Міністерство освіти і науки України
Вищий приватний навчальний заклад
міжнародний економіко-гуманітарний університет
імені академіка Степана Дем'янчука

Д.Б. Охота

ТЕХНОЛОГІЇ КОМП'ЮТЕРНОЇ БЕЗПЕКИ

КНИГА1

Науковий керівник:
Р.М.Літнарович, доцент,к.т.н.

Рівне – 2011 р.

УДК 614.2 Охота Д.Б. Технології комп'ютерної безпеки. Монографія. МЕГУ, Рівне, 2011.-97 с. Okhota D.B. Technologies of computer safety. Monograph. IEGU, Rivne, 2011.-97 p.

Рецензенти: В.Г.Бурачек, доктор технічних наук, професор
Є.С. Парняков, доктор технічних наук, професор
В.О.Боровий , доктор технічних наук, професор
Відповідальний за випуск: Й.В. Джунь, доктор фізико-математичних наук, професор

Послідовно розглядаються основні поняття побудови сучасних технологій комп'ютерної безпеки. Монографія містить актуальний матеріал довідково-аналітичного характеру по наступних темах: основи безпеки даних в комп'ютерних системах, ідентифікація і аутентифікація користувачів, захист даних від несанкціонованого доступу, основи захисту даних від комп'ютерних вірусів, основи криптографії, криптографічні методи захисту інформації, стандарти захисту інформації.
Ключові слова: комп'ютерна безпека, інформаційна безпека, захист, інформація.

Последовательно рассматриваются основные понятия построения современных технологий компьютерной безопасности. Монография содержит актуальный материал справочно аналитического характера по следующим темам: основы безопасности данных в компьютерных системах, идентификация и аутентификация пользователей, защита данных от несанкционированного доступа, основы защиты данных от компьютерных вирусов, основы криптографии, криптографические методы защиты информации, стандарты защиты информации.
Ключевые слова: компьютерная безопасность, информационная безопасность, защита, информация.

The basic concepts of construction of modern technologies of computer safety are consistently examined. A monograph contains aktual material certificate analytical character on the followings themes: bases of safety of information in the computer systems, authentication and authentification of users, protection of data from an unauthorized division, bases of protection of data from computer viruses, bases of cryptography, cryptographic methods of priv, standards of priv.
Keywords: computer safety, informative safety, defence, information

© **Охота Д.Б.**

Дмитро Борисович Охота,
спеціаліст системотехнік, магістрант
інформаційних технологій

Зміст

Вступ

Забезпечення безпечної діяльності комп'ютерних систем необхідне для будь-яких підприємств і установ починаючи від державних організацій і закінчуючи невеликими приватними фірмами, не залежно від виду їх діяльності. Розходження полягає лише в засобах, методах та в обсязі забезпечення безпеки.

Якщо пріоритет збереження безпеки особистості є природним, то пріоритет інформації над матеріальними цінностями вимагає більш докладного розгляду. Це стосується не тільки інформації, що складає державну чи комерційну таємницю, але і відкритої інформації.

У комп'ютерної безпеки, термін уразливість (англ. vulnerability) використовується для позначення недоліку в системі, використовуючи який, можна порушити її цілісність і викликати неправильну роботу. Уразливість може бути результатом помилок програмування, недоліків, допущених при проектуванні системи, ненадійних паролів, вірусів і інших шкідливих програм, скриптових, а також SQL-ін'єкцій. Деякі відомі уразливості тільки теоретично, інші ж активно використовуються і мають відомі експлойти.

Зазвичай уразливість дозволяє атакуючому "обдурити" додаток - змусити його зробити дію, на яку у того не повинно бути прав. Це робиться шляхом впровадження будь-яким чином в програму даних або коду в такі місця, що програма сприйме їх як "свої". Деякі уразливості з'являються через недостатню перевірки даних, які вводяться користувачем, і дозволяють вставити в інтерпретований код довільні команди (SQL-ін'єкція, XSS). Інші уразливості з'являються із-за більш

складних проблем, таких як запис даних в буфер без перевірки його межами (переповнення буфера).

Метод інформування про вразливості є одним з пунктів спору в співтоваристві комп'ютерної безпеки. Деякі фахівці відстоюють негайне повне розкриття інформації про вразливості, як тільки вони знайдені. Інші радять повідомляти про вразливості тільки тим користувачам, які піддаються найбільшому ризику, а повну інформацію публікувати лише після затримки або не публікувати зовсім. Такі затримки можуть дозволити тим, хто був сповіщений, виправити помилку за допомогою розробки і застосування патчів, але також можуть і збільшувати ризик для тих, хто не знає деталі.

Існують інструментальні засоби, які можуть допомогти у виявленні вразливостей в системі. Хоча ці інструменти можуть забезпечити аудитору хороший огляд можливих вразливостей, існуючих в мережі, вони не можуть замінити участь людини в їх оцінці.

Для забезпечення захищеності і цілісності системи необхідно постійно стежити за нею: встановлювати оновлення, і використовувати інструменти, які допомагають протидіяти можливим атакам. Уразливості виявлялися у всіх основних операційних системах, включаючи Microsoft Windows, Mac OS, різні варіанти UNIX (у тому числі GNU/Linux) і OpenVMS. Так як нові уразливості знаходять безперервно, єдиний шлях зменшити ймовірність їх використання проти системи - постійна пильність.

1 Основи безпеки даних в комп'ютерних системах

1.1. Основні поняття щодо захисту інформації в автоматизованих системах

Як вважають західні фахівці, витік 20% комерційної інформації в 60 випадках з 100 призводить до банкрутства фірми. Жодна, навіть процвітаюча фірма не проіснує більше трьох діб, якщо її інформація, що складає комерційну таємницю, стане відомою. Таким чином, економічна та інформаційна безпека виявляються тісно взаємозалежними.

Збитки від діяльності конкурентів, що використовують методи шпигунства, складають у світі до 30% усього збитку, а це мільярди доларів. Точну цифру збитків указати не можна внаслідок того, що ні злочинці, ні потерпілі не прагнуть піддавати гласності зроблені дії. Перші, мабуть, через страх відповідальності за вчинене, а другі - через страх втратити імідж. Цим пояснюється високий рівень латентності правопорушень і відсутність інформації про них в засобах масової інформації. Тому до публіки доходить менш 1% від усіх випадків порушень, що мають карний характер і які приховати неможливо.

Таким чином, задачі безпеки будь-яких видів доводиться вирішувати щораз при розгляді всіляких аспектів людської діяльності. Але, як бачимо, всі види безпеки тісно пов'язані з інформаційною безпекою (ІБ) і, більш того, їх неможливо забезпечити без забезпечення ІБ. Отже, предметом нашого подальшого розгляду буде саме захист інформації в інформаційних автоматизованих системах.

Особливістю терміну "інформація" є те, що, з одного боку, він є інтуїтивно зрозумілим практично для всіх, а з іншого

боку - загальновизнаного його трактування в науковій літературі не існує. Одночасно слід особливо зазначити, що як наукова категорія "інформація" складає предмет вивчення для всіляких областей знань: філософії, інформатики, кібернетики і т.д.

Інформація - це відомості про осіб, факти, предмети, події, явища і процеси, незалежно від форми їх уявлення.

Захист інформації - комплекс заходів, проведених із метою запобігання (зниження до безпечного рівня) можливостей витікання, розкрадання, втрати, поширення, знищення, перекручування, підробки або блокування інформації.

Для правильної побудови системи захисту необхідно визначити:

1. Види дій над інформацією.

2. Що з себе являє автоматизована система.

3. Які існують загрози безпеки автоматизованих систем.

4. Заходи протидії загрозам безпеки.

5. Принципи побудови систем захисту.

Види дій над інформацією:

1. Блокування інформації (користувач не може дістати доступ до інформації; за відсутності доступу сама інформація не втрачається).

Причини: відсутність устаткування, фахівця, програмного забезпечення.

2.Порушення цілісності (втрата, вихід з ладу носія; спотворення, тобто порушення смислової значущості; порушення логічної зв'язаності; втрата достовірності (наявна інформація не відповідає реальному стану)).

3.Порушення конфіденційності (з інформацією ознайомлюються суб'єкти, на яких це не покладено).

Рівень допуску до інформації визначає її власник. Порушення конфіденційності може відбутися із-за неправильної роботи системи обмеження доступу або наявності побічного каналу доступу.

4. Несанкціоноване тиражування (під захистом розуміється захист авторських прав і прав власності на інформацію).

Автоматизована система (АС) - це організаційно-технічна система, що об'єднує обчислювальну систему, фізичне середовище, персонал і оброблювану інформацію.

Захист нформації в АС (information security, computer system security) - діяльність, яка спрямована на забезпечення безпеки оброблюваної в АС інформації та АС у цілому і дозволяє запобігти або ускладнити можливість реалізації загроз, а також знизити величину потенційних збитків внаслідок реалізації загроз.

Комплексна система захисту інформації (КСЗІ) - сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в АС.

Причини пошкодження інформації: 79% - низька кваліфікація користувачів; 20% - заплановані розкрадання; 1% - віруси.

Типові структури АС:

1. Автономні робочі станції (один або декілька ПК, **не** зв'язаних між собою. На будь-якому з них користувачі працюють роздільно в часі. Обмін інформацією відбувається тільки через змінні носії (дискети, диски)).

Об'єкти захисту в автономних робочих станціях:

- власне робоча станція;
- змінні носії інформації;
- користувачі і робочий персонал;
- пристрої візуального представлення інформації (монітор, принтер тощо);
- прилади-джерела побічних електромагнітних випромінювань і наведень.

2. Локальні системи колективного користування (створюються для колективної обробки інформації і (або) сумісного використання ресурсів; устаткування розміщене в межах одного приміщення, будівлі або групи близько розташованих будівель).

Структури локальних систем колективного користування:

1.*Без виділеного сервера (однорангові мережі)* (не вимагають централізованого управління; будь-який користувач сам робить свої ресурси доступними іншим; використовується однотипна операційна система (ОС)).

2.З виділеним сервером/серверами (побудовані на робочих станціях і серверах; вимагають централізованого адміністративного управління).

3.Багатотермінальні системи на базі малих і великих комп'ютерів (основні ресурси зосереджені на сервері. Робочі станції - термінали. Загальне керівництво здійснює адміністратор. На центральному комп'ютері і робочих станціях використовуються різні ОС).

4.Багатосегментні локальні мережі (складаються з декількох сегментів, будь-який з яких є мережею з виділеним сервером. Об'єднання здійснюється через міст, в якості якого може використовуватися або виділений сервер, або спеціальний пристрій. Будь-яким сегментом управляє свій адміністратор. У будь-якому сегменті може використовуватися своя ОС).

5. *Змішані мережі* (включають всі раніше розглянуті системи).

Об'єкти захисту:

- всі робочі станції;
- виділені сервери і центральний комп'ютер;
- локальні канали зв'язку;
- реквізити доступу.

6. Глобальні системи колективного користування (розміщені на значній відстані один від одного; об'єднані через глобальні канали зв'язку, які не належать власнику).

Використовуються для сумісної обробки інформації і сумісного використання ресурсів.

Відмінності від локальних систем:

- можуть знаходитися на значній відстані одна від одної;
- канали зв'язку не належать власнику системи;
- канали зв'язку є комутованими і взаємозв'язаними;
- для використання каналів зв'язку необхідний пристрій сполучення;
- подібні системи відкриті і підключитися до них можуть всі охочі. Об'єкти захисту включають в себе все те ж, що й **в** локальних системах

колективного користування, а також:

- глобальні канали зв'язку;
- інформація, що передається по глобальних каналах зв'язку;
- інформація про реквізити доступу в глобальні системи колективного користування.

1.2. Загрози безпеки даних та їх особливості

Загроза - потенційно можлива подія, дія, процес або явище, яке може привести до нанесення збитку інтересам певної фізичної чи юридичної особи.

Реалізацією загрози є порушення роботи системи. Загрози поділяються на природні та штучні.

Природні загрози - загрози, викликані дією на АС об'єктивних фізичних процесів або стихійних природних явищ, незалежних від людини.

Штучні загрози - такі, що викликані діяльністю людини.

Природні загрози - це стихійні лиха, магнітні бурі, радіоактивне випромінювання, опади тощо, а також загрози опосередковано технічного характеру, пов'язані з надійністю технічних засобів обробки інформації і підсистем забезпечення АС.

Штучні поділяються на:

- *ненавмисні* - загрози, пов'язані з випадковими діями людей, через незнання, халатність, цікавість, але без злого наміру.

Наприклад: ненавмисне псування носіїв інформації; запуск програм, не передбачених службовою необхідністю; необережні дії, що призводять до розголошування конфіденційної інформації; розголошування реквізитів доступу в АС; псування каналів зв'язку.

• *навмисні* - дії людини, що здійснюються умисне для дезорганізації роботи системи, виведення її з ладу, для незаконного проникнення в систему і несанкціонованого доступу до інформації.

Наприклад: фізичне знищення системи; розкрадання носіїв інформації; читання залишкової інформації з ОЗП; несанкціоноване копіювання; вербування персоналу тощо.

Система складових загроз безпеки даних представлена в табл. 1.1.

Таблиця 1.1 Класифікаційні складові загроз безпеки інформації

Параметр класифікації	Значення параметра	Зміст
	1.1. Фізична цілісність	- знищення (спотворення);
	1.2. Логічна цілісність	- спотворення;
1. Види	1.3. Конфіденційність	- несанкціоноване отримання;
	1,4. Порушення прав власності	- привласнення чужого права
2. Природа походження	2.1. Випадкова	- відмови, збої, помилки, стихійні біди;
	2.2. Навмисна	- зловмисні дії людей
	3.1, Об'єктивні	-кількісна або якісна
3.Передумови		недостатність елементів систем;
появи	3.2. Суб'єктивні	-розвідувальні органи іноземної держави

	4.1. Люди	-сторонній персонал;
4. Джерела загрози	4.2. Технічні пристрої	-пристрої обробки, зберігання, передачі інформації;
	4.3. ПЗ (ППЗ, СМЗ)	-помилки;
	4.4. Зовнішнє середовище	-атмосфера, побічні явища

1.3. Канали проникнення та принципи побудови систем захисту

Сучасні засоби перехоплення інформації дозволяють на відстані в десятки і сотні, а іноді і більше метрів реєструвати різної природи побічні інформативні сигнали, що виникають при роботі технічних засобів, і за результатами цієї реєстрації відновлювати оброблювану, передану, прийняту, копійовану інформацію.

Інформацію можна одержувати не тільки шляхом перехоплення побічних інформативних сигналів, але й за результатами прямої реєстрації сигналів, що циркулюють в інформаційних ланцюгах технічних систем (насамперед, у лініях зв'язку). Реалізувати засоби перехоплення тут, як правило, легше, ніж у випадку побічних випромінювань і наведень.

При роботі деяких технічних засобів поряд з електромагнітними полями розсіювання можуть виникати інформативні акустичні і вібраційні поля, що, поширюючись у навколишньому просторі чи по твердих конструкціях, можуть впливати на елементи і вузли інших технічних пристроїв. Під впливом таких полів у цих елементах створюється

інформативний сигнал, що забезпечує умови витоку інформації. Розглянемо деякі приклади.

Телефонний апарат, навіть у випадку, якщо розмова не здійснюється, може служити причиною виникнення каналу проникнення інформації, тому що в його складі є викличний дзвоник і телефон. В останніх пристроях під впливом акустичного поля індукується електромагнітне поле інформативного сигналу. Аналогічні властивості можуть мати також елементи інших технічних засобів (елементи електричних годинників, електродинамічні гучномовці, деякі датчики пожежної та охоронної сигналізації).

Таким чином, перехоплення конфіденційних розмов може здійснюватися за допомогою подібних технічних пристроїв. У найпростішому варіанті створюється прихована провідна лінія (чи використовується вже існуюча лінія), до якої підключається мікрофон, часто постачений підсилювачем і фільтром.

В даний час існують дуже ефективні оптичні системи, що дозволяють з космосу (з відстані біля сотні кілометрів) розрізняти навіть номерні знаки автомобіля, тому сфотографувати документ із відстані декількох сотень метрів не є великою проблемою.

Найбільш дорогими засобами перехоплення мови є лазерні системи, що забезпечують посилку зондувального сигналу на скло вікон. Скло під дією коливань повітря, викликаного розмовою, вібрує, що легко уловлюється на відстані декількох сотень метрів лазерним променем і розшифровується.

Класифікація каналів проникнення в систему:

1. За способом: прямі та непрямі (не вимагають безпосереднього проникнення в приміщення АС).

2. За типом основного засобу для реалізації загрози: людина, програма, апаратура.

3. За способом отримання інформації: фізичний, електромагнітний, інформаційний.

Заходи протидії загрозам:

1. Правові або законодавчі - закони, укази, нормативні акти, що регламентують правила поводження з інформацією і визначають відповідальність за порушення цих правил.

2. Морально-етичні - норми поведінки, які традиційно склалися або складаються в суспільстві у міру розповсюдження обчислювальної техніки. Невиконання цих норм веде до падіння авторитету, престижу організацій, країни, людей.

3. Адміністративні (організаційні) - заходи організаційного характеру, регламентуючі процеси функціонування АС, діяльність персоналу з метою максимального утруднення або виключення реалізації погроз безпеки. До них відносяться:

• організація явного або прихованого контролю над роботою користувачів;

• організація обліку зберігання, використання, знищення документів і носіїв інформації;

• організація охорони і надійного пропускного режиму;

- заходи, здійснювані при підборі і підготовці персоналу;

- заходи щодо розробки правил доступу до інформації;

• заходи при проектуванні, розробці, модифікації технічних засобів і ПЗ.

4. Фізичні - застосування різного роду технічних засобів охорони (ТЗО) і споруд, призначених для створення фізичних перешкод на шляхах проникнення в систему.

5. *Технічні* - засновані на використанні технічних пристроїв і програм, що входять в склад АС і виконують функції захисту: засоби аутентифікації, апарати шифрування та ін.

Принципи побудови систем захисту:

1 *Принцип системності.* Системний підхід припускає необхідність обліку всіх взаємозв'язаних взаємодій і елементів, що змінюються в часі, умов і чинників, істотно значущих для розуміння і рішення проблеми забезпечення безпеки.

2. Принцип комплексності. Припускає будувати систему з різнорідних засобів, що перекривають всі існуючі канали реалізації загрози безпеки і що не містять слабких місць на стику окремих компонентів. Принцип комплектності полягає у використанні всіх видів і форм захисту в повному об'ємі: жодна частина СЗ не може бути вилучена без збитку для всієї системи.

3. *Принцип безперервного захисту.* Захист повинен існувати без розривів у просторі та часі. Це безперервний цілеспрямований процес, що припускає не тільки захист в

експлуатації, але і проектування захисту на стадії планування системи. Захист повинен бути без розривів у просторі та часі. Це безперервний, цілеспрямований процес. Під час нештатних ситуацій захист повинен бути посилений.

4. Принцип розумної достатності. Вкладення засобів в системи захисту повинно бути побудовано так, щоб одержати максимальну віддачу. Витрачати на СЗ треба від 10 до 35 відсотків суми можливого збитку. Вкладення засобів в СЗ повинно бути таким, щоб одержати максимальну віддачу.

5. *Принцип гнучкості управління і застосування.* Припускає, що не міняючи функціональної бази можна змінити СЗ.

6. Принцип відвертості алгоритмів і механізмів захисту. Захист не повинен забезпечуватися тільки за рахунок секретності структур і алгоритмів функціонування. Знання алгоритмів і механізму захисту не дає можливості навіть автору проникнути в систему.

7. *Принцип простоти застосування захисних заходів і засобів.* Механізми захисту повинні бути інтуїтивно зрозумілими і простими в застосуванні. Використання СЗ не повинно бути пов'язане із знанням спеціальних мов і виконанням робіт, що вимагають значних трудовитрат. АС повинна функціонувати так, щоб вихідна інформація могла бути надана в потрібний час в потрібне місце, в потрібному вигляді і лише певній людині, а також забезпечувати захист самої себе.

1.4 Основи фізичного захисту об'єктів

Фізичні заходи захисту інформації базуються на застосуванні всілякого роду механічних, електро- або електронно-механічних пристроїв, спеціально призначених для створення фізичних перешкод на можливих шляхах проникнення і доступу потенційних порушників до компонентів системи і інформації, а також технічних засобів візуального нагляду, зв'язку та охоронної сигналізації.

Основні канали фізичного витоку інформації:

1. Електромагнітний канал. Причиною його виникнення є електромагнітне поле, пов'язане з протіканням електричного струму в технічних засобах АС. Електромагнітне поле може індукувати струми в близько розміщених провідних лініях.

Електромагнітний канал, в свою чергу, ділиться на наступні канали:

> радіоканал (високочастотне випромінювання);

> низькочастотний канал;

> мережевий канал (наводки на мережу електроживлення);

> канал заземлення (наводки на проводи заземлення);

> лінійний канал (наводки на лінії зв'язку між ПЕОМ).

2. *Акустичний (віброакустичний) канал.* Він пов'язаний з розповсюдженням звукових хвиль в повітрі або пружних коливань в інших середовищах, які виникають при роботі засобів відображення інформації АС.

3. Оптичний канал. Він пов'язаний з можливістю отримання інформації за допомогою оптичних засобів.

Система охорони - сукупність технічних систем охорони (ТСО) і систем охорони, призначених для виконання завдань по охороні об'єкту.

ТСО - вид техніки, призначеної для використання силами охорони з метою підвищення надійності виявлення порушника і забезпечення санкціонованого доступу до об'єкта.

Порушник - особа або група осіб, що не санкціоновано проникаючих або проникли на об'єкт охорони.

Об'єкт охорони - ділянка місцевості з розташованими на ній будівлями, спорудами, приміщеннями в будівлях, окремими предметами, доступ **до** яких стороннім особам заборонений.

Технічні системи охорони: /. *Периметричні засоби виявлення:*

- стаціонарні;
- мобільні.

2. Об 'єктні засоби виявлення.

3. Засоби збору і відображення інформації:

- виявлення факту проникнення;
- певний контроль за системою охорони;
- реєстрація фактів спрацювання пристрою виявлення.

4. Засоби управління доступом:

- кодоблокувальні пристрої;
- домофони;
- магнітні карти;
- механічні пристрої («вертушки» на КПП, ворота, шлагбауми тощо).

5. *Технічні засоби спостереження:* телесистеми спостереження, оптичні пристрої (перископи), прилади нічного бачення.

6. Технічні засоби попередження:

- на паперовому носії;
- мультимедійні (звукові сигнали, відеозображення).

7. *Технічні засоби дії:*

- електроогорожі;
- сигнальні й індикаторні речовини (системи).

8. Інженерні споруди.

2 Ідентифікація і аутентифікація користувачів

2.1 Поняття про ідентифікацію користувача та її особливості

Ідентифікація - привласнення суб'єктам або об'єктам доступу ідентифікатора або порівняння пред'явленого ідентифікатора з переліком привласнених ідентифікаторів.

Ідентифікація об'єкта - це його впізнання, ототожнення із чим-небудь. Якщо ж говорити про області інформаційних технологій, то даний термін звичайно означає встановлення особистості користувача. Цей процес необхідний для того, щоб система надалі змогла ухвалити рішення щодо видачі людині дозволу для роботи на комп'ютері, доступу **до** закритої інформації тощо. Таким чином, ідентифікація є одним з основних понять в інформаційній безпеці.

Сьогодні існує декілька способів ідентифікації користувачів. У кожного з них є свої переваги і недоліки, завдяки чому деякі технології підходять для використання в одних системах, інші - в інших. Однак у багатьох випадках немає строго певного рішення. А тому як розроблювачам програмного забезпечення, так і користувачам приходиться самостійно думати, який спосіб ідентифікації реалізовувати в продуктах.

Існує три найпоширеніших види ідентифікації:

1. Парольна ідентифікація

Ще не дуже давно парольна ідентифікація була чи ледве не єдиним способом визначення особистості користувача. Справа в тому, що парольна ідентифікація найбільш проста як у реалізації, так й у використанні. Суть її зводиться до

наступного. Кожен зареєстрований користувач системи одержує набір персональних реквізитів (звичайно використаються пари: логін-пароль). Далі при кожній спробі входу людина повинна вказати свою інформацію. Оскільки вона унікальна для кожного користувача, то на підставі її система й робить висновок про особистість та ідентифікує.

Недоліком парольної ідентифікації є значна залежність надійності ідентифікації від користувачів, точніше від обраних ними паролів. Справа в тому, що більшість людей використовують ненадійні ключові слова, які легко підбираються. Фахівці в області інформаційної безпеки радять використати довгі паролі, що складаються з безладного сполучення букв, цифр і різних символів.

2. Апаратна ідентифікація

Цей принцип ідентифікації ґрунтується на визначенні особистості користувача за певним предметом, ключем, що перебуває в його ексклюзивному користуванні. Мова йде про спеціальні електронні ключі. На даний момент найбільше поширення одержали два типи пристроїв. До першого ставляться всілякі карти. їх досить багато, і працюють вони за різними принципами. Так, наприклад, досить зручні у використанні безконтактні карти (їх ще називають проксіміті-карти), які дозволяють користувачам проходити ідентифікацію як у комп'ютерних системах, так й у системах доступу в приміщення. Найбільш надійними вважаються смарт-карти - аналоги звичних багатьом людям банківських карт. Крім того, є й більш дешеві, але менш стійкі до злому карти: магнітні, зі штрих-кодом і т.д.(рис. 3.1).

Рис. 3.1. Картки ідентифікації користувача

Іншим типом ключів, які можуть використатися для апаратної ідентифікації, є так звані токени (рис. 3.2). Ці пристрої мають власну захищену пам'ять і підключаються безпосередньо до одного з портів комп'ютера (USB, LPT).

Рис. 3.2. Токен

Головним достоїнством застосування апаратної ідентифікації є досить висока надійність. У пам'яті токенів можуть зберігатися ключі, підібрати які хакерам не вдасться. Крім того, у них реалізовано чимало різних захисних механізмів. А вбудований мікропроцесор дозволяє електронному ключу не тільки брати участь у процесі ідентифікації користувача, але й виконувати деякі інші корисні функції.

Недоліком апаратної ідентифікації є висока ціна. Взагалі ж останнім часом вартість як самих електронних ключів, так і програмного забезпечення, що може працювати з ними, помітно знизилася. Проте для введення в експлуатацію

системи майнової ідентифікації однаково будуть потрібні деякі вкладення. Все-таки кожного зареєстрованого користувача потрібно забезпечити персональними токенами. Крім того, згодом деякі типи ключів можуть зношуватися або можуть бути загублені користувачами.

3. Біометрична ідентифікація

Біометрія - це ідентифікація людини за унікальними, властивими тільки їй біологічними ознаками. Сьогодні експлуатується вже більше десятка різних біометричних ознак. Причому для найпоширеніших з них (відбитки пальців і райдужна оболонка ока) існує безліч різних за принципом дії сканерів (рис. 3.1). Так що користувачам, що вирішили використати біометричну ідентифікацію, є із чого вибрати.

Рис. 3.3. Дактилоскопічний сканер

Головною перевагою біометричних технологій є найвища надійність. І дійсно, усі знають, що двох людей з однаковими відбитками пальців у природі просто не існує. Правда, сьогодні вже відомо кілька способів обману дактилоскопічних сканерів. Наприклад, потрібні відбитки пальців можуть бути перенесені на плівку або до пристрою може бути прикладена велика фотографія пальця зареєстрованого користувача. Втім, треба зізнатися, що сучасні пристрої вже не попадаються на такі прості виверти. Так що зловмисникам доводиться

видумувати все нові й нові способи обману біометричних сканерів.

Основним недоліком біометричної ідентифікації є вартість устаткування. Адже для кожного комп'ютера, що входять до цієї системи, необхідно придбати власний сканер. Варто також відзначити, що подібні дешеві сканери недовговічні. Крім того, у них досить високий відсоток помилок другого роду (відмова в доступі зареєстрованому користувачеві). Тому користувачеві доводиться вибирати, який пристрій придбати - дорожчий й кращий або дешевший й гірший.

Багатофакторна ідентифікація. Поступово все більшого поширення одержує багатофакторна ідентифікація, коли для визначення особистості застосовується відразу кілька параметрів.

Рис. 3.4. Пристрій для багатофакторної ідентифікації

Причому комбінуватися ці фактори можуть у довільному порядку. Втім, сьогодні в переважній більшості випадків використається тільки одна пара: парольний захист і токен. У цьому випадку користувач може не боятися підбору його пароля зловмисником (без електронного ключа вона працювати не буде), а також крадіжки токена (він не буде працювати без пароля). Втім, у деяких системах застосовуються максимально надійні процедури ідентифікації.

У них одночасно використаються паролі, токени й біометричні характеристики людини.

2.2 Основні принципи та методи аутентифікації

Аутентифікацією - називається процедура верифікації належності ідентифікатора суб'єкту.

Аутентифікація здійснюється на основі того чи іншого секретного елемента (аутентифікатора), який є у розпорядженні як суб'єкта, так і інформаційної системи. Звичайно, інформаційна система має в розпорядженні не сам секретний елемент, а деяку інформацію про нього, на основі якої приймається рішення про адекватність суб'єкта ідентифікатору. Наприклад, перед початком інтерактивного сеансу роботи більшість операційних систем запитують у користувача його ім'я та пароль. Введене ім'я є ідентифікатором користувача, а його пароль - аутентифікатором. Операційна система зазвичай зберігає не сам пароль, а його хеш-суму, що забезпечує складність відновлення пароля.

В інформаційних технологіях використовуються такі методи аутентифікації:

Ø однобічна аутентифікація, коли клієнт системи для доступу до інформації доводить свою аутентичність;

Ø двобічна аутентифікація, коли, крім клієнта, свою аутентичність повинна підтверджувати і система (наприклад, банк);

Ø трибічна аутентифікація, коли використовується так звана нотаріальна служба аутентифікації для підтвердження достовірності кожного з партнерів в обміні інформацією.

Методи аутентифікації також умовно можна поділити на однофакторні та двофакторні.

Однофакторні методи діляться на:

• *логічні* (паролі, ключові фрази, які вводяться з клавіатури комп'ютера чи клавіатури спеціалізованого пристрою);

• *ідентифікаційні* (носієм ключової інформації є фізичні об'єкти: дискета, магнітна карта, смарт-карта, штрих-кодова карта тощо. Недоліки: для зчитування інформації з фізичного об'єкта (носія) необхідний спеціальний рідер; носій можна загубити, випадково пошкодити, його можуть викрасти або зробити копію).

• ***біометричні*** (в їх основі - аналіз унікальних характеристик людини, наприклад: відбитки пальців, малюнок райдужної оболонки ока, голос, обличчя. Недоліки: біометричні методи дорогі і складні в обслуговуванні; чутливі до зміни параметрів носія інформації; володіють низькою достовірністю; призначені тільки для аутентифікації людей, а не програм або інших ресурсів).

Аутентифікація за відбитками пальців. Ця біометрична технологія, цілком імовірно, в майбутньому використовуватиметься найширше. Переваги засобів доступу по відбитку пальця - простота використання, зручність і надійність. Весь процес ідентифікації здійснюється досить швидко і не вимагає особливих зусиль від користувачів.

Вірогідність помилки при ідентифікації користувача набагато менша порівняно з іншими біометричними методами.

Використання геометрії руки. Цей метод сьогодні застосовується в більш ніж 8000 організацій, включаючи Колумбійський законодавчий орган, Міжнародний Аеропорт Сан-Франциско, лікарні і імміграційні служби. Переваги ідентифікації по геометрії долоні порівнянні з аутентифікацією **по** відбитку пальця в питаннях надійності, хоча пристрій для прочитування відбитків долонь займає більше місця. Найбільш досконалий пристрій, Напсікеу, сканує як внутрішню, так і бічну сторону руки.

Аутентифікація за райдужною оболонкою ока. Перевага сканування райдужної оболонки полягає в тому, що зразок плям на оболонці знаходиться на поверхні ока, і від користувача не вимагається спеціальних зусиль. Фактично відеозображення ока може бути відскановане на відстані метра, що робить можливим використання таких сканерів в банкоматах. Ідентифікуючі параметри можуть скануватися і кодуватися, зокрема, і у людей з ослабленим зором, але непошкодженою райдужною оболонкою.

Аутентифікація за сітківкою ока. Сканування сітківки відбувається з використанням інфрачервоного світла низької інтенсивності, направленого через зіницю до кровоносних судин на задній стінці ока. Сканери для сітківки ока набули великого поширення в надсекретних системах контролю доступу, оскільки ці засоби аутентифікації характеризуються одним з найнижчих відсотків відмови в доступі зареєстрованим користувачам і майже нульовим відсотком помилкового доступу.

Аутентифікація за рисами особи (за геометрією особи) - один з напрямів, що швидко розвиваються, в біометричній індустрії. Розвиток цього напряму пов'язаний з швидким зростанням мультимедійних відео-технологій. Проте більшість розробників поки зазнають труднощі в досягненні високого рівня виконання таких пристроїв. Проте можна чекати появу в найближчому майбутньому спеціальних пристроїв ідентифікації особи за рисами обличчя в залах аеропортів для захисту від терористів і т. ін.

Двофакторні методи аутентифікації отримують в результаті комбінації двох різних однофакторних методів, частіше всього ідентифікаційного та логічного. Наприклад: «пароль + дискета», «магнітна карта + PIN».

Кожен клас методів має свої переваги і недоліки. Майже всі методи аутентифікації страждають на один недолік - вони, насправді, аутентифікують не конкретного суб'єкта, а лише фіксують той факт, що аутентифікатор суб'єкта відповідає його ідентифікатору. Тобто всі відомі методи не захищені від компрометації аутентифікатора.

3 Захист даних від несанкціонованого доступу (НСД)

3.1 Основні принципи захисту даних від НСД.

Одним з напрямків захисту інформації в інформаційних системах є технічний захист інформації (ТЗІ). У свою чергу, питання ТЗІ розбиваються на два великих класи завдань: захист інформації від несанкціонованого доступу і захисту інформації від витоку технічними каналами. Під НСД мається на увазі доступ до інформації, що порушує встановлену в інформаційній системі політику розмежування доступу. Під

технічними каналами розуміються канали сторонніх електромагнітних випромінювань і наведень, акустичні канали, оптичні канали й ін.

Захист від НСД може здійснюватися в різних складових інформаційної системи:

1. Прикладне й системне ПЗ.

2. Апаратна частина серверів і робочих станцій.

3. Комунікаційне устаткування й канали зв'язку.

4. Периметр інформаційної системи.

Для захисту інформації на рівні прикладного й системного ПЗ використовуються:

- системи розмежування доступу до інформації;
- системи ідентифікації й аутентифікації;
- системи аудиту й моніторингу;
- системи антивірусного захисту.

Для захисту інформації на рівні апаратного забезпечення в икористовуються:

- апаратні ключі;
- системи сигналізації;

Ø засоби блокування пристроїв і інтерфейсів вводу-виводу інформації.

У комунікаційних системах використовуються наступні засоби мережевого захисту інформації:

Ø **міжмережеві екрани (Firewall)** - для блокування атак із зовнішнього середовища (Casio PIX Firewall, Symantec Enterprise FirewallTM, Alteon Switched Firewall). Вони управляють проходженням мережевого трафіка відповідно до правил (policies) безпеки. Як правило, міжмережеві екрани встановлюються на вході мережі й розділяють внутрішні (частки) **і** зовнішні (загального доступу) мережі;

Ø **системи виявлення вторгнень (IDS - Intrusion Detection System)** - для

виявлення спроб несанкціонованого доступу як ззовні, так і усередині мережі, захисту від атак типу «відмова в обслуговуванні» (Cisco Secure IDS, Intruder Alert і NetProwel від компанії Symantec. Дані системи здатні запобігти шкідливим діям, що дозволяє знизити час простою в результаті атаки та витрати на підтримку працездатності мережі;

Ø **засоби створення віртуальних приватних мереж (VPN - Virtual Private Network)** - для організації захищених каналів передачі даних через незахищене середовище (Symantec Enterprise VPN, Cisco IOS VPN, Cisco VPN concentrator. Віртуальні приватні мережі забезпечують прозоре для користувача з'єднання локальних мереж, зберігаючи при цьому конфіденційність і цілісність інформації шляхом її динамічного шифрування;

Ø **засоби аналізу захищеності** - для аналізу захищеності корпоративної мережі й виявлення можливих каналів реалізації погроз інформації (Symantec Enterprise Security Manager, Symantec NetRecon). їхнє застосування дозволяє запобігти можливим атакам на корпоративну мережу, оптимізувати витрати на захист інформації й контролювати поточний стан захищеності мережі.

Для захисту периметра інформаційної системи створюються:

Ø системи охоронної й пожежної сигналізації;

Ø системи цифрового відеоспостереження;

Ø системи контролю й керування доступом (СККД).

При створенні програмно-апаратних засобів захисту від есанкціонованого доступу керуються наступними принципами:

1) принцип обґрунтованості доступу (виконавець повинен мати достатню «форму допуску» до закритої інформації, відомості про яку потрібні йому для повноцінного виконання професійних обов'язків);

2) принцип достатньої глибини контролю доступу (СЗІ повинні включати механізми контролю доступу до всіх видів інформаційних і програмних ресурсів);

3) принцип розмежування потоків інформації (не дозволяє переписувати закриту інформацію на незакриті носії; здійснюється мічення на носії інформації і ідентифікація цих носіїв);

4) принцип чистоти повторно використовуваних ресурсів (звільнення від закритої інформації ресурсів при їх видаленні);

5) принцип персональної відповідальності (виконавець повинен нести персональну відповідальність за свою діяльність в системі, включаючи всі дії із закритою інформацією);

6) принцип цілісності засобів захисту (засоби захисту повинні точно виконувати свої функції і бути ізольовані від користувача).

3.2 Моделі управління доступом

Моделі управління доступом визначають правила управління доступом до інформації, дозволами в системі так, щоб система завжди була безпечна. Властивості моделей управління доступом:

1) Модель управління доступом повинна бути адекватною модельованій системі.

2) Модель повинна бути простою і абстрактною і не складною для розуміння.

Існують матричні та багаторівневі моделі управління доступом.

Матричні моделі управління доступом:

1. Модель Лемпсона.

Основа моделі - правила доступу, що визначають можливий вид доступу суб'єкта до об'єкта доступу. Як об'єкти

виступають пасивні елементи матриці. Як суб'єкти - активні елементи. Суб'єкти можуть бути також і об'єктами доступу. Дана модель дозволяє динамічно передавати права об'єктів.

Недоліки цієї моделі:

- не всі суб'єкти доступу мають доступ до всіх об'єктів (матриця сильно розріджена);

- дана модель не відстежує потоки інформації. Модифікації моделі Лемпсона:

1) Списки управління доступом до об'єктів,

У даній моделі повноваження доступу визначаються у вигляді списку кортежів для всіх суб'єктів, що мають доступ до даного об'єкту. Така модель застосовується в системах Novell.

Переваги даної моделі:

- економія пам'яті;

- зручність отримання відомостей про суб'єктів, що мають доступ до даного об'єкта.

Недоліки:

- незручність отримання відомостей про об'єкти, до яких має доступ даний суб'єкт;

- незручність відстежування обмежень і залежностей.

2) Списки повноважень суб'єктів (профіль суб'єкта).

У даній моделі повноваження доступу суб'єкта представляються у вигляді списку кортежів для всіх об'єктів, до яких він має доступ. Профіль суб'єкта використовується для відстежування подій аудиту в ОС Microsoft Windows NT.

Переваги моделі:

- економія пам'яті;

- зручність отримання відомостей про об'єкти, до яких має доступ даний суб'єкт.

Недолік: незручність отримання відомостей про суб'єктів, які мають доступ до даного об'єкта. 2. Атрибутна схема.

Атрибутні способи задання матриці доступу засновані на привласненні суб'єктам і об'єктам певних міток (атрибутів, що містять значення). Така схема використовується в ОС сімейства UNIX. Матриця задана в неявному вигляді. Обчислення рівня доступу суб'єкта до об'єкта відбувається динамічно.

3.3 Технічні можливості зловмисника і засоби знімання інформації

Не слід недооцінювати можливості непрофесіоналів щодо здійснення комп'ютерних злочинів. Нелояльні співробітники, що мають доступ до комп'ютерів, грають головну роль в більшості фінансових злочинів. Це швидше організаційна, ніж технічна проблема. Якщо найманим службовцям добре платять, то мало вірогідно, що вони представлять загрозу безпеці.

Статистика наводить сумні дані про те, що лише чверть співробітників банку цілком лояльна, чверть, безумовно, настроєна до фірми вороже і не має моральних обмежувачів. Лояльність же другої половини співробітників залежить виключно від обставин.

Процедури безпеки можуть забезпечувати перевірку паролів і строгий контроль доступу до цінних загальних даних, але зловмисника, обізнаного у внутрішньому устрої системи, практично неможливо зупинити. Однією з найуразливіших точок будь-якої організації з погляду безпеки стає її персонал, і, відповідно, великого значення набувають грамотна реалізація внутрішньої політики і робота з персоналом.

Для побудови надійного захисту необхідно виявити можливі погрози безпеці інформації, оцінити їх наслідки, визначити необхідні заходи і засоби захисту і оцінити їх ефективність.

Технічний канал просочування інформації - сукупність фізичних полів, що несуть конфіденційну інформацію, конструктивних елементів взаємодії систем і технічних засобів порушника для реєстрації і зняття інформації.

Розглянемо деякі типові канали просочування інформації:

- знімання інформації, що передається по телефонних лініях, лініях радіо- і пейджинговому зв'язку;

- знімання мовної інформації з подальшою передачею її по радіоканалу («жучки»), по дротяних лініях (по мережі або по пожежній сигналізації);

• знімання мовної інформації через конструкції будівель (стетоскопи), з віконних отворів (лазерний мікрофон або направлений мікрофон);

• запис переговорів в людних місцях (направлений мікрофон);

• знімання і дешифрування побічних випромінювань з комп'ютера або іншої оргтехніки;

• запис на диктофон переговорів.

Знімання інформації за допомогою мікрофонів. В тому випадку, якщо є постійний доступ до об'єкта контролю, можуть бути використані прості мініатюрні мікрофони, сполучні лінії яких виводять в сусідні приміщення для реєстрації і подальшого прослуховування акустичної інформації. Такі мікрофони діаметром 2,5 мм можуть вловлювати нормальний людський голос з відстані до 10-15 м.

Разом з мікрофоном в контрольованому приміщенні, як правило, встановлюють мініатюрний підсилювач з компресором для збільшення динамічного діапазону акустичних сигналів і забезпечення передачі акустичній інформації на значні відстані. Ці відстані в сучасних виробах досягають до 500 метрів і більше. Тобто служба безпеки фірми, що займає багатоповерховий офіс " (або зловмисник), може прослуховувати будь-яке приміщення в будівлі. При цьому дротяні лінії від декількох приміщень зводяться в **одне** місце **на** спеціальний пульт і операторові залишається лише вибірково прослуховувати будь-яке з них та, за необхідності, записувати розмови на магнітофон або жорсткий диск комп'ютера.

Для одночасної реєстрації акустичних сигналів від декількох приміщень (від 2-х до 16-ти) існують багатоканальні реєстратори створені на базі ПК. Такі реєстратори найчастіше використовуються для контролю акустичної інформації приміщень і телефонних розмов. Вони мають різні додаткові функції, такі як визначення вхідних і вихідних номерів телефонів, ведення журналів і протоколів сеансів зв'язку і ін.

Передача інформації по спеціально прокладених проводах. Недоліком таких проводів є можливість їх виявлення і перевірки призначення при візуально-технічному контролі. У сучасніших системах використовуються якнайтонші (товщиною з волосину) оптичні волокна, які можливо вплести в килимове покриття і т.д.

Мікрофони можуть бути введені через вентиляційні канали на рівень контрольованого приміщення, яке може прослуховуватися з іншого приміщення. При цьому досить встановити диктофон з можливістю запису на декілька годин, який має можливість управління записом за рівнем акустичного сигналу, і всі розмови в контрольованому приміщенні записуватимуться досить тривалий час без зміни касет.

Направлені мікрофони. Існує декілька модифікацій направлених мікрофонів, що сприймають і підсилюють звуки, які йдуть тільки з одного напряму, і що ослабляють решту всіх звуків. У простих з них вузька діаграма спрямованості формується за рахунок використання довгої трубки. У складніших конструкціях можуть використовуватися декілька трубок різної довжини. Високі параметри мають також вузько направлені мікрофони, в яких діаграма спрямованості створюється параболічним концентратором звуку.

За кордоном широко представлені трубчасті мікрофони, зроблені в формі парасольки («в англійському стилі»). У нього вбудований підсилювач і є вихід на навушники. Дальність дії їх становить не більше 30 м.

У міських умовах неможливо проводити знімання інформації з відстані, що перевищує 100 м. Сотні метрів можуть бути досягнуті у виняткових випадках типу: заповідник, ранній ранок, туман, над озером тощо.

Диктофони і магнітофони. Для акустичної розвідки використовуються радіомікрофони, мініатюрні диктофони і магнітофони замасковані під предмети повсякденного попиту: книгу, письмові прилади, пачку цигарок, авторучку тощо.

Сучасні диктофони забезпечують безперервний запис мовної інформації від 30 хвилин до декількох годин. Вони оснащені системами акустичного запуску, тобто управлінням по рівню акустичного сигналу, автореверсами, системами індикації дати і часу запису та дистанційним керуванням. Вибір диктофонів сьогодні дуже великий. З описаними функціями можна підібрати модель фірм OLYMPUS, SONY, Panasonic, Uher.

У деяких моделях диктофонів як носій інформації використовуються цифрові мікрочіпи і міні-диски, записану на такому диктофоні мовну інформацію можна переписувати на жорсткі диски комп'ютерів для зберігання, архівації і подальшого прослуховування.

Перевагою цифрових диктофонів є те, що вони мають малі габарити і вагу, можуть записувати до 20 годин мовної інформації, мають хорошу чутливість вбудованого мікрофону (до 8 м) і широкий динамічний діапазон. Час безперервної

роботи від одного елементу живлення може складати до 80 годин в режимі запису і до 2-х років в режимі очікування.

Як правило, цифрові диктофони оснащені системою голосової активації (VAS), що дозволяє ефективно стискати паузи в повідомленнях, збільшуючи таким чином реальний час запису. Кожен проведений запис маркується часом і датою за допомогою вбудованого годинника реального часу.

На відміну від касетних, цифрові диктофони тяжче виявити під час роботи. Касетні виявляються спеціальними приладами типу TRD-800, PTRD-18, PTRD-19 і ін. за електромагнітними випромінюваннями працюючого двигуна стрічкопротяжного механізму. Цифрові диктофони виявляються із значно менших відстаней. Зокрема портативний прилад ST-041 виявляє цифрові диктофони на відстані 20-30 см, а стаціонарний комплекс ST-0110 на відстані 50-70 см.

Знімання інформації, передаваної по телефонних лініях. Це простий, один з найрезультативніших і найбільш дешевий спосіб. Прослуховування розмови на телефонній лінії, як правило, здійснюється на відрізку «станція-абонент» або ж відразу з апарату (крім випадків, коли цим займаються спецслужби, які підключаються після АТС і техніку яких в цьому випадку практично неможливо виявити).

Телефонні абонентські лінії зазвичай складаються з трьох ділянок: магістрального (від АТС до розподільно"" шафи (РІП)), розподільного (від РШ до розподільної коробки (КРТ)), абонентської проводки (від КРТ до телефонного апарату). Останні дві ділянки - розподільний і абонентський є найуразливішими з погляду перехоплення інформації. Підслуховуючий пристрій може бути встановлене в будь-якому місці, де є доступ до телефонних проводів, телефонного

апарату, розетки або в будь-якому місці лінії аж до КРТ. Підключення до телефонних ліній здійснюється не тільки гальванічно (прямим під'єднуванням), а і за допомогою індукційних або ємкісних датчиків. Таке під'єднування практично не виявляється за допомогою тих апаратних засобів, які широко використовуються для пошукових цілей.

Найпоширенішими з подібних засобів прослуховування є телефонні контролери, радіо ретранслятори, які частіше називаються телефонними передавачами, або телефонними закладками.

Телефонні закладки підключаються паралельно або послідовно в будь-якому місці телефонної лінії і мають значний термін служби, оскільки живляться від телефонної мережі. Ці вироби надзвичайно популярні в промисловому шпигунстві завдяки простоті і дешевизні. Для маскування телефонні закладки випускаються у вигляді конденсаторів, реле, фільтрів і інших стандартних елементів і вузлів, що входять до складу телефонного апарату.

Перехоплення факсимільної інформації. Перехоплення факсів принципово не відрізняється від перехоплення телефонних повідомлень. Завдання доповнюється тільки обробкою отриманого повідомлення. Зазвичай комплекси перехоплення і реєстрації факсимільних повідомлень складаються з:

- Ø ПК з необхідними, але цілком доступними ресурсами;
- Ø пакета програмного забезпечення;
- Ø стандартного аудіо-контролера (SoundBlaster);

Ø пристрою підключення до лінії (адаптер).

Комплекси забезпечують автоматичне виявлення (визначення мовне або факсимільне повідомлення), реєстрацію факсимільних повідомлень на жорсткий диск з подальшою можливістю автоматичної демодуляції, дескремблювання зареєстрованих повідомлень і виводу їх на дисплей і друк.

Перехоплення розмов **по радіотелефонах і стільниковому зв'язку.** Для перехоплення розмов по радіотелефонах досить налаштувати приймач (сканер) на його частоту, що знаходиться в зоні прийому, і встановити відповідний режим модуляції.

Для перехоплення переговорів, що ведуться по мобільному стільниковому зв'язку, необхідно використовувати складнішу апаратуру. В даний час існують різні комплекси контролю стільникової системи зв'язку стандартів AMPS, DAMPS, NAMPS, NMT-450, NMT-450i, які розроблені та виготовлені в Росії та країнах Західної Європи. Комплекси дозволяють виявляти і супроводжувати по частоті вхідні і витікаючі дзвінки абонентів стільникового зв'язку, визначати вхідні і витікаючі номери телефонів абонентів, здійснювати стеження по частоті за каналом під час телефонної розмови, зокрема при переході з соти на соту в стільнику. Кількість абонентів, що задаються для контролю, може досягати до 16 і більше. Є можливість вести автоматичний запис переговорів на диктофон, вести на жорсткому диску ПК протокол записів на диктофон, здійснювати повний моніторинг всіх повідомлень, передаваних по службовому каналу, а також визначати радіочутність всіх базових станцій в точці їх прийому з ранжуванням по рівнях сигналів, що приймаються від базових станцій.

Вартість подібних комплексів залежно від стандарту контрольованої системи зв'язку і об'ємів вирішуваних завдань може складати від 5 до 60 тисяч доларів.

3.4 Технічні засоби захисту даних від їх витоку

Захист інформації від її витоку технічними каналами зв'язку забезпечується наступними засобами **й** заходами:

Ø використанням екранованого кабелю й прокладкою проводів і кабелів в екранованих конструкціях;

Ø установкою на лініях зв'язку високочастотних фільтрів;

Ø побудовою екранованих приміщень («капсул»);

Ø використанням екранованого устаткування;

Ø установкою активних систем зашумлення.

З метою оцінки стану технічного захисту інформації, що обробляється або циркулює в інформаційних системах, комп'ютерних мережах, системах зв'язку, і підготовки обґрунтованих виводів для прийняття відповідних рішень звичайно проводиться експертиза в сфері технічного захисту інформації.

Розглянемо основні поняття, що існують при розгляді технічних засобів захисту даних від їх витоку:

Основні технічні засоби і системи (ОТЗС) - технічні засоби і системи, а також їх комунікації, використовувані для обробки, зберігання і передачі закритої інформації.

Допоміжні технічні засоби і системи (ДТЗС) - технічні засоби, системи і засоби комунікації, не призначені для обробки, зберігання і передачі закритої інформації, але встановлені спільно з ОТЗС (засоби передачі даних по радіозв'язку, кондиціонери і сигналізації).

Інформаційний сигнал - сигнал у вигляді електричних, електромагнітних і інших фізичних полів, при перехопленні якого може бути розкрита інформація, циркулююча в ОТЗС.

Контрольована зона - територія, на якій виключена можливість перебування сторонніх осіб і транспортних засобів.

Засоби захисту від знімання інформації по акустичному каналу: 1 *Акустичні* ***генератори*** *перешкод:*

> *портативні (кишенькові) генератори перешкод* (захищають невеликі площі. Генерують шум звукової частоти, забезпечуючи маскування розмови і погіршення розбірливості мови. Для людини вони не чутні. Площа зашумлення становить 6-8 $м^2$);

> настільні генератори перешкод;

> *стаціонарні генератори аудіоперешкод* (мають в своєму складі вібродатчики, що перешкоджають зніманню інформації по вібро-акустичному каналу).

2. Спеціальний матеріал - прозорий пластик «Сонар» (з нього виготовляються спеціальні кабіни, в яких можна безпечно вести переговори).

3. ***Засоби захисту від записуючих диктофонів*** (детектори роботи електродвигуна; диктофоношукачі (PTRD-01 - виконаний у вигляді жезла завдовжки 24 см, діаметром 20 мм; радіус дії- до 1,5 м).

Засоби виявлення засобів знімання і передачі інформації:

1. *Апаратура контролю і пошуку по електромагнітним імпульсам (ЕМІ).*

(виявляє активно працюючі пристрої, що створюють ЕМІ): детектори випромінювання, сканери, аналізатори спектра, селективні мікровольтметри, частотоміри, програмно-апаратні комплекси з радіомоніторингом.

2. *Апарати для виявлення* ***непрацюючих пристроїв*** (нелінійні локатори, ендоскопи, дефектоскопи, металошукачі, рентгенівські комплекси).

Захист розмов по телефонних лініях:

> фіксація факту знімання інформації;

> підвищення конфіденційності;

> дискретизація мови з подальшим шифруванням (оцифровування, шифрування мови і передача за допомогою модему);

> аналогове скремблювання.

Скремблювання - зміна характеристик мовного сигналу так, щоб одержаний сигнал, володіючи властивостями

нерозбірливості і невпізнання, займав таку ж смугу частот, як і відкритий мовний сигнал.

Скремблери поділяються на аналогові і комбіновані. Принцип роботи аналогових скремблерів заснований на тимчасовій або частотній перестановці мовного сигналу. Комбіновані скремблери діють аналогічно, але на базі цифрової обробки сигналу.

4 Основи захисту даних від комп'ютерних вірусів

4.1 Шкідливі програми на ЕОМ

Шкідлива програма - це будь-яке програмне забезпечення, призначене для забезпечення діставання несанкціонованого доступу **до** інформації, що зберігається на ЕОМ, з метою спричинення шкоди (збитку) власникові інформації або власникові ЕОМ (мережі ЕОМ).

Однією з найнебезпечніших програм є комп'ютерний вірус.

Комп 'ютерний вірус - це спеціально написана програма, здатна мимоволі приєднуватися до інших програм, створювати свої копії та упроваджуватися у файли, системні області комп'ютера або мережі з метою порушення роботи комп'ютера і створення всіляких перешкод.

Класифікацію комп'ютерних вірусів наведено в таблиці 5.1.

Таблиця 5.1 Класифікація комп'ютерних вірусів

№ з/п	За алгоритмом роботи	За середовищем розповсюдження	За ОС	За деструктивними можливостями	За типом носія
1.	Звичайні	Файлові	Ms-dos	Нешкідливі (жарти)	На гнучких магнітних дисках
2.	Шифровані віруси	Завантажувальні	Windows	Небезпечні (ушкоджують ПО)	На жорстких
3.	Приховані	Макровіруси	**UNIX**	Дуже небезпечні (ушкоджують ПК)	На CD(DVD)-дисках
4.	Поліморфні	Мережеві			На flash-носіях
5.	Макрокомандні	Резидентні			
6.	Скрипти				

До шкідливих програм, крім вірусів, відносяться також мережеві черв'яки, троянські коні (логічні бомби), intended-віруси, конструктори вірусів і поліморфік-генератори.

Мережеві черв'яки - програми, що розповсюджуються по мережі і не залишають своєї копії на магнітному носії або диску.

До *троянських коней* відносяться програми, що завдають будь-яку руйнівну дію, в залежності від яких-небудь умов або при кожному запуску знищують інформацію на дисках, зупиняють роботу операційної системи і т.д. Найпоширенішою різновидністю "троянських програм" є широко відомі програми масового використання (редактори, ігри, транслятори і т.п.), в які вбудовані, так звані "логічні бомби", що спрацьовують у випадку виникнення деякої події. Різновидністю "логічної бомби" є "бомба з годинниковим механізмом", яка запускається у визначенні моменти часу.

Потрібно зазначити, що "троянські програми" не можуть самостійно розмножуватися і розповсюджуватися по локальній обчислювальній мережі самими користувачами, зокрема, через загальнодоступні банки даних і програм. У порівнянні з вірусами "троянські коні" не одержали широкого поширення внаслідок достатньо простих причин: вони або знищують себе разом з іншими даними на диску, або демаскують свою присутність і знищуються постраждалим користувачем.

Серед шкідливих програм слід відмітити також *«люті жарти» (hoax)*. До них відносяться програми, що не заподіюють комп'ютеру якоїсь прямої шкоди, проте виводять повідомлення про те, що така шкода вже заподіяна або буде заподіяною за яких-небудь умов, або попереджують

користувача про неіснуючу небезпеку. До «лютих жартів» відносяться, наприклад, програми, що лякають користувача повідомленнями про форматування диска (хоча ніякого форматування насправді не відбувається), виявляють віруси в неінфікованих файлах, виводять дивні вірусоподібні повідомлення у залежності від почуття гумору автора такої програми.

До intended-*вірусів* відносяться програми, що на перший погляд є стовідсотковими вірусами, але не спроможні розмножуватися через помилки. Наприклад, вірус, що при інфікації «забуває» передбачити активізацію вірусу, що розмножується тільки один раз - з «авторської» копії. Інфікувавши якийсь файл, вони втрачають спроможність до подальшого розмноження. Частіше всього intended-віруси з'являються при неякісній перекомпіляції якогось вже існуючого вірусу, або через недостатнє знання мови програмування, або через незнання технічних тонкощів операційної системи.

Конструктор вірусів - це програма, що призначена для виготовлення нових комп'ютерних вірусів. Відомі конструктори вірусів для DOS, Windows і макровірусів. Вони дозволяють генерувати вихідні тексти вірусів (ASM-файли), об'єктні модулі і (або) безпосередньо інфікувати файли.

Поліморфік-генератори, як і конструктори вірусів, не є вірусами в буквальному значенні цього слова, оскільки в їхній алгоритм не закладаються функції розмноження, тобто відкриття, закриття і запису у файли, читання і запису секторів і т.д. Головною функцією подібного роду програм є шифрування тіла вірусу і генерація відповідного розшифровувача. Звичайні поліморфні генератори поширюються їхніми авторами без обмежень у вигляді файла-

архіву. Основним файлом в архіві будь-якого генератора є об'єктний модуль, що містить цей генератор. В усіх генераторах, що зустрічалися, цей модуль містить зовнішню (external) функцію - виклик програми генератора. У такий спосіб автору вірусу, якщо він бажає створити справжній поліморфік-вірус, не потрібно розробляти власний за- чи розшифровувач. За бажанням він може підключити до свого вірусу будь-який відомий поліморфік-генератор.

4.2 Засоби захисту від комп'ютерних вірусів та їх особливості

Для захисту від різноманітних вірусів існує декілька видів антивірусів, які за своїм призначенням поділяють на детектори, фаги, ревізори, фільтри та вакцини. Розглянемо їх характеристики більш докладно.

Детектори (сканери) - перевіряють оперативну або зовнішню пам'ять на наявність вірусу за допомогою розрахованої контрольної суми або сигнатури і складають список ушкоджених програм. Якщо детектор - резидентний, то програма перевіряється і тільки в разі відсутності вірусів вона активується. Детекторами є, наприклад, програма MS Anti Virus.

Фаги (поліфаги) - виявляють та знешкоджують вірус (фаг) або кілька вірусів. Сучасні версії поліфагів, як правило, можуть проводити евристичний аналіз файлу, досліджуючи його на наявність коду, характерного для вірусу (додання частини однієї програми в іншу, шифрування коду тощо). Фагами є, наприклад, програми Aidstest, DrWeb.

Дуже часто функції детектора та фага суміщені в одній програмі, а вибір режиму роботи здійснюється завданням

відповідних параметрів (опцій, ключів). На початку вірусної ери кожний новий вірус визначався та лікувався окремою програмою. При цьому для деяких з вірусів (наприклад, VIENNA) цих програм було не менше десятка. Згодом окремі програми почали виявляти та лікувати декілька типів вірусів, тому їх стали звати полідетекторами та поліфагами відповідно.

Сучасні антивірусні програми знаходять і знешкоджують багато тисяч різновидів вірусів і заради простоти їх звуть коротко детекторами та фагами. Серед детекторів та фагів найбільш відомими та популярними є програми Aidstest, DrWeb (фірма «ДиалогНаука», Росія), Scan, Clean (фірма McAfee Associates, США), Norton AntiVirus (фірма Symantec Corporation, США). Ці програми періодично поновлюються, даючи користувачеві змогу боротися з новими вірусами.

Ревізори - програми, що контролюють можливі засоби зараження комп'ютера, тобто вони можуть виявити вірус, невідомий програмі. Ці програми перевіряють стан BOOT-сектора, FAT-таблиці, атрибути файлів. При створенні будь-яких змін користувачеві видається повідомлення (навіть у разі відсутності вірусів, але наявності змін).

При першому запуску ревізор утворює таблиці, куди заносить інформацію про вільну пам'ять, Partition Table, Boot-сектор, директорії, файли, що містяться у них, погані кластери тощо. При повторному запуску ревізор сканує пам'ять та диски і видає повідомлення про всі зміни, що відбулися у них з часу останнього сеансу ревізії. Нескладний аналіз цих змін дозволяє надійно визначити факт зараження комп'ютера вірусами. Серед ревізорів найбільш популярною є програма ADinf (фірма «ДиалогНаука», Росія).

Свого часу, коли не було надійних засобів боротьби з вірусами, широкого поширення набули так звані *фільтри.* Ці антивірусні програми блокують операцію записування на диск і виконують її тільки при вашому дозволі. При цьому легко визначити, чи то ви санкціонували команду на запис, чи то вірус 'Намагається щось заразити. До числа широко відомих свого часу фільтрів можна віднести програми VirBlk, FluShot та ін.

Зараз фільтри майже не використовують, оскільки вони, по-перше, дуже незручні, бо відволікають час на зайвий діалог, по-друге, деякі віруси можуть обманювати їх.

Сторожі - резидентні програми, які постійно зберігаються у пам'яті комп'ютера й у визначений користувачем час перевіряють оперативну пам'ять комп'ютера, файли, BOOT-сектор, FAT-таблицю. Сторожем є, наприклад, програма AVP.

Вакцини - це програми, які використовуються для оброблення файлів та завантажувальних секторів з метою передчасного виявлення вірусів. Існують три рубежі захисту від комп'ютерних вірусів:

1. Запобігання надходженню вірусів.

2. Запобігання вірусній атаці, якщо вірус усе-таки потрапив у комп'ютер.

3. Запобігання руйнівним наслідкам, якщо атака відбулася. Є три методи реалізації рубіжної оборони:

1. «Програмні методи захисту».

2. Апаратні методи захисту.

3. Організаційні методи захисту.

Основним засобом захисту інформації є резервне копіювання найцінніших даних. У разі втрати інформації внаслідок будь-якої з названих вище причин, жорсткий диск треба відформатувати й підготувати до нової експлуатації. На «чистий» диск установлюють операційну систему з дистрибутивного компакт-диска, потім під її керуванням треба встановити все необхідне програмне забезпечення, яке теж беруть з дистрибутивних носіїв. Відновлення комп'ютера завершують відновленням даних, які беруть з резервних носіїв.

Створюючи план заходів з резервного копіювання інформації, необхідно враховувати, що резервні копії повинні зберігатися окремо від комп'ютера. Робто, наприклад, резервне копіювання інформації на окремому жорсткому дискові того самого комп'ютера лише створює ілюзію безпеки. Відносно новим і досить надійним методом зберігання даних є зберігання їх на віддалених серверах в Інтернеті. Є служби, які безплатно надають простір для зберігання даних користувача.

Допоміжним засобом захисту інформації є антивірусні програми та засоби апаратного захисту. Рак, наприклад, просте відключення перемички на материнській платі не дозволить здійснити стирання перепрограмовуваної мікросхеми ПЗП (флеш-BIOS), незалежно від того, хто буде намагатися зробити це: комп'ютерний вірус чи неакуратний користувач.

Існує досить багато програмних засобів антивірусного захисту, їхні можливості такі:

1. Створення образу жорсткого диска на зовнішніх носіях. У разі виходу з ладу інформації в системних ділянках жорсткого диска, збережений «образ диска» може дозволити відновити якщо не всю інформацію, то принаймні її більшу частину. Цей засіб може захистити від утрати інформації під час апаратних збоїв та неакуратного форматування жорсткого диска.

2. Регулярне сканування жорсткого диска в пошуках комп'ютерних вірусів. Сканування звичайно виконують автоматично під час кожного ввімкнення комп'ютера або при розміщенні зовнішнього диска у зчитувальному пристрої. Під час сканування треба мати на увазі, що антивірусна програма шукає вірус шляхом порівняння коду програми з кодами відомих їй вірусів, що зберігаються в базі даних. Якщо база даних застаріла, а вірус є новим, то програма сканування його не виявить. Для надійної роботи варто регулярно оновлювати антивірусну програму. Так, наприклад, руйнівні наслідки атаки вірусу W95.CIM. 1075 («Чорнобиль»), який знищив інформацію на сотнях тисяч комп'ютерів ... 26 квітня 1999 року, були пов'язані не з відсутністю засобів захисту від нього, а з тривалою затримкою (більше року) в оновленні цих засобів.

3. Контроль за змінами розмірів та інших атрибутів файлів. Оскільки на етапі розмноження деякі комп'ютерні віруси змінюють параметри заражених файлів, програма контролю може виявити їх діяльність і попередити користувача.

4. Контроль за зверненням до жорсткого диска. Оскільки найнебезпечніші операції, пов'язані з діяльністю комп'ютерних вірусів, так чи інакше спрямовані на модифікацію даних, записаних на жорсткому дискові,

антивірусні програми можуть контролювати звернення до нього та попереджати користувача щодо підозрілої активності.

5 Основи криптографії

5.1 Основні терміни та поняття

Криптографія (від грецького kryptos - прихований і graphein - писати) -наука про математичні методи забезпечення конфіденційності і автентичності інформації.

Розвинулась дана наука з практичної потреби передавати важливі відомості найнадійнішим чином. Для сучасної криптографії характерне використання відкритих алгоритмів шифрування, що припускають використання обчислювальних засобів. Відомо більш десятка перевірених алгоритмів шифрування, які при використанні ключа достатньої довжини і коректної реалізації алгоритму роблять шифрований текст недоступним для криптоаналізу. Широко використовуються такі алгоритми шифрування, як Twofish, IDEA, RC4 та ін.

В криптографії застосовуються такі поняття:

Шифрування- процес перетворення звичайної інформації (відкритого тексту) в шифротекст.

Дешифрування - процес перетворення зашифрованої інформації **у** придатну для читання інформацію.

Кодування - заміна логічних (смислових) елементів, наприклад, слів.

Шифром називається пара алгоритмів шифрування-дешифрування.

Дія шифру керується як алгоритмами, так і в кожному випадку, ключем.

Ключ - це секретний параметр (в ідеалі, відомий лише двом сторонам) для окремого контексту під час передачі повідомлення.

Ключі мають велику важливість, оскільки без змінних ключів алгоритми шифрування легко зламуються і непридатні для використання в більшості випадків. Історично склалось так, що шифри часто використовуються для шифрування та дешифрування без виконання додаткових процедур, таких як аутентифікація або перевірка цілісності.

Алфавіт - кінцева множина, використовувана для кодування інформаційних знаків.

Текст - впорядкований набір з елементів алфавіту

Відкритий текст - початкове повідомлення, яке повинен захистити криптограф.

Стійкість - здатність протистояти спробам техніки і знаннями криптоаналізу розшифрувати перехоплене повідомлення, розкрити ключ шифру або порушити цілісність, достовірність інформації.

Криптостійкість - характеристика шифру, визначальна його стійкість до процесу дешифрування. Вимірюється кількість всіляких ключів, середній час, який потрібен для криптоаналізу з одним ключем.

В англійській мові слова *криптографія* та *криптологія* інколи мають однакове значення. В той час, як деколи під

криптографією може розумітись використання та дослідження технологій шифрування, а під *криптологією* — дослідження криптографії.

Дослідження характеристик мов, що мають будь-яке відношення до криптрлогії, таких як частоти появи певних літер, комбінацій літер, загальні шаблони тощо, називається ***криптолінгвістикою.***

Система криптографічного захисту повинна забезпечувати:

Ø **Конфіденційність** - інформація повинна бути захищена від несанкціонованого прочитання як при зберіганні, так і при передачі. Якщо порівнювати з паперовою технологією, то це аналогічно запечатуванню інформації в конверт. Зміст стає відомим тільки після **того,** як буде відкритий запечатаний конверт. Криптографічний захист забезпечується шифруванням.

Ø **Контроль доступу** - інформація повинна бути доступна тільки для того, кому вона призначена. Якщо порівнювати з паперовою технологією, то тільки дозволений одержувач може відкрити запечатаний конверт. У системах криптографічного захисту це забезпечується шифруванням.

Ø **Аутентифікація** - можливість однозначно ідентифікувати відправника. Якщо порівнювати з паперовою технологією, то це аналогічно підпису відправника. У системах криптографічного захисту забезпечується електронним цифровим підписом і сертифікатом.

Ø **Цілісність** - інформація повинна бути захищена від несанкціонованої модифікації як при зберіганні, так і при передачі. У системах криптографічного захисту

забезпечується електронним цифровим підписом і імітозахистом.

Ø **Невідмовність** - відправник не може відмовитися від довершеної дії. Якщо порівнювати з паперовою технологією, то це аналогічно пред'явленню відправником паспорта перед виконанням дії. У системах криптографічного захисту забезпечується електронним цифровим підписом і сертифікатом.

З ускладненням інформаційних взаємодій в людському суспільстві виникли і продовжують виникати нові завдання по їх захисту, деякі з них були вирішені в рамках криптографії, що привело до розвитку принципово нових підходів і методів.

5.2 Історія і законодавча база криптографії

Найперші форми тайнопису вимагали не більше ніж аналог олівця **та** паперу, оскільки в ті часи більшість людей не могли читати. Поширення писемності серед ворогів викликало потребу саме в криптографії.

Основними типами класичних шифрів є перестановочні шифри, які змінюють порядок літер в повідомленні, та підстановочні шифри, які систематично замінюють літери або групи літер іншими літерами або групами літер. Одним із ранніх підстановочних шифрів був ***шифр Цезаря,*** в якому кожна літера в повідомленні замінювалась літерою через декілька позицій із абетки. Цей шифр отримав ім'я Юлія Цезаря, який його використовував зі зсувом в 3 позиції для спілкування з генералами під час військових кампаній, "подібно до коду EXCESS-3 в булевій алгебрі.

Стеганографія (тобто приховування факту наявності повідомлення взагалі) також була розроблена в давні часи. Зокрема, Геродот приховав повідомлення - татуювання на поголеній голові раба - під новим волоссям. До сучасних прикладів стеганографії належать невидимі чорнила, мікрокрапки, цифрові водяні знаки, що застосовуються для приховування інформації.

Після відкриття частотного аналізу арабським вченим аль-Кінді в 9-му столітті, майже всі такі шифри стали більш-менш легко зламними досвідченим фахівцем. Класичні шифри зберегли популярність, в основному, у вигляді головоломок (криптограм). Це тривало до винаходу поліалфавітного шифру Альберті Леоном-Баттістою приблизно в 1467 році (хоча існують свідчення того, що знання про такі шифри існували серед арабських вчених). Винахід Альберті полягав в тому, щоб використовувати різні шифри (наприклад, алфавіти підстановки) для різних частин повідомлення. Йому також належить винахід того, що може вважатись першим шифрувальним приладом: колесо, що частково реалізовувало його винахід.

В поліалфавітному шифрі Вігнера алгоритм шифрування використовує ключове слово, яке керує підстановкою літер в залежності від того, яка літера ключового слова використовується. В середині XIX ст. Чарльз Беббідж показав, що поліалфавітні шифри цього типу залишились частково беззахисними перед частотним аналізом.

Хоча частотний аналіз є потужною та загальною технікою, шифрування на практиці часто було ефективним, оскільки багато із криптоаналітиків не знали цю техніку. Дешифрування повідомлень без частотного аналізу практично означало необхідність знання використаного шифру,

спонукуючи таким чином для отримання алгоритму до шпигунства, підкупу, крадіжок, зрад тощо.

В XIX столітті було визнано, що збереження алгоритму шифрування в таємниці не забезпечує захист від зламу. Саме збереження в таємниці ключа має бути достатньою умовою захисту інформації нормальним шифром. Цей фундаментальний принцип було вперше проголошено в 1883 р. Огюстом Кірхґоффом, і загальновідомий як принцип Кірхґоффа.

Одним з найперших механічних приладів для допомоги в шифруванні був створений ще в стародавній Греції. Це *скітало* - палиця, що використовувалась спартанцями в якості перестановочного шифру. В Середньовіччя було винайдено інші засоби, такі як дірочний шифр, що також використовувався для часткової стенографії. Разом із винаходом поліалфавітних шифрів було розроблено досконаліші засоби, такі як власний винахід Альберті - шифрувальний диск табула ректа Йогана Тритеміуса та мультициліндр Томаса Джефферсона (повторно винайдений Базерієсом приблизно в 1900 році).

Декілька механічних шифрувально/дешифрувальних приладів було створено на початку 20-го століття, і багато запатентовано, серед них роторні машини- найвідомішою серед них є автомат Енігма (рис.6.1) (реалізовував складний електро-механічний поліалфавітний шифр для захисту таємних повідомлень), що використовувався Німеччиною з кінця 20-х років і до завершення Другої світової війни.

Рис. 6.1. Прилад Енігма

Поява цифрових комп'ютерів та електроніки після Другої світової війни зробило можливим появу складніших шифрів. Більше того, комп'ютери дозволяли шифрувати будь-які дані, які можна представити в комп'ютері у двійковому виді, на відміну від класичних шифрів, які розроблялись для шифрування письмових текстів. Це зробило непридатними для застосування лінгвістичні підходи в криптоаналізі.

Комп'ютери знайшли застосування у криптоаналізі, що певною мірою, компенсувало підвищення складності шифрів.

Широкі академічні дослідження криптографії з'явились порівняно нещодавно - починаючи з середини 1970-х разом із появою відкритої специфікації стандарту DES (Data Encryption Standard) Національного Бюро Стандартів СІЛА, публікацій Діффі-Хелмана та оприлюдненням алгоритму RSA. Відтоді криптографія перетворилась на загальнопоширений інструмент для передачі даних в комп'ютерних мережах та захисту інформації взагалі. Сучасний рівень безпеки багатьох криптографічних методів базується на складності деяких обчислювальних проблем, таких як розклад цілих чисел або проблеми з дискретними логарифмами.

Зараз криптографія інтенсивно використовує математичний апарат, включно з теорією інформації, теорією обчислювальної складності, статистики, комбінаторики, абстрактної алгебри та теорії чисел. Криптографія є також не звичним відгалуженням інженерії. Існують дослідження з приводу взаємозв'язків між криптографічними проблемами та квантовою фізикою.

Законодавчою базою криптографії в Україні є «Положення про порядок розроблення, виготовлення та експлуатації засобів криптографічного захисту

конфіденційної інформації» (від 30.04.2004), розроблене відповідно до Законів України «Про інформацію», «Про підприємництво», «Про захист прав споживачів», Положення про порядок здійснення криптографічного захисту інформації в Україні, затвердженого Указом Президента України від 22 травня 1998 р., та Інструкцій про умови і правила провадження підприємницької діяльності.

Це Положення визначає вимоги до порядку розроблення, виробництва та експлуатації засобів криптографічного захисту конфіденційної інформації та відкритої інформації з використанням електронного цифрового підпису.

Вимоги цього Положення обов'язкові для виконання:

Ø суб'єктами господарювання незалежно від форм власності, діяльність яких пов'язана з розробленням, виробництвом, сертифікаційними випробуваннями (експертними роботами) та експлуатацією засобів криптографічного захисту конфіденційної інформації, а також відкритої інформації з використанням електронного цифрового підпису;

Ø державними органами в частині розроблення, виробництва, сертифікаційних випробувань (експертних робіт) та експлуатації засобів криптографічного захисту відкритої інформації з використанням електронного цифрового підпису.

В свою чергу дія даного Положення не поширюється на діяльність, пов'язану із розробленням, виробництвом та експлуатацією засобів криптографічного захисту конфіденційної інформації, що є державною власністю.

6 Криптографічні методи захисту інформації

6.1 Сучасні криптосистеми та їх особливості

Всі сучасні криптосхеми побудовані за принципом Кірхґоффа, тобто секретність зашифрованих повідомлень визначається секретністю ключа. Це означає, що, навіть якщо криптоаналітик знає алгоритм шифрування, він однаково не зможе розшифрувати повідомлення, якщо не має відповідного ключа. Всі класичні блочні шифри, в тому числі ГОСТ і DES, відповідають цьому принципу й спроектовані таким чином, аби унеможливити розкриття ефективніше, аніж шляхом повного перебору в межах усього ключового простору, тобто всіх можливих значень ключа. Зрозуміло, що стійкість таких шифрів визначається розміром ключа.

На формулювання поняття захисту робить вплив велика кількість різнопланових чинників, основними з яких виступають:

Ø вплив інформації на ефективність схвалюваних рішень;

Ø концепції побудови і використання захищених інформаційних систем;

Ø технічна оснащеність інформаційних систем;

Ø характеристики інформаційних систем і їх компонентів з погляду погроз збереженню інформації;

Ø потенційні можливості зловмисної дії на інформацію, її отримання і використання;

Ø наявність методів і засобів захисту інформації.

Розвиток підходів до захисту інформації відбувається під впливом перерахованих чинників, при цьому можна умовно виділити три періоди розвитку систем захисту інформації:

перший - відноситься до часу, коли обробка інформації здійснювалася за традиційними (ручними, паперовими) технологіями;

другий - для обробки інформації на регулярній основі застосовувалися засоби електронно-обчислювальної техніки перших поколінь;

третій - використання ІТ прийняло масовий і повсюдний характер. Криптосистеми діляться на симетричні (із закритим ключем) і несиметричні (з відкритим ключем). Симетричні в свою чергу діляться на блокові і потокові.

При використанні блокової криптосистеми перетворення здійснюється над цілим блоком тексту (причому блок має достатньо велику довжину).

Потоковою називається криптосистема з послідовним виконанням перетворень над елементами відкритого тексту.

При використанні потокових шифрів виробляється деяка послідовність (псевдовипадкова), яка називається «гаммою», з допомогою якої шифрується інформація.

Вимоги до потокових шрифтів:

1. Період гамми повинен бути достатньо великим для шифрування повідомлень різної довжини.

2. Гамма повинна бути важко передбаченою.

3. Генерація гамми не повинна бути дуже трудомісткою.

Слід зазначити, що алгоритми криптосистем з відкритим ключем (СВК) можна використовувати за трьома напрямками:

1. Як самостійні засоби захисту даних, що передаються чи зберігаються.

2. Як засіб для розподілу ключів. Алгоритми СВК більш трудомісткі, ніж традиційні криптосистеми. Обмін великими інформаційними потоками здійснюють за допомогою звичайних алгоритмів. А за допомогою СВК розподіляють ключі незначного інформативного обсягу.

3. Як засіб автентифікації користувачів (електронний підпис). Найбільш розповсюджені криптосистеми з відкритим ключем на сьогоднішній день:

1. Система Ель-Гамаля.

2. Криптосистеми на основі еліптичних рівнянь.

3. Алгоритм RSA.

Незважаючи на досить велике число різних криптосистем, найбільш популярна криптосистема RSA, яка розроблена в 1977 році і отримала назву на честь її творців: Рона Ривеста, Ади Шамира і Леонарда Адлемана.

Вони скористалися тим фактом, що перебування великих простих чисел в обчислювальному відношенні здійснюється легко, але розкладання на множники добутку двох таких чисел практично нездійсненне. Доведено (теорема Рабина), що розкриття шифру RSA еквівалентне такому розкладанню. Тому для будь-якої довжини ключа можна дати нижню оцінку числа операцій для розкриття шифру, а з урахуванням продуктивності сучасних комп'ютерів оцінити і необхідний на це час.

Можливість оцінити захищеність алгоритму RSA стала однією з причин популярності цієї криптосхеми на тлі десятків інших схем. Тому алгоритм RSA використовується в банківських комп'ютерних мережах, особливо для роботи з видаленими клієнтами (обслуговування кредитних карток). В даний час алгоритм RSA активно реалізується як у вигляді самостійних криптографічних продуктів, так і вбудованих засобів в популярних додатках.

Криптосистема Ель-Гамаля є альтернативою RSA й при однаковому розмірі ключа забезпечує ту ж криптостійкість.

На відміну від RSA, метод Ель-Гамаля заснований на проблемі дискретного логарифма. Якщо підносити число до степеня в скінченому полі досить легко, то відновити аргумент

за значенням (тобто знайти логарифм) досить важко. Основу системи складають параметри p і g - числа, перше з яких - просте, а друге - ціле.

Еліптичні криві - математичний об'єкт, що може бути визначений над будь-яким полем (скінченим, дійсним, раціональним або комплексним).

У криптографії звичайно використовуються скінченні поля. Еліптична крива є безліччю точок (x,y), що задовольняють наступне рівняння: y2 = x3 + ax + b, а також нескінченно віддалена точка.

Для точок на кривій досить легко вводитися операція додавання, що грає ту ж роль, що й операція множення в криптосистемах RSA і Ель-Гамаля. У реальних криптосистемах на базі еліптичних рівнянь використовується рівняння: y2 = x3 + ax + b тосі p, де p - просте.

Проблема дискретного логарифма на еліптичній кривій полягає в наступному: дана точка O на еліптичній кривій порядку r (кількість точок на кривій) і інша **точка** Y на цій же кривій. Потрібно знайти єдину точку x таку, що Y = x, тобто Y є x-им ступенем O.

Які б не були складні і надійні 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 генерований одним з них, а потім певним чином знову ж у конфіденційному порядку переданий іншому. Тобто у загальному випадку для передачі ключа знову ж потрібне використання відповідної їй криптосистеми.

6.2 Класичні техніки шифрування

Класифікувати способи засекречування передаваних повідомлень можна по-різному, проте визначальних чинників всього два:

1. Чи використовуються для засекречування властивості матеріальних носіїв і матеріального середовища передачі інформації або воно здійснюється незалежно від них.

2. Чи ховається секретне повідомлення або воно просто робиться недоступним для всіх, окрім одержувача.

Усе різноманіття існуючих криптографічних методів можна звести до наступних класів перетворень:

Перестановки - метод криптографічного перетворення, що полягає в перестановці символів вихідного тексту за більш-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-менш складним правилом. Для

забезпечення високої криптостійкості потрібне використання великих ключів.

Гамування є також широко застосовуваним криптографічним перетворенням. Принцип шифрування гамуванням полягає в генерації гами шифру за допомогою датчика псевдовипадкових чисел і накладенні отриманої гами на відкриті дані оборотним чином. Процес дешифрування даних зводиться до повторної генерації гами шифру при відомому ключі і накладенні такої гами на' зашифровані дані. Метод гамування стає ненадійним, якщо зловмиснику стає відомий фрагмент вихідного тексту і відповідна йому шифрограма.

На даний час широко використовується блокове шифрування. Блокові шифри на практиці зустрічаються частіше, ніж «чисті» перетворення того чи іншого класу в шрифти більш високої криптостійкості. Російський і американський стандарти шифрування засновані саме на цьому класі шифрів.

У 1977 р. був розроблений, опублікований і прийнятий у світі відкритий національний стандарт шифрування даних, що не складають державної таємниці, - алгоритм DES (Data Encryption Standart). Статус DES як національний стандарт США викликав до нього цікавість із боку розроблювачів устаткування й платіжних систем. Це алгоритм з блочним шифром з ключем довжиною 56 біт. До сьогоднішнього часу найбільш ефективними методами дешифрування алгоритму DES так і залишились методи, засновані на повному переборі всіх його можливих варіантів. Решта методів побудовані на знанні додаткової інформації або відносяться до усічених версій алгоритмів.

Стандарт шифрування даних DES, розроблений фірмою IBM, є державним стандартом для шифрування цифрової інформації, рекомендований Асоціацією Американських Банкірів. Алгоритм БЕ8 вимагає від зловмисника перебору 72 квадриліонів можливих ключових комбінацій, забезпечуючи високий ступінь захисту при невеликих витратах. При частій зміні ключів алгоритм задовільно вирішує проблему перетворення конфіденційної інформації в недоступну.

Згодом консорціум e-payment опублікував проект специфікації 3DES, першого у світі міжплатформенного методу керування ключами алгоритму потрійного DES, що став стандартом для захисту інформації в банківській і фінансовій сферах. DES - це 64-бітовий блочний шифр з 64-бітовим ключем. Останній біт кожного байта в ключі є бітом парності, так що ефективна довжина ключа складає тільки 56 біт. Потрійний DES (Tгiple DES) чи 3DES - це DES, що виконується тричі з різними ключами. Таким чином, потрійний DES - це 64-бітовий блочний шифр з 168-бітовим ключем (плюс 24 біта парності). Експерти вважають 3DES дуже надійним. Недоліком є те, що він значно повільніше всіх інших алгоритмів: DES сам по собі доволі повільний через застосування бітових перестановок, що ефективно розробляються на спеціальних мікросхемах, але набагато гірше на універсальних комп'ютерах, а з 3DES потрібно виконати три операції, щоб отримати захищеність двох. Єдина причина, чому варто застосовувати потрійний DES, - це те, що він дуже добре вивчений.

7 Криптографічні методи захисту інформації (продовження)

7.1 Симетричні та асиметричні алгоритми шифрування інформації

Симетричні алгоритми шифрування - алгоритми, які застосовуються при шифруванні інформації, особливість яких полягає у тому, що ключ шифрування та розшифрування однаковий, тобто з його допомогою можна як зашифрувати, так і розшифрувати (відновити) повідомлення.

Ці алгоритми шифрування були єдиними загально відомими до липня 1976 року.

Симетричні алгоритми шифрування поділяються на потокові та блочні.

Потокові алгоритми шифрування послідовно обробляють текст повідомлення. В потокових шифрах, потік шифротексту обчислюється на основі внутрішнього стану алгоритму, який змінюється протягом його дії. Зміна стану керується ключем та, в деяких алгоритмах, потоком відкритого тексту. RC4 є прикладом добре відомого та широко розповсюдженого потокового шифру.

Блочні алгоритми працюють з блоками фіксованого розміру. Як правило, довжина блоку дорівнює 64 бітам, але в алгоритмі AES використовуються блоки довжиною 128 біт. Блочний шифр подібний до поліалфавітного шифру Альберті: отримують фрагмент відкритого тексту та ключ і видають на виході шифротекст такого самого розміру. Оскільки повідомлення зазвичай довші за один блок, потрібен деякий метод склеювання послідовних блоків. Було розроблено

декілька методів, що відрізняються в різних аспектах. Вони є режимами дії блочних шифрів та мають обережно обиратись під час застосування блочного шифру в криптосистемі.

До найбільш відомих симетричних алгоритмів, які досить добре себе зарекомендували, належать Twofish, Serpnt, AES (або Рейндайль), Blowfish, CAST5, RC4, TDES (3DES), та IDEA.

Асиметричні алгоритми шифрування — алгоритми шифрування, які використовують різні ключі для шифрування та дешифрування даних.

Головне досягнення асиметричного шифрування в тому , що воно дозволяє людям, що не мають існуючої домовленості про безпеку, обмінюватися секретними повідомленнями. Необхідність відправникові й одержувачеві погоджувати таємний ключ по спеціальному захищеному каналу цілком відпала. Прикладами криптосистем з відкритим ключем є Elgamal (названа на честь автора, Тахіра Ельгамаля), RSA, Diffie-Hellman і DSA (Digital Signature Algorithm - винайдений Девідом Кравіцом).

Проблема керування ключами була вирішена криптографією з відкритим, або асиметричним, ключем, концепція якої була запропонована Уітфілдом Діффі і Мартіном Хеллманом у 1975 році.

Криптографія з відкритим ключем - це асиметрична схема, у якій застосовуються пари ключів: відкритий (public key), що зашифровує дані, і відповідний йому закритий (private key), що їх розшифровує. Відкритий ключ поширюється по усьому світу, у той час як закритий тримається в таємниці.

Хоча ключова пара математично зв'язана, обчислення закритого ключа з відкритого в практичному плані нездійсненна. Кожний, у кого є відкритий ключ, зможе зашифрувати дані, але не зможе їх розшифрувати. Тільки людина, яка володіє відповідним закритим ключем, може розшифрувати інформацію.

Поява шифрування з відкритим ключем стала технологічною революцією, яка зробила стійку криптографію доступною масам.

В основному, симетричні алгоритми шифрування вимагають менше обчислень, ніж асиметричні. На практиці це означає, що якісні асиметричні алгоритми в сотні або в тисячі разів повільніші за якісні симетричні алгоритми. Недоліком симетричних алгоритмів є необхідність мати секретний ключ з обох боків передачі інформації. Так як ключі є предметом можливого перехоплення, їх необхідно часто змінювати та передавати по безпечних каналах передачі інформації під час розповсюдження.

Симетричні алгоритми шифрування не завжди використовуються самостійно. В сучасних криптосистемах використовуються комбінації симетричних та асиметричних алгоритмів для того, щоб отримати переваги обох схем. До таких систем належить SSL, PGP та GPG.

7.2 Цифрові підписи

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

Робота зі створення ЕЦП стала можливою з появою систем автоматизації діловодства і документообігу (САДД), що включають програмно-апаратне забезпечення обробки ЕЦП.

Електронний цифровий підпис став актуальним з розвитком банківських технологій і поширенням систем безготівкових розрахунків. Процедура цифрового підписування полягає у тому, що на основі вмісту файлу і ключа підписування обчислюється визначений набір символів, що зветься цифровим підписом. Алгоритми обчислень можуть відрізнятися, але всі вони використовують стискання вихідного документа за допомогою хеш-функції. На основі таємного ключа підписування і хеш-функції формується цифровий підпис і визначений відкритий ключ, щоб отримувач зміг його перевірити.

Потенційному шахраю, який би взявся за підписом автора відшукати його секретний ключ, треба розв'язати комбінаторну задачу з таким обсягом комп'ютерного перебору варіантів, якого вистачить практично на все його життя. Адресату, що отримав документ електронною поштою, досить запустити програму, що на основі вмісту файлу і обчислює певне значення і порівнює його з відкритим зразком цифрового підпису. Рівність значень доводить, що документ не модифікувався, тобто саме цей документ завізовано відповідним секретним ключем підписування. Цифровий

підпис робить юридично чинним документом не роздрукування документа, а сам комп'ютерний файл.

ЕЦП може служити аналогом усякого роду печаток і штампів організації. Адже вони видаються визначеному працівникові канцелярії підприємства з єдиною функцією - засвідчувати підпису керівників організації.

Електронна форма документа, збережена й оброблювана САДД, являє собою реєстраційну картку (РК) і один або кілька файлів із умістом документа. В ній утримуються зведення про реєстраційний номер і дату документа, а також інші реквізити для його пошуку, класифікації і контролю виконання.

Реєстраційні картки документів заповнюються одними працівниками -секретарями і виконавцями, а підпис на документах ставлять інші люди, як правило, керівники.

Корпоративна САДД - це кілька установок системи в центральному органі підприємства і його дочірніх організацій.

Кожна із САДД установлена на локальній мережі окремої організації, а між собою системи можуть спілкуватися по електронній пошті. Природно САДД повинні уміти використовувати ЕЦП як для підпису і перевірки підпису файлів, так і при прийомі і передачі повідомлень по електронній пошті. Ряд із пропонованих на вітчизняному ринку САДД мають таку можливість, у тому числі одна з розповсюджених у Росії САДД - «СПРАВА» компанії «Електронні офісні системи».

Для того, щоб використовувати ЕЦП у САДД, потрібні:

Ø «секретні» ключі для користувачів із правом нанесення підпису;

Ø «несекретні» сертифікати ключів, за допомогою яких здійснюється перевірка підписів іншими користувачами.

Для того, щоб створити секретний ключ і сертифікат, а вони створюються одночасно, потрібен центр керування ключовою системою (ЦККС). У функції ЦККС може входити:

Ø створення ключів і сертифікатів;

Ø перевірка їхньої дійсності;

Ø ведення списку відкликаних сертифікатів (сертифікатів ключів, що перестали діяти внаслідок різних причин, наприклад, скінчився термін дії ключа або ключ скомпрометований - загублений і т.п.).

Якщо передбачається обмін підписаними документами з зовнішніми організаціями, то можна скористатися послугами, наданими центрами колективного користування, що їх засвідчують. А можна створити і корпоративний ЦККС, діяльність якого поширюється тільки на власну організацію і підвідомчі їй підприємства або установи. Склад подібного ЦККС може бути мінімальний: окремий комп'ютер, що працює під керуванням ОС Windows 2000 Server, програмне забезпечення (ПО), що керує Microsoft Certificate Services, і ПО криптопровайдера, що має сертифікат ФАПСИ, наприклад, Криптопро CSP для формування ключів ЕЦП.

Секретні ключі, записані ЦККС на ключових носіях, передаються користувачам, що мають право підпису. Як

ключові носії можуть використовуватися дискети, інтелектуальні карти і т.п.

Використання ЕЦП в майбутньому дозволить скоротити непродуктивні витрати і значно збільшити швидкість поширення документів. Може значно зменшитися обсяг споживання паперу за рахунок виключення копіювання екземплярів документів при їхньому розсиланні в підрозділи і підвідомчі організації. Стануть непотрібними журнали передачі документів, аркуші узгодження й інші супровідні документи. Знизиться потреба в копіювальній техніці і видаткових матеріалах, а також звільнить виконавців документів від рутинних операцій при узгодженні й оформленні документів.

В Україні всі стосунки електронний документів та підписів визначаються Законами України «Про електронні документи та електронний документообіг» та «Про електронний цифровий підпис».

7.3 Адміністрування ключами

Крім вибору криптографічної системи, що підходить для конкретної інформаційної системи, важлива проблема - адміністрування ключами. Якою б не була складною й надійною сама криптосистема, вона заснована на використанні ключів. Якщо для забезпечення конфіденційного обміну інформацією між двома користувачами процес обміну ключами тривіальний, то в ІС, де кількість користувачів складає десятки й сотні, управління ключами -серйозна проблема.

Під ключовою інформацією розуміється сукупність усіх діючих у ІС ключів. Якщо не забезпечене досить надійне

управління ключовою інформацією, то, заволодівши нею, зловмисник одержує необмежений доступ до всієї інформації.

Адміністрування ключами - інформаційний процес, що містить в собі три елементи:

1.Генерацію ключів.

2.Накопичення ключів (організація їхнього збереження, обліку й вилучення).

3.Розподіл ключів між користувачами.

У загальному випадку задача управління ключами зводиться до створення такого протоколу розподілу ключів, який повинен забезпечувати:

Ø можливість розосередження розподілу ключів;

Ø взаємне підтвердження дійсності учасників сеансу;

Ø підтвердження вірогідності сеансу механізмом запиту-відповіді, використання для цього програмних або апаратних засобів;

Ø використання під час обміну ключами мінімального числа повідомлень.

8. Стандарти із захисту інформації

8.1 Світові стандарти із захисту даних в комп'ютерних системах

Критерії безпеки комп'ютерних систем Міністерства оборони США, що отримали назву «Оранжева книга» (за кольором обкладинки), були розроблені Міністерством оборони США в 1983 році (перша версія) з метою визначення вимог безпеки, які висуваються до апаратного, програмного і спеціального забезпечення комп'ютерних систем і розробки відповідної методології аналізу політики безпеки, що реалізується в КС військового призначення.

У цьому документі були вперше нормативно визначене таке поняття, як «політика безпеки». Відповідно до «Оранжевої книги» *безпечна КС* - це система, яка підтримує керування доступом до оброблюваної в ній інформації таким чином, що відповідно авторизовані користувачі або процеси, що діють від їх імені, отримують можливість читати, писати, створювати і видаляти інформацію. Запропоновані в цьому документі концепції захисту і набір функціональних вимог послужили основою для формування інших стандартів безпеки інформації.

В «Оранжевій книзі» запропоновано три категорії вимог щодо безпеки -політика безпеки, аудит та коректність, у рамках яких сформульовано шість базових вимог безпеки. Перші чотири вимоги спрямовані безпосередньо на забезпечення безпеки інформації, дві інші - на якість самих засобів захисту:

Ø ***Вимога 1 (політика безпеки)*** - система має підтримувати точно визначену політику безпеки, можливість

доступу до об'єктів повинна визначатися на основі їх ідентифікації і набору правил керування доступом;

Ø ***Вимога 2 (мітки)*** - кожен об'єкт повинен мати мітку, що використовується як атрибут контролю доступу;

Ø ***Вимога 3 (ідентифікація та аутентифікація)*** - всі суб'єкти повинні мати унікальні ідентифікатори; контроль доступу здійснюється на основі ідентифікації та аутентифікації суб'єкта та об'єкта доступу;

Ø ***Вимога 4 (реєстрація й облік)*** - **всі** події, що мають відношення до безпеки, мають відстежуватися і реєструватися **в** захищеному протоколі;

Ø ***Вимога 5 (контроль коректності функціонування засобів захисту)*** -засоби захисту перебувають під контролем засобів перевірки коректності, засоби захисту незалежні від засобів контролю коректності;

Ø ***Вимога 6 (безперервність захисту)*** - захист має бути постійним і безперервним у будь-якому режимі функціонування системи захисту і всієї системи в цілому.

Наступними після «Оранжевої книги» були розроблені «Критерії безпеки інформаційних технологій» (далі «Європейські критерії»). Вони були вперше опубліковані в 1991 році, а розроблені чотирма європейськими країнами: Францією, Німеччиною, Нідерландами та Великобританією.

«Європейські критерії» розглядають такі основні завдання інформаційної безпеки:

Ø захист інформації від НСД з метою забезпечення конфіденційності;

Ø забезпечення цілісності інформації шляхом захисту її від несанкціонованої модифікації або знищення;

Ø забезпечення працездатності систем за допомогою протидії загрозам відмови в обслуговуванні.

Загальна оцінка рівня безпеки системи складається з функціональної потужності засобів захисту і рівня адекватності їх реалізації.

Ефективність визначається функціональними критеріями, які розглядаються на трьох рівнях деталізації: перший - цілі безпеки, другий - специфікації функцій захисту, третій - механізми захисту. Специфікації функцій захисту розглядаються з точки зору таких вимог:

- ідентифікація й аутентифікація;

- керування доступом;

- підзвітність;

- аудит;

- повторне використання об'єктів;

-цілісність інформації;

-надійність обслуговування;

- безпечний обмін даними.

Набір функцій безпеки специфікується за допомогою визначених класів-шаблонів. Всього визначено десять класів (Р-С1, Р-С2, Р-В1, Р-В2, Р-В3, Р-ІН, Р-АУ, Р-ВІ, Р-ОС, Р-ВХ) за зростаючими вимогами.

«Європейські критерії» визначають також сім рівнів адекватності - від ЕО до Е6 (за зростанням вимог при аналізі ефективності та коректності засобів захисту).

«Федеральні критерії безпеки інформаційних технологій» розроблялись як одна із складових «Американського федерального стандарту з обробки інформації'» і мали замінити «Оранжеву книгу». Розробниками стандарту виступили Національний інститут стандартів і технологій США та Агентство національної безпеки США. Перша версія документа була опублікована в грудні 1992 р.

Цей документ розроблений на основі результатів численних досліджень у галузі забезпечення інформаційних технологій 80-х - початку 90-х років, а також на основі досвіду використання «Оранжевої книги». Документ являє собою основу для розробки і сертифікації компонентів інформаційних технологій з погляду забезпечення безпеки.

Створення документа мало такі цілі:

1.Визначення універсального й відкритого для подальшого розвитку базового набору вимог безпеки до сучасних інформаційних технологій.

2.Удосконалення існуючих вимог і критеріїв безпеки.

3.Приведення у відповідність прийнятих у різних країнах вимог і критеріїв безпеки інформаційних технологій.

4. Нормативне закріплення основних принципів інформаційної безпеки.

Стандарт є узагальненням основних принципів забезпечення безпеки шформаційних технологій, розроблених у 80-ті роки, та забезпечує наступність стосовно них з метою збереження досягнень у галузі захисту інформації

Основними об'єктами вимог безпеки «Федеральних критеріїв» є продукти ІТ, під якими розуміється сукупність апаратних та програмних засобів, яка являє собою готовий до використання засіб обробки інформації і постачається споживачеві.

«Федеральні критерії» містять положення, що стосуються тільки окремих продуктів ІТ, а саме власних засобів забезпечення безпеки ІТ-продуктів, тобто механізмів захисту, вбудованих безпосередньо в ці продукти у вигляді відповідних програмних, апаратних чи спеціальних засобів. Для підвищення ефективності їх роботи можуть використовуватися зовнішні системи захисту і засоби забезпечення безпеки, до яких належать як технічні засоби, так і організаційні заходи, правові і юридичні норми.

Ключовим поняттям «Федеральних критеріїв» є поняття профілю захисту -нормативного документа, що регламентує всі аспекти безпеки ІТ-продукту у вигляді вимог до його проектування, технології розробки і кваліфікаційного аналізу.

«Єдині критерії безпеки інформаційних технологій» є результатом спільних зусиль авторів європейських «Критеріїв безпеки інформаційних технологій», «Федеральних критеріїв безпеки шформаційних технологій» і «Канадських критеріїв безпеки комп'ютерних систем», спрямованих на об'єднання

основних положень цих документів і створення єдиного міжнародного стандарту безпеки інформаційних технологій. Робота над цим наймасштабнішим в історії стандартів інформаційної безпеки проектом почалася в червні 1993 року з метою подолання концептуальних і технічних розбіжностей між указаними документами, їх узгодження і створення єдиного міжнародного стандарту. Перша версія «Єдиних критеріїв» була опублікована в січні 1996 р. Розробниками документа виступили США, Велика Британія, Канада, Франція і Нідерланди.

Розробка цього стандарту мала такі основні цілі:

о уніфікація національних стандартів у сфері оцінки безпеки ІТ;

о підвищення рівня довіри до оцінки безпеки ІТ;

о скорочення витрат на оцінку безпеки ІТ на основі взаємного визнання сертифікатів.

Нові критерії були покликані забезпечити взаємне визнання результатів стандартизованої оцінки безпеки на світовому ринку ІТ.

Розробка версії 1.0 критеріїв була завершена в січні 1996 року і схвалена ІСО (Міжнародна організація зі стандартизації) у квітні 1996 року. Був проведений ряд експериментальних оцінок на основі версії 1.0, а також організоване широке обговорення документа.

У травні 1998 року була опублікована версія 2.0 документа і на її основі в червні 1999 року був прийнятий міжнародний стандарт ІСО/МЕК 15408. Офіційний текст стандарту видано 1

грудня 1999 року. Зміни, внесені в стандарт на завершальній стадії його прийняття, враховані у версії 2.1, ідентичній початковій основі.

Єдині критерії узагальнили зміст і досвід використання «Оранжевої книги», розвинули рівні гарантованості європейських критеріїв, втілили в реальні структури концепцію профілів захисту «Федеральних критеріїв США».

У єдиних критеріях здійснено класифікацію широкого набору функціональних вимог і вимог довіри до безпеки, визначено структури їх групування і принципи цільового використання.

«Єдині критерії» розділяють вимоги безпеки на дві категорії: функціональні вимоги і вимоги адекватності.

Функціональні вимоги регламентують функціонування компонентів ІТ-продукту, що забезпечують безпеку, і визначають можливості засобів захисту. Функціональні вимоги представляються у вигляді складної, але добре опрацьованої формальної ієрархічної структури, що складається з класів, розбитих на розділи.

Адекватність являє собою характеристику ІТ-продукту, що показує, наскільки ефективно забезпечується заявлений рівень безпеки, а також ступінь коректності реалізації засобів захисту. Вимоги адекватності жорстко структуровані і регламентують усі етапи проектування, створення й експлуатації ІТ-продукту з погляду надійності роботи засобів захисту і їхньої адекватності функціональним вимогам, завданням захисту і загрозам безпеки.

Є сім стандартних рівнів адекватності, причому рівень вимог адекватності зростає від першого рівня до сьомого. Кожен рівень характеризується набором вимог адекватності, що регламентують застосування різних методів і технологій розробки, тестування, контролю і верифікації ІТ-продукту:

Рівень 1. Функціональне тестування.

Рівень 2. Структурне тестування.

Рівень 3. Методичне тестування і перевірка.

Рівень 4. Методична розробка, тестування й аналіз.

Рівень 5. Напівформальні методи розробки і тестування.

Рівень 6. Напівформальні методи верифікації розробки і тестування.

Рівень 7. Формальні методи верифікації розробки і тестування.

Таким чином, вимоги «Єдиних критеріїв» охоплюють практично всі аспекти безпеки ІТ-продуктів і технології їх створення, а також містять усі вихідні матеріали, необхідні споживачам і розробникам для формування профілів і проектів захисту. Крім того, стандарт є практично всеосяжною енциклопедією інформаційної безпеки, тому може використовуватися як довідник з безпеки інформаційних технологій.

Цей стандарт ознаменував собою новий рівень стандартизації інформаційних технологій, піднявши його на міждержавний рівень.

8.2 Державний стандарт України із захисту інформації

У 1997 р. Департаментом спеціальних телекомунікаційних систем та захисту інформації служби безпеки України була розроблена перша версія системи нормативних документів із технічного захисту інформації в комп'ютерних системах від НСД. Ця система включає чотири документи:

1.Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

2.Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

3.Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

4.Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.

Нормативний документ технічного захисту інформації (НД ТЗІ) «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу» визначає концепцію вирішення завдань захисту інформації в комп'ютерних системах і створення нормативних і методологічних документів, що регламентують питання:

- визначення вимог щодо захисту КС від несанкціонованого доступу;

- створення захищених КС і засобів їх захисту від несанкціонованого доступу;

- оцінки захищеності КС і їх придатності для вирішення завдань споживача.

Документ призначено для постачальників (розробників), споживачів (замовників, користувачів) КС, які використовуються для обробки (у тому числі збирання, збереження, передачі і т. п.) критичної інформації (інформації, що вимагає захисту), а також для державних органів, що здійснюють функції контролю за обробкою такої інформації.

Інформаційні ресурси держави або суспільства в цілому, а також окремих організацій і фізичних осіб являють собою певну цінність, мають відповідне матеріальне вираження і вимагають захисту від різноманітних за своєю сутністю впливів, які можуть призвести до зниження цінності інформаційних ресурсів.

Кінцевою метою всіх заходів щодо захисту інформації є забезпечення безпеки інформації під час її обробки в АС. Захист інформації повинен забезпечуватись на всіх стадіях життєвого циклу АС, на всіх технологічних етапах обробки інформації й в усіх режимах функціонування.

У випадку, якщо в АС планується обробка інформації, порядок обробки і захисту якої регламентується законами України або іншими нормативно-правовими актами (наприклад, інформація, що становить державну таємницю), для обробки такої інформації в цій АС необхідно мати дозвіл відповідного уповноваженого державного органу. Підставою для видачі такого дозволу є висновок експертизи АС, тобто перевірки відповідності реалізованої КСЗІ встановленим нормам.

Якщо порядок обробки і захисту інформації не регламентується законодавством, експертиза може виконуватись у необов'язковому порядку за поданням замовника (власника АС або інформації).

У процесі експертизи оцінюється КСЗІ АС у цілому. У тому числі виконується й оцінка реалізованих у КС засобів захисту. Засоби захисту від НСД, реалізовані в комп'ютерній системі, слід розглядати як підсистему захисту від НСД у складі КСЗІ. Характеристики фізичного середовища, персоналу, оброблюваної -інформації, організаційної підсистеми істотно впливають на вимога до функцій захисту, що реалізуються КС.

Як КС можуть виступати: ЕОМ загального призначення або персональна ЕОМ; операційна система; прикладна або інструментальна програма (пакет програм); локальна обчислювальна мережа, як сукупність апаратних засобів, ПЗ, що реалізує протоколи взаємодій, мережевої операційної системи і т. ін., ОС автоматизованої системи, яка реально функціонує, у найбільш загальному випадку - сама АС або її частина.

Далі викладається концепція забезпечення ЗІ. Визначаються поняття загрози інформації, політики безпеки, комплекс засобів захисту та об'єкти комп'ютерної системи, визначення несанкціонованого доступу і модель порушника.

Наступний документ присвячений класифікації автоматизованих систем і подає функціональні профілі захищеності оброблюваної інформації від НСД («Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу»).

У цьому документі за сукупністю характеристик АС (конфігурація апаратних засобів ОС і їх фізичне розміщення, кількість різноманітних категорій оброблюваної інформації, кількість користувачів і категорій користувачів) виділено три ієрархічні класи АС, вимоги до функціонального складу КЗЗ яких істотно відрізняються.

Клас «1» - одномашинний однокористувацький комплекс, який обробляє інформацію однієї або кількох категорій конфіденційності.

Істотні особливості: о у кожний момент часу з комплексом може працювати тільки один користувач, хоча у загальному випадку осіб, що мають доступ до комплексу, може бути декілька, але всі воші повинен мати однакові повноваження (права) щодо доступу до інформації, яка обробляється; о технічні засоби (носії інформації і засоби В/У) з точки зору захищеності належать до однієї категорії і всі можуть використовуватись для збереження і/або обробки всієї інформації.

Приклад: автономна персональна ЕОМ, доступ до якої контролюється з використанням організаційних заходів.

Клас «2» - локалізований багатомашинний багатокористувацький комплекс, який обробляє інформацію різних категорій конфіденційності.

Істотна відмінність від попереднього класу - наявність користувачів з різними повноваженнями щодо доступу та технічних засобів, які можуть одночасно здійснювати обробку інформації різних категорій конфіденційності.

Приклад: ЛОМ.

Клас «3» - розподілений багатомашинний багатокористувацький комплекс, який обробляє інформацію різних категорій конфіденційності.

Істотна відмінність від попереднього класу - необхідність передачі інформації через незахищене середовище або, у загальному випадку, наявність вузлів, що реалізують різну політику безпеки.

Приклад: глобальна мережа.

У межах кожного класу АС класифікуються на підставі вимог до забезпечення певних властивостей інформації. З точки зору безпеки інформація характеризується трьома властивостями: конфіденційністю, цілісністю і доступністю.

Перелік функціональних послуг безпеки та рівнів гарантій, їх структура і семантичне позначення наведені в НД ТЗІ «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу».

У документі «Термінологія в галузі захисту інформації в комп'ютерних системах від НСД» визначено та пояснено 128 основних найбільш поширених термінів, які подані українською, російською та англійською мовами.

ЛІТЕРАТУРА

І.Антонюк А.А., Волощук А.Г., Суслов В.Ю., Ткач А.В. Что такое Оранжевая книга? (Из истории компьютерной безопасности) // Безопасность информации. - №2. - 1996.

2.Антонюк А.А., Заславская Е.А., Лащевский В.И. Некоторые вопросы разработки политики безопасности информации // Защита информации: Сб. науч. тр. -К.: КМУГА, 1999. - 188 с.

3.Баричев С. Криптография без секретов. - М., 1998.

4.Галатенко В.А. Информационная безопасность: практический подход. -М.: Наука, 1998.-301 с.

5.Герасименко В.А. Защита иформации в автоматизированых системах обработки даных. - М.: Энергоатомиздат, 1994. - В 2-х томах.

6.Домарев В.В. Защита информации и безопасность компьютерных систем. - К.: Изд. «ДиаСофт», 1999. - 480 с.

7.Жельников В. Криптография от папируса до компьютера. - М.: ABF, 1996.-336 с.

8.Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. - НД ТЗІ 1.1-001-98, ДСТСЗІ СБ України, Київ, 1998.

9.Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. -НД ТЗІ 2.2.-002 -98, ДСТСЗІ СБ України, Київ, 1998.

10.Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. - НД ТЗІ 2.2-001-98, ДСТСЗІ СБ України, Київ, 1998.

11. Корченко А.Г. Несанкционированный доступ в компьютерные системы и методы защиты. -Киев: КМУГА, 1998.

12. http://www.infobezpeka.com/publications/?id=92

13. http://www.bestreferat.ru/referat-143075.html

Дмитро Борисович Охота,
спеціаліст системотехнік, магістрант
інформаційних технологій

ТЕХНОЛОГІЇ КОМП'ЮТЕРНОЇ БЕЗПЕКИ

КНИГА1

ІН 11М

Комп'ютерний набір, верстка і макетування та дизайн в редакторі Microsoft® Office® Word 2003 Д.Б. Охота. Науковий керівник Р. М. Літнарович, доцент, кандидат технічних наук

Міжнародний Економіко-Гуманітарний Університет ім. акад. Степана Дем'янчука

Кафедра математичного моделювання
33027,м.Рівне,Україна
Вул.акад. С.Дем'янчука,4, корпус 1
Телефон:(+00380) 362 23-73-09
Факс:(+00380) 362 23-01-86
E-mail:mail@regi.rovno.ua
E-mail:__dima__90__@mail.ru