи захисту дозволяє залучити точні математичні методи. Тобто довести, що дана система в заданих умовах підтримує ПБ. У цьому суть доказового підходу до захисту інформації, який дозволяє говорити про «гарантовано захищену систему». Зміст «гарантованого захисту» в тому, що при дотриманні початкових умов свідомо виконуються всі правила ПБ. Термін «гарантований захист» уперше зустрічається в стандарті міністерства оборони США щодо вимог до захищених систем («Помаранчева книга»).

Відзначимо відмінність ПБ від уживаного поняття НСД. Перша відмінність полягає в тому, що політика визначає як дозволені, так і недозволені доступи. Друга відмінність ПБ за своїм визначенням конструктивна, може бути основою визначення деякого автомата чи апарата для своєї реалізації.

Приклад 3. Сформулюємо просту політику безпеки в деякій установі. Ціль, що стоїть перед захистом – забезпечення таємності інформації. ПБ полягає в наступному: кожен користувач користується своїми і тільки своїми даними, не обмінюючись з іншими користувачами. Легко побудувати систему, що підтримує цю політику. Кожен користувач має свій персональний комп’ютер у персональній кімнаті, куди не допускаються сторонні особи. Легко бачити, що сформульована вище політика реалізується в цій системі. Будемо називати таку політику тривіальною розмежувальною (дискреційною) політикою.

ПБ визначається неоднозначно і, звичайно, завжди пов’язана з практичною реалізацією системи і механізмів захисту. Наприклад, ПБ у прикладі 3 може цілком змінитися, якщо в організації немає достатнього числа комп’ютерів і приміщень для підтримки цієї політики. Побудова ПБ звичайно відповідає таким крокам:

1 крок. В інформацію вноситься структура цінностей і проводиться аналіз ризику.

2 крок. Визначаються правила для будь-якого процесу користування даним видом доступу до елементів інформації, що має дану оцінку цінностей.

Однак реалізація цих кроків є складним завданням. Результатом помилкового чи бездумного визначення правил ПБ, як правило, є руйнування цінності інформації без порушення політики. Таким чином, навіть добра система захисту може бути «прозорою» для зловмисника при поганій ПБ.

Приклад 4. Нехай банківські рахунки зберігаються в зашифрованому вигляді у файлах ПЕОМ. Для шифрування, природно, використовується блокова система шифру, що для надійності реалізована поза комп’ютером і оперується за допомогою довіреної особи. Провівши аналітику механізмів захисту, служба безпеки банку переконана адміністрацію, що якщо шифр стійкий, то зазначеним способом інформація добре захищена. Справді, прочитати її при надійному шифрі неможливо, але службовець банку, що знає стандарти заповнення рахунків і має доступ до комп’ютера, може замінити частину шифротексту у своєму рахунку на шифротекст у рахунку багатого клієнта.

Якщо формати збіглися, то рахунок такого службовця з великою ймовірністю зросте. У цьому прикладі акцентується увага на те, що в такій ситуації небезпека для цілісності інформації є значно вищою від небезпеки для порушення таємності, а обрана ПБ добре захищає від порушень таємності, але не орієнтована на небезпеку для цілісності.

Приклад 5. Якщо невдало вибрати ПБ, то можна показати, як користувач, що не має доступу до секретної інформації, реалізує канал витоку секретних даних про те, де в пустелі знаходиться колодязь з водою (нехай, для простоти, у розглянутій місцевості є тільки один колодязь). Отже, інформація про карту будь-якої ділянки пустелі є загальновідомою, але координати колодязя є секретною інформацією. Для одержання секретної інформації користувач робить послідовність запитів у базу даних, причому кожен наступний запит (можна говорити про кроки алгоритму користувача) визначається відповіддю на попередній.

І крок. Розбивається район (для зручності – прямокутник) на вертикальні смути і робиться запит на ці ділянки в базу даних. Відповідно до вибраної ПБ відповідь подається у двох формах:

1) відмова від показу карти, якщо вона секретна, оскільки користувачеві, що не має допуску до секретної інформації, база даних, природно, не повинна її показувати;

2) представлення карти на екрані, якщо ділянка не містить колодязя. Якщо є відмова в доступі, то висновок – в даній смузі є колодязь.

2 крок. Смуга, де є колодязь (тобто де є відмова в доступі), розбивається на окремі ділянки по горизонталі, і знову робиться запит у базу даних. Відмова знову означає, що в даній ділянці є колодязь.

У результаті обчислюються координати колодязя, причому це можна зробити з будь-якою заданою точністю (залежно від рівня дискретизації ділянок пустелі). Таким чином, ПБ дотримана, однак відбувся витік секретної інформації.

Зрозуміло, що ПБ можна відкоригувати таким чином: нехай будь-який користувач одержує карту за запитом, але користувач з допуском до секретної інформації одержує карту з нанесеним колодязем, а користувач без такого доступу – без колодязя. У цьому випадку канал, побудований вище, не працює і ПБ надійно захищає інформацію.

Згідно із [17] під *ПБ інформації* слід розуміти набір законів, правил, обмежень, рекомендацій і т. ін., які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз. Термін «політика безпеки» може бути застосований щодо організації, АСУ, ОС, послуги, що реалізується системою (набору функцій) тощо. Чим дрібніший об’єкт, до якого застосовується даний термін, тим конкретнішими і формальнішими стають правила. Далі для скорочення замість словосполучення «політика безпеки інформації» може використовуватись словосполучення «політика безпеки», а замість

словосполучення «політика безпеки інформації, що реалізується послугою» – «політика послуги» тощо.

ПБ інформації в АСУ є частиною загальної політики безпеки організації і може успадковувати, зокрема, положення державної політики у галузі захисту інформації. Для кожної АСУ ПБ інформації може бути індивідуальною і залежить від технології обробки інформації, що реалізується, особливостей ОС, фізичного середовища і багатьох інших чинників Тим більше одна й та сама АСУ може реалізовувати декілька різноманітних технологій обробки інформації. Тоді і ПБ інформації в такій АСУ буде складеною, і її частини, що відповідають різним технологіям, можуть істотно відрізнятися.

ПБ інформації, що реалізуються різними КС, будуть відрізнятися не тільки тим, що реалізовані в них функції захисту можуть забезпечувати захист від різних типів загроз, а й у зв'язку з тим, що ресурси КС можуть істотно відрізнятись. Так, якщо операційна система оперує файлами, то СКБД має справу із записами, розподіленими в різних файлах.

Для визначення і формалізації процесу розробки ПБ в деякій організації звичайно необхідно розробляти два комплекти документів:

1. Узагальнена політика (program-level).
2. Проблемно-орієнтована (окрема) політика (issue-specific).

Основна функція *узагальненої ПБ* є визначення програми ЗІ, призначення відповідальних за її виконання осіб, формулювання цілей і об'єктів захисту, а також вироблення схеми для забезпечення додержання розроблених правил і вказівок. Компонентами узагальненої ПБ вважаються призначення, сфера поширення, визначення цілей ЗІ, розподіл відповідальності за виконання і методи забезпечення додержання правил.

Проблемно-орієнтована ПБ необхідна для виділення певних проблемних сфер і визначення позицій організації щодо них.

Якщо узагальнена ПБ описує глобальні аспекти ЗІ і її схему, то окремі ПБ розробляються для деяких видів діяльності й у деяких випадках для конкретних систем (наприклад, для захисту електронної кореспонденції). Таким чином, окремі ПБ стандартизують роботу і зменшують потенційний ризик, який виникає при некоректному використанні інформаційних ресурсів. Проблемно-орієнтована ПБ частково визнає керівні принципи при створенні функціональних інструкцій для співробітників організації. Формуючи окрему ПБ, виділяють такі її компоненти: формулювання проблеми, визначення позиції організації, визначення сфери поширення, ролей і відповідальності, а також призначення осіб для контактів у даному питанні. Частина ПБ, яка регламентує правила доступу користувачів і процесів до ресурсів КС, складає правила розмежування доступу.

Створення життєздатної ПБ важливе і складне завдання, яке вимагає розуміння цілей ЗІ, а також потенційної користі від її розробки. Тому необхідно розробляти структурні підходи для формування ПБ, які включали б способи розподілу обов'язків, підходи для розробки узагальненої й окремих компонент у

вигляді узгодженої політики ЗІ, а також рекомендації щодо формування на її основі наборів функціональних інструкцій. Політика ЗІ допомагає визначити стандарти, керівні інструкції і правила для всіх працівників б організації.

Таким чином, до складу будь-якої СЗІ обов'язково має входити ПБ та набір апаратних і програмних компонент, використання яких регламентовано політикою, що забезпечує збереження інформації. Для більшої впевненості в надійності СЗІ необхідна також наявність строгих доказів її повноти і коректності.

Основними етапами формального підходу до перевірки СЗІ на повноту і коректність є:

1) визначення об'єктів і цілей захисту;
2) розробка політики,
3) доведення того, що при її додержанні інформація не компрометується
4) визначення набору функцій для підтримки політики;
5) доведення того, що набір функцій забезпечує додержання політики;
6) вибір апаратного і програмного забезпечення для реалізації функцій ЗІ.

Для формального доведення у пунктах 3 і 5 можуть використовуватися математичні методи, якщо сама ПБ була визначена достатньо строго, можливо, у термінах деякої формальної мови. Популярні підходи до формалізації ґрунтуються на станах системи або на її діях. У підході, який ґрунтується на станах, функціонування системи розглядається як послідовність станів, де стан – це набір значень множини змінних. Підхід, який ґрунтується на діях, розглядає діяльність системи у вигляді реакцій на події.

Ці два різних підходи в певному сенсі еквівалентні. Дії можуть бути змодельовані зміною стану, а стани можуть бути представлені класами еквівалентності послідовностей дії. Однак описані підходи звичайно базуються на різних формальних теоріях. Моделювання станів у більшості випадків ґрунтується на логіці, а специфікації представляються формулами в деякій логічній системі. При моделюванні дії звичайно користуються алгеброю, а специфікаціями є об'єкти, з якими оперують алгебраїчними методами. Основою доведень, які проводяться в п. 3 і 5, як правило, є набір теорем. Однак, проводити подібний аналіз для кожної системи складно і дорого. Крім того, методика проведення аналізу державних систем конфіденційна інформація.

Вихід було знайдено в тому, що умови теорем, які доводять підтримку ПБ, формулюються без доведення у вигляді стандарту. Саме такий підхід уперше застосували американці в 1983 р., опублікувавши відкрито проект стандарту із ЗІ в електронних системах обробки даних («Помаранчева книга»), де сформульовано вимоги гарантованої підтримки двох класів політик дискреційної та мандатної. Пізніше цей метод було застосовано в 1987 р. для опису гарантовано захищених розподілених мереж, у яких підтримуються ті самі політики, а в 1991 р. – для опису вимог гарантовано захищених баз даних. Цей же шлях використали канадці і європейські держави, створивши свої стандарти з ЗІ. В Україні також розроблено стандарт захисту, аналогічний канадському. Наведені вище підходи до

формалізації політики ЗІ дають можливість проаналізувати розроблені стандарти на повноту і коректність.

При розробці і проведенні її в життя доцільно керуватися наступними засадами:

– неможливість минати захисні засоби;
– посилення самої слабкої ланки;
– неприпустимість переходу у відкритий стан;
– мінімізація привілеїв;
– поділ обов'язків;
– багаторівневий захист;
– розмаїтість захисних засобів;
– простота і керованість інформаційної системи;
– забезпечення загальної підтримки заходів безпеки.

Стосовно до міжмережних екранів принцип *неможливості минати захисні засоби* означає, що всі інформаційні потоки в мережу, що захищається, і з її повинні проходити через екран. Не повинно бути «таємних» модемних чи входів тестових ліній, що йдуть в обхід екрана.

Надійність будь-якої оборони визначається самою *слабкою ланкою*. Часто самою слабкою ланкою виявляється не комп'ютер чи програма, а людина, і тоді проблема забезпечення інформаційної безпеки здобуває нетехнічний характер.

Принцип *неприпустимості переходу у відкритий стан* означає, що при будь-яких обставинах (у тому числі позаштатних), СЗІ або цілком виконує свої функції, або повинна цілком блокувати доступ.

Принцип *мінімізації привілеїв* наказує виділяти користувачам і адміністраторам тільки ті права доступу, що необхідні їм для виконання службових обов'язків.

Принцип *поділу обов'язків* припускає такий розподіл ролей і відповідальності, при якому одна людина не може порушити критично важливий для організації процес. Це особливо важливо, щоб запобігти зловмисні чи некваліфіковані дії системного адміністратора.

Принцип *багаторівневого захисту* наказує не покладатися на один захисний рубіж, яким би надійним він ні здавався. За засобами фізичного захисту повинні випливати програмно-технічні засоби, за ідентифікацією й автентифікацією – керування доступом і, як останній рубіж, – протоколювання й аудит. Ешелонована оборона здатна принаймні затримати зловмисника, а наявність такого рубежу, як протоколювання й аудит, істотно утрудняє непомітне виконання злочинних дій.

Принцип *різноманітності захисних засобів* рекомендує організовувати різні за своїм характером оборонні рубежі, щоб від потенційного зловмисника було потрібно оволодіння різноманітними і, по можливості, несумісними між собою навичками подолання СЗІ.

Принцип *простоти і керованості* інформаційної системи в цілому і СЗІ особливо визначає можливість формального чи неформально доказу коректності реалізації механізмів захисту. Тільки в простій і керованій системі можна перевірити погодженість конфігурації різних компонентів і здійснити централізоване адміністрування.

Принцип *загальної підтримки заходів безпеки* – носить нетехнічний характер. Рекомендується із самого початку передбачити комплекс заходів, спрямований на забезпечення лояльності персоналу, на постійне навчання, теоретичне і, головне, практичне.

10.2. Види політик безпеки

Серед ПБ найбільш відомі дискреційна, мандатна і рольова. Основою *дискреційної* політики безпеки (ДПБ) є дискреційне управління доступом, яке визначається двома властивостями:

– всі суб'єкти і об'єкти повинні бути однозначно ідентифіковані;

– права доступу суб'єкта до об'єкта системи визначаються на основі деякого зовнішнього відносно системи правила.

ДПБ реалізується за допомогою матриці доступу, яка фіксує множину об'єктів та суб'єктів, доступних кожному суб'єкту. Існує декілька варіантів задавання матриці доступу.

1. *Листи можливостей*: для кожного суб'єкта створюється лист (файл) усіх об'єктів, до яких він має доступ;

2. *Листи контролю доступу*: для кожного об'єкта створюється список усіх суб'єктів, що мають доступи до нього.

До переваг ДПБ можна віднести відносно просту реалізацію відповідних механізмів захисту. Саме цим зумовлений той факт, що більшість поширених сьогодні захищених АСУ забезпечують виконання положень ДПБ.

Однак багатьох проблем захисту ця політика розв'язати не може. Наведемо найбільш суттєві вади ДПБ.

1. Один із найсуттєвіших недоліків цього класу політик тс, що вони не витримують атак за допомогою «Троянського коня». Це, зокрема, означає, що СЗІ, яка реалізує ДПБ, погано захищає від проникнення вірусів у систему й інших засобів прихованої руйнівної дії.

2. Наступна проблема ДПБ – це автоматичне визначення прав. Так як об'єктів багато і їх кількість безперервно змінюється, то задати заздалегідь вручну перелік прав кожного суб'єкта на доступ до об'єктів неможливо. Тому матриця доступу різними способами агрегується.

Наприклад, як суб'єкти залишаються тільки користувачі, а у відповідну клітину матриці вставляються формули функцій, обчислення яких визначає права доступу суб'єкта, породженого користувачем, до об'єкта. Звичайно, ці функції

можуть змінюватися з часом. Зокрема, можливе вилучення прав після виконання деякої події. Можливі модифікації, які залежать від інших параметрів.

3. Ще одна з найважливіших проблем при використанні ДПБ – це проблема контролю поширення прав доступу. Найчастіше буває, що власник файлу передає вміст файлу іншому користувачеві і той, таким чином, набуває права власника на цю інформацію. Отже, права можуть поширюватися, і навіть якщо перший власник не хотів передати доступ іншому суб'єкту до своєї інформації, то після декількох кроків передача прав може відбутися незалежно від його волі. Виникає задача про умови, за якими в такій системі деякий суб'єкт рано чи пізно отримає необхідний йому доступ.

4. При використанні ДПБ виникає питання визначення правил поширення прав доступу й аналізу їх впливу на безпеку АСУ. У загальному випадку при використанні ДІЬ перед органом, який її реалізує і який при санкціонуванні доступу суб'єкта до об'єкта керується деяким набором правил, стоїть задача, яку алгоритмічно розв'язати неможливо; перевірити, призведуть його дії до порушень безпеки чи ні.

Основу *мандатної (повноважної)* політики безпеки (МПБ) становить мандатне управління доступом , що передбачає:

– всі суб'єкти і об'єкти повинні бути однозначно ідентифіковані;

– задано лінійно упорядкований набір міток секретності;

– кожному об'єкту системи присвоєна мітка секретності, яка визначає цінність інформації, що міститься в ньому – його рівень секретності в АС;

– кожному суб'єкту системи присвоєна мітка секретності, яка визначає рівень довіри до нього в АСУ – максимальне значення мітки секретності об'єктів, до яких, суб'єкт має доступ; мітка секретності суб'єкта називається його рівнем доступу.

Основна мета МПБ – запобігання витоку інформації від об'єктів з високим рівнем доступу до об'єктів з низьким рівнем доступу, тобто протидія виникненню в АСУ інформаційних каналів зверху вниз. Вона оперує, таким чином, поняттями інформаційного потоку і цінності (певним значенням мітки секретності) інформаційних об'єктів.

Цінність інформаційних об'єктів часто дуже важко визначити. Однак досвід показує, що в будь-якій АСУ майже завжди для будь-якої пари об'єктів X та Y можна сказати, який із них більш цінний. Тобто, можна вважати, що таким чином фактично визначається деяка однозначна функція $c(X)$, яка дозволяє для будь-яких об'єктів X та Y сказати, що коли Y більш цінний об'єкт, ніж X, то $c(Y) > c(X)$. І навпаки, з огляду на однозначність, якщо $c(X) > c(Y)$, то Y – більш цінний об'єкт, ніж X. Тоді потік інформації від X до Y дозволяється, якщо $c(X) < c(Y)$, і не дозволяється, якщо $c(X) > c(Y)$.

Таким чином, МПБ має справу з множиною інформаційних потоків, яка ділиться на дозволені і недозволені дуже простою умовою значенням наведеної

функції. Інакше кажучи, управління потоками інформації здійснюється через контроль доступів.

МПБ в сучасних системах захисту на практиці реалізується мандатним контролем. Він реалізується на найнижчому апаратно-програмному рівні, що дозволяє досить ефективно будувати захищене середовище для механізму мандатного контролю. Пристрій мандатного контролю називають монітором звернень. Мандатний контроль ще називають обов'язковим, оскільки його має проходити кожне звернення суб'єкта до об'єкта, якщо вони знаходяться під захистом СЗІ. Організовується він так: кожний об'єкт має мітку з інформацією про свій рівень секретності; кожний суб'єкт також має мітку з інформацією про те, до яких об'єктів він має право доступу. Мандатний контроль порівнює мітки і приймає рішення про допуск.

Найчастіше МПБ описують у термінах, поняттях і визначеннях властивостей моделі Белла-Лападула [5]. У рамках цієї моделі доводиться важливе твердження, яке вказує на принципову відмінність систем, що реалізують мандатний захист, від систем з дискреційним захистом: якщо початковий стан системи безпечний і всі переходи системи зі стану до стану не порушують обмежень, сформульованих ПБ, то будь-який стан системи безпечний.

Наведемо ряд переваг МПБ порівняно з ДПБ.

1. Для систем, де реалізовано МПБ, характерним є більш високий ступінь надійності. Це пов'язано з тим, що за правилами МПБ відстежуються не тільки правила доступу суб'єктів системи до об'єктів, а й стан самої АСУ. Таким чином, канали витоку в системах такого типу не закладені первісно (що є в положеннях ДПБ), а можуть виникнути тільки при практичній реалізації систем внаслідок помилок розробника.
2. Правила МПБ більш ясні і прості для розуміння розробниками і користувачами АСУ, що також є фактором, який позитивно впливає на рівень безпеки системи.
3. МПБ стійка до атак типу «Троянський кінь».
4. МПБ допускає можливість точного математичного доведення, що дана система в заданих умовах підтримує ПБ.

Однак МПБ має дуже серйозні вади – вона складна для практичної реалізації і вимагає значних ресурсів обчислювальної системи. Це пов'язано з тим, що інформаційних потоків у системі величезна кількість і їх не завжди можна ідентифікувати. Саме ці вади часто заважають її практичному використанню.

МПБ прийнята всіма розвинутими державами світу. Вона розроблялася, головним чином, для збереження секретності (тобто конфіденційності) інформації у військових організаціях. Питання ж цілісності за її допомогою не розв'язуються або розв'язуються частково, як побічний результат захисту секретності.

Розглянемо ще один вид ПБ – *рольову ПБ*. Рольову політику безпеки не можна віднести ані до дискреційної, ані до мандатної, тому що керування доступом у ній здійснюється як на основі матриці прав доступу для ролей, так і за допомогою

правил, які регламентують призначення ролей користувачам та їх активацію під час сеансів. Отже, рольова модель є цілком новим типом політики, що базується на компромісі між гнучкістю керування доступом, яка є характерною для ДПБ, і жорсткістю правил контролю доступу, яка притаманна МПБ.

У РПБ класичне поняття *суб'єкт* замішується поняттями користувач і роль. *Користувач* – це людина, яка працює з системою і виконує певні службові обов'язки. *Роль* – це активно діюча в системі абстрактна сутність, з якою пов'язаний обмежений, логічно зв'язаний набір повноважень, необхідних для здійснення певної діяльності.

РПБ є досить поширеною, тому що вона, на відміну від інших більш строгих і формальних політик, є дуже близькою до реального життя. Справді, користувачі, що працюють у системі, діють не від свого власного імені – вони завжди здійснюють певні службові обов'язки, тобто виконують деякі ролі, які аж ніяк не пов'язані з їх особистістю.

Тому цілком логічно здійснювати керування доступом і призначати повноваження не реальним користувачам, а абстрактним (не персоніфікованим) ролям, які представляють учасників певного процесу обробки інформації. Такий підхід до ПБ дозволяє врахувати розподіл обов'язків і повноважень між учасниками прикладною інформаційного процесу, оскільки з точки зору РПБ має значення не особистість користувача, що здійснює доступ до інформації, а те, які повноваження йому необхідні для виконання його службових обов'язків. Наприклад, у реальній системі обробки інформації можуть працювати системний адміністратор, менеджер БД і користувач.

У такій ситуації РПБ дає змогу розподілити повноваження між цими ролями відповідно до їх службових обов'язків: ролі адміністратора призначаються спеціальні повноваження, які дозволять йому контролювати роботу системи і керувати її конфігурацією; роль менеджера баз даних дає змогу здійснювати керування сервером БД; а права простих користувачів обмежуються мінімумом, необхідним для запуску прикладних програм. Крім того, кількість ролей у системі може не відповідати кількості реальних користувачів – один користувач, якщо він має різні повноваження, може виконувати (водночас або послідовно) кілька ролей, а кілька користувачів можуть користуватись однією і тією ж роллю, якщо вони виконують однакову роботу.

При використанні РПБ керування доступом здійснюється в дві стадії: по перше, для кожної ролі вказується набір повноважень, що являють собою набір прав доступу до об'єктів і кожному користувачу призначається список доступних йому ролей.

10.3. Організація секретного діловодства

Під час роботи із захисту комерційної таємниці необхідно звернути особливу увагу на документи фірми, оскільки більшість комерційних структур у нашій

країні основні обсяги комерційної інформації, у тому числі конфіденційної, зберігають у документах.

Керівник фірми повинен упорядкувати відповідним чином процеси фіксації секретної інформації в ділових паперах і організувати їх рух таким чином, щоб викрадення конфіденційних документів було б настільки складним, щоб воно ставало економічно невигідним для викрадача.

При роботі з документами, що містять конфіденційну інформацію, слід дотримуватися наступних правил:

– строгий контроль (чи особисто через службу безпеки) за допуском персоналу до секретних документів;

– встановлення конкретних осіб з керівництва фірми, що організують і контролюють секретне діловодство фірми; наділення їх відповідними повноваженнями;

– розробка інструкції (пам’ятки) по роботі із секретними документами, ознайомлення з нею відповідних працівників фірми;

– контроль за прийняттям відповідними службовцями письмових зобов’язань про збереження комерційної таємниці фірми;

– уведення системи матеріального й іншого стимулювання працівникам фірми, що мають доступ до її секретів;

– впровадження в повсякденну практику механізмів і технологій захисту комерційної таємниці фірми;

– особистий контроль з боку керівника фірми служби внутрішньої безпеки і секретного діловодства.

Імовірність витоку секретної інформації з документів особливо велика в процесі їх пересилання. Очевидно, що в комерційних структур немає можливостей скористатися послугами воєнізованої кур’єрської доставки. Тому доставку секретних документів і цінностей приходиться здійснювати власними силами із залученням охоронців фірми чи звертатися в спеціальні фірми.

Фірми, відповідальні за схоронність, використання і своєчасне знищення секретних документів, повинні бути захищені від спокуси торгівлі секретами фірми простим, але радикальним способом – гарною платою за роботу.

У процесі збереження і пересилання секретних документів фірми можуть бути застосовані засоби захисту і сигналізації про несанкціонований доступ до них. Одна з новинок – невидиме світлочутливе покриття, наносимо на документи, що виявляється під впливом світла, указуючи тим самим на факт несанкціонованого ознайомлення з чи документами їхнього фотографування.

Фахівцям з питань захисту комерційної інформації відомі й інші технології і системи охорони конфіденційних документів фірми від несанкціонованого доступу чи можливого витоку конфіденційних зведень. За інформацією з даного питання варто звертатися в організації і служби, що спеціально займаються даною проблемою. Для ведення секретного діловодства повинні залучатися люди, що пройшли спеціальну підготовку, і в чесності яких немає сумнівів. Крім того, ці

люди повинні бути відповідним чином підготовлені і навчені, тому що професійні недоліки і відступ від правил у їх роботі можуть занадто дорого коштувати фірмі.

Приміщення, у яких ведеться робота із секретними документами, повинні добре охоронятися, а доступ туди повинен бути закритий для сторонніх облич. Ці приміщення повинні мати міцні перекриття і стіни, посилені металеві двері, міцні віконні рами з подвійним склом і ґратами, щільні штори. Сховище повинне бути обладнане охоронною і пожежною сигналізацією і ретельно охоронятися силами внутрішньої охорони. Доступ у сховище строго обмежений. Не рекомендується розташовувати таке приміщення на першому й останньому поверхах будинку. Секретні документи зберігаються у сейфах або вогнестійких металевих шафах з надійними замками і запорами.

Різні прийоми ведення секретного діловодства спрямовані на запобігання витоку комерційних секретів. Наприклад, документи, що містять комерційну таємницю, діляться по ступеню таємності відображеної в них інформації і забезпечуються відповідним грифом таємності.

Навіть та таємниці фірми, що ретельно охороняються можуть стати надбанням конкурентів зі звичайних публікацій, якщо пустити цю справу на самоплив. Тому один зі службовців фірми обов’язково повинен бути наділений самими широкими владними повноваженнями, щоб займатися попередньою цензурою брошур, що готуються, рекламних оголошень, прес-релізів і інших матеріалів для симпозіумів, виставок, конгресів, а також виступів, наукових і інших публікацій співробітників фірми.

Інтереси охорони секретів фірми найчастіше знаходяться у важко розв’язному протиріччі з особистими амбіціями, самолюбством, академічною незалежністю співробітників фірми, що бажають професійно самоствердуватися в науковому світі, серед своїх колег, у суспільній чи колективній групі.

Не менш легкий для дозволу конфлікт між прагненням зберегти комерційні таємниці фірми і бажанням використовувати в рекламних цілях деякі найбільш вражаючі дані з таємної інформації, особливо ті з них, що, безсумнівно, допомогли б розширити збут вироблених товарів і послуг.

Співробітник, що здійснює цензуру відкритих публікацій рекламного, наукового і популяризаторського характеру, що готуються персоналом чи фірми по її замовленнях, повинен керуватися простим, але ефективним правилом. Суть його в тому, щоб у максимально можливому ступені роздрібнити, роз’єднати за часом, у просторі і по авторах ту таємну інформацію, без якого неможливе опублікування згаданих робіт.

Звичайно, усе це ускладнює здійснення персоналом фірми науково-дослідних і дослідно-конструкторських робіт, але зате істотно перешкоджає збору секретної інформації про фірму конкурентами і недоброзичливцями. Цей бар’єр переборний лише за допомогою великих витрат.

Контрольні питання

1. Визначте поняття «політика безпеки», «гарантований захист».
2. У чому відмінність термінів «політика безпеки» і «несанкціонований доступ»?
3. Перерахуйте кроки побудови політики безпеки.
4. Яка основна функція узагальненої політики безпеки?
5. Назвіть основні етапи формального підходу до перевірки СЗІ на повноту і коректність.
6. Перерахуйте засади, яким доцільно керуватися при формалізації політики захисту інформації.
7. Поясніть сутність принципу поділу обов’язків.
8. Поясніть сутність принципу багаторівневого захисту.

Література для самопідготовки

1. Антонюк А.О. Основи захисту інформації в автоматизованих системах управління / Антонюк А.О. – Київ: Видавничий дім "КМ академія", 2003. – С. 79–91.
2. Мельников В.В. Защита информации в компьютерных системах / Мельников В.В. – М.: Финансы и статистика. Электроинформ, 1997. – С.88–131.

ЛЕКЦІЯ 11. СТЕГАНОГРАФІЯ ЯК НАУКА ПРО ПРИХОВАННЯ ПЕРЕДАЧІ ДАНИХ

11.1. Поняття стеганографії. Вимоги до стегосистем.
11.2. Додатки стеганографії.
11.3. Стеганографічні методи захисту інформації.

11.1. Поняття стеганографії. Вимоги до стегосистем

Стеганографія – це метод організації зв'язку, який властиво приховує саму наявність зв'язку. На відміну від криптографії, де ворог точно може визначити чи є передане повідомлення зашифрованим текстом, методи стеганографії дозволяють вбудовувати секретні повідомлення в невинні послання так, щоб неможливо було запідозрити існування вбудованого таємного послання.

Слово «стеганографія» у перекладі із грецького буквально означає «тайнопис» (steganos – секрет, таємниця; graphy – запис). До неї відноситься величезна множина секретних засобів зв'язку, таких як «невидиме» чорнило, мікрофотознімки, умовне розташування знаків, таємні канали й засобу зв'язку на плаваючих частотах тощо.

Стеганографія займає свою нішу в забезпеченні безпеки: вона не замінює, а доповнює криптографію. Приховання повідомлення методами стеганографії значно знижує ймовірність виявлення самого факту передачі повідомлення. А якщо це повідомлення до того ж зашифроване, то воно має ще один, додатковий, рівень захисту.

У цей час у зв'язку з бурхливим розвитком обчислювальної техніки й нових каналів передачі інформації з'явилися нові стеганографічні методи, в основі яких лежать особливості представлення інформації в комп'ютерних файлах, обчислювальних мережах тощо. Це дає можливість говорити про становлення нового напрямку – комп'ютерної стеганографії.

Незважаючи на те, що стеганографія як спосіб приховання секретних даних відома вже протягом тисячоріч, комп'ютерна стеганографія – молодий напрямок, що розвивається. Як і будь-який новий напрямок, комп'ютерна стеганографія,

незважаючи на велику кількість відкритих публікацій і щорічних конференцій, довгий час не мала єдиної термінології.

Донедавна для опису моделі стеганографічної системи використовувалася запропонована 1983 р. Сіммонсом [3] так звана «проблема ув'язнених». Вона полягає в тому, що дві особи (Аліса й Боб) прагнуть обмінюватися секретними повідомленнями без втручання охоронця (Віллі), що контролює комунікаційний канал. При цьому є ряд припущень, які роблять цю проблему більш-менш вирішальною. Перше припущення полегшує розв'язок проблеми й полягає в тому, що учасники інформаційного обміну можуть розділяти секретне повідомлення (наприклад, використовуючи кодову клавішу) перед передачею. Інше припущення, навпаки, ускладнює вирішення проблеми, тому що охоронець має право не тільки читати повідомлення, але й модифікувати їх.

Пізніше, на конференції Information Hiding: First Information Workshop в 1996 р. було запропоновано використовувати єдину термінологію й обговорені основні терміни [4]. *Стеганографічна система* або *стегосистема* – це сукупність засобів і методів, які використовуються для формування схованого каналу передачі інформації.

При побудові стегосистеми повинні враховуватися наступні положення:

1. Супротивник має повне представлення про стеганографічну систему й деталі її реалізації. Єдиною інформацією, яка залишається невідомою потенційному супротивникові, є ключ, за допомогою якого тільки його власник може встановити факт присутності й зміст схованого повідомлення.
2. Якщо супротивник якимось чином довідається про факт існування прихованого повідомлення, це не повинно дозволити йому отримати подібні повідомлення в інших даних доки ключ зберігається в таємниці.
3. Потенційний супротивник повинен бути позбавлений яких-небудь технічних і інших переваг у розпізнаванні або розкритті змісту таємних повідомлень.

Узагальнена модель стегосистеми представлена на рис. 11.1.

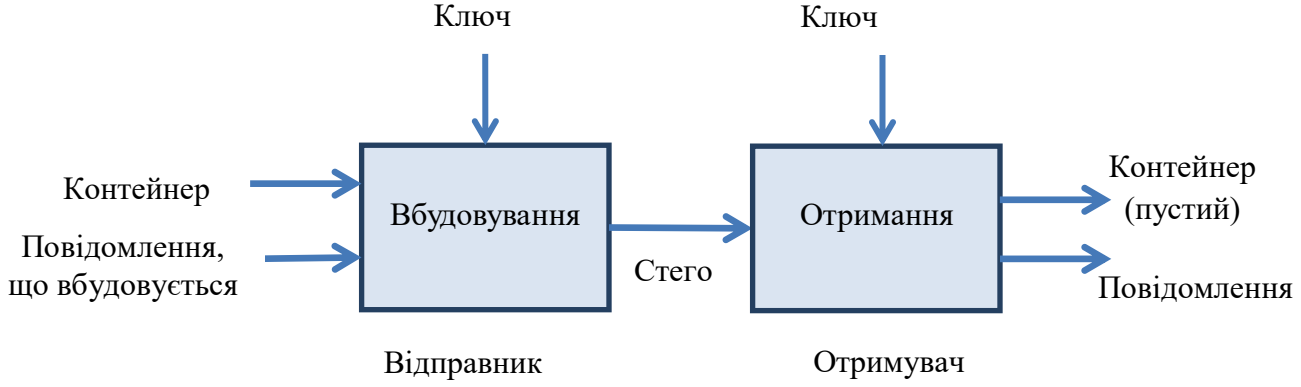

Рис. 11.1. Узагальнена модель стегосистеми

В якості даних може використовуватися будь-яка інформація: текст, повідомлення, зображення тощо. В загальному випадку доцільно використовувати слово «повідомлення», тому що повідомленням може бути як текст або зображення, так і, наприклад, аудіодані. Далі для позначення приховуваної інформації, будемо використовувати саме термін повідомлення.

Контейнер – це будь-яка інформація, призначена для приховання таємних повідомлень.

Порожній контейнер – контейнер без вбудованого повідомлення; заповнений контейнер або стегоконтейнер, що містить вбудовану інформацію.

Вбудоване (сховане) повідомлення – повідомлення, що вбудовується в контейнер.

Стеганографічний канал або просто *стегоканал* – канал передачі стего.

Стегоключ або просто *ключ* – секретний ключ, необхідний для приховання інформації. Залежно від кількості рівнів захисту (наприклад, вбудовування у попередньо зашифроване повідомлення) у стегосистемі може бути один або кілька стегоключів.

За аналогією із криптографією, по типу стегоключа стегосистеми можна поділити на два типи: із секретним ключем; із відкритим ключем.

У стегосистемі із секретним ключем використовується один ключ, який повинен бути визначений або до початку обміну секретними повідомленнями, або переданий по захищеному каналу. У стегосистемі з відкритим ключем для вбудовування й добування повідомлення використовуються різні ключі, які відрізняються таким чином, що за допомогою обчислень неможливо отримати один ключ із іншого. Тому один ключ (відкритий) може передаватися відкрито по незахищеному каналу зв’язку. Крім того, дана схема добре працює й при взаємній недовірі відправника й одержувача.

Будь-яка стегосистема повинна відповідати наступним вимогам:

1. Властивості контейнера повинні бути модифіковані, щоб зміну неможливо було виявити при візуальному контролі. Ця вимога визначає якість приховання впроваджуваного повідомлення: для забезпечення безперешкодного проходження стегоповідомлення по каналу зв’язку воно жодним чином не повинне привернути увагу атакуючого.

2. Стегоповідомлення повинне бути стійким до викривлень, у тому числі й зловмисних. У процесі передачі зображення (звук або інший контейнер) може піддаватися різним трансформаціям: зменшуватися або збільшуватися, перетворюватися в інший формат тощо. Крім того, воно може бути стиснуте, у тому числі й з використанням алгоритмів стискування із втратою даних.

3. Для збереження цілісності, для повідомлення, що вбудовується, необхідно використовувати код з виправленням помилки.

4. Для підвищення надійності, повідомлення, що вбудовується, повинне бути продубльовано.

11.2. Додатки стеганографії

Сьогодні можна виділити три тісно пов’язані між собою напрямки додатків стеганографії: приховання даних (повідомлень), цифрові водяні знаки й заголовки (рис. 11.2).

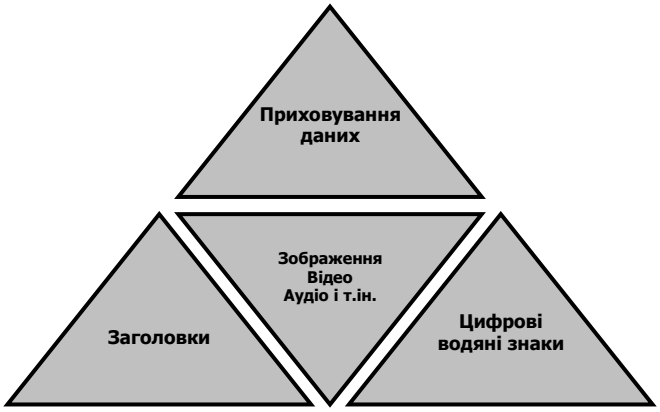

Рис. 11.2. Напрями використання стеганографії

Приховання впроваджуваних даних, які в більшості випадків мають великий обсяг, висуває серйозні вимоги до контейнера: розмір контейнера в кілька разів повинен перевищувати розмір даних, що вбудовуються.

Цифрові водяні знаки використовуються для захисту авторських або майнових прав на цифрові зображення, світлини або інші оцифровані твори мистецтва. Основними вимогами, які висуваються до таких вбудованих даних, є надійність і стійкість до викривлень. Цифрові водяні знаки мають невеликий обсяг, однак, з врахуванням вищезазначених вимог, для їх вбудовування використовуються більш складні методи, ніж для вбудовування просто повідомлень або заголовків.

Третій додаток – *заголовки*, використовується в основному для маркування зображень у великих електронних сховищах (бібліотеках) цифрових зображень, аудіо- і відеофайлів. У цьому випадку стеганографічні методи використовуються не тільки для впровадження ідентифікуючого заголовка, але й інших індивідуальних ознак файлу. Впроваджувані заголовки мають невеликий обсяг, а висунуті до них вимоги мінімальні: заголовки повинні вносити незначні викривлення й бути стійкі до основних геометричним перетворенням.

Кожен з перерахованих вище додатків вимагає певного співвідношення між стійкістю вбудованого повідомлення до зовнішніх впливів (у тому числі й стегоаналізу) і розміром самого повідомлення, що вбудовується. Для більшості сучасних методів, що використовуються для приховання повідомлення в цифрових контейнерах, має місце наступна залежність надійності системи від обсягу даних, що вбудовуються (рис. 11.3).

Наведена залежність показує, що при збільшенні обсягу даних, що вбудовуються, знижується надійність системи (при незмінності розміру контейнера). Таким чином, використаний у стегосистемі контейнер накладає обмеження на розмір даних, що вбудовуються.

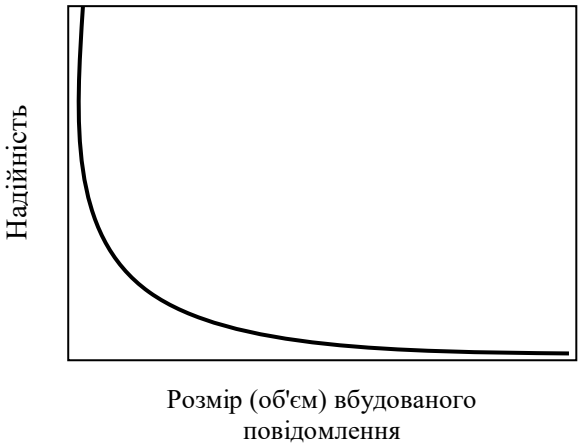

Рис.11.3. Залежність між надійністю і розміром повідомлення

Істотний вплив на надійність стегосистеми й можливість виявлення факту передачі схованого повідомлення виявляє вибір контейнера. Наприклад, досвідчене око цензора з художньою освітою легко виявить зміну колірної гами при впровадженні повідомлення в репродукцію «Мадонни» Рафаеля або «Чорного квадрата» Малевича.

По довжині контейнери можна розділити на два типи: *неперервної* (*потокової*) і *обмеженої* (*фіксованої*) довжини. Особливістю потокового контейнера є те, що неможливо визначити його початок або кінець. Більш того, немає можливості дізнатися заздалегідь, якими будуть наступні шумові біти, що призводить до необхідності включати біти, що приховуються у потік у реальному часі, а самі біти вибираються за допомогою спеціального генератора, що задає відстань між послідовними бітами в потоці.

У неперервному потоці даних труднощі для одержувача – це визначити, коли починається приховане повідомлення. При наявності в потоковому контейнері сигналів синхронізації або границь пакета, приховане повідомлення починається одразу після одного з них. У свою чергу, для відправника можливі проблеми, якщо він не впевнений у тому, що потік контейнера буде досить довгим для розміщення цілого таємного повідомлення.

При використанні контейнерів фіксованої довжини відправник заздалегідь знає розмір файлу й може вибрати біти, що приховують інформацію, у підходящій псевдовипадковій послідовності. З іншого боку, контейнери фіксованої довжини, як це вже відзначалося вище, мають обмежений обсяг повідомлення, що й іноді вбудовується, може не поміститися у файл-контейнер.

Інший недолік полягає в тому, що відстані між бітами, що приховують інформацію рівномірно розподілені між найбільш коротким і найбільш довгим заданими відстанями, у той час як дійсний випадковий шум буде мати експонентний розподіл довжин інтервалу. Звичайно, можна породити псевдовипадкові експоненціальні розподілені числа, але цей шлях звичайно занадто трудомісткий. Однак на практиці найчастіше використовуються саме контейнери фіксованої довжини, як найпоширеніші й доступні.

Можливі наступні варіанти контейнерів.

1. Контейнер *генерується стегосистемою*. Прикладом може служити програма Mandelsteg, у якій у якості контейнера для вбудовування повідомлення генерується фрактал Мандельброта. Такий підхід можна назвати конструюючою стеганографією.

2. Контейнер *обирається з деякої множини контейнерів*. У цьому випадку генерується велика кількість альтернативних контейнерів, щоб потім вибрати найбільш підходящий для приховання повідомлення. Такий підхід можна назвати *селектуючою стеганографією*. У цьому випадку при виборі оптимального контейнера з множини згенерованих найважливішою вимогою є природність контейнера. Єдиною же проблемою залишається те, що навіть оптимально організований контейнер дозволяє сховати незначну кількість даних при дуже великому обсязі самого контейнера.

3. Контейнер *надходить ззовні*. У цьому випадку відсутня можливість вибору контейнера й для приховання повідомлення обирається перший контейнер, що отримано, який може не завжди підходити для повідомлення, що вбудовується. Назвемо це *безальтернативною стеганографією*.

11.3. Стеганографічні методи захисту інформації

Провівши аналіз сучасної наукової літератури, можна виділити чотири напрями стеганографії – це класична, цифрова, лінгвістична та квантова стеганографія. *Класична (традиційна) стеганографія* – спосіб приховування даних, що здійснюється за допомогою технічних засобів ЗІ. Перша згадка [2] про класичні стеганографічні методи у літературі приписується Геродоту, що описав випадок передачі повідомлення Демартом, який зіскоблював віск з дощечок, писав листа прямо на дереві, а потім заново покривав дощечки воском.

Сучасна класична стеганографія (рис. 11.4) включає в себе хімічні та фізичні методи.

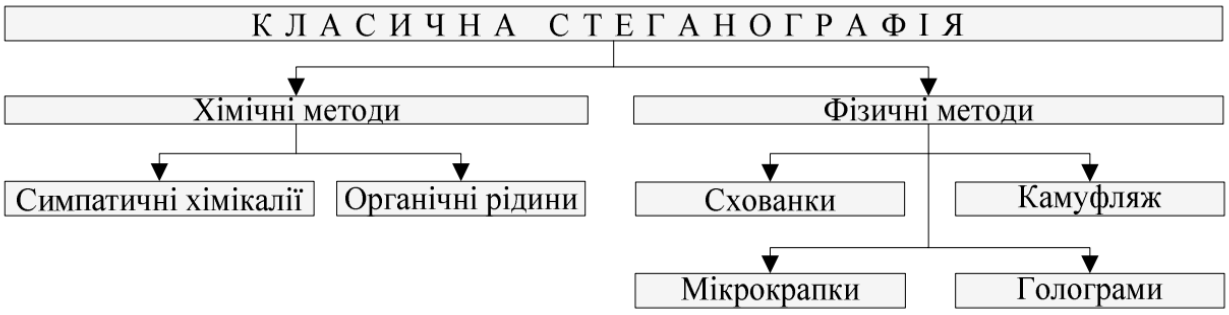

Рис. 11.4. Методи класичної стеганографії

Загалом, хімічні методи стеганографії зводяться до застосування невидимого чорнила. До цих методів відносяться *симпатичні хімікалії* і *органічні рідини*. Симпатичні хімікалії є одним з найбільш поширених методів класичної стеганографії. Зазвичай, процес запису здійснюється наступним чином: перший

шар – наноситься важливий запис невидимим чорнилом, другий шар – нічого не значущий запис видимим чорнилом.

Текст записаний таким чином, що проявляється тільки при певних умовах (нагрівання, освітлення, хімічний проявник тощо). Органічні рідини мають схожі властивості з симпатичними хімікаліями: при нагріванні вони темніють (в них міститься велика кількість вуглецю).

До *фізичних* методів можна віднести різного виду схованки, методи камуфляжу та мікрокрапки. У даний час фізичні методи представляють інтерес в галузі дослідження різних носіїв інформації з метою запису на них даних, які б не виявлялися звичайними методами зчитування. Особливий інтерес присутній до стандартних носіїв інформації, засобів обчислювальної, аудіо- та відеотехніки. Крім цього, з'явився цілий ряд нових технологій, які, базуючись на традиційній стеганографії, використовують останні досягнення мікроелектроніки (голограми).

Схованки для таємних послань використовувалися з часів Стародавньої Греції, замасковані в осях возів, сандалях і підкладках плащів. Схованки для послання можуть приймати найрізноманітніші форми. Для прикладу, персів, що облягали одне із грецьких міст, спритно обдурив один грек Гістіей, зумівши таємно передати послання Мілетському правителю Арістагору. Гістіей оголив наголо свого раба, наніс послання йому на голову і почекав поки волосся відросте. Природно, що обшук гінця на виїзді з міста не дав результатів і послання знайшло адресата.

У наш час Інтернет став сучасною версією подібної схованки. *Мікрокрапки* для стеганографії були розроблені в Німеччині у період між світовими війнами. Пізніше вони стали використовуватися багатьма країнами для передачі секретних повідомлень звичайною поштою. Замість галогенідів срібла стали використовуватися світлочутливі матеріали на основі аніліну, що значно ускладнило пошук мікрокрапок. Після зведення Берлінської стіни для виготовлення мікрокрапок використовувалися спеціальні фотокамери. З того часу мікрокрапки прикріплювалися до непримітного листа і пересилалися поштою.

Мікрокрапки, зважаючи на малий розмір, як правило, залишалися непоміченими. Адресат отримува влиста (рис. 11.5, а) і читав послання у мікрокрапці за допомогою мікроскопа (рис. 11.5, б).

а *б*

Рис. 11.5. Приклад застосування мікрокрапок у стеганографії: а) конверт з мікрокрапкою; б) спеціальний кишеньковий мікроскоп для читання мікрокрапок

Метод на *голографічній основі* полягає в тому, що у зображення-контейнер вбудовуються не безпосередньо конфіденційні дані, а їх голограма. Цей метод має найвищий рівень стійкості до злому. Застосування голографічного підходу, дозволяє здійснювати вбудовування конфіденційних даних у звичайні фотографії на паперовій або пластиковій основі. Основний недолік даного методу пов'язаний з обмеженим обсягом вбудовуваних даних. Найбільш доцільно застосовувати голографічний підхід для приховування невеликих зображень, відновлення яких допускає незначну втрату якості: зразки підписів, відбитків пальців тощо.

На рис. 11.6, а) представлений контейнер із вбудованим факсимільним зразком підпису, а на рис. 11.6, б) показаний результат відновлення.

а *б*

Рис. 11.6. Використання голограм в стеганографії: а) контейнеріз вбудованим факсимільним зразком підпису; б) результат відновлення

Метод *камуфляжу* полягає у тому, що конфіденційне повідомлення маскується таким чином, щоб «зливатися» із забарвленням предмету, який виконує роль контейнера.

Таким чином, проаналізувавши методи класичної стеганографії, можна підбити певні підсумки та виділити їх переваги й недоліки. До переваг класичної стеганографії можна віднести доступність засобів реалізації, а основними недоліками є складність практичної реалізації та можливість випадкового вияву таємного послання.

Цифрова стеганографія – заснована на приховуванні або вбудовуванні додаткової інформації в цифрові об'єкти, викликаючи при цьому деякі їх спотворення (рис. 11.7). Як правило, дані об'єкти є мультимедійними і внесення спотворень, які знаходяться нижче порога чутливості середньостатистичної людини, не призводить до їх помітних змін.

Приховування даних у *просторовій області* може здійснюватися за допомогою наступних методів:

1) метод *заміни найменш значущого біта* (НЗБ), що полягає в заміні останніх значущих бітів в контейнері на біти приховуваного повідомлення;

2) метод *псевдовипадкового інтервалу* – полягає у довільному розподілі бітів секретного повідомлення по контейнеру, в результаті відстань між вбудовуваними бітами визначається псевдовипадково;

3) метод *псевдовипадкової перестановки заснований* на тому, що генератор псевдовипадкових чисел (ПВЧ) утворює послідовність індексів $j_1, j_2, ..., j_{lM}$ та зберігає *k*-й біт повідомлення в пікселі з індексом j_k. Таким чином, секретні біти будуть рівномірно розподілені по всьому бітовому просторі контейнера;

Рис. 11.7. Методи цифрової стеганографії

4) метод *блокового приховування* полягає в тому, що зображення-оригінал розбивається на l_M неперетинних блоків $\Delta_i (1 \le i \le l_m)$ довільної конфігурації, для кожного з яких обчислюється біт парності $b(\Delta_i) : b(\Delta_i) = \sum_{J=\Delta i}^{\mathrm{mod}\,2} LSB(C_j)$.

У кожному блоці виконується приховування одного секретного біта M_i. Якщо біт парності $b(\Delta_i \ne M_i)$, то відбувається інвертування одного з НЗБ блоку $\Delta_i d$ в результаті чого $b(\Delta_i = M_i)$;

5) метод *заміни палітри* полягає в наступному: палітра з Nкольорів визначається як список пар індексів (i, Δ_i), що визначає відповідність між індексом і його вектором забарвлення . Кожному пікселю зображення ставиться у відповідність певний індекс у таблиці. Оскільки порядок кольорів у палітрі не важливий для відновлення загального зображення, конфіденційна інформація може бути прихована шляхом перестановки кольорів у палітрі;

6) метод *квантування зображення* відбувається таким чином, що інформація приховується за рахунок коригування різницевого сигналу Δ_i. Стеганоключ представляє собою таблицю, яка кожному можливому значенню Δi ставить у відповідність визначений біт;

7) метод *Куттера-Джордана-Боссена* – це алгоритм вбудовування в канал синього кольору зображення, яке має {R,G,B} кодування, оскільки досинього кольору зорова система людини є найменш чуттєвою;

8) метод *Дармстедтера-Делейгла-Квісквотера-Макка* базується на елементарному перцепційному (чуттєвому) сприйнятті і дозволяє пристосовувати вбудовування до вмісту блоків контейнера. Перед вбудовуванням конфіденційна

інформація перетворюється у вектор двійкових даних, а кожен біт вбудовується в окремий блок.

Приховування даних в частотній області зображення можливе при використанні таких методів:

1) метод *відносної заміни величин коефіцієнтів дискретно косинусного перетворення (ДКП)* (метод Коха і Жао) – один із найпоширеніших на сьогодні методів приховування секретної інформації в частотній області зображення. Даний метод базується на відносній заміні величин коефіцієнтів ДКП. На початковому етапі зображення розбивається на блоки розміром 8 × 8 пікселів і, в результаті певних перетворень, ДКП застосовується до кожного блоку, потім отримуємо матрицю 8 × 8 коефіцієнтів ДКП. Кожен блок при цьому призначений для приховування 1 біта даних;

2) метод *Бенгама-Мемона-Ео-Юнга є* оптимізованою версією попереднього методу, причому, оптимізація проведена за двома напрямами:

а) для вбудовування використовуються не всі блоки, а лише ті, які найбільш підходять для цього;

б) в частотній області вибирається не 2 а 3 коефіцієнти ДКП;

3) метод *Хсу і Ву* полягає у вбудовуванні цифрового водяного знака у масив коефіцієнтів ДКП блоків зображення-контейнера;

4) метод *Фрідріха* є комбінацією двох алгоритмів – відповідно до одного з них, приховувані дані вбудовуються в низькочастотні, у іншому – в середньо частотні ДКП коефіцієнти.

До методів розширення спектру можна віднести: метод розширення спектру за допомогою прямої псевдовипадкової послідовності (РСПП) полягає в тому, що інформаційний сигнал, при розширенні спектру прямою послідовністю, модулюється функцією, яка приймає псевдовипадкові значення у встановлених межах і множиться на тимчасову константу – частоту (швидкість) проходження елементів сигналу.

Даний псевдовипадковий сигнал містить складові на всіх частотах, які, при їх розширенні модулюють енергію сигналу в широкому діапазоні;метод розширення спектру за допомогою стрибкоподібного перебудовування частот – передавач миттєво змінює одну частоту несучого сигналу на іншу, секретним ключем при цьому є псевдовипадковий закон зміни частот; метод розширення спектру за допомогою компресії з використанням лінійночастотної модуляції (ЛЧМ) заснований на тому, що при компресії з використанням ЛЧМ сигнал модулюється функцією, частота якої змінюється в часі.

Приховування даних в аудіосигналах можливе при використанні наступних методів:

1) *кодування найменш значущих біт* (часова область) відбувається шляхом використання звукового сигналу із заміною НЗБ кожної точки здійснення вибірки, представленої двійковою послідовністю;

2) *фазового кодування* (частотна область) полягає в заміні фази вихідного звукового сегмента на опорну фазу, характер зміни якої відображає собою дані, які необхідно приховати;

3) *розширення спектру* (часова область) використовує технологію РСПП, яка розширює сигнал даних (повідомлення), множачи його на сигнал несучої та псевдовипадкову шумову послідовність, що характеризується широким частотним спектром;

4) приховування даних з *використанням ехо-сигналу* полягає у вбудовуванні даних в аудіосигнал-контейнер шляхом введення в нього ехо-сигналу. Дані приховуються зміною трьох параметрів ехо-сигналу: початкової амплітуди, швидкості загасання і зсуву.

До методів приховування даних в тексті належать:

1) синтаксичні та семантичні методи. До синтаксичних методів [12] відносять методи зміни пунктуації та методи зміни структури і стилю тексту. Семантичні методи подібні до синтаксичних, вони визначають два синоніми котрі відповідають значенням приховуваних біт. Для використання семантичних методів потрібна таблиця синонімів;

2) методи довільного інтервалу ґрунтуються на трьох методах (заміни інтервалу між реченнями, заміни кількості пробілів у кінці текстових рядків, зміни кількості пропусків між словами вирівняного за шириною тексту). Для приховування даних вони використовують вільне місце в тексті.

Проаналізувавши методи цифрової стеганографії, можна виділити їх переваги та недоліки. До переваг можна віднести:

– простоту реалізації методів;
– високу стійкість до атак;
– візуальну незмінність між модифікованим і первинним повідомленнями;
– наявність вільного програмного забезпечення для реалізації методів.

До недоліків цифрової стеганографії можна віднести:

– високу чутливість до найменших спотворень контейнера;
– ймовірність виникнення помилок при детектуванні;
– складність вбудовування інформації в контейнер (у випадку великого об’єму таємного послання).

Лінгвістична стеганографія – напрям, який вивчає методи приховування конфіденційної інформації в непримітний текст, застосовуючи мовні властивості та лінгвістичні ресурси. Лінгвістичні методи стеганографії (рис. 11.8) поділяються на дві основні категорії: умовне письмо і семаграми.

До умовного письма відносять: жаргонний код, геометричну систему, нульовий шифр і шифр «решітка». *Жаргонний код* передбачає використання не привертаючих увагу слів, які мають зовсім інше реальне значення, а текст складається так, щоб виглядати максимально непримітно і правдоподібно.

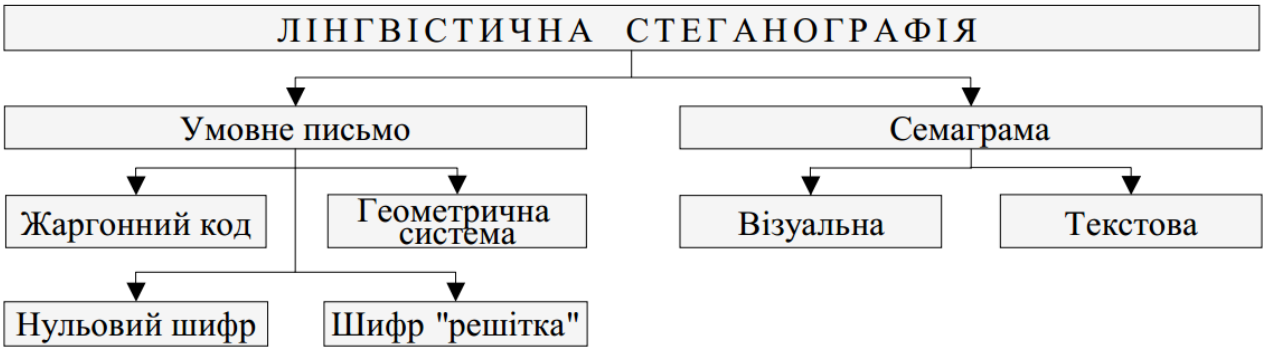

Рис. 11.8.Методи лінгвістичної стегранографії

Жаргонні коди включають в себе нанесення піктограм, таємну термінологію або типову розмову, яка передає особливий зміст внаслідок того, що ключ відомий тільки певним особам. При застосуванні *геометричної системи* мають значення слова, розташовані на сторінці в певних місцях або в точках перетину геометричної фігури заданого розміру.

Нульовий шифр приховує повідомлення відповідно до певного, заздалегідь підготовленого, набору правил (наприклад, «прочитайте кожне п’яте слово» або «подивіться на третю букву в кожному слові»). Шифр «решітка» застосовує шаблон, який використовується для приховування повідомлення-контейнера. Слова, які з’являються в отворах шаблону, є прихованим повідомленням.

Іншу категорію лінгвістичних методів становлять *семаграми* – таємні повідомлення, в яких значеннями шифру є будь-які символи (крім літер і цифр). Наприклад, ці повідомлення можуть бути передані в малюнку, що містить крапки і тире для читання за кодом Морзе.

Візуальна семаграма використовує, на перший погляд, нешкідливі звичайні фізичні об’єкти для передачі повідомлення. Наприклад, умовний знак рукою, розміщення предметів на столі в певній послідовності, характерні зміни в дизайні веб-сайту – все це семаграми. Текстова семаграма приховує повідомлення, змінюючи зовнішній вигляд тексту-контейнера (наприклад, ледь помітні зміни в розмірі або типі шрифту, додавання додаткових пробілів, різних завитків у буквах рукописного тексту).

Основною перевагою методів лінгвістичної стеганографії є можливість передавання повідомлення великої довжини, а головними недоліками – можливість випадкового вияву алгоритму кодування (здатність людини відчути суттєву різницю між модифікованим і первинним повідомленнями) та складність процесу кодування повідомлення.

Квантова стеганографія аналогічно традиційним аналогам має за мету приховування самого факту передачі інформації. Квантова стеганографія ще не набула масовості, але у деяких працях пропонуються моделі систем ЗІ, що використовують квантові властивості. Даний напрям є синтезом класичної і квантової інформатики та заснований на злитті понять квантової фізики та класичної теорії інформації.

Контрольні питання

1. Визначте поняття «стеганографія», «контейнер».
2. Перерахуйте положення, які повинні враховуватися при побудові стеганографічних систем.
3. Перерахуйте вимоги, що ставляться перед стеганографічними системами?
4. Для чого використовуються цифрові водяні знаки?
5. Які недоліки притаманні стегосистемі при використанні контейнерів фіксованої довжини?
6. Назвіть можливі варіанти контейнерів.
7. Назвіть стеганографічні методи захисту інформації.

Література для самопідготовки

1. Хорошко В.О. Методы и средства защиты информации / Хорошко В.О., Чекатов И. О. – Киев: ГУИКТ. – 2007. – С.444–475.
2. Мельников В.В. Защита информации в компьютерных системах / Мельников В.В. – М.: Финансы и статистика. Электроинформ, 1997.– С.135–150.

ЛЕКЦІЯ 12. ОСОБЛИВОСТІ ЗАХИСТУ ІНФОРМАЦІЇ В БАЗАХ ДАНИХ

12.1. Загрози в БД.
12.2. Реалізація системи захисту в MS SQL Server.

12.1. Загрози в базах даних

БД розглядаються як надійне сховище структурованих даних, забезпечене спеціальним механізмом для їх ефективного використання в інтересах користувачів (процесів). Таким механізмом є система керування базою даних (СКБД).

Під *СБКД* розуміють програмні або апаратно-програмні засоби, що реалізовують функції управління даними, такі як: перегляд, сортування, вибірка, модифікація, виконання операцій визначення статистичних характеристик тощо. БД розміщуються:

1) на комп'ютерній системі користувача;
2) на спеціально виділеній ЕОМ (сервері).

Як правило, на комп'ютерній системі користувача розмішаються особисті або персональні бази даних, які обслуговують процеси одного користувача. У обчислювальних мережах БД розмішаються на серверах. У локальних і корпоративних мережах, як правило, використовуються централізовані БД. Загальнодоступні глобальні мережі мають розподілені БД. У таких мережах сервери розміщуються на різних об'єктах мережі.

Як сервери часто використовуються спеціалізовані ПЕОМ, пристосовані до зберігання великих об'ємів даних, збереження, що забезпечують, і доступність інформації, а також оперативність обробки запитів, що поступають. У централізованих БД простіше вирішуються проблеми зашиті інформації від умисних загроз, підтримки актуальності і несуперечності даних. Перевагою розподілених баз даних, за умови дублювання даних, є їх висока захищеність від стихійних лих, аварій, збоїв технічних засобів, а також диверсій.

Захист інформації в базах даних, на відміну від захисту даних у файлах, має і свої особливості:

– необхідність обліку функціонування СКБД при виборі механізмів захисту;

– розмежування доступу до інформації реалізується не на рівні файлів, а на рівні частин БД;

– при створенні засобів захисту інформації в базах даних необхідно враховувати взаємодію цих засобів не лише з ОС, але і з СКБД. При цьому можливе вбудовування механізмів захисту в СКБД або використання їх у вигляді окремих компонент.

Для більшості СУБД надання їм додаткових функцій можливе тільки на етапі розробки СКБД. У експлуатовані системи управління базами даних додаткові компоненти можуть бути внесені шляхом розширення або модифікації мови управління. Таким шляхом можна здійснювати нарощування можливостей, наприклад, в СКБД Кліппер.

У сучасних БД досить успішно вирішуються завдання розмежування доступу, підтримка фізичної цілісності і логічного збереження даних. Алгоритми розмежування доступу до записів і навіть до полів записів відповідно до повноважень користувача добре відпрацьовані, і здолати цей захист зловмисник може лише за допомогою фальсифікації повноважень або впровадження шкідницьких програм. Розмежування доступу до файлів БД і до частин баз даних здійснюється СКБД шляхом встановлення повноважень користувачів і контролю цих повноважень при допуску до об’єктів доступу.

Повноваження користувачів встановлюються адміністратором СКБД. Зазвичай стандартним ідентифікатором користувача є пароль, що передається в зашифрованому виді. У розподілених КС процес підтвердження достовірності користувача доповнюється спеціальною процедурою взаємної аутентифікації видалених процесів. БД, що містять конфіденційну інформацію, зберігаються на зовнішніх пристроях, що запам’ятовують, в зашифрованому виді.

Фізична цілісність баз даних досягається шляхом використання відмовостійких пристроїв, побудованих, наприклад, за технологією RAID.

RAID (англ. redundant array of independent/inexpensive disks) – це надлишковий масив незалежних/недорогих дисків для комп’ютера. Дисковий масив – це набір дискових пристроїв, що працюють разом, щоб підвищити швидкість і надійність системи вводу/виводу. Цим набором пристроїв управляє спеціальний *RAID-контролер* (контролер масиву), який забезпечує функції розміщення даних по масиву; а для решти всієї системи дозволяє представляти весь масив як один логічний пристрій вводу/виводу. За рахунок паралельного виконання операцій читання і запису на кількох дисках, масив забезпечує підвищену швидкість обмінів в порівнянні з одним великим диском.

Логічне збереження даних означає неможливість порушення структури моделі даних. Сучасні СКБД забезпечують таку логічну цілісність і несуперечність на етапі опису моделі даних.

У базах даних, працюючих з конфіденційною інформацією, необхідно додатково використовувати криптографічні засоби ЗІ. Для цієї мети використовується шифрування як за допомогою єдиного ключа, так і за допомогою індивідуальних ключів користувачів. Застосування шифрування з індивідуальними ключами підвищує надійність механізму розмежування доступу, але істотно ускладнює управління.

Можливі два режими роботи із зашифрованими БД:

1) для виконання запиту необхідний файл або частина файлу розшифровується на зовнішньому носії, з відкритою інформацією виконуються необхідні дії, після чого інформація на зовнішньому запам'ятовуючому пристрої знову зашифровується.

Перевагою такого режиму є незалежність функціонування засобів шифрування і СКБД, які працюють послідовно один за одним. В той же час збій або відмова в системі може привести до того, що на зовнішньому запам'ятовуючому пристрої частина БД залишиться записаною у відкритому виді.

2) виконання СКБД запитів користувачів без розшифрування інформації на зовнішньому запам'ятовуючому пристрої. Пошук необхідних файлів, записів, полів, груп полів не вимагає розшифрування. Розшифрування проводиться в оперативній пам'яті безпосередньо перед виконанням конкретних дій з даними.

Такий режим можливий, якщо процедури шифрування вбудовані в СКБД. При цьому досягається високий рівень захисту від несанкціонованого доступу, але реалізація режиму пов'язана з ускладненням СКБД. Надання СКБД можливості підтримки такого режиму роботи здійснюється, як правило, на етапі розробки СКБД.

При побудові захисту БД необхідно враховувати ряд специфічних загроз безпеки інформації, пов'язаних з концентрацією в БД великої кількості різноманітної інформації, а також з можливістю використання складних запитів обробки даних. До таких загроз відносяться:

1) інтерференція;

2) агрегація;

3) комбінація дозволених запитів для отримання закритих даних.

Під *інтерференцією* розуміється отримання конфіденційної інформації з відомостей з меншою мірою конфіденційності шляхом висновків. Якщо враховувати, що в базах даних зберігається інформація, що отримана з різних джерел в різний час, відрізняється мірою узагальненості, то аналітик може отримати конфіденційні відомості шляхом порівняння, доповнення і фільтрації даних, до яких він допущений.

Крім того, він обробляє інформацію, отриману з відкритих БД, засобів масової інформації, а також використовує прорахунки осіб, що визначають міру важливості і конфіденційності окремих явищ, процесів, фактів, отриманих результатів. Такий спосіб отримання конфіденційних відомостей, наприклад, по

матеріалах засобів масової інформації, використовується давно, і показав свою ефективність.

Близьким до інтерференції є інший спосіб добування конфіденційних відомостей – *агрегація*. Під агрегацією розуміється спосіб отримання важливіших відомостей в порівнянні з важливістю тих окремо взятих даних, на основі яких і виходять ці відомості. Так, зведення про діяльність одного відділення або філії корпорації мають певну вагу. Дані ж за усю корпорацію мають куди велику значущість.

Якщо інтерференція і агрегація є способами добування інформації, які застосовуються не лише відносно БД, то *спосіб спеціального комбінування запитів* використовується тільки при роботі з БД. Використання складних, а також послідовності простих логічно пов'язаних запитів дозволяє отримувати дані, до яких доступ користувачеві закритий. Така можливість є, передусім, в базах даних, що дозволяють отримувати статистичні дані. При цьому окремі записи, поля, (індивідуальні дані) є закритими.

В результаті запиту, в якому можуть використовуватися логічні операції AND, OR, NOT, користувач може отримати такі величини як кількість записів, сума, максимальне або мінімальне значення. Використовуючи складні перехресні запити і наявну в його розпорядженні додаткову інформацію про особливості запису (поля), що цікавить, зловмисник шляхом послідовної фільтрації записів може дістати доступ до потрібного запису (полю).

Протидія подібним загрозам здійснюється наступними методами:

1) блокування відповіді при неправильному числі запитів;
2) спотворення відповіді шляхом округлення і іншої умисної корекції даних;
3) розподіл БД;
4) випадковий вибір запису для обробки;
5) контекстно-орієнтований захист;
6) контроль запитів, що поступають.

Метод *блокування* відповіді при неправильному числі запитів припускає відмова у виконанні запиту, якщо в ньому міститься більше певного числа співпадаючих записів з попередніх запитів. Таким чином, цей метод забезпечує виконання принципу мінімального взаємозв'язку питань. Цей метод складний в реалізації, оскільки необхідно запам'ятовувати і порівнювати усі попередні запити.

Метод *корекції* полягає в незначній зміні точної відповіді на запит користувача. Для того, щоб зберегти прийнятну точність статистичної інформації, застосовується так званий свопінг даних. Суть його полягає у взаємному обміні значень полів запису, внаслідок чого усі статистики 1-го порядку, що включають 1 атрибутів, виявляються захищеними для усіх 1, менших або рівніших деякому числу. Якщо зловмисник зможе виявити деякі дані, то він не зможе визначити, до якої конкретно запису вони відносяться.

Застосовується також метод *розподілу баз даних* на групи. У кожну групу може бути включено не певнішого числа записів. Запити дозволені до будь-якої безлічі груп, але забороняються до підмножини записів з однієї групи. Застосування цього методу обмежує можливості виділення даних зловмисником на рівні не нижче за групу записів. Метод розподілу баз даних не знайшов широкого застосування із-за складності отримання статистичних даних, оновлення і реструктуризації даних.

Ефективним методом протидії дослідженню баз даних є *метод випадкового вибору записів* для статистичної обробки. Така організація вибору записів не дозволяє зловмисникові простежити множину запитів.

Суть *контекстно-орієнтованого* захисту полягає в призначенні атрибутів доступу (читання, вставка, видалення, оновлення, управління тощо) елементам БД (записам, полям, групам полів) залежно від попередніх запитів користувача.

Наприклад, нехай користувачеві доступні в окремих запитах поля: «ідентифікаційні номери» і «прізвища співробітників», а також 2ідентифікаційні номери» і «розмір заробітної плати». Зіставивши відповіді по цих запитах, користувач може отримати закриту інформацію про заробітну плату конкретних працівників. Для виключення такої можливості користувачеві слід заборонити доступ до поля «ідентифікатор співробітника» в другому запиті, якщо він вже виконав перший запит.

Одним з найбільш ефективних методів захисту інформації в БД є *контроль запитів*, що надходять, на наявність «підозрілих» запитів або комбінації запитів. Аналіз подібних спроб дозволяє виявити можливі канали отримання несанкціонованого доступу до закритих даних.

12.2. Реалізація системи захисту в MS SQL Server

SQL Server 6.5 підтримує 3 режими перевірки при визначенні прав користувача: стандартний (standard); інтегрований (integrated security); змішаний (mixed).

Стандартний режим захисту припускає, що кожен користувач повинен мати обліковий запис як користувач домена NT Server. Обліковий запис користувача домена включає ім’я користувача і його індивідуальний пароль.

Користувачі доменів можуть бути об’єднані в групи. Як користувач домена користувач дістає доступ до певних ресурсів домена. Як один з ресурсів домена і розглядається SQL Server. Але для доступу до SQL Server користувач повинен мати обліковий запис користувача MS SQL Server.

Цей обліковий запис також повинен включати унікальне ім’я користувача сервера і його пароль. При підключенні до операційного середовища користувач задає своє ім’я і пароль користувача домена. При підключенні до сервера БД користувач задає своє унікальне ім’я користувача SQL Server і свій пароль.

Інтегрований режим припускає, що для користувача задається тільки один обліковий запис в операційній системі, як користувача домена, а SQL Server ідентифікує користувача за його даними в цьому обліковому записі. В цьому випадку користувач задає тільки одне своє ім'я і один пароль.

У разі *змішаного режиму* частина користувачів може бути підключена до сервера з використанням стандартного режиму, а частина з використанням інтегрованого режиму.

У MS SQL Server 7.0 залишено тільки 2 режими: інтегрований, що називається Windows NT Authentication Mode (Windows NT Authentication), і змішаний – Mixed Mode (Windows NT Authentication and SQL Server Authentication). Алгоритм перевірки аутентифікації користувача в MS SQL Server 7.0 наведений на рис. 12.1.

При спробі підключення до сервера БД спочатку перевіряється, який метод аутентифікації визначений для цього користувача. Якщо визначений Windows NT Authentication Mode, то далі перевіряється, чи має цей користувач домена доступ до ресурсу SQL Server, якщо він має доступ, то виконується спроба підключення з використанням імені користувача і пароля, визначених для користувача домена; якщо цей користувач має права підключення до SQL Server, то підключення виконується успішно, інакше користувач отримує повідомлення про те, що цьому користувачеві не дозволено підключення до SQL Server.

При використанні змішаного режиму аутентифікації засобами SQL Server проводиться послідовна перевірка імені користувача (login) і його пароля (password); якщо ці параметри задані коректно, то підключення завершується успішно, інакше користувач також отримує повідомлення про неможливість підключитися до SQL Server.

Для СУБД Oracle завжди використовується на додаток до імені користувача і пароля в операційному середовищі його ім'я і пароль для роботи з сервером БД.

Перевірка повноважень

Другим завданням при роботі з БД, як вказувалося раніше, являється перевірка повноважень користувачів. Повноваження користувачів зберігаються в спеціальних системних таблицях, і їх перевірка здійснюється ядром СКБД при виконанні кожної операції. Логічно для кожного користувача і кожного об'єкту в БД як би будується деяка умовна матриця, де по одному виміру розташовані об'єкти, а по іншому – користувачі. На перетині кожного стовпця і кожного рядка розташований перелік дозволених операцій для цього користувача над цим об'єктом.

З першого погляду здається, що ця модель перевірки досить стійка. Але складність виникає тоді, коли ми використовуємо непряме звернення дооб'єктів. Наприклад, користувачеві user_N не дозволений доступ до таблиці Tab1, але цьому користувачеві дозволений запуск процедури SP_N, що зберігається, яка робить вибірку з цього об'єкту. За умовчанням усі процедури, що зберігаються, запускаються під ім'ям їх власника.

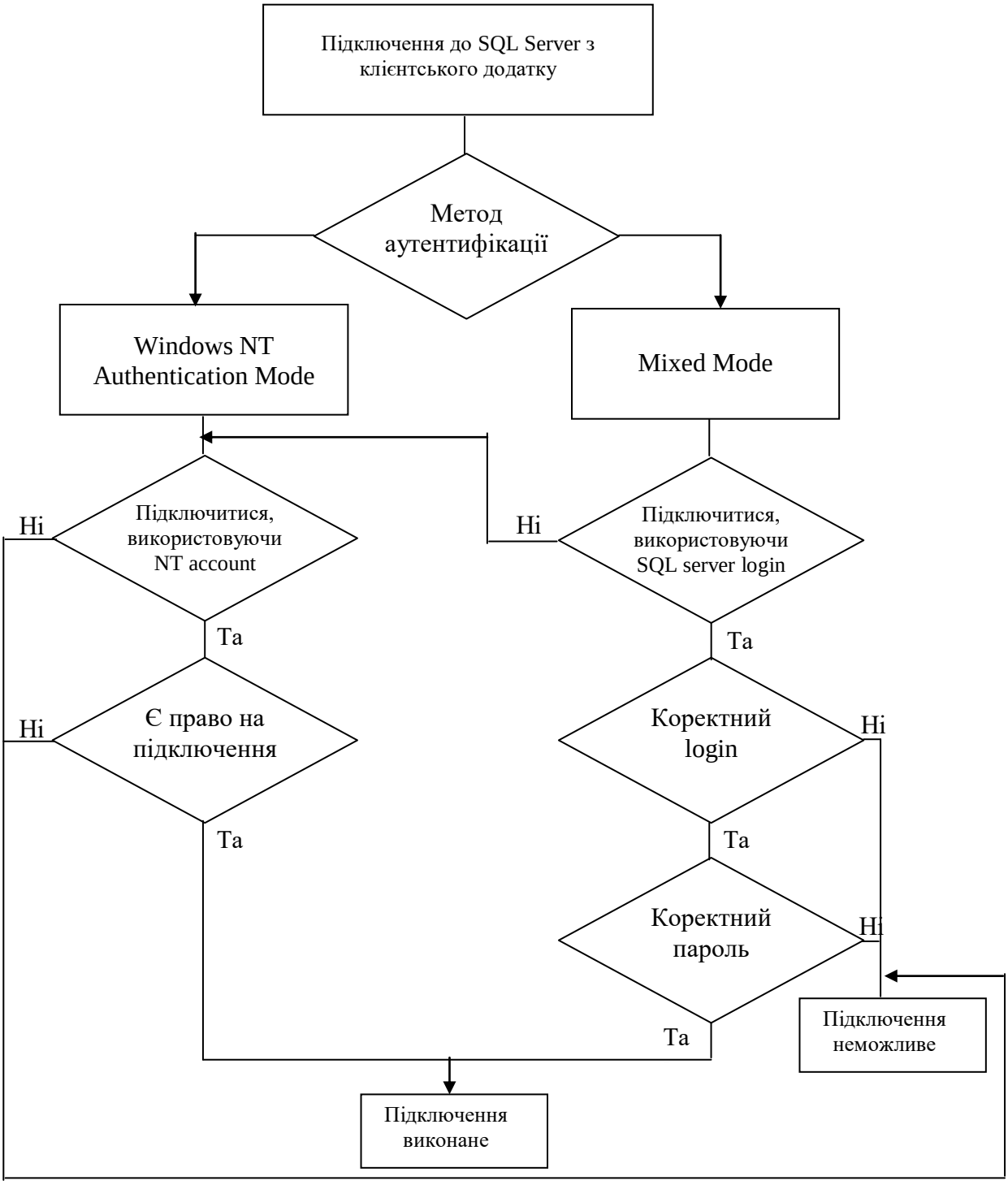

Рис. 12.1. Алгоритм перевірки аутентифікації користувача в MS SQL Server 7.0

Такі проблеми повинні вирішуватися організаційними методами. При дозволі доступу деяких користувачів необхідно пам’ятати про можливість непрямого доступу. У будь-якому випадку проблема захисту ніколи не була чисто технічним завданням, це комплекс організаційно-технічних заходів, які повинні забезпечити максимальну конфіденційність інформації, що зберігається в БД.

Крім того, при роботі в мережі існує ще проблема перевірки достовірності повноважень. Ця проблема полягає в наступному. Припустимо, процесу 1 дані

повноваження по роботі з БД, а процесу 2 такі повноваження не дані. Тоді безпосередньо процес 2 не може звернутися до БД, але він може звернутися до процесу 1 і через нього дістати доступ до інформації з БД.

Тому в безпечному середовищі має бути присутній модель перевірки достовірності, яка забезпечує підтвердження заявлених користувачами або процесами ідентифікаторів. Перевірка повноважень набула ще більшого значення в умовах масового поширення розподілених обчислень. При існуючому високому рівні зв'язності обчислювальних систем необхідно контролювати усі звернення до системи.

Проблеми перевірки достовірності зазвичай відносять до сфери безпеки комунікацій і мереж, тому ми не будемо їх тут більше обговорювати, за винятком наступного зауваження. У цілісній системі комп'ютерної безпеки, де чітке виконання програми захисту інформації забезпечується за рахунок взаємодії відповідних засобів в операційних системах, мережах, базах даних, перевірка достовірності має пряме відношення до безпеки БД.

Помітимо, що модель безпеки, заснована на базових механізмах перевірки повноважень і перевірки достовірності, не вирішує таких проблем, як вкрадені призначені для користувача ідентифікатори і паролі або зловмисні дії деяких користувачів, що мають повноваження, наприклад, коли програміст, що працює над обліковою системою, що має повний доступ до облікової БД, вбудовує в код програми «Троянського коня» з метою розкрадання або навмисної зміни інформації, що зберігається в БД.

Такі питання виходять за рамки нашого обговорення засобів захисту БД, але слід проте уявляти собі, що програма забезпечення інформаційної безпеки повинна охоплювати не лише технічні області (такі як захист мереж, баз цих і операційних систем), але і проблеми фізичного захисту, надійності персоналу (приховані перевірки), аудит, різні процедури підтримки безпеки виконувані вручну і частково автоматизовані.

В Microsoft SQL Server 2005 реалізована досить пристойна підтримка *криптографії*. За допомогою вбудованих засобів можна шифрувати дані, використовуючи як симетричні, так і асиметричні алгоритми. Є підтримка операції хешування й електронному підпису. Реалізована непогана система керування ключами (наскільки це взагалі можливо без використання спеціальних пристроїв). Цих можливостей цілком достатньо, щоб побудувати криптографічну систему захисту даних, звичайно, якщо поставлене завдання взагалі можна розв'язати застосуванням криптографії.

Але щоб скористатися всіма можливостями, що надаються SQL Server, у додаток повинен бути вбудовано відповідна функціональність. Причому це стосується не тільки коду, але й структури БД, у яку, імовірно, також буде потрібно внести зміни, що зумовлені особливостями роботи із зашифрованими даними. Застосування криптографії може привести до падіння продуктивності додатка за рахунок додаткових витрат на шифрування й розшифрування. Крім

того, марність використання індексів на зашифрованих даних також може позначитися на продуктивності додатка не кращим чином. Усе це повинне бути враховане в додатку, а захищатися повинні тільки ті дані, для яких це дійсно потрібно.

В Microsoft SQL Server 2008 з'явився новий розв'язок для позначених вище проблем – це *прозоре шифрування БД* (Transparent Data Encryption або TDE). TDE дозволяє шифрувати бази даних цілком. Коли сторінка даних скидається з оперативної пам'яті на диск, вона шифрується. Коли сторінка завантажується назад в оперативну пам'ять, вона розшифровується. Таким чином, база даних на диску виявляється повністю зашифрованою, а в оперативній пам'яті – ні.

Основною перевагою TDE є те, що шифрування й розшифрування виконуються абсолютно прозоро для додатків. Отже, одержати переваги від використання TDE може будь-який додаток, що використовує для зберігання своїх даних Microsoft SQL Server 2008. При цьому модифікацію або доробку додатка проводити не потрібно.

На жаль, Transparent Data Encryption (TDE) буде доступно тільки в Enterprise- і Developer-редакціях SQL Server 2008.

Ієрархія ключів

Для розв'язку цього завдання в SQL Server застосовується спеціальна ієрархія ключів. У контексті TransparentDataEncryption (TDE) вона будується таким чином:

– Для кожної БД, яка шифрується за допомогою Transparent Data Encryption (TDE) створюється спеціальний ключ – Database Encryption Key (DEK). Цей ключ використовується для шифрування даних.

– Database Encryption Key (DEK) шифрується сертифікатом, який повинен бути створений у БД master.

Далі – стандартно:

– Цей сертифікат шифрується головним ключем БД master.

– Головний ключ БД master шифрується головним ключем служби (Service Master Key або SMK).

– Головний ключ служби (SMK) шифрується за допомогою DPAPI.

Уся ієрархія наведена на рис. 12.2.

Така схема дозволяє SQL Server у будь-який момент часу одержати доступ до ключа,за допомогою якого зашифрована БД, а, отже, і до зашифрованих даних. І в той же час, ніхто інший одержати доступ до цих даних не може. Але нажаль, це теорія, а на практиці є дуже обмежений список загроз, яким здатне протистояти Transparent Data Encryption (TDE).

Якщо зловмисник зміг одержати доступ до даних, що захищаються, через SQL Server, то Transparent Data Encryption (TDE) виявляється абсолютно безкорисним. Дані зашифровані тільки на диску, а в пам'яті – ні. Зашифрована база даних виглядає для користувачів абсолютно так само, як і незашифрована.

Для захисту від адміністраторів Transparent Data Encryption (TDE) так само безсило. Адміністратор SQL Server може шифрування просто відключити.

Системний адміністратор при бажанні також зможе знайти тисячу й один спосіб одержати доступ до зашифрованих даних (навіть якщо він не є адміністратором SQL Server).

Рис. 12.2. Ієрархія ключів

Що реально може зробити Transparent Data Encryption (TDE), так це захистити файли баз даних і резервні копії на випадок їх викрадення. І це вже непогано. Якщо зняти копію з файлів активної БД не так просто (хоча й можливо), то викрадення резервної копії при наявності до них доступу не представляє ніяких проблем (які можуть бути проблеми сунути носій з резервною копією в кишеню).

Але й отут є свої обмеження. Файли БД і резервні копії будуть надійно захищені, тільки якщо зловмисникові не вдасться разом з даними роздобути й ключ. Якщо йому це вдасться, то він без проблем розшифрує секретні дані. Самою слабкою ланкою тут є головний ключ служби (SMK), який перебуває на вершині ієрархії ключів і який захищається за допомогою DPAPI.

Також слід зазначити, що Transparent Data Encryption (TDE) – це не заміна криптографічним можливостям, які є в SQL Server 2005. Якщо шифрування в SQL Server 2005 працює на рівні значень і стовпців («cell-level»-шифрування), то Transparent Data Encryption (TDE) працює на набагато більш високому рівні – на рівні бази даних.

Завдання, які вирішуються за допомогою обох підходів багато в чому перетинаються, але в кожного з них є свої переваги й недоліки. Обидва підходи

використовують ті самі криптографічні алгоритми (з тими ж довжинами ключів), так що криптографічно вони забезпечують однаковий рівень захисту даних.

Настроювання TDE

Щоб зашифрувати базу даних за допомогою Transparent Data Encryption (TDE), потрібно виконати наступні кроки:

1. Створити головний ключ БД master (якщо він не був створений раніше):

```
USEmaster
go
CREATEMASTERKEYENCRYPTIONBYPASSWORD = 'My$Strong$Password$123'
```

2. Створити або імпортувати сертифікат, закритий ключ якого повинен бути зашифрований головним ключем БД master:

```
CREATECERTIFICATEDEK_EnccertWITHSUBJECT = 'DEK Encryption Certificate'
```

3. Далі в базі даних, яку ми збираємося шифрувати, потрібно створити Database Encryption Key (DEK). DEK шифрується сертифікатом, який ми створили на попередньому кроці.

```
USEMysecretdb
go
CREATEDATABASEENCRYPTIONKEYWITHALGORITHM = AES_256
ENCRYPTIONBYSERVERCERTIFICATEDEK_Enccert
```

Перевірити, що Database Encryption Key (DEK) дійсно створений, можна за допомогою системного представлення sys.dm_database_encryption_keys.

```
SELECTDB_NAME(database_id), * FROMsys.dm_database_encryption_keys
```

	(No column name)	database_id	encryption_state	create_date	regenerate_...	modify_date	set_date	opened_date
1	MySecretDB	9	1	2008-01-14 ...	2008-01-14 ...	2008-01-14...	NULL	2008-01-14 ...

У цей момент усе готове для того, щоб включити шифрування БД.

```
ALTERDATABASEMysecretdbSETENCRYPTIONON
```

Із цього моменту починається процес первісного шифрування БД. Він виконується «на фоні» в окремому потоці. Відстежити прогрес виконання цієї операції можна по стовпцю percent_complete уже згаданого нами раніше системного представлення sys.dm_database_encryption_keys. Так, якщо виконати наведений нижче запит у процесі виконання первісного шифрування бази даних, то ми можемо одержати, наприклад наступний результат:

```
SELECTDB_NAME(database_id),                                    encryption_state,
percent_completeFROMsys.dm_database_encryption_keys
```

	(No column name)	encryption_state	percent_complete
1	tempdb	3	0
2	MySecretDB	2	43.20966

А коли процес первісного шифрування бази даних буде завершений, запит поверне наступний результат.

	(No column name)	encryption_state	percent_complete
1	tempdb	3	0
2	MySecretDB	3	0

У стовпці encryption_state утримується інформація про поточний стан бази даних. Згідно SQL Server Books Online (BOL), у контексті Transparent Data Encryption (TDE) БД може перебувати в одному з наступних станів:

0 – Database Encryption Key (DEK) не створений.
1 – Database Encryption Key (DEK) створений, але БД не зашифрована.
2 – Виконується первісне шифрування.
3 – БД зашифрована.
4 – Іде зміна ключа.
5 – Іде розшифрування.

Контрольні питання

1. Визначте поняття «система керування базою даних», «».
2. Назвіть особливості захисту інформації в базах даних.
3. Назвіть режими роботи із зашифрованими базами даних.
4. Зо розуміється під терміном «агрегація» при добуванні конфіденційної інформації?
5. Перерахуйте методи протидії несанкціонованому доступу до баз даних.
6. Що передбачає стандартний режим захисту баз даних SQL Server 6.5?
7. Дайте визначення поняттям «фізична цілісність бази даних».

Література для самопідготовки

1. Антонюк А.О. Основи захисту інформації в автоматизованих системах управління / Антонюк А.О. – Київ: Видавничий дім "КМ академія", 2003. – С.126–136.
2. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа / Щеглов А.Ю. – СПб: Наука и техника, 2004.– С.68–93.

ЛЕКЦІЯ 13. ОЦІНКА ЕФЕКТИВНОСТІ СЗІ В АСУ

13.1. Моделювання комплексних СЗІ.
13.2. Підходи до оцінки ефективності комплексних СЗІ.

13.1. Моделювання комплексних СЗІ

Оцінка ефективності функціонування КСЗІ є складним науково-технічним завданням. Комплексна СЗІ оцінюється в процесі розробки КС, в період експлуатації і при створенні (модернізації) СЗІ для вже існуючих КС. При розробці складних систем поширеним методом проектування є синтез з подальшим аналізом. Система синтезується шляхом узгодженого об'єднання блоків, пристроїв, підсистем і аналізується (оцінюється) ефективність отриманого рішення. З безлічі синтезованих систем вибирається краща за наслідками аналізу, який здійснюється за допомогою моделювання.

Моделювання КСЗІ полягає в побудові образу (моделі) системи, з певною точністю відтворюючого процеси, що відбуваються в реальній системі. Реалізація моделі дозволяє отримувати і досліджувати характеристики реальної системи.

Для оцінки систем використовуються аналітичні і імітаційні моделі. У *аналітичних моделях* функціонування досліджуваної системи записується у вигляді математичних або логічних співвідношень. Для цих цілей використовується могутній математичний апарат: алгебра, функціональний аналіз, різницеві рівняння, теорія вірогідності, математична статистика, теорія множин, теорія масового обслуговування і так далі.

При *імітаційному моделюванні* система представляється у вигляді деякого аналога реальної системи. В процесі імітаційного моделювання на ПЕОМ реалізуються алгоритми зміни основних характеристик реальної системи відповідно до еквівалентних реальним процесам математичними і логічними залежностями.

Моделі діляться також на детерміновані і стохастичні. Моделі, які оперують з випадковими величинами, називаються стохастичними. *Оскільки* на процеси

захисту інформації основний вплив роблять випадкові чинники, то моделі систем захисту є стохастичними.

Моделювання КСЗІ є складним завданням, тому що такі системи відносяться до класу складних організаційно-технічних систем, яким властиві наступні особливості:

1) складність формального представлення процесів функціонування таких систем, головним чином, із-за складності формалізації дій людини;

2) різноманіття архітектури складної системи, яке обумовлюється різноманіттям структур її підсистем і множинністю шляхів об'єднання підсистем в єдину систему;

3) велике число взаємозв'язаних між собою елементів і підсистем;

4) складність функцій, що виконуються системою;

5) функціонування систем в умовах неповної визначеності і випадковості процесів, що надають дію на систему;

6) наявність безлічі критеріїв оцінки ефективності функціонування складної системи;

7) існування інтегрованих ознак, властивих системі в цілому, але не властивих кожному елементу окремо (наприклад, система з резервуванням є надійною, при ненадійних елементах);

8) наявність управління, що часто має складну ієрархічну структуру;

9) розгалуженість і висока інтенсивність інформаційних потоків.

Для подолання цих складнощів застосовуються:

– спеціальні методи неформального моделювання;
– декомпозиція загального завдання на ряд окремих завдань;
– макромоделювання.

Спеціальні методи неформального моделювання

Спеціальні методи неформального моделювання засновані на застосуванні неформальної теорії систем. Основними складовими частинами неформальної теорії систем є:

а) структуризація архітектури і процесів функціонування складних систем;

б) неформальні методи оцінювання;

в) неформальні методи пошуку оптимальних рішень**.**

Структуризація є розвитком формального опису систем, поширеного на організаційно-технічні системи.

Прикладом структурованого процесу є конвеєрне виробництво. У основі такого виробництва лежать два принципи:

– строга регламентація технологічного процесу виробництва;
– спеціалізація виконавців і устаткування.

Передбачається, що конструкція продукції, що виробляється відповідає наступним вимогам:

а) виріб складається з конструктивних ієрархічних елементів (блоків, вузлів, схем, деталей і тому подібне);

б) максимальна простота, уніфікованість і стандартність конструктивних рішень і технологічних операцій.

В даний час процес виробництва технічних засобів КС достатньо повно структурований. Структурне програмування також вписується в рамки структурованих процесів. На основі узагальнення принципів і методів структурного програмування можуть бути сформульовані умови структурованого опису систем, що вивчаються, і процесів їх функціонування:

– повнота відображення основних елементів;

– адекватність;

– простота внутрішньої організації елементів опису і взаємозв'язків елементів між собою;

– стандартність і уніфікованість внутрішньої структури елементів і структури взаємозв'язків між ними;

– модульність;

– гнучкість, під якою розуміється можливість розширення і зміни структури одних компонентів моделі без істотних змін інших компонентів;

– доступність вивчення і використання моделі будь-якому фахівцеві середньої кваліфікації відповідного профілю.

В процесі проектування систем необхідно отримати їх характеристики. Деякі характеристики можуть бути отримані шляхом вимірювання. Інші виходять з використанням аналітичних співвідношень, а також в процесі обробки статистичних даних. Проте існують характеристики складних систем, які не можуть бути отримані приведеними методами. До таких характеристик СЗІ відноситься вірогідність реалізації деяких загроз, окремі характеристики ефективності систем захисту та інші.

Вказані характеристики можуть бути отримані єдино доступними методами – методами ***неформального оцінювання.*** Суть методів полягає в залученні для отримання деяких характеристик фахівців-експертів у відповідних галузях знань.

Найбільшого поширення з неформальних методів оцінювання набули методи експертних оцінок. Методом експертних оцінок є алгоритм підбору фахівців-експертів, завдання правил отримання незалежних оцінок кожним експертом і подальшої статистичної обробки отриманих результатів. Методи експертних оцінок використовуються давно, добре відпрацьовані. В деяких випадках вони є єдино можливими методами оцінювання характеристик систем.

Неформальні методи пошуку оптимальних рішень можуть бути розподілені по двох групах:

– методи неформального зведення складного завдання до формального опису і рішення задачі формальними методами;

– неформальний пошук оптимального рішення.

Для моделювання систем захисту інформації доцільно використовувати наступні теорії і методи, що дозволяють звести рішення задачі до формальних алгоритмів:

1) теорія нечітких множин;
2) теорія конфліктів;
3) теорія графів;
4) формально-евристичні методи;
5) еволюційне моделювання.

Методи *теорії нечітких множин* дозволяють отримувати аналітичні вирази для кількісних оцінок нечітких умов приналежності елементів до тієї або іншої множини. Теорія нечітких множин добре узгоджується з умовами моделювання систем захисту, оскільки багато початкових даних моделювань (наприклад, характеристики загроз і окремих механізмів захисту) не є строго визначеними.

Теорія конфліктів є відносно новим напрямом дослідження складних людино-машинних систем. Конфлікт між зловмисником і системою захисту, що розгортається на тлі випадкових загроз, є класичним для застосування теорії конфлікту. Дві протиборчі сторони переслідують строго протилежні цілі. Конфлікт розвивається в умовах неоднозначності і слабкої передбачуваності процесів, здатності сторін оперативно змінювати цілі. Теорія конфліктів є розвитком теорії ігор. Теорія ігор дозволяє:

– структурувати завдання, представити його в доступному вигляді, знайти області кількісних оцінок, впорядкувань, переваг, виявити домінуючі стратегії, якщо вони існують;

– до кінця вирішити завдання, які описуються стохастичними моделями.

Теорія ігор дозволяє знайти рішення, оптимальне або раціональне в середньому. Вона виходить з принципу мінімізації середньої риски. Такий підхід не цілком адекватно відображає поведінку сторін в реальних конфліктах, кожен з яких є унікальним. У теорії конфліктів зроблена спроба подолання цих недоліків теорії ігор. Теорія конфліктів дозволяє вирішувати ряд практичних завдань дослідження складних систем. Проте вона ще не набула широкого поширення і відкрита для подальшого розвитку.

З *теорії графів* для дослідження систем захисту інформації найбільшою мірою застосуємо апарат мереж Петрі. Управління умовами у вузлах мережі Петрі дозволяє моделювати процеси подолання захисту зловмисником. Апарат мереж Петрі дозволяє формалізувати процес дослідження ефективності СЗІ.

До *формально-евристичних методів* віднесені методи пошуку оптимальних рішень не на основі строгих математичних, логічних співвідношень, а ґрунтуючись на досвіді людини, наявних знаннях і інтуїції. Отримувані рішення можуть бути далекі від оптимальних, але вони завжди будуть кращі за рішення, що отримуються без евристичних методів.

Найбільшого поширення з евристичних методів набули лабіринтові і концептуальні методи.

Відповідно до лабіринтової моделі завдання представляється людині у вигляді лабіринту можливих шляхів рішення. Передбачається, що людина володіє здатністю швидкого відсікання безперспективних шляхів руху по лабіринту. В

результаті серед шляхів, що залишилися, з великою вірогідністю знаходиться шлях, що веде до рішення поставленої задачі.

Концептуальний метод припускає виконання дій з концептами. Під концептами розуміються узагальнені елементи і зв'язки між ними. Концепти виходять людиною, можливо і неусвідомлено, в процесі побудови структурованої моделі. Відповідно до концептуального методу набір концепт універсальний і йому відповідають механізми обчислення, трансформації і формування стосунків, що є у людини. Чоловік проводить уявний експеримент із структурованою моделлю і породжує обмежену ділянку лабіринту, в якому вже нескладно знайти рішення.

Еволюційним моделюванням є різновид імітаційного моделювання. Особливість його полягає в тому, що в процесі моделювання удосконалюється алгоритм моделювання.

Суть неформальних методів безпосереднього пошуку оптимальних рішень полягає в тому, що людина бере участь не тільки в побудові моделі, але і в процесі її реалізації.

Декомпозиція задачі по оцінці ефективності функціонування КСЗІ

Складність функцій, значна частка нечітко визначених певних початкових даних, велика кількість механізмів захисту, складність їх взаємних зв'язків і багато інших чинників роблять практично нерозв'язною проблему оцінки ефективності системи в цілому за допомогою одного якого-небудь методу моделювання.

Для вирішення цієї проблеми застосовується метод декомпозиції (розділення) загального завдання оцінки ефективності на ряд окремих завдань. Досить просто вирішується окреме завдання оцінки ефективності методу шифрування за умови, що атака на шифр можлива тільки шляхом перебору ключів, і відомий метод шифрування.

Головна складність методу декомпозиції при оцінці систем полягає в обліку взаємозв'язку і взаємного впливу окремих завдань оцінювання і оптимізації. Цей вплив враховується як при рішенні задачі декомпозиції, так і в процесі отримання інтегральних оцінок. Наприклад, при рішенні задачі захисту інформації від електромагнітних випромінювань використовується екранування металевими екранами, а для підвищення надійності функціонування системи необхідне резервування блоків, у тому числі і блоків, що забезпечують безперебійне живлення. Вирішення цих двох окремих завдань взаємозв'язане, наприклад, при створенні КСЗІ на літаючих апаратах, де існують строгі обмеження на вагу. При декомпозиції завдання оптимізації комплексної системи захисту доводиться всякий раз враховувати загальний ліміт ваги устаткування.

Макромоделювання

При оцінці складних систем використовується також макромоделювання. Таке моделювання здійснюється для загальної оцінки системи. Завдання при цьому

спрощується за рахунок використання при побудові моделі тільки основних характеристик. До макромоделювання вдаються в основному для отримання попередніх оцінок систем.

На макрорівні можна, наприклад, досліджувати необхідне число рівнів захисту, їх ефективність по відношенню до передбачуваної моделі порушника з урахуванням особливостей КС і фінансових можливостей проектування і побудови КСЗІ.

Вибір показників ефективності і критеріїв оптимальності комплексної СЗІ

Ефективність систем оцінюється за допомогою показників ефективності. Іноді використовується термін – показник якості. Показниками якості, як правило, характеризують ступінь досконалості якого-небудь товару, пристрою, машини. Відносно складних людино машинних систем переважно використання терміну *показник ефективності функціонування*, який характеризує ступінь відповідності оцінюваної системи своєму призначенню.

Прикладом показника ефективності є криптостійкість шифру, яка виражається часом або вартістю злому шифру. Цей показник для шифру DES, наприклад, залежить від однієї характеристики – розрядності ключа. Для методів заміни криптостійкість залежить від кількості використовуваних алфавітів заміни, а для методів перестановок – від розмірності таблиці і кількості використовуваних маршрутів Гамільтона.

Для того, щоб оцінити ефективність системи захисту інформації або порівняти системи по їх ефективності, необхідно задати деяке правило переваги. Таке правило або співвідношення, засноване на використанні показників ефективності, називають критерієм ефективності. Для отримання критерію ефективності при використанні деякої множини до показників використовують ряд підходів.

Методи, засновані на *ранжуванні показників* по важливості. При порівнянні систем однойменні показники ефективності зіставляються в порядку убування їх важливості за визначеними алгоритмами.

Прикладами таких методів можуть служити лексикографічний метод і метод послідовних поступок.

Лексикографічний метод доцільний, якщо ступінь відмінності показників по важливості великий. Дві системи порівнюються спочатку по найбільш важливому показнику. За оптимальну вважається така система, у якої краще цей показник. При рівності найважливіших показників порівнюються показники, які займають по рангу другу позицію. При рівності і цих показників порівняння триває до отримання переваги в *i*-м показнику

Оцінка ефективності СЗІ може здійснюватися також *методом Парето*. Суть методу полягає в наступному. При використанні n показників ефективності системі відповідає крапка в *n*-мірному просторі. У *n*-мірному просторі будується область парето-оптимальних рішень. У цій області розташовуються незрівняні рішення, для яких поліпшення якого-небудь показника неможливе без погіршення

інших показників ефективності. Вибір найкращого рішення з числа парето-оптимальних може здійснюватися по різних правилах.

13.2. Підходи до оцінки ефективності комплексної СЗІ

Ефективність КСЗІ оцінюється як на етапі розробки, так і в процесі експлуатації. У оцінці ефективності КСЗІ, залежно від показників, що використовуються і способів їх отримання, можна виділити три підходи:

– класичний;
– офіційний;
– експериментальний.

Класичний підхід

Під класичним підходом до оцінки ефективності розуміється використання критеріїв ефективності, отриманих за допомогою показників ефективності. Значення показників ефективності виходять шляхом моделювання або обчислюються по характеристиках реальної КС. Такий підхід використовується при розробці і модернізації КСЗІ. Проте можливості класичних методів комплексного оцінювання ефективності стосовно КСЗІ обмежені через низку обставин. Високий ступінь невизначеності початкових даних, складність формалізації процесів функціонування, відсутність загальновизнаних методик розрахунку показників ефективності і вибору критеріїв оптимальності створюють значні труднощі для застосування класичних методів оцінки ефективності.

Офіційний підхід

Велику практичну значущість має підхід до визначення ефективності КСЗІ, який умовно можна назвати офіційним. Політика безпеки інформаційних технологій проводиться державою і повинна спиратися на нормативні акти. У цих документах необхідно визначити вимоги до захищеності інформації різних категорій конфіденційності і важливості.

Вимоги можуть задаватися переліком механізмів захисту інформації, які необхідно мати в КС, щоб вона відповідала певному класу захисту. Використовуючи такі документи, можна оцінити ефективність КСЗІ. В цьому випадку критерієм ефективності КСЗІ є її клас захищеності.

Безперечною перевагою таких класифікаторів (стандартів) є простота використання. Основним недоліком офіційного підходу до визначення ефективності систем захисту є те, що не визначається ефективність конкретного механізму захисту, а констатується лише факт його наявності або відсутності. Цей недолік в якійсь мірі компенсується завданням в деяких документах достатньо докладних вимог до цих механізмів захисту.

У всіх розвинених країнах розроблені свої стандарти захищеності комп'ютерних систем критичного застосування. Так, в міністерстві оборони США використовується стандарт TCSEC (Department of Defence Trusted Computer System Evaluation Criteria), який відомий як Помаранчева книга.

Згідно книги для оцінки інформаційних систем розглядається чотири групи безпеки: A, B, C, D. В деяких випадках групи безпеки діляться додатково на класи безпеки.

Група A (гарантований або такий, що перевіряється захист) забезпечує гарантований рівень безпеки. Методи захисту, реалізовані в системі, можуть бути перевірені формальними методами. У цій групі є тільки один клас – A1.

Група B (повноважний або повний захист) представляє повний захист КС. У цій групі виділені класи безпеки B1,B2 і B3.

Клас B1 (захист через грифи або мітки) забезпечується використанням в КС грифів секретності, що визначають доступ користувачів до частин системи.

Клас B2 (структурований захист) досягається розділенням інформації на захищені і незахищені блоки і контролем доступу до них користувачів.

Клас B3 (області або домени безпеки) передбачає розділення КС на підсистеми з різним рівнем безпеки і контролем доступу до них користувачів.

Група C (виборчий захист) представляє вибірковий захист підсистем з контролем доступу до них користувачів. У цій групі виділені класи безпеки C1 і C2.

Клас C1 (виборчий захист інформації) передбачає розділення в КС користувачів і даних. Цей клас забезпечує найнижчий рівень захисту КС.

Клас C2 (захист через керований або контрольований доступ) забезпечується роздільним доступом користувачів до даних.

Групу D (мінімальній безпеці) складають КС, перевірені на безпеку, але які не можуть бути віднесені до класів A, B або C.

Організація захисту інформації в обчислювальних мережах міністерства оборони США здійснюється відповідно до вимог керівництва «The Trusted Network Interpretation of Department of Defense Trusted Computer System Evaluation Guidelines». Цей документ отримав назву Червона книга (як і попередній – за кольором обкладинки).

Подібні стандарти захищеності КС прийняті і в інших розвинених країнах. Так, в 1991 р. Франція, Німеччина, Нідерланди і Великобританія прийняли узгоджені «Європейські критерії», в яких розглянуто 7 класів безпеки від E0 до E6.

Класи підрозділяються на чотири групи, що відрізняються якісним рівнем захисту:

– перша група містить тільки один сьомий клас;

– друга група характеризується дискреційним захистом і містить шостий і п’ятий класи;

– третя група характеризується мандатним захистом і містить четвертий, третій і другий класи;

– четверта група характеризується верифікованим захистом і містить тільки перший клас.

Одним із найпоширеніших підходів до оцінки якості захисту інформації є визначений поділ реалізованих функцій і завдань, експлуатаційних характеристик і вимог у відповідність технічним завданням на створення системи захисту. Інший спосіб, який використовується у вітчизняній та закордонній практиці – це аналіз функціональної надійності системи, яка також характеризує якісний рівень системи інформаційної безпеки (СІБ).

Кількісний рівень захисту АСУ характеризується двома основними групами показників:

1. Відносна кількісна оцінка, яка є числом (клас, категорія, нормалізоване значення), що вимагає порівняння з іншими числами, прийнятими як еталон. Для їх визначення використовуються експертні оцінки. Найбільш важливим моментом якісного оцінювання є питання про корекцію та узгодження похибок, які виникають через суб'єктів незалежних оцінок – експертів. Найбільш популярним методом проведення експертизи є метод Делфі і його модифікації. Експертиза може бути спрямована на оцінку ефективності системи захисту, рівня допустимого ризику, рівня захищеності окремих підсистем тощо.

2. Абсолютна кількісна оцінка захисту інформації в АСУ може характеризувати витрати, виражені в грошовому еквіваленті, частоту несприятливих подій або інші показники, які є значущими в частині забезпечення захисту інформації. Абсолютні кількісні показники можуть бути систематизовані в наступні різновиди:

1. *Технічні*. У цю групу входять:

– кількість загроз, що розпізнаються, визначає кількість загроз, що можуть розпізнаватися та оброблятися. Загроза вважається розпізнаною, якщо її характеристики збігаються з описами, що знаходяться в системі інформаційної безпеки (СІБ);

– якість протистояння загрозам – визначається здатністю СІБ адекватно реагувати на розпізнані загрози. У реальному житті виникають загрози, на які АСУ досить важко реагувати. У такій ситуації бажано відзначати у протоколі ті дії, які здійснюються загрозою;

– зменшення продуктивності АСУ у цілому – відображає зменшення продуктивності АСУ унаслідок необхідності реалізації дій, передбачених політикою безпеки. Прикладами можуть служити плати шифрування, які зменшують швидкість передачі даних через необхідність шифрувати при передачі і дешифрувати при прийомі даних тощо.

2. *Організаційні*. Цей вид показників характеризує кількість додатково залученого персоналу для обслуговування СІБ. При реалізації функцій безпеки залучається додатковий персонал – інженери, програмісти, адміністратори систем, менеджери АСУ із безпеки.

3. *Економічні*. До даного різновиду належать наступні показники:

– вартість створення, впровадження, експлуатації та навчання користувачів і підтримки СІБ (усі витрати всіх етапів життєвого циклу СІБ, у тому числі і

витрати на дослідження, придбання технологій ноу-хау, спеціальної апаратури, і програмного забезпечення та ін.). До них також належить заробітна плата працівників, котрі виконують специфічні для СІБ роботи;

– витрати специфічних матеріалів. Передбачає використання спеціальних витратних матеріалів у роботі СІБ. Як приклад можна розглядати додаткові магнітні носії, необхідні для реалізації резервного копіювання;

– витрати на відновлення нормальної роботи після реалізації загрози. У них включаються витрати інформаційних, технічних, трудових і інших ресурсів на відновлення нормальної роботи АСУ;

– коефіцієнт зменшення потенційних утрат, що характеризує відношення між показником зменшення втрат і величини можливих утрат.

Оцінка ефективності захисту повинна обов'язково враховувати як об'єктивні обставини, так і ймовірні фактори.

Питання оцінки ефективності СЗІ від НСД:

1. Оцінка коректності реалізації механізмів захисту СЗІ від НСД. На практиці провести таку оцінку є досить важким завданням. Оскільки можливий варіант, коли встановлена у Вашій інформаційній системі СЗІ від НСД не перехоплює і не аналізує лише один подібний спосіб звернення до файлового об'єкту, і, за великим рахунком, вона стає цілком даремною (рано чи пізно, зловмисник виявить даний недолік засобів захисту і скористається ним). Звідси отримуємо вимогу до коректності реалізації СЗІ від НСД – вона повинна контролювати доступ до ресурсу за будь-якого способу звернення до ресурсу (ідентифікації ресурсу).

2. Оцінка достатності (повноти) набору механізмів захисту у складі СЗІ від НСД. Тут ситуація багато в чому схожа із ситуацією, описаною вище. Наприклад, вимога до достатності механізмів у СЗІ від НСД для захисту конфіденційних даних у нормативних документах виглядає наступним чином: «Чи повинен здійснюватися контроль доступу суб'єктів до ресурсів, що захищаються відповідно до матриці доступу». Природно виникає неоднозначність визначення того, що віднести до ресурсів, які захищаються? Крім того, необхідно розуміти, що безліч комп'ютерних ресурсів (особливо, коли мова йде про універсальну ОС) для корпоративних додатків зайві, в першу чергу, це стосується всіляких зовнішніх пристроїв.

Існують наступні методи та засоби оцінки ефективності СЗІ:

1. Метод порівняльного багатовимірного аналізу. Цей метод створений для визначення ступеня взаємного впливу загроз та причин їх виникнення (і як результат – оцінка ефективності системи захисту інформації). Суть методу можна звести до такого узагальненого алгоритму:

– складається перелік об'єктів, що оцінюються, і вибираються ознаки, за якими буде проводитись оцінка. В даному випадку під об'єктами оцінки будемо розуміти показники захищеності обчислювальної системи, а під ознаками – сукупність параметрів, що характеризують ці показники;

– цей перелік слугує основою для формування матриці ознак *X(n,w)*, де *n* – кількість ознак, а *w* – кількість об'єктів, що оцінюються. Кожному об'єкту ставиться у відповідність рядок матриці із *n* ознак;

– через те, що дані, які зведені в матрицю, описують різні властивості об'єктів і мають різні одиниці виміру, вихідна матриця нормалізується відповідно до формули:

$$Z_{ik} = \frac{x_{ik} - \bar{x}_k}{s_k}; \quad (1)$$

– середнє арифметичне ознаки *k* по усіх об'єктах:

$$\bar{x}_k = \frac{1}{w}\sum_{i=1}^{w} x_{ik}; \quad (2)$$

– стандартне відхилення ознаки *k*; Z_{ik}– нормалізоване значення ознаки *k* для одиниці об'єкта *i*;

$$s_k = \left[\frac{1}{w}\sum_{i=1}^{w}(x_{ik} - \bar{x}_k)^2\right]^{\frac{1}{2}}$$

– проводиться розрахунок елементів матриці відстаней між показниками захищеності з урахуванням усіх елементів матриці ознак:

$$W = \frac{1}{n}\sum_{k=1}^{n}\left|z_{rk} - z_{sk}\right|, \ (r, s = 1,2,3,\ldots,w).$$

По отриманій матриці відстаней між показниками здійснюються їх зіставлення між собою, яке дає змогу впорядкувати показники за ступенем важливості, встановити залежності між ними, оцінити ступінь їх взаємного впливу.

2. Методи аналізу ризиків АСУ.

На даний час при побудові СЗІ АСУ особливого значення набуває завдання побудови моделей загроз інформації. Існує чимало алгоритмів, які здійснюють аналіз ризиків АСУ. До найбільш відомих алгоритмів належать CRAMM і RiskWatch. Зазначені алгоритми мають ряд переваг та набули широкого поширення.

Метод CRAMM був розроблений Службою Безпеки Великобританії за завданням Британського уряду і використовується як державний стандарт,починаючи з 1985 р., урядовими і комерційними організаціями Великобританії.

Версії програмного забезпечення CRAMM, орієнтовані на різні типи організацій, відрізняються один від одного своїми базами знань. Для комерційних організацій є Комерційний профіль, для урядових організацій – Урядовий профіль. Урядовий варіант профілю, також дозволяє проводити аудит на відповідність вимогам американського стандарту ITSEC.

CRAMM припускає поділ усієї процедури на три послідовних етапи. Завданням першого етапу є відповідь на питання: «Чи достатньо для захисту системи застосування засобів базового рівня, що реалізують традиційні функції безпеки, чи необхідно провести більш детальний аналіз?» На другому етапі проводиться ідентифікація ризиків і оцінюється їх величина. На третьому етапі вирішується питання про вибір адекватних контрзаходів.

Методика CRAMM для кожного етапу визначає набір вихідних даних, послідовність заходів, анкети для проведення запитів, списки перевірки і набір звітних документів. Якщо за результатами проведення першого етапу встановлено, що рівень критичності ресурсів є дуже низьким і існуючі ризики свідомо не перевищать деякого базового рівня, то до системи висувається мінімальний набір вимог безпеки. У цьому випадку велика частина заходів другого етапу не виконується, а здійснюється перехід до третього етапу, на якому генерується стандартний список контрзаходів для забезпечення відповідності базового набору вимог безпеки.

На другому етапі проводиться аналіз загроз безпеки та цілісності. Вихідні дані для оцінки аудитор отримує від уповноважених представників організації в ході відповідних запитів. На третьому етапі вирішується завдання управління ризиками, що складається у виборі адекватних контрзаходів.

Рішення про впровадження в систему нових механізмів безпеки або про модифікацію діючих приймає керівництво організації. Завданням аудитора є обґрунтування рекомендованих контрзаходів для керівництва організації.

Метод RiskWatch. Програмне забезпечення RiskWatch розробляється американською компанією RiskWatchInc. і є потужним засобом аналізу і управління ризиками. В сімейство RiskWatch входять програмні продукти для проведення різних видів аудиту безпеки.

У методі RiskWatch як критерії для оцінки та управління ризиками використовуються «прогнозування річних втрат» (ALE) і «повернення від інвестицій» (ROI). Сімейство програмних продуктів RiskWatch має масу переваг.

RiskWatch допомагає провести аналіз ризиків і зробити обґрунтований вибір заходів і засобів захисту. Використовувана в програмі методика включає в себе 3 фази.

Перша фаза – визначення предмету дослідження. На даному етапі описуються параметри організації – тип організації, склад досліджуваної системи. Опис формалізується у ряді підпунктів. Далі кожен з обраних пунктів описується докладно. Для полегшення роботи аналітика в шаблонах даються списки категорій захищених ресурсів, утрат, загроз, уразливих місць і заходів захисту. З них потрібно вибрати ті, що реально присутні в організації.

Друга фаза – введення даних, що описують конкретні характеристики системи. Дані можуть вводитися вручну або імпортуватися зі звітів, створених інструментальними засобами дослідження вразливості комп’ютерних мереж. На цьому етапі докладно описуються ресурси, втрати та класи інцидентів. Класи

інцидентів отримуються шляхом зіставлення категорії втрат і категорії ресурсів. Для виявлення можливих уразливостей використовується опитувальник, база якого містить більше 600 питань. Питання пов'язані з категоріями ресурсів. Допускається коректування питань, виключення або додавання нових, встановити частоту виникнення кожної з виділених загроз, ступінь вразливості і цінність ресурсів. Усе це використовується і надалі для розрахунку ефективності впровадження засобів захисту.

Третя фаза – оцінка ризиків. Спочатку встановлюється зв'язок між ресурсами, втратами, загрозами і вразливими місцями, виділеними на попередніх етапах. Для ризику розраховуються математичні очікування втрат за рік:

$$L = P \cdot V, \qquad (5)$$

де L – сума втрат від загроз інформації за рік; P – частота виникнення загроз протягом року; V – вартість ресурсу, який під загрозою.

Розглянуті методики дозволяють оцінити чи переоцінити рівень поточного стану інформаційної безпеки АСУ, розробити концепцію і політику безпеки АСУ, а також запропонувати плани захисту від виявлених загроз і вразливих місць.

Недоліки розглянутих методів аналізу:

1. *Обмежена область застосування*. Методика аналізу інформаційних ризиків CRAMM набагато краще підходить для аудиту вже існуючих АСУ, що знаходяться на стадії експлуатації, ніж для інформаційних систем, що знаходяться на стадії розробки.

2. *Нехтування комплексним підходом при аналізі ризиків*. Метод RiskWatch робить аналіз ризиків на програмно-технічному рівні захисту, без урахування організаційних та адміністративних чинників. Метод не враховує комплексний підхід до інформаційної безпеки. Крім того, RiskWatch розглядає ризики як математичне очікування втрат. Ця методика не враховує багатьох факторів, які впливають на безпеку інформації.

3. *Неможливість розширення бази знань*. Сучасні засоби аналізу інформаційних ризиків (наприклад, CRAMM) не передбачають розширення їх бази знань. Відсутність зазначеної можливості викликає суттєві труднощі під час процедури аналізу ризиків конкретної організації.

4. *Висока вартість ліцензії*. Існуючі засоби для аналізу інформаційних ризиків характеризуються високою вартістю ліцензії.

Контрольні питання

1. Визначте поняття «модель загроз», «електронні віруси».
2. Які типи моделей використовуються для оцінки систем захисту інформації?
3. Який вигляд мають аналітичні моделі?
4. Який вигляд мають імітаційні моделі?
5. Назвіть особливості складних організаційно-технічних систем?
6. Назвіть основні складові частини неформальної теорії систем.
7. Перерахуйте умови структурованого опису систем.

Література для самопідготовки

1. Бобунов А.І. Захист інформації в автоматизованих системах / Бобунов А.І., Шестаков В.І. Захист інформації в автоматизованих системах: Навчальний посібник. – Житомир: ЖВІРЕ, 2004. – С. 156–164.
2. Малюк А.А. Введение в защиту информации в автоматизированных системах / Малюк А.А., Пазизин С.В., Погожин Н.С. – М.: Горячая линия-Телеком, 2001. – С. 126-138.
3. Завгородний В.И. Комплексная защита информации в компьютерных системах: учебное пособие / Завгородний В.И. . – М.: Логос; ПБОЮЛ Н.А. Егоров, 2001. - С. 216–245.

СПИСОК ЛІТЕРАТУРИ

1) Закон України від 25.06.93 № 3323-XII-ВР "Про науково-технічну інформацію".

2) Закон України "Про інформацію". Із змінами, внесеними згідно із Законом від 07.02.2002 № 3047-III-ВР.

3) Закон України "Про Державну таємницю". Із змінами і доповненнями, внесеними Законом України від 21.09.1999 №1079-XIV.

4) Закон України від 05.07.94 № 80/94-ВР "Про захист інформації в автоматизованих системах"

5) Закон України "Про Національну програму інформатизації" Із змінами, внесеними згідно із Законом від 13.09.2001 № 2684-III-ВР.

6) Закон України "Про зв'язок" Із змінами, внесеними згідно із Законом від 04.07.2002 № 36-IV-ВР.

7) Закон України від 15 грудня 2005 року № 3200-IV "Про основи національної безпеки України".

8) Бобунов А. І. Захист інформації в автоматизованих системах : навчальний посібник / А. І. Бобунов, В. І. Шестаков. – Житомир : ЖВІРЕ, 2004. – 172 с.

9) Антонюк А. О. Основи захисту інформації в автоматизованих системах управління / А. О. Антонюк. – Київ : Видавничий дім "КМ академія", 2003. – 242 с.

10) Малюк А. А. Введение в защиту информации в автоматизированных системах / Малюк А. А., Пазизин С. В., Погожин Н. С. – М. : Горячая линия-Телеком, 2001. – 148 с.

11) Завгородний В. И. Комплексная защита информации в компьютерных системах : учебное пособие / В. И. Завгородний. – М. : Логос; ПБОЮЛ Н.А. Егоров, 2001. – 264 с.

12) Алферов А. П. Основы криптографии : учебное пособие / Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. – М. : Гелиос АРВ, 2001.– 480 с.

13) Кукацкий А. В. Обнаружение атак / А. В. Кукацкий. – СПб. : БХВ-Петербург, 2001. – 624 с.

14) Курбатов В. А. Руководство по защите от внутренних угроз информационной безопасности / В. Ю. Скиба, В. А. Курбатов. – СПб. : Питер, 2008. – 320 с.

15) Белов Е. Основы информационной безопасности : учебное пособие для вузов / Белов Е., Лось В., Мещеряков А. – М. : "Студио", 2006. – 356 с.

16) Купер М. Анализ типовых нарушений безопасности в сетях : [пер. с англ.] / Норткат С., Купер М., Фирноу М., Фредерик К. – М. : «Вильямс», 2001. – 464 с.

17) Щеглов А. Ю. Защита компьютерной информации от несанкционированного доступа / А. Ю. Щеглов. – СПб. : Наука и техника, 2004. – 384 с.

18) Коваленко М. М. Комп’ютерні віруси і захист інформації / М. М. Коваленко. – К. : Наукова думка, 1999. – 267 с.

19) Хоффман Л. Современные методы защиты информации / Л. Хоффман. – [пер. с англ.] / Хоффман Л. [под ред. В.А. Герасименко]. – М. : Сов. радио, 1980. – 264 с.

20) Хорошко В. О. Методы и средства защиты информации / В. О. Хорошко, И. О. Чекатов. – Киев : ГУИКТ, 2007. – 341 с.

21) Мельников В. В. Защита информации в компьютерных системах / В. В. Мельников. – М. : Финансы и статистика; Электроинформ, 1997. – 368 с.

22) Малюк А. А. Информационная безопасность : концептуальные и методологические основы защиты информации: [учеб. пособие для вузов]. – М. : Горячая линия-Телеком, 2004. – 280 с.

23) Мамаев М. Технологии защиты информации в Интернете. Специальный справочник / М. Мамаев, С. Петренко. – СПб. : Питер, 2002. – 848 с.

24) Защита информации в компьютерных системах и сетях / [под ред. В. Ф. Шаньгина]. – 2-е изд., перераб. и доп. – М. : Радио и связь, 2001. – 376 с.

25) Фергюсон Н. Практическая криптография / Н. Фергюсон, Б. Шнайер. : [пер. с англ]. – М. : Издательский дом "Вильямс", 2005. – 424 с.

26) Введение в криптографию под ред. В. В. Ященко // http://nature.web.ru/db/msg.html?mid=1157083&uri=node1.html

27) Казарин О. В. Безопасность программного обеспечения компьютерных систем // http://citforum.ru/security/articles/kazarin

28) Ростовцев А. Г., Михайлова Н. В. Методы криптоанализа классических шифров//http://www.ssl.stu.neva.ru/psw/crypto/rostovtsev/cryptoanalysis.html

29) Федотов Н. Н. Защита информации (Учебный курс) // http://www.college.ru/UDP/texts/index.html