Міністерство освіти України
Тернопільська академія народного господарства
Національна Академія Наук України
Інститут кібернетики імені В.М.Глушкова

В.К.Задірака
О.С.Олексюк
М.О.Недашковський

МЕТОДИ ЗАХИСТУ БАНКІВСЬКОЇ ІНФОРМАЦІЇ

Навчальний посібник

Рекомендовано Міністерством освіти України

Київ -"Вища школа"

1999

УДК 621.391.7 : 336.71 (075.8)
ББК 65.050.9(2) я73
3-15

Рецензенти:
Корнійчук М. Т., д-р техн. наук, голов. наук. співроб. Київського міжнародного університету цивільної авіації;
Хлобистов В. В., д-р фіз.-мат. наук, голов. наук. співроб. ф-ту кібернетики Київського національного університету ім. Тараса Шевченка

Редакція літератури з історії, права, економіки
Редактор *В.В.Півень*

Методи захисту банківської інформації: Навчальний посібник / В.К.Задірака, О.С. Олексюк, М.О.Недашковський. – К.: Вища шк., 1999, - 261 с.

ISBN 5-11-004777-4

Викладено методи сучасної криптографії та застосування їх до проектування безпечних електронних банківських систем. Висвітлено найактуальніші сучасні проблеми: методи симетричної та асиметричної криптографії, криптографічні протоколи, методи цифрового підпису, методологія захисту автоматизованих систем обробки інформації, електронні платежі, програмні та апаратні засоби для автоматизації банківських систем, методи захисту комерційної таємниці.

Для студентів та спеціалістів у галузі безпеки інформації, автоматизації банківських операцій, адміністраторів безпеки обчислювальних систем, а також студентів економічних спеціальностей, які вивчають дисципліни: “Основи захисту інформації”, “Захист інформації в комп’ютерних системах та мережах”, “Інформаційна безпека бізнесу”, “Захист інтелектуальної власності” тощо.

ББК 65.050.9(2) я73

ISBN 5-11-004777-4

ЗМІСТ

СПИСОК СКОРОЧЕНЬ

АКА – автоматичний касовий апарат
АСОД – автоматизована система обробки даних
АСОІ – автоматизована система обробки інформації
АНБ – Агентство національної безпеки
АР – аналіз ризику
АРМ – автоматизоване робоче місце
Атаки:
“В” – “вірус”
“ЖП” – “жадібні програми”
“ЗП” – “загарбники паролів”
“ЗС” – “збирання сміття”
“Л” – “люк”
“М” – “маскарад”
НСД – несанкціонований доступ
“ПК” – “приховані канали”
“С” – “салямі”
“ТК” – “троянський кінь”
“Ч” – “черв’як”
“ШП” – “шкідливі програми”
АТС – автоматизована електронна станція
ВПБ – виборча політика безпеки
ВУД – виборче управління доступом
ГК – головний ключ
ГПВЧ – генератор псевдовипадкових чисел
ГР – гарячий резерв
ДК – дебітова картка
ДОБ – достовірча обчислювальна база
ЕБС – електронна банківська система
ЕОМ – електронна обчислювальна машина
ЕП – електронні платежі
ЕПД – електронні платіжні документи
ЗАЗ – засекречена апаратура зв’язку
ЗМІ – засоби масової інформації
ІК – інтелектуальна картка
КК – кредитна картка
КАП – код автентифікації повідомлень
КЦ – контроль цілісності КД – контроль доступу
ЛОМ – локальна обчислювальна мережа
МД – матриця доступу
НВІС – надвелика інтегральна схема
НБУ – національний банк України
ОЕД – обмін електронними документами
“ОК” – “Оранжева книга”
ОС – операційна система
ПБ – політика безпеки
ПВЧ – псевдовипадкові числа
ПЕОМ – персональна електронно-обчислювальна машина
ППБ – повноважна політика безпеки
ТЗППІ – технічні засоби переробки та передачі інформації
ЦРК – центр розповсюдження ключів
ЯБ – ядро безпеки
Capstone – підсистема SCIPJACK
Clipper – підсистема SKIPJACK
DES – Data Encryption Algorythm – криптосистема з секретним ключем
DSA – Digital Signature Algorythm – алгоритм цифрового підпису
MAA – Message Autentification Algorythm – стандарт для захисту цілісності даних
MAC – Message Autentification Code – код перевірки достовірності даних
MASTER CARD – кредитна картка
PC - персональний комп’ютер
PIN – персональний ідентифікаційний номер
POS – розрахунок в точці продажу
RSA – (Rivest, Shamir, Adleman)– криптосистема з відкритими ключами
SKIPJACK – криптосистема з секретним ключем
SWIFT – (The Society for Worldwide inter-bank Financial Telecomunication) – система електронних платежів
VISA – кредитна картка

ВІД АВТОРІВ

Ялтинська конференція. Рузвельт написав записку і передав її Черчілю. Черчіль прочитав і спалив. Потім написав у відповідь записку Рузвельту. Той прочитав, розірвав її на дрібні клаптики і викинув у корзинку.

Сталін дав вказівку з'ясувати, що було в записках. Кращі дешифрувальщики бились кілька місяців, відновлюючи їх за попелом та уривками речень. Нарешті текст записки Черчіля було відновлено повністю: "Не хвилюйтесь. Старий яструб не випаде з гнізда." Проте розшифрувати цю фразу так і не вдалось. Сталіну не давали спокою ці слова до кінця війни. Пізніше він розповів про них Хрущову. Через кілька років Хрущов поїхав до Великої Британії, зустрівся з Черчілем, запитав про записки, якими вони з Рузвельтом обмінялися під час Ялтинської конференції.

— *Ми довго бились над нею і не змогли її розшифрувати. Може, ви розкриєте зміст цієї фрази? Справа давня.*

— *У мене тоді розстібнулись гудзики на штанях. Пан Рузвельт попередив мене, а я його заспокоїв.*

(Фольклор)

До 70-х років XX ст. суспільство мало розумілося в криптографії. Була відома лише класична (симетрична) криптографія. Кількість робіт з цієї тематики була досить скромною. Більшості людей було відомо, що військові та розвідувальні організації користуються для зв'язку спеціальними кодами або кодуючою апаратурою, але лише деякі мали поняття про криптографію.

У другій половині 70-х років ситуація різко змінилась. По-перше, з розвитком мереж зв'язку і широким використанням ЕОМ необхідність у криптографічному захисті даних стали усвідомлювати все ширші прошарки суспільства. По-друге, винахід американців У. Діффі і М. Е. Хеллмана – криптографії з відкритим ключем – створив сприятливий грунт для задоволення комерційних потреб у секретності, усунувши такий суттєвий недолік класичної криптографії, як складність розповсюдження ключів.

Водночас зріс інтерес до математичних аспектів криптографії. Криптографічні алгоритми нерідко грунтувалися на математичних методах і тому були цікавими для математиків. Створення і відгадування криптографічних алгоритмів вважалось випробуванням інтелектуальних здібностей. Однак попит на спеціальні знання в галузі криптографії був обмеженим.

В Україні попит на методи і засоби захисту інформації почав виявлятись у другій половині 80-х років.

Кілька років тому виникла нагальна потреба використання криптографічних методів у приватному секторі. Сьогодні велика кількість конфіденційної інформації передається між ЕОМ звичайними лініями зв'язку. Тому потрібні спеціалісти, які володіють криптологічними методами, знають відповідні стандарти, здатні використовувати (або розробляти) програмне й апаратне забезпечення для гарантування таємності та цілісності закритої інформації.

Питання підготовки відповідних спеціалістів в Україні стоїть на сьогодні досить гостро. Навчальної літератури з цієї проблематики немає. Водночас до навчальних планів вищих закладів освіти широко вводяться відповідні курси.

Маємо надію, що посібник приверне увагу студентів і спеціалістів до нової дисципліни, яка за рубежем бурхливо розвивається і повинна стати доступною для вітчизняних спеціалістів з математичних методів підтримки безпеки та конфіденційності комп'ютерного спілкування і комунікацій у комп'ютерних мережах (зокрема захист інформаційних потоків у банківських системах).

Комп'ютерні системи – один з найвразливіших компонентів сучасних банків та фінансових організацій, які приваблюють зловмисників і тому потребують захисту.

Як захищати свої системи? Від кого? Скільки це коштуватиме? До яких заходів треба вдатися в критичних ситуаціях? На ці та багато інших запитань дає відповідь даний навчальний посібник. У ньому також висвітлюються елементи сучасної криптології та проблеми автоматизації банківських розрахунків.

Посібник підготовлено на основі курсу лекцій, прочитаних в Інституті банківського бізнесу Тернопільської академії народного господарства впродовж 1996-1998 р. З 1998 р. відповідний курс читають у Київському національному університеті імені Тараса Шевченка. Слід зазначити, що в Україні в цьому напрямі робляться лише перші кроки, в той час, як в розвинених країнах курс з основ захисту інформації вже давно викладають і він посів своє місце у прикладній математичній освіті.

Автори прагнули зробити посібник доступним для якомога ширшого читацького кола. З цією метою матеріал подано в оглядовому вигляді. Сподіваємося, що кожен лектор отримає достатньо матеріалу для компонування власного курсу лекцій.

Матеріал, викладений в посібнику, грунтується на роботах з основного та додаткового списку літератури.

Посібник підготував авторський колектив Інституту кібернетики ім. В. М. Глушкова НАН України та Тернопільської академії народного господарства Міноствіти України. Окремі розділи та параграфи написали:

- Задірака В.К. – від авторів; передмова; список скорочень; розділ 1; розділ 2, §2.1.; короткий словник термінів безпеки інформації; список літератури;
- Олексюк О.С. – розділ 2, §2.2, §2.3, §2.4; розділ 3, §3.2, §3.3; додатки до 3-го розділу;
- Недашковський М.О. – розділ 3, §3.1.

Автори висловлюють щиру подяку В.Л.Задіраці і Н.С.Добровольській за технічну допомогу в оформленні рукопису.

Відгуки та пропозиції щодо навчального посібника надсилайте за адресою: 252680, Київ-187, ГСП, Проспект Глушкова 40, Інститут кібернетики ім.В.М.Глушкова НАНУ.

Київ – Тернопіль
1999 р.

Автори

ПЕРЕДМОВА

Невіглас зневажає науку, неосвічені
люди захоплюються нею, тоді коли
мудреці користуються нею.

(Френсіс Бекон)

Термін “криптологія” походить від грецьких коренів, що означають “таємний” і “слово”, і використовується для означення всієї області таємного зв’язку.

Криптологія поділяється на дві частини: *криптографію* (шифрування) та *криптоаналіз*. Криптографи прагнуть знайти методи забезпечення таємності та (чи) автентичності (істинності) повідомлень, а криптоаналітики – виконати обернену задачу, розкриваючи шифр або підроблюючи кодовані сигнали так, щоб вони були прийняті як справжні.

Початкове повідомлення, до якого криптограф застосовує своє мистецтво, зветься відкритим текстом, а результат його роботи – шифрованим текстом, або криптограмою. Для управління процесом шифрування криптограф завжди використовує таємний ключ. Часто (але не завжди) він передає його яким-небудь надійним способом (наприклад, у дипломаті, прикріпленому наручниками до руки кур’єра) людині (або машині), якій він пізніше має надіслати криптограму, виготовлену за допомогою цього ключа.

Майже загальноприйняте припущення у криптографії полягає в тому, що криптоаналітики зловмисника мають повний текст криптограми. Крім того, криптограф майже завжди користується правилом: стійкість шифру цілком залежить від таємності ключа. Інакше кажучи, весь механізм шифрування, крім значення таємного ключа, відомий криптоаналітику зловмисника. Якщо криптограф виходить лише з цих двох припущень, він розробляє систему, стійку при аналізі на основі лише шифрованого тексту. Якщо до того ж криптограф припускає, що криптоаналітики зловмисника можуть дістати (тим чи іншим шляхом) кілька уривків відкритого тексту і відповідних йому шифрованих текстів, виготовлених за допомогою таємного ключа, то розробляється система, стійка при аналізі на основі відкритого тексту.

Упродовж тисячоліть криптографія використовувалася для захисту військового та дипломатичного зв’язку. Однак з початком інформаційної епохи виникла нагальна потреба використання її в приватному секторі. Сьогодні багато конфіденційної інформації (історії хвороб, юридичні документи, дані фінансових договорів) передається між ЕОМ звичайними лініями зв’язку. Проблемами забезпечення таємності та достовірності такої інформації займаються висококваліфіковані фахівці.

Навіть у приватному секторі криптоаналіз може відігравати значну роль. ”Дружній криптоаналітик” може знайти непередбачені вразливі місця шифрів, що дає можливість виправити їх або відмовитись від їх використання. Яскравий приклад – розкриття американцем А.Шаміром криптосистеми Р.Меркля-М.Е.Хеллмена з відкритими ключами, що засновувалась на задачі про укладку ранця. Тим самим Шамір попередив вірогідне практичне застосування цього зручного шифру, а водночас і можливий успіх криптоаналітиків.

Період до 1949 р. можна по праву назвати ерою донаукової криптології. Криптологію тих часів слід розглядати швидше як мистецтво, а не як науку. Більш як 2000 років тому Юлій Цезар писав Цицерону та іншим друзям до Риму, використовуючи шифр, у якому кожна буква відкритого тексту замінювалась третьою за ліком (циклічно) буквою латинського алфавіту. Сьогодні ми б описали шифр Цезаря рівнянням

$$Y = X \oplus Z \ , \qquad (1)$$

де Y – буква шифртексту; X – буква відкритого тексту; Z – таємний ключ (обраний Цезарем ключ дорівнював числу 3); $\oplus$ означає додавання за модулем 26 ($23 \oplus 3=0$, $23 \oplus 4=1$ тощо).

Сьогодні будь-який школяр, який хоч трохи знайомий з латиною та має уявлення про прийоми криптоаналізу, розгадає цей шифр, маючи лише кілька речень шифрованого тексту. Дійсно, лише впродовж двох тисячоліть після Цезаря криптоаналітики мали явну перевагу над криптографами. Нарешті 1926 р. Г.Вернам, інженер Американської телефонної та телеграфної компанії надрукував шифр, призначений для використання з двійковим кодом Бодо. Шифр Вернама подібний до шифру Цезаря: він описується рівнянням (1), а $\oplus$ означає додавання за модулем 2 ($0 \oplus 0=0$, $0 \oplus 1=1$, $1 \oplus 1=0$). Нова ідея, висунута Вернамом, полягала в тому, щоб використовувати ключ лише один раз. При цьому кожен біт шифрується з використанням нового випадкового біта ключа. Це потребує передачі таємним каналом ключа, об'єм якого дорівнює об'єму тексту, що шифрується. Однак це дає можливість, як ми побачимо далі, створювати дійсно стійкий шифр. Вернам і насправді вважав свій шифр стійким і знав, що ця властивість губиться при повторному використанні бітів ключа, але він це не довів. Ми називаємо період до 1949 р. ерою донаукової криптології ще й тому, що досягнення тих часів засновані на інтуїції та "вірі", які не підкріплені доказами. Наприклад, у криптологічних службах Великої Британії лише з початком другої світової війни зрозуміли, що математики можуть зробити внесок у розвиток криптології.

Публікація 1949 р. статті Н.Е.Шеннона "Теорія зв'язку в таємних системах" розпочала нову еру наукової криптології з таємними ключами. Шеннон розробив теорію систем таємного зв'язку. Він не тільки довів неможливість розкриття таємного ключа Вернама, а й розробив чіткі межі об'єму таємного ключа, який передається захищеним каналом уявному одержувачеві.

Справжнім вибухом стала поява 1976 р. статті американців У.Діффі і М.Е.Хеллмана "Нові напрями в криптографії". Автори вперше показали, що таємний зв'язок можливий без будь-якої передачі таємного ключа між відправником та одержувачем. Це був початок нової епохи з відкритими ключами, що триває і сьогодні.

РОЗДІЛ 1

ЕЛЕМЕНТИ КРИПТОЛОГІЇ

Помилятися людині властиво, але цілковито
все заплутати може тільки комп'ютер.

(5-й закон ненадійності)

1.1. Шифри з таємними ключами

Криптосистемою з таємними ключами називають систему, що відповідає схемі, наведеній на рис.1:

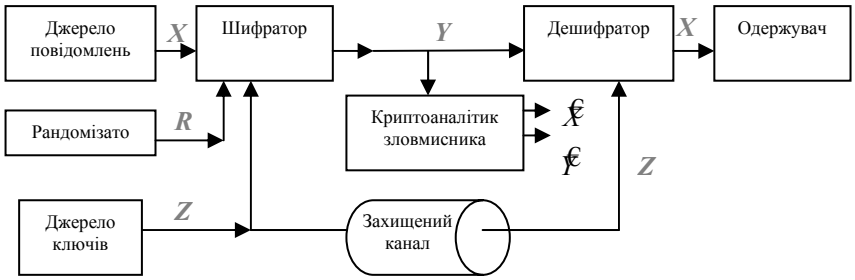

Рис.1. Схема криптосистеми з таємними ключами

Важлива складова таких систем – "захищений канал", яким таємний ключ $Z = [Z_1, Z_2, ..., Z_n]$, створений у джерелі ключа і захищений від "допитливих очей" криптоаналітика, передається уявному одержувачу. Для того щоб підкреслити факт використання одного і того ж ключа в шифраторі та дешифраторі одержувача повідомлень, криптосистеми з таємними ключами називають ***одноключовими*** або ***симетричними*** системами. Знаки ключа – це символи деякого кінцевого алфавіту, в ролі якого ми будемо часто використовувати алфавіт $\{0,1\}$. Джерело повідомлень створює відкритий текст $X = [X_1, X_2, ..., X_M]$, а рандомізатор – рандомізуючу послідовність $R = [R_1, R_2, ..., R_J]$. Шифратор створює криптограми $Y = [Y_1, Y_2, ..., Y_N]$ як функцію *X, R, Z.* Для того щоб підкреслити, що криптограма Y є функцією лише відкритого тексту X, конкретний вигляд якої визначається таємним ключем Z і рандомізуючою послідовністю R, запишемо це перетворення у вигляді:

$$Y = E_{ZR}(X). \tag{2}$$

Як видно з рис.1 дешифратор у змозі також виконати зворотне перетворення без знання рандомізуючої послідовності. Отже, запис

$$X = D_Z(Y) \tag{3}$$

виражає той факт, що відкритий текст X є функцією криптограми Y, конкретний вигляд якої визначається лише таємним ключем Z.

Криптоаналітики зловмисника спостерігають лише криптограму Y і роблять оцінку $\hat{X}$ відкритого тексту та (або) оцінку $\hat{Z}$ таємного ключа. Ми припускаємо, що криптоаналітику відомі всі деталі процесу шифрування та розшифрування, крім X, R і особливо Z.

Рандомізація – давно відомий прийом шифрування. В англійській мові літера "е" зустрічається набагато частіше, ніж інші літери. Англійський текст можна перетворити на такий, що містить символи більшого алфавіту, заміною літери "е" випадковими символами, які вибираються з "е-групи" символів більшого алфавіту, а також заміни інших англійських літер, які часто зустрічаються, випадковими символами, які вибираються з груп відповідних літер. В отриманому тексті всі символи більшого алфавіту зустрічаються з приблизно однаковою частотою. Шифрування такого рандомізованого тексту зводить нанівець спроби розкрити на основі

аналізу частот окремих символів. Однак після розшифрування законний адресат може зняти рандомізацію замінивши лише кожен символ з “е-групи” літерою “е” тощо, (йому не потрібно заздалегідь повідомляти, які саме випадкові заміни будуть зроблені). Такі рандомізовані шифри називають також **“*шифрами з багаторазовою підстановкою*”**, або **“*рівночастотними шифрами*”**.

Ми будемо вважати, що *X*, *Z* та *R* статистично незалежні.

1.1.1. Теоретична і практична стійкість

Шеннон розглядав проблему стійкості криптографічних систем з двох протилежних точок зору. Спочатку він поставив питання про ***теоретичну стійкість***: ”Наскільки надійна система, якщо криптоаналітик противника не обмежений у часі та володіє всіма необхідними засобами для аналізу криптограм?”. Висновок такий: об’єм секретного ключа для побудови теоретично стійкого шифру неприпустимо великий для більшості випадків. Тому Шеннон розглядав також питання про ***практичну стійкість***: “Чи надійна система, якщо в розпорядженні криптоаналітика обмежений час та обчислювальні можливості для аналізу перехоплених криптограм?” Системи з відкритими ключами, які розглядаються далі, повинні мати практичну стійкість, але не можуть забезпечити теоретичну стійкість.

1.1.2. Цілковита секретність

Перше припущення Шеннона щодо теоретичної стійкості виходить з того, що секретний ключ використовується тільки один раз, тобто після шифрування *M* знаків відкритого тексту потрібно замінити секретний ключ *Z* та рандомізатор *R.* Друге припущення засновується на тому, що криптоаналітику підсильна тільки криптограма *Y*, і тому він може зробити лише аналіз на основі шифртексту. Цілковита секретність, за визначенням Шеннона, означає, що відкритий текст *X* і криптограма *Y* статистично незалежні, тобто $P(X = x; Y = y) = P(X = x)$ для всіх можливих відкритих текстів $X = (X_1, ..., X_M)$ і криптограм *Y.*

Шеннон довів, що для того щоб система була цілковито секретною, ключ не повинен бути коротшим за відкритий текст $(K \geq M)$; нижня межа досягається в шифрі Вернама, коли довжина ключа дорівнює довжині відкритого тексту.

Система Вернама широко відома як шифр блокнот, яким користувалися розвідники деяких країн під час другої світової війни. Розвідникам видавався блокнот з випадковим секретним ключем, який міг бути використаний для шифрування лише одного повідомлення. У криптологічних колах, мабуть, були переконані в неможливості розкриття такого шифру, однак доведення цього факту вперше було зроблено Шенноном.

1.1.3. Достовірність і обман

Раніше вже наголошувалося на тому, що метою криптографії є забезпечення секретності та автентичності повідомлень. Чи можна, отримавши криптограму, розшифрувавши її та встановивши правильний відкритий текст, бути впевненим у тому, що вона надіслана саме “дружньою” стороною, а не ще кимось, хто має секретний ключ? Відповідь у загальному випадку буде негативною. Систематичне вивчення проблем автентифікації проведено американцем Г.Сімонсом, який створив теорію автентифікації, схожу в багатьох відношеннях з теорією секретного зв’язку Шеннона.

Для того щоб розглянути питання про теоретичну стійкість автентифікації в постановці Сімонса, криптоаналітик повинен знаходитись у більш вигідних умовах, ніж ті, що показані на рис.1. Ці зміни проілюстровано на рис.2.

Рис.2. Зміни до рис.1 для аналізу порушень автентичності

Тепер криптоаналітик створює підроблену криптограму $\hat{Y}$ і надсилає її у дешифратор одержувача. Така фальшива криптограма може бути розпізнана, при цьому отриманий з неї фальшивий відкритий текст $\hat{X}$ не надійде до одержувача. Через це зв'язок між дешифратором і одержувачем на рис.2 показано пунктиром.

Сімонс, як і Шеннон, припускав, що секретний ключ Z використовується тільки один раз для утворення однієї автентичної криптограми Y. Проте при цьому він усвідомлював, що в цьому разі криптоаналітик може вдатися до двох зовсім різних дій. Він може спробувати створити підроблену криптограму $\hat{Y}$, не дочекавшись справжньої криптограми Y (спроба імітації). Саме тому зв'язок між шифратором джерела повідомлень і криптоаналітиком показано на рис.2 пунктиром. Спроба імітації вважається успішною, коли дешифратор адресата прийме $\hat{Y}$ як справжню криптограму (навіть, коли пізніше з'ясується, що $\hat{Y}$ збігається з Y). Криптоаналітик може також створити після надходження Y (спроба підміни). Така спроба вважається успішною, якщо дешифратор одержувача прийме $\hat{Y}$ за оригінальну криптограму, і до того ж $\hat{Y}$ буде розшифровано в $\hat{X} \neq X$.

1.1.4. Розсіювання і перемішування

Шеннон виділив два загальних принципи, які використовують у практичних шифрах: розсіювання та перемішування. ***Розсіюванням*** він назвав поширення впливу одного знака відкритого тексту на багато знаків шифртексту, що дає можливість приховати статистичні властивості відкритого тексту. Розвитком цього принципу є поширення впливу одного знака ключа на багато знаків шифртексту, що запобігає відновленню ключа частинами. Перемішування, за Шенноном, — це використання таких шифруючих перетворень, які ускладнюють відновлення взаємозв'язку статистичних властивостей відкритого і шифрованого текстів. Однак шифр має не тільки ускладнювати розкриття, а й забезпечувати легкість шифрування та розшифрування (у разі, якщо відомий секретний ключ). Так, поширений спосіб розсіювання та перемішування полягає у використанні складеного шифру, тобто такого, що може бути реалізований у вигляді деякої послідовності простих шифрів, кожен з яких робить невеликий внесок у велике сумарне розсіювання і перемішування.

У складених шифрах як прості найчастіше використовуються звичайні підстановки і перестановки. При перестановці просто перемішують символи відкритого тексту, причому конкретний вид перемішування визначає секретний ключ.

Розподіл частот окремих символів у зашифрованому тексті такий самий, що й у відкритому тексті, однак розподіл більш високих порядків виявляється перемішаним. При підстановці кожен символ відкритого тексту замінюють іншим символом того ж алфавіту, а конкретний вид перестановки визначає секретний ключ. Розподіл частот окремих символів у відкритому тексті зберігається незмінним і у шифртексті. У шифрі Цезаря використовується звичайна підстановка з 26 можливими значеннями секретного ключа. Проте, якщо підстановка робиться в дуже великому алфавіті, а ймовірність повторення кожного символу відкритого тексту під час використання одного ключа мала, то статистичні властивості шифртексту дають мало інформації

криптоаналітику, і такий шифр стає дуже добрим. Криптограф досягає цього, застосовуючи підстановку до “окремих символів”, які містять кілька символів з алфавіту вихідного відкритого тексту. При багаторазовому чередуванні простих підстановок і перестановок можна отримати дуже стійкий шифр (криптоалгоритм) з гарним розсіюванням і перемішуванням.

1.1.5. Стандарт шифрування даних (DES)

DES – це один з найкращих прикладів криптоалгоритму, розробленого відповідно до принципів розсіювання та перемішування. У ньому відкритий текст X, криптограма Y та *ключ* Z — двійкові послідовності, $M = N = 64$ та $K = 56$. У загальному випадку допустимі всі 2^{64} можливих значень X. Оскільки $M = N = 64$, то DES є підстановкою, хоча і в дуже великому алфавіті, який містить $2^{64} \approx 10^{19}$ символів! При використанні криптоалгоритму DES у режимі, який називається електронною кодовою книгою, послідовні 64-бітові “блоки” відкритого тексту шифруються з використанням одного ключа, але незалежно. Будь-який шифр, що використовується у такий спосіб, називається ***блочним шифром.***

Криптоалгоритм DES є суперпозицією шифрів, яка складається з 16 послідовних “циклів”, у кожному з яких досить прості перестановки поєднуються з підстановками в 4-бітових групах. У кожному “проході” використовується лише 48-біт ключа, однак вони вибираються з повного 56-бітового ключа.

Алгоритм DES був розроблений фірмою IBM в 1974 р. Одна з вимог полягала в можливості публікації алгоритму без втрати його стійкості.

Діффі і Хеллман опублікували проект спеціалізованої багатопроцесорної обчислювальної машини, вартість якої (за їхніми підрахунками) становила близько 20 млн дол., що могла б розкрити DES шляхом повного перебору приблизно за 12 год. Пізніше Хеллман запропонував інший варіант машини вартістю близько 4 млн дол., яка після одного року попередніх обчислень могла б розкривати 100 криптограм впродовж однієї доби.

У наш час у США діє інший стандарт — SKIPJACH. Не слід, однак, забувати, що розмір секретного ключа можна збільшити, шифруючи багаторазово з різними ключами, тобто застосовуючи суперпозицію шифрів, утворених з DES.

1.2. Шифри з відкритими ключами

1.2.1. Одностороння функція

З робіт Шеннона випливає, по-перше, що в теоретично стійких секретних системах потрібно передавати захищеними каналами ключі неприпустимо великого об’єму. По-друге, вирішення питань практичної стійкості сприяло скоріше вдосконаленню відомих криптографічних методів, ніж появі нових. Однак зауваження Шеннона про те, що “проблема створення доброго шифру є проблемою знаходження найбільш складних задач, що задовольняють певні умови, можна скласти наш шифр так, щоб розкриття його було еквівалентне (або містило б в собі) вирішенню деякої проблеми, про яку відомо, що для її вирішення потрібний великий обсяг робіт”, знайшло відгук у плідних роздумах Діффі та Хеллмана. Їхня відома стаття 1976 р. містила приголомшливе повідомлення про те, що можлива побудова практично стійких секретних систем, які зовсім не потребують передавання секретного ключа.

Розглянемо два визначення: “одностороння функція” та “одностороння функція з потаємним ходом”.

Одностороння функція – це деяка функція f така, що для довільного x з її області визначення $f(x)$ легко обчислюється; однак практично для всіх y з її області значень знаходження x, для якого $y = f(x)$, обчислювально нездійсненне. Це визначення, проте, не є математично точним.

Одностороння функція з потаємним ходом — це множина оборотних функцій f з параметром Z, таких, що при даному Z можна знайти алгоритми E_Z і D_Z, які дають можливість легко обчислити відповідно $f_Z(x)$ для всіх x з області визначення і $f_Z^{-1}(y)$ для всіх y з області значень, однак практично для всіх Z і практично для всіх y з області значень f_Z знаходження $f_Z^{-1}(y)$ обчислювально нездійсненне навіть при відомому E_Z. Це визначення також не є математично точним, але воно широко використовується в криптографії.

1.2.2. Відкрите розповсюдження ключів

Як одну з можливих односторонніх функцій Діффі і Хеллман запропонували функцію дискретного піднесення до степеня

$$f(x) = a^x \pmod p, \tag{4}$$

де x – ціле число від 1 до (p-1) включно; обчислення провадяться за модулем p, де p – велике просте число; a – ціле число ($1 \le a \le p$), степені якого $a, a^2, ..., a^{p-1}$ дорівнюють (у деякому порядку) 1, 2, …, p-1. Наприклад, при p=7 можна вибрати a=3, оскільки a=3, $a^2 = 2$, $a^3 = 6$, $a^4 = 4$, $a^5 = 5$, $a^6 = 1$ (в алгебрі таке "a" називають примітивним елементом скінченого поля $GF(p)$ і відомо, що такі "a" завжди існують).

Якщо $y = a^x$, то природно записати:

$$x = \log_a(y) \ , \tag{5}$$

а задачу обернення $f(x)$ назвати задачею знаходження дискретних логарифмів. Навіть при дуже великих p, наприклад, $p \sim 2^{1000}$ можна легко обчислити $f(x)$ піднесенням до квадрату та множенням. Наприклад, для того щоб обчислити $a^{53} = a^{32+16+4+1}$ потрібно спочатку знайти a^2, $a^4 = (a^2)^2$, $a^8 = (a^4)^2$, $a^{16} = (a^8)^2$ і $a^{32} = (a^{16})^2$; для цього потрібно 5 операцій множення. Далі слід помножити a^{32} послідовно на a^{16}, a^4 і a, що потребує ще трьох операцій. Отже, результат дістають за вісім операцій (за модулем p). Навіть при $p \sim 2^{1000}$ обчислення $f(x)$ для довільного цілого числа x потрібно менше ніж 2000 операцій множення (за модулем p).

Якщо функція дискретного піднесення до степеня дійсно одностороння, то обчислення $\log_x y$ має бути нездійсненним практично для всіх y $(1 \le y < p)$. Невдовзі М.Е.Хеллман і С.Поліг з'ясували, що дискретні логарифми складно обчислити за умови, коли не тільки p велике, але і $p-1$ має великий простий множник (найкраще всього, якщо це друге просте число, помножене на 2). За цієї додаткової умови кращі відомі алгоритми для знаходження дискретних логарифмів потребують приблизно $\sqrt{p}$ множень (за модулем p) у порівнянні з приблизно $2\log_2 p$ множень при дискретному піднесенні до степеня. Якщо складність обчислення функції дискретних логарифмів дійсно така, то при зазначеному обмеженні на $p-1$ функція дискретного піднесення до степеня є односторонньою, але точно це не доведено.

Діффі і Хеллман запропонували простий метод використання дискретних логарифмів для обміну секретними ключами між користувачами мережі з використанням лише відкритих повідомлень. Припустімо,

що всім користувачам відомі a і p. Кожен користувач, скажімо, користувач i, випадково вибирає ціле число x_i, яке знаходиться між 1 і $p-1$, і тримає його в секреті. Далі він обчислює y_i:

$$y_i = a^{x_i} (\mathrm{mod}\, p). \tag{6}$$

Користувач не тримає y_i в секреті, а розміщує його в завірений відкритий довідник, доступний для всіх користувачів. Надалі, якщо користувачі i та j побажають встановити секретний зв'язок, користувач i візьме із довідника y_j і з допомогою свого секретного x_i обчислить Z_{ij}:

$$Z_{ij} = (y_j)^{x_i} = (a^{x_j})^{x_i} = a^{x_j x_i} (\mathrm{mod}\, p). \tag{7}$$

У такий самий спосіб і користувач j обчислить Z_{ji}. Однак $Z_{ij} = Z_{ji}$ і користувачі i та j можуть з цього моменту використовувати Z_{ij} як секретний ключ у класичній криптосистемі. Якщо зловмисник зміг би розв'язати задачу обчислення дискретних логарифмів, то зміг би за відомими з довідника y_i і y_j розв'язати рівняння $x_i = \log_a y_i$ і обчислити Z_{ij}, як і користувач i. Видимо, зловмисник не може визначити Z_{ij} іншим шляхом (хоч це і не доведено). Схема, яку ми описали, дістала назву ***системи відкритого розповсюдження ключів Діффі і Хеллмана***. Це перша система, яка дає можливість відмовитися від передачі секретних ключів. На сьогодні її вважають однією з найстійкіших і найзручніших систем з відкритими ключами.

Зазначимо, що описана система відкритого розповсюдження ключів дає змогу обійтися без захищеного каналу для передачі секретних ключів, але не відміняє необхідності автентифікації. Держатель загальнодоступного довідника повинен бути впевненим, що несекретне y_i помістив у довіднику саме користувач i, а користувач i — мати впевненість, що y_j надіслав йому саме держатель довідника. Не треба забувати і про те, що у системах із секретними ключами користувач повинен бути впевненим не тільки в тому, що ключ Z зберігався в секреті під час передавання, а й у тому, що він надісланий вірним відправником. Методи з відкритими ключами усувають одну з цих проблем. Вони не створюють нової задачі автентифікації, а, скоріше, акцентують на необхідне її розв′язання.

1.2.3. Криптосистеми RSA та Ель-Гамаля

Грунтуючись на визначенні односторонньої функції з потаємним ходом, Діффі і Хеллман запропонували структуру криптосистеми з відкритими ключами для мережі з багатьма користувачами. Кожен користувач i випадково вибирає значення Z_i показника і тримає його в секреті. Далі він формує алгоритм E_{Z_i} і розміщує його у відкритому довіднику. Він також формує алгоритм D_{Z_i} і тримає його в секреті. Якщо користувач j хоче послати секретне повідомлення X користувачу i, він бере з довідника алгоритм E_{Z_i} і використовує його для отримання криптограми $y = f_{Z_i}(X)$, яку надсилає користувачу i. Користувач i використовує свій секретний алгоритм D_{Z_i} для обчислення $f_{Z_i}^{-1}(y) = X$. Якщо f_Z дійсно є односторонньою функцією, то ця криптосистема забезпечує безумовну практичну стійкість.

Діффі і Хеллман зазначали, що якщо при всіх показниках Z область визначення функції f_Z збігається з її областю значень, то з допомогою такої односторонньої функції можна отримати цифрові підписи. Якщо користувач i хоче надіслати несекретне повідомлення X (будь-якому користувачу мережі або всім одночасно) і "підписати" його так, щоб у одержувача була можливість безпомилково визначити відправника, він просто

використовує свій секретний алгоритм для отримання $Y = f_{Z_i}^{-1}(X)$, яке надсилається одержувачу. Кожен користувач може, знаючи відкритий алгоритм E_{Z_i}, отримати $f_{Z_i} = X$. Однак ніхто, крім користувача i, не зміг би перетворити доступне для розуміння повідомлення X в Y, оскільки лише користувач i в змозі обчислити $f_{Z_i}^{-1}$. Зрозуміло, користувач i може надіслати користувачу j також секретне повідомлення з підписом. Для цього він повинен зашифрувати Y, користуючись відкритим ключем E_{Z_j} користувача j, і не посилати Y у відкритому вигляді.

У 1976 р. Діффі і Хеллману ще не були відомі односторонні функції з потаємним ходом. Вперше така функція була запропонована у 1978 р. американцями Р.Л.Рівестом, А.Шаміром і Л.Адлманом (від перших літер їхніх прізвищ утворено скорочення RSA), які працювали в Массачусетському технологічному інституті. Одностороння функція RSA надзвичайно проста, але для її опису потрібні деякі відомості з елементарної теорії чисел.

Нехай НЗД (i, n) — це найбільший загальний дільник цілих чисел i та n, які водночас не дорівнюють нулеві. Наприклад, НЗД (12,18)=6.

Для кожного додатного цілого n функція Ейлера $\psi(n)$ визначається як число додатних цілих i, не більших за n і таких, що НЗД(i, n)=1 (при n=1, за визначенням, $\psi(1) = 1$). Наприклад, $\psi(6) = 2$, оскільки з усіх $1 \le i \le 6$ лише $i = 1$ та $i = 5$ дають НЗД(i,6)=1. Очевидно, що для простого числа p маємо $\psi(p) = p - 1$. Не важко також помітити, що для двох нерівних простих чисел p і q

$$\psi(pq) = (p-1)(q-1). \tag{8}$$

Наприклад, $\psi(6) = \psi(2 \cdot 3) = 1 \cdot 2 = 2.$ Знаменита теорема Ейлера гласить: для будь-яких цілих чисел x і n (x<n)

$$X^{\psi(n)} = 1 (\mathrm{mod}\, n) \tag{9}$$

за умови, що НЗД (x, n)=1.

Останній необхідний нам факт з теорії чисел походить від Евкліда. Якщо e і m задовольняють умови 0<e<m і НЗД(m,e)=1, то існує лише одне d, таке, що 0<d<m і

$$d \cdot e = 1 (\mathrm{mod}\, n), \tag{10}$$

і, крім того, d може бути обчислене за допомогою "розширеного" алгоритму Евкліда для знаходження НЗД(m, e).

Одностороння функція RSA з потаємним ходом є просто дискретним піднесенням до степеня:

$$f_Z(x) = x^e (\mathrm{mod}\, n), \tag{11}$$

де x – додатне ціле, яке не перевищує $n = p \cdot q$, потаємний хід $Z = \{p, q, e\}$, p і q – великі нерівні числа, такі, що $\psi(n) = (p-1)(q-1)$, має великий простий множник, а e – додатне ціле, яке не перевищує $\psi(n)$, для якого НЗД$(e, \psi(n))$=1.

Алгоритм E_Z швидкого обчислення f_Z знайти легко — це метод піднесення до квадрату і множення. Публікація цього алгоритму зводиться до публікації значень n і e.

Обернена функція має вигляд:

$$f_Z^{-1}(y) = y^d (\mathrm{mod} n), \tag{12}$$

де d – єдине додатне ціле, що менше за n і задовольняє умову

$$d \cdot e = 1 (\mathrm{mod}\, \psi(n)). \tag{13}$$

Алгоритм D_Z (у разі, якщо відомо *Z*) для обчислення f_Z^{-1} обчислюють також методом піднесення до квадрату і множенням. Показник *d*, необхідний при розшифруванні, знаходять за допомогою алгоритму Евкліда, який визначає НЗД($e, \psi(n)$).

Той факт, що функція (12) дійсно є функцією, оберненою до функції (11), доводиться так. Рівність (13) еквівалентна (в звичайній цілочисельній арифметиці)

$$d \cdot e = \psi(n) \cdot Q + 1 \qquad (14)$$

Для деякого Q з (11) і (14) отримаємо:

$$(x^e)^d = x^{\psi(n)\cdot Q+1} (\mathrm{mod}\, n) = (x^{\psi(n)})^Q \cdot x (\mathrm{mod}\, n) = x (\mathrm{mod}\, n), \qquad (15)$$

де в останній рівності використано теорему Ейлера (9). Рівність (15) показує, що операція піднесення числа до степеня *d* (за модулем *n*) обернена відносно операції піднесення до степеня *e* (за модулем *n*). Залишається лише показати, чому автори вважали (і більшість спеціалістів вважають і тепер), що обернення функції f_Z тільки за відомими *n* і *e* обчислювально неспроможне. Покажемо також, як можна випадково обрати два великих нерівних простих числа *p* і *q* так, щоб зловмисник не зміг їх вгадати.

Зловмиснику відомі лише *n* і *e*. Проте, розклавши $n = p \cdot q$ на множники, він матиме повну інформацію про "потаємний хід" $Z = \{p, q, e\}$ і, отже, також зможе легко розшифрувати повідомлення, як і законний одержувач. Стійкість криптосистеми RSA заснована на припущенні про те, що будь-який спосіб обернення функції f_Z еквівалентний розкладанню $n = p \cdot q$ на множники, тобто знаючи спосіб обернення f_Z, можна (лише з невеликими додатковими витратами за часом) розкласти *n* на множники.

Чи дійсно розкладання на множники обчислювально нездійсненне? Відповідь буде позитивною, якщо довжина вибраних *p* і *q* більша ніж 150 десяткових знаків і якщо, звичайно, не відбудеться "революційного прориву" в задачі розкладання на множники. Рівест показав, що час роботи всіх кращих за часом відомих алгоритмів розкладання на множники обмежене однією і тією ж функцією $L(N) = \exp(\sqrt{\log N \log\log N})$, яка зростає на порядок при подовженні числа на 15 десяткових знаків (у діапазоні від 50 до 200 знаків). Сучасні ЕОМ здатні за один день роботи розкласти на множники число довжиною 80 десяткових знаків. Для розкладу ж 200-значного числа $n = p \cdot q$ треба десятки тисяч років. Цікаво, що кращі відомі алгоритми розв'язання задачі дискретних логарифмів (за модулем *p*) і кращі алгоритми розкладання *n* на множники потребують при $p \approx n$ приблизно однакової кількості обчислень (детальніше порівняння наведено в 1.2.4). Через це функція RSA і функція Діффі-Хеллмана (4) мають приблизно однакові підстави називатися "односторонніми".

Залишається показати, як можна випадково вибирати великі прості числа *p* і *q*, необхідні в системі RSA. Теорема Чебишева стверджує, що частка позитивних цілих чисел, менших, ніж деяке ціле *m* і які є простими, близька до $(\ln m)^{-1}$. Наприклад, частка цілих чисел, менших ніж 10^{100}, і які є простими, близька до $(\ln 10^{100})^{-1} \approx 1/230$. Оскільки 90 відсотків цих чисел знаходяться між 10^{99} *і* 10^{100}, частка простих чисел в цьому діапазоні також становить 1/230. Через це, якщо абсолютно випадково вибрати число в діапазоні від 10^{99} до 10^{100}, то воно буде простим з ймовірністю близько 1/230. Цю ймовірність легко подвоїти, якщо вибрати тільки непарні числа. У такому разі для знаходження простого числа потрібно лише біля 115 проб.

Як відрізнити прості числа від складених? Є досить простий спосіб, який дає змогу достатньо точно визначити, чи є ціле число простим, хоча він і не дає можливості розкласти на множники знайдені з його допомогою складені числа. Такі перевірки (тести) грунтуються на теоремі Ферма, яка стверджує, що для будь-якого позитивного числа *b*, яке не перевищує деякого простого числа *p*,

$$b^{p-1} = 1(\mathrm{mod}\, p). \qquad (16)$$

Наприклад, $2^4 = 1(\mathrm{mod}\, 5)$. Якщо треба визначити, чи є ціле число r простим, можна вибрати будь-яке додатне ціле число *b*, менше за r, і перевірити, чи справедлива рівність

$$b^{r-1} = 1(\mathrm{mod}\, r). \qquad (17)$$

Якщо рівність не справджується, то виходячи з теореми Ферма можна бути цілком впевненим, що r – не просте число. Якщо ж рівність справджується, то можна лише припускати, що r – просте число, і тому назвати його псевдопростим за основою *b*. Виявляється, що якщо r – складене число, воно є псевдопростим лише для менш ніж половини (в дійсності значно менше за половину) можливих основ *b*. Отже, якщо r – досить велике, а t різних основ *b* вибрані незалежно і зовсім випадково, складове число r витримає тести Ферма (17) за всіма основами *b* з ймовірністю не більшою за 2^{-t}. Якщо, скажімо, *t*=100, і число r витримує всі *t* незалежних тестів Ферма, то можна бути майже впевненим, що воно просте. Такі "ймовірнісні тести" вперше запропонували американці Р.Соловей і Ф.Штрасен, пізніше їх розвинув М.Рабін. Ці тести використовуються для пошуку простих чисел серед випадкових непарних цілих чисел і знаходження у такий спосіб пар простих чисел, необхідних для односторонньої функції RSA, або, точніше, для знаходження пар чисел, які можна з достатньою впевненістю вважати простими.

Крім "ймовірнісних тестів" існують також "детерміновані" (кращий з них – метод еліптичних кривих) і гіпотетичні тести (які гарантують простоту чисел при виконанні деякої гіпотези (Рімана, Баха)). Найекономічнішими за числом операцій є ймовірнісні тести. Потім ідуть гіпотетичні, а детерміновані потребують найбільшого числа операцій.

Існують надвеликі інтегральні схеми (НВІС), що виконують шифрування і розшифрування за алгоритмом RSA з швидкістю кілька кілобайтів на секунду. Ці НВІС можна використовувати для виконання тестів Ферма і знаходження необхідних великих простих чисел *p* і *q*. Для більшості застосувань криптографії такі швидкості надто малі. У цьому разі все ж бажано використовувати криптосистему RSA для розповсюдження секретних ключів, які потім будуть використані у високошвидкісних шифрах з секретними ключами, таких як SKIPJACK DES або деякі поточні шифри. Крім того, бажано використовувати алгоритми RSA в режимі "цифрових підписів" для автентифікації.

Опишемо систему Т.Ель-Гамаля в полі GF(*q*), де *q* – основа або степінь основи (тут $q = 2^n$). Нехай α – первісний елемент поля. Відправник має: a – особистий ключ і α^{-a} – відкритий ключ; аналогічно одержувач має *b* і α^{-b}. Для того щоб надіслати одержувачу секретне повідомлення *M*, відправник обирає випадкове ціле число r і надсилає пару $\left(\alpha^r, \alpha^{-br} \cdot m\right)$. Тут *m* – це *M* в розрядному поданні. Одержувач обчислює $(\alpha^r)^b \cdot \alpha^{-br} \cdot m$, відновлюючи *m*. Якщо *M* є ключем, обраним відправником, це можна розглядати як механізм ключового обміну (це неавтентифікований ключовий обмін, оскільки третя особа може замаскуватися під "відправника до одержувача", але протокол може бути модифіковано). Надсилаючи підписане повідомлення *M* одержувачу, відправник знову вибирає випадкове ціле число r і обчислює α^r. Нехай *R* буде цілим представленням α^r з $0 \le R \le q-1$. Відправник також обчислює $S = (M + \alpha R) r^{-1} (\mathrm{mod}\, q-1)$ і посилає повідомлення M разом з підписом (α^r, S). Одержувач перевіряє підпис, обчислюючи $(\alpha^{-a})^R (\alpha^r)^S$, а також визначає, чи дорівнює він α^M. Для передачі секретного підписаного повідомлення для кожного підпису потрібно вибрати нову величину *r*. Кожного разу, уникаючи обчислення r^{-1}, можна змінити протокол так: відправник обчислює $S = -(M - rR)\alpha^{-1} (\mathrm{mod}\, q-1)$ і одержувач перевіряє, чи $(\alpha^r)^R (\alpha^{-a})^S$ дорівнює α^M.

Були запропоновані також інші односторонні функції з потаємним ходом. Деякі з них виявилися ненадійними, інші перспективними, але поки що нікому не вдалося довести, що яка-небудь функція є односторонньою з потаємним ходом.

Висловлювалися сподівання, що нова теорія, яка швидко розвивається, – теорія обчислювальної складності, зокрема теорія NP-повноти Карпа, дасть можливість довести, що деякі функції є односторонніми або односторонніми з потаємним ходом. Це передбачення, вперше висловлене Діффі і Хеллманом, до цих пір призводило в основному до провалів, таких, як провал криптосистеми Меркля і Хеллмана, заснованої на задачі про укладання ранця. Наприклад, обернення односторонньої функції Меркля і Хеллмана, заснованої на задачі про укладання ранця, в дійсності виявилось простою задачею, замаскованою під NP-повну. Шамір, розкриваючи цей шифр, не розв'язав NP-повну задачу, а лише зняв маскування.

1.2.4. Порівняльний аналіз криптосистем

Порівнюються алгоритми, засновані на квадратичному решеті для розв'язання задач факторизації та підходу Купершміта для обчислення дискретних логарифмів в $GF(2^n)$. Результати порівняння використовуються для порівняння практичної складності між криптосистемами RSA і Ель-Гамаля в полі з характеристикою 2.

Стійкість криптосистем RSA і Ель-Гамаля еквівалентна відповідно складності чисельної факторизації та обчислення дискретних логарифмів у скінчених полях.

Асимптотична оцінка часу багатьох алгоритмів факторизації має вигляд: $L^C(N)$, де $L(N) = \exp(\sqrt{\log N \log\log N})$. Оскільки в теоретичну оцінку (апріорну) входить константа C, яка для різних алгоритмів різна, викликає інтерес отримання апостеріорних оцінок, які є більш точними.

Відповідь на запитання: "Який має бути розмір поля $GF(2^n)$, щоб обчислення дискретних логарифмів у цьому полі було б таким же трудомістким, як і задача факторизації m-бітового цілого?" дає практичний порівняльний аналіз складності відповідних програм (для числа бітів, які мають практичний інтерес).

Алгоритм Купершмідта з удосконаленням Олдижко [52] для комп'ютера з 32-розрядною мантисою потребує $h^2 2^{m-2} p(h+1,m)^{-1} p(M,m)^{-1}$ зсувів і додавань, де – $m \approx n^{1/3}(\ln n)^{2/3}$, $\deg w_1(x)/v_1(x) \approx h+1$; $\deg w_2(x)/v_2(x) \approx M$ $(w_i(x), v_i(x), i) = 1,2$ – многочлени, які використовуються на першому етапі алгоритму [52]), $p(r,m)$ – ймовірність того, що всі незвідні множники двочленного поліному степені r мають степінь не вищу, ніж m.

Число елементарних операцій для алгоритму квадратичного решета оцінюється величиною

$$3 \ln\ln B b r(u)^{-1},$$

де b – число твірних базису $FB\{p_1, \ldots, p_b\}$, $p_1 = -1$, $p_2 = 2$, $p_i < B$; $r(u) \approx e^{-u\ln u}$.

Для факторизації чисел вигляду $N = r^e \pm S$, де r і S – невеликі цілі числа, алгоритм Полларда (number field seive) "працює" за час $\exp\left((C+0(1))(\ln N)^{1/3}(\ln\ln N)^{2/3}\right)$, де $C \approx 1{,}526$. Для факторизації за допомогою цього алгоритму довільних цілих чисел $C = 3^{2/3} \approx 2{,}08$.

Д.Гордон [44] зауважує, що алгоритм "решета числового поля" (number field seive), який застосовується для факторизації чисел, може бути запроваджений для обчислення дискретних логарифмів для непарних полів $GF(p)$. При цьому час роботи алгоритму асимптотично може бути оцінений виразом

$$L_x[\nu, C] = e^{(C+0(1))x^{\nu}(\ln x)^{1-\nu}}.$$

Причому для: факторизації цілого N (загальне решето числового поля) $L_{\ln N}[1/3, 2.08]$; факторизації цілого N (алгоритм Купершмідта з попередніми обчисленнями) $L_{\ln N}[1/3, 1.639]$; обчислення дискретних логарифмів в $GF(P)$ (за допомогою решета числового поля) $L_{\ln p}[1/3, 2.08]$; обчислення дискретних логарифмів в $GF(2^n)$ (алгоритм Купершмідта) $L_{\ln}[1/3, c]$, $1{,}3507 \le c \le 1{,}4047$.

Наведемо порівняння (в бітах) N і n, які забезпечують однакову безпеку для алгоритмів квадратного решета і Купершмідта:

Факторизація *(m)*	Дискретні логарифми *(n)*
332	400+
512	700+

У роботі [49] показано, що використання суперсингулярних еліптичних кривих в $GF(q^k)$ з k=4 дає можливість для еліптичних кривих в $GF(2^n)$ з $n \approx 175$ чи 200 забезпечити ту ж складність дискретного логарифмування, що і факторизація 512-бітового числа.

Отже, обчислення дискретних логарифмів в $GF(2^n)$ здійснити легше, ніж факторизацію m-бітового цілого N при використанні кращих за кількістю відомих на сьогодні алгоритмів для кожної з задач. Наприклад, криптосистема Ель-Гамаля в $GF(2^n)$ є менш безпечною, ніж RSA, яка використовує m-бітовий модуль N. Це може бути компенсовано завдяки використанню більшого числа бітових розрядів n для систем в $GF(2^n)$.

1.3. Криптографічні протоколи

1.3.1. Що таке протокол?

Протокол – це певна послідовність дій, за допомогою яких дві або більше сторони спільно виконують деяке завдання. Так, криптосистему з відкритими ключами можна розглядати як протокол, заснований на односторонній функції з потаємним ходом. За допомогою цього протоколу споживачі системи і держатель загальнодоступного довідника спільно забезпечують конфіденційність повідомлень, що передаються між користувачами.

1.3.2. Протокол розповсюдження ключів

Багато спеціалістів, особливо ті, що скептично ставляться до систем з відкритими ключами, вважають задачу управління ключами (тобто задачу захищеного розподілу і заміни секретних ключів) головною практичною задачею в криптографії. Наприклад, якщо система містить S користувачів, і для кожної можливої пари користувачів потрібен окремий секретний ключ, то знадобляться $S(S-1)/2$ різних ключів, що у великій системі небажано. Малоймовірно, що хто-небудь з користувачів посилатиме секретні повідомлення великому числу інших користувачів, хоча, звичайно, заздалегідь невідомо, хто з ким виявить бажання встановити секретний зв'язок. Ця задача часто розв'язується з допомогою протоколу розповсюдження ключів. Він вимагає завчасно розповсюдити тільки S секретних ключів, але дозволяє встановити секретний зв'язок між будь-якими двома користувачами. Цей протокол включає новий об'єкт – центр розповсюдження ключів (ЦРК).

Протокол розповсюдження ключів:

1) ЦРК передає по захищеному каналу випадково вибраний секретний ключ Z_i користувачеві i, $i = \overline{i,s}$;
2) коли користувач i бажає встановити секретний зв'язок з користувачем j, він посилає загальною мережею (і, можливо, відкритим текстом) запит до ЦРК з вимогою секретного ключа для зв'язку;

3) ЦРК випадково вибирає новий секретний ключ Z_{ij}, який утворює частину відкритого тексту. Другу частину становить "заголовок", у якому зазначені користувачі *i, j*. ЦРК шифрує цей відкритий текст 2 рази з допомогою прийнятого в системі шифру, використовуючи два ключі Z_i, Z_j, після чого посилає загальною мережею першу криптограму користувачу *i*, а другу – користувачу *j*;
4) користувачі *i, j* розшифровують отримані криптограми і отримують секретний ключ для розшифрування наступних повідомлень, які передаватимуться між ними.

Цей протокол здається дуже простим, але його стійкість при криптоаналізі потребує від використаного в системі шифру не тільки стійкості при аналізі на основі шифрованого тексту. Це пояснюється тим, що на кроці 3) криптоаналітику доступні дві криптограми, отримані з одного і того самого відкритого тексту при використанні різних ключів. Це може бути корисним для криптоаналітика, хоча і дає йому менше інформації, ніж він міг би отримати при аналізі на основі вибраного відкритого тексту.

Отже, якщо використаний у системі шифр витримує аналіз на основі вибраного відкритого тексту, то такий аналіз витримує і протокол. Слід зазначити, що використовуючи шифр у протоколі, слід уважно стежити за тим, щоб стійкість, забезпечена шифром, не порушилася.

1.3.3. Триетапний протокол Шаміра

Цей протокол показує, що секретність можна забезпечити, не розповсюджуючи попередньо ні секретних, ні відкритих ключів. Він передбачає, що між двома користувачами існує такий засіб зв'язку, як безшовна оптична лінія чи заслуговуючий на довіру, але дуже цікавий поштар, який не дозволяє виконати імітацію чи підміну повідомлень, але дає зловмиснику можливість читати всі повідомлення, що проходять каналами зв'язку. Крім того, використовується криптосистема з секретними ключами, а шифруюча функція $E_Z(i)$ є комутативною, тому для будь-якого відкритого тексту *x* і ключів Z_1 і Z_2

$$E_{Z_2}(E_{Z_1}(x)) = E_{Z_1}(E_{Z_2}(x)), \qquad (18)$$

тобто результат дворазового шифрування не залежить від того, в якому порядку використовуються ключі Z_1 і Z_2. Такою властивістю володіє багато шифрів.

Протокол шифрування:

1) користувачі *A* і *B* випадково вибирають особисті секретні ключі Z_A і Z_B;
2) коли користувач *A* бажає надіслати секретне повідомлення *X* користувачу *B*, він зашифрує *X* з використанням ключа Z_A і надсилає отриману криптограму $Y_1 = E_{Z_A}(X)$ відкритим і захищеним від імітації та підміни каналом користувачу *B*;
3) користувач *B*, прийнявши Y_1, вважає її відкритим текстом і зашифрує з використанням свого ключа Z_B. Він надсилає отриману криптограму $Y_2 = E_{Z_B}(Y_1) = E_{Z_B}(E_{Z_A}(X))$ відкритим і захищеним каналом користувачу *A*;
4) користувач *A*, прийнявши Y_2, розшифровує її з допомогою свого ключа Z_A. Згідно з комутативною властивістю (18) це знімає попереднє шифрування з використанням Z_A, в результаті чого отримують $Y_3 = E_{Z_B}(X)$. Далі користувач *A* надсилає Y_3 відкритим і захищеним від імітації та підміни каналом користувачу *B*;
5) користувач *B*, прийнявши Y_3, розшифровує її з допомогою свого ключа Z_B і отримує секретне повідомлення *X*, що передане *A*.

Який шифр з секретними ключами можна використовувати в цьому протоколі? Чи придатний у цьому разі шифр з ключем одноразового використання, який забезпечує повну секретність? При його використанні три криптограми набувають вигляду

$$\left.\begin{aligned} Y_1 &= X \oplus Z_A; \\ Y_2 &= X \oplus Z_A \oplus Z_B; \\ Y_3 &= X \oplus Z_B. \end{aligned}\right\} \qquad (19)$$

Криптоаналітик спостерігає всі три криптограми і тому може обчислити $Y_1 + Y_2 + Y_3 = X$, де використана та властивість, що дві однакові величини при додаванні за модулем 2 дають 0. Отже, при використанні шифру з ключем одноразового використання, триетапний протокол є зовсім ненадійним. Причиною цього, як видно з (19), є та властивість протоколу, що кожен шифр використовується в ньому в "півтора рази", тоді як шифр, що розглядається, надійний лише при одноразовому використанні.

Алгоритм RSA пасує для протоколу Шаміра, оскільки зловмисник зможе його розкрити лише у тому разі, якщо зможе розв'язати задачу розкладання на множники.

1.4. Доповнення

1.4.1. Встановлення справжності

Дослідимо різні методи перевірки ідентичності та встановлення справжності користувачів і систем. Передусім слід дослідити взаємозв'язок між встановленням справжності та визначенням прав (повноважень), які в сукупності визначають, який доступ дозволяється до захищених ресурсів.

Ідентифікація – це присвоєння об'єкту унікального імені або числа. Встановлення справжності полягає в перевірці, чи є особа або об'єкт, який перевіряється, насправді тим, за кого себе видає. Визначення прав (повноважень) встановлює, чи надано особі або об'єкту і якою мірою право звертатися до захищеного ресурсу. Ці перевірки використовують одночасно для прийняття рішення про доступ.

1.4.1.1. Ідентифікація і встановлення справжності

Ідентифікація є заявкою на встановлення ідентичності. До ідентифікатора по можливості слід вводити контрольні цифри або використовувати інші засоби самоконтролю з метою мінімізації шансів помилкової ідентифікації. Ідентифікація потрібна не лише для розпізнання, а також для обліку звернень. Однак її не можна використовувати саму по собі, без додаткового встановлення справжності, якщо в системі потрібен певний ступінь безпеки.

Встановлення справжності полягає в перевірці, чи є особа (об'єкт) тим, за кого себе видає. Для цього може вимагатися інформація різного характеру. Хоча особистість встановлюють звичайно тільки один раз, в установах, які забезпечують високий ступінь безпеки, може стати потрібною періодична перевірка за певних умов. Повторне встановлення справжності може бути бажаним, наприклад, після всіх системних збоїв.

Для визначення користувачів ЕОМ застосовують паролі та інші методи діалогу.

1.4.1.2. Паролі

Метод паролів потребує, щоб користувач ввів (надрукував, набрав на клавіатурі) рядок символів (пароль) для перевірки їх в ЕОМ. Якщо пароль відповідає тому, який зберігається в ЕОМ для цього користувача, він може користуватися всією інформацією, доступ до якої йому дозволений (паролі можна також використовувати незалежно від користувача для захисту файлів тощо).

У схемі з простим паролем користувачу дозволяється самому вибирати пароль так, щоб його можна було легко запам'ятати. Слід потурбуватися про те, щоб пароль не був надто очевидним.

Якщо зареєстрований користувач вибирає менш очевидний пароль, він для кращого запам'ятовування може записати його. У цьому разі є ризик випадкового знаходження сторонньою особою пароля на викинутому аркуші паперу, такому, наприклад, як використаний протокол з пульту терміналу.

Один з часто застосовуваних методів передбачає залишати пропуски в ряді символів і в кінці пароля. У такому разі незаконно одержаний незахищений аркуш паперу з паролем не дасть можливості автоматично розкрити його таємницю.

Довжина пароля і безпечний час. Чим більша довжина пароля, тим безпечнішою буде система, і потрібно буде більше зусиль для його відгадування. Цю ситуацію можна подати термінами очікуваного часу розкриття, або очікуваного безпечного часу. ***Очікуваний безпечний час*** – напівдобуток числа можливих паролів і часу, потрібного для того, щоб перевірити кожен пароль.

Збільшення довжини пароля тільки на один символ значно збільшує час, потрібний зловмиснику для його розкриття при систематичних спробах, організованих за допомогою ЕОМ. Так, якщо очікуваний безпечний час для трисимвольного пароля, вибраного з 26-символьного алфавіту, становитиме 3 міс., очікуваний безпечний час для чотирисимвольного пароля дорівнюватиме 78 міс. (6,5 року).

Недоліком схеми з простим паролем є те, що пароль може легко використати інша особа без відома зареєстрованого користувача (навіть до кінця місяця, поки йому буде подано рахунок). Одним з шляхів вирішення цієї проблеми є видача системою на термінал користувача кожного разу, коли він спілкується з системою, чергового номера, за яким зареєстровано його звернення до системи на цей день і тривалість роботи. На термінал можна вивести також поточний рахунок на певний момент часу. Якщо за цей час хто-небудь скористався чужим рахунком, уважний користувач зможе це виявити.

1.4.1.3. Модифікація схеми простих паролів

Деякі зміни в схемі простого пароля збільшують ступінь безпеки, правда, за рахунок складнішого програмування і збільшення труднощів для користувача.

При зверненні користувача до системи у нього можуть бути запитані окремі символи з пароля, вибрані ЕОМ. Позиції запитаних символів можна отримати за допомогою деякої процедури перетворення, прив'язаної до годинника ЕОМ, або виробити генератором псевдовипадкових чисел. Будь-яке незаконне підключення до лінії зв'язку або обшукування корзин для використаного паперу може дати в результаті пошуків лише невелику частину пароля, яка, найімовірніше, буде непридатною для наступного звернення. Очевидно, пароль треба змінювати досить часто, оскільки стороння особа може врешті-решт скласти пароль з окремих символів.

У схемі одноразового використання паролів користувачу видається список з N паролів. Такі ж N паролі зберігаються в ЕОМ (звичайно, у зашифрованому вигляді). Після використання пароля користувач викреслює його з списку. Якщо навіть незареєстрована особа отримала якимось чином перший пароль, система не реагуватиме на жоден запит з цим паролем, оскільки вона вже використала його і очікує наступний.

Паролі одноразового використання можуть застосовуватись також для встановлення справжності підтвердження про відключення ЕОМ від обслуговування користувача і підтвердження справжності вимог користувача про відключення від ЕОМ. Це зменшує можливість використання системи досвідченим зловмисником, який, підслуховуючи на незахищеній лінії зв'язку і посилаючи фальшиве повідомлення користувачу про відключення, потім використовує лінію зв'язку на власний розсуд, маскуючись під перевіреного користувача.

1.4.1.4. Метод "запит – відповідь"

У цьому методі набір відповідей на *m* стандартних і *n* орієнтованих на користувача запитань зберігається в ЕОМ і керується операційною системою. Коли користувач робить спробу підключитися до роботи, операційна система вибірково задає йому деякі (або всі) з цих запитань. Користувач повинен дати правильну відповідь на всі запитання, щоб отримати дозвіл на доступ до системи.

1.4.1.5. Встановлення користувачем справжності системи

Пароль можна використовувати не тільки для встановлення справжності користувача по відношенню до системи, а й для зворотного встановлення справжності. Це має важливе значення, наприклад, у мережах ЕОМ. Якщо у мережі немає системи встановлення справжності, будь-хто може втрутитись у лінію зв'язку і відтворити процес входження в роботу від запитуваної ЕОМ (скажімо, ЕОМ "*С*"). Користувач, гадаючи, що він спілкується з ЕОМ "*С*", надасть сторонній особі в сеансі зв'язку запитувану ним інформацію (включаючи пароль).

Один з шляхів зменшення цієї загрози полягає в тому, що ЕОМ, після того як вона встановила справжність користувача, виводить на друк терміналу користувача встановлений ним пароль, який заздалегідь повинен бути переданий в ЕОМ адміністративними каналами забезпечення безпеки. Для цього можна використовувати простий пароль або пароль одноразового використання.

Для встановлення справжності системи по відношенню до користувача і навпаки можна також використовувати криптографічні методи перетворення інформації. Користувач вводить з клавіатури своє ім'я, яке в незакодованому вигляді надсилає лініями зв'язку в ЕОМ. Машина розглядає ім'я точно так, як це робить система з паролями. Замість секретного пароля в ЕОМ зберігається ключ перетворення секретності для кожного імені. ЕОМ завантажує цей ключ у свій шифрувальний пристрій, вмикає його і робить спробу зв'язатися з користувачем. Тим часом користувач уже завантажив свою копію ключа в свій шифрувальний пристрій і увімкнув його. Тепер, якщо ключі виявилися ідентичними, обмін деякої стандартної послідовності символів – режим "рукостискання" буде успішним. Якщо вони не ідентичні, обмін не відбудеться і обидва "партнери" (користувач і ЕОМ) отримають потоки бітів, що не збігаються. Якщо обмін проходить успішно, ЕОМ "впевнена" в ідентичності користувача, а користувач – в ідентичності ЕОМ. Секрет, який використовується для встановлення особистості, полягає в тому, що ключ перетворення не повинен передаватися лініями зв'язку. Якщо зв'язок закінчується, кожна сторона, що бере участь у передачі повідомлень, буде одразу ж попереджена про ситуацію, що склалася.

1.4.1.6. Головні застережні заходи при роботі з паролями

1. Паролі не слід зберігати в обчислювальній системі у явній формі – вони завжди мають бути зашифровані.
2. Паролі не треба друкувати (відображати) у явному вигляді на терміналі, у тому числі на розпечатках.
3. Чим більший період часу використовується один пароль, тим більша ймовірність того, що він не буде розкритий.
4. Система ніколи не повинна виробляти новий пароль у кінці сеансу зв'язку.

1.4.1.7. Процедура встановлення справжності

Для усунення деяких недоліків описаних раніше методів операційна система може вимагати, щоб користувач встановив свою справжність з допомогою коректної обробки алгоритмів. Ця процедура може бути

виконана як між двома ЕОМ, так і між користувачем і ЕОМ. Вона забезпечує більший ступінь безпеки, ніж багато інших схем, але водночас є більш складною і потребує додаткових витрат часу для користувача. Як і завжди, тут потрібно знайти компроміс між потрібним рівнем безпеки і простотою виконання.

У всіх випадках, коли є відмова в доступі, слід зробити реєстраційний запис і здійснити затримку в часі.

1.4.2. Встановлення повноважень

Інколи після здійснення процедури встановлення справжності можуть бути перевірені повноваження запитів, які вводяться певним користувачем, терміналом або іншим ресурсом.

Якщо надається дозвіл на виконання певної дії, вважають, що об'єкт, який робить запит, має повноваження по відношенню до цієї дії. Буде надано дозвіл на доступ, чи ні, залежить від кількох чинників: прав користувача на доступ, прав терміналу на доступ, дії власне елемента даних і його значення, або, наприклад, часу дня.

Система забезпечення безпеки підтримує деякі профілі повноважень кожного користувача, терміналу, процедури або іншого ресурсу, який здійснює доступ до елементів даних. Ці профілі встановлюються в системі за допомогою спеціальної привілейованої програми. Її можна подати у вигляді матриці встановлення повноважень.

Залежно від ступеня секретності даних додатково можуть бути виконані інші можливі дії, а саме: одноденна затримка дій щодо встановлення (зміни) профілю (період заморожування); затримка встановлення (зміни) профілю до того часу, поки другий уповноважений користувач не здійснив такі ж дії ("дружня" система, що вимагає двох підписів для значних змін); затримка встановлення (зміни) профілю до того часу, поки не буде подано сигнал від специфічного користувача в системі ("наказ керуючого").

Мета цих заходів полягає в тому, щоб забезпечити роль арбітра, який знімає "кайдани" для виконання повноважень.

1.4.2.1. Матриця встановлення повноважень

Кожен елемент A_{ij} в матриці встановлення повноважень визначає права доступу *i*-го ресурсу до *j*-го ресурсу. Елементи матриці встановлення повноважень звичайно містять біти, що відповідають діям, які можуть бути виконані з терміналу при зверненні до елемента даних. Однак у разі необхідності елементи матриці можуть містити показники процедур. Наприклад, рішення про *доступ* грунтується на:

а) історії доступів інших ресурсів. Користувач *A* може записувати дані в файл *F* тільки в тому випадку, якщо він не читав файл *G*;

б) значенні певних внутрішньосистемних змінних. Доступ може бути здійснений користувачем відповідної групи тільки з 7 до 19 год., виключаючи роботу з спеціального терміналу 72.

Матриця встановлення повноважень є в дійсності "серцем" системи забезпечення безпеки.

Звичайно матриця встановлення повноважень зберігається як окремий зашифрований файл і її рядки містяться в оперативній пам'яті лише у разі необхідності.

1.4.2.2. Рівні повноважень

Встановлення повноважень може також грунтуватися на рівнях повноважень, пов'язаних з ресурсами. Запит на доступ відхиляється у всіх випадках, коли рівень повноважень терміналу або користувача, що запитує дозвіл на доступ, нижчий, ніж рівень повноважень операції і (або) запитуючих даних.

1.4.3. Перетворення секретної інформації. Традиційні методи

1.4.3.1. Прямі підстановки

Кожний знак початкового тексту замінюється одним або кількома знаками. Одним з важливих підкласів прямих підстановок є моноалфавітні підстановки, в який встановлюється взаємно однозначна відповідність між кожним знаком a_i алфавіту повідомлень A і відповідним знаком h_j зашифрованого тексту.

Усі методи моноалфавітної підстановки можна подати як числові перетворення літер початкового тексту, які розглядаються як числа. Кожна літера в тексті множиться на деяке число і додається до деякого іншого числа:

$$c = (ap + S) \bmod k, \tag{20}$$

де a - десятковий коефіцієнт; S – коефіцієнт зсуву; k – розмір алфавіту.

1.4.3.2. Багатоалфавітні підстановки

При багатоалфавітних підстановках послідовно і циклічно змінюються алфавіти, що використовуються. При n-алфавітній підстановці знак m_1 з початкового повідомлення замінюється знаком з алфавіту B_1, m_2 – відповідним з алфавіту B_2,…, m_n – знаком з алфавіту B_n, m_{n+1} – знову з алфавіту B_1 і т.д.:

Вхідний знак	m_1	m_2	m_3	m_4	m_5	m_6	m_7	m_8	m_9	…
Алфавіт підстановки	B_1	B_2	B_3	B_4	B_1	B_2	B_3	B_4	B_1	…

Ефект використання багатоалфавітної підстановки полягає в тому, щоб забезпечити маскування природної частотної статистики початкової мови L, оскільки конкретний знак з алфавіту A може бути перетворений на кілька різних знаків шифрувального алфавіту B. Ступінь забезпечення захисту теоретично пропорційний довжині періоду в послідовності алфавітів, які використовуються.

1.4.3.3. Монофонічні шифри

Багатоалфавітний шифр підстановки зрівнює частоту появи зашифрованих знаків, захищаючи шифр від розкриття з допомогою частотного аналізу. Для знаків, які зустрічаються часто, потрібна відносно велика кількість зашифрованих еквівалентів. Водночас для знаків, які використовуються нечасто, може виявитися достатнім один або два зашифровані знаки.

Якщо в багатоалфавітній підстановці число знаків у ключі перевищує загальне число вихідних знаків, які шифруються, ключ використовується лише один раз, початковий текст не може бути викрадений зловмисником, зашифрований текст теоретично не можна розкрити.

1.4.3.4. Частотний аналіз

Більшість штучних мов (і всі природні мови) мають характерне частотне розподілення літер та інших знаків. Наприклад, E – літера, що найчастіше зустрічається в англійській мові, а Z – найрідше. Багато повідомлень, які зашифровані методом перестановки або одноалфавітної підстановки, зберігають характерний частотний розподіл і, отже, дають криптоаналітику шлях до розкриття шифру.

Справа дуже ускладнюється, коли криптоаналітик стикається з рівномірним розподілом символів, які отримуються при використанні багатоалфавітної підстановки.

1.4.3.5. Складені перетворення

Часто ефективність шифрування можна підвищити за рахунок використання послідовності перетворень. Це значно ускладнить роботу зловмисника з розкриття системи. Розглянемо такий приклад. Якщо періоди багатоалфавітних перетворень $T_1, T_2, \ldots, T_S$ є взаємно простими, то період складеного перетворення $T = T_1, T_2, \ldots, T_S$ дорівнюватиме добутку періодів $u_1, u_2, \ldots, u_S$ складових перетворень. Оскільки період став довшим, то і складене перетворення стало безпечнішим. Складене у такий спосіб перетворення набагато безпечніше, ніж будь-яка його складова.

Безумовно, слід бути уважним при використанні складених перетворень. Можна ненавмисно так "перешифрувати" початковий текст, що врешті-решт отримаємо повідомлення, ідентичне оригіналу або досить схоже на нього. При застосуванні функції *f* до початкового повідомлення і наступному перешифруванні його за допомогою функції *g* треба слідкувати, щоб $g \neq f^{-1}$.

1.4.4. Перетворення секретної інформації. Програмне забезпечення, орієнтоване на ЕОМ

Методи шифрування, для реалізації яких треба обчислювати велику кількість випадкових комбінацій, виконуються досить просто і швидко за допомогою ЕОМ. Дослідимо деякі, орієнтовані на ЕОМ, криптографічні методи.

1.4.4.1. Генератори псевдовипадкових чисел

Як можна отримати послідовності елементів ключа? Генератори псевдовипадкових чисел (ГПВЧ) – один з найважливіших криптографічних засобів. Ці алгоритми не тільки генерують послідовності ключів, у яких числа довільно розподілені між 1 і деяким максимальним *m* і генерують всі *m* цих чисел у такій формі, яка виглядає "довільною" до того, як вони почнуть використовувати свій період повторно.

Дійсно, випадкові числа не викликають цікавості, тому що вони не можуть бути легко повторені. Якщо вони використовувалися для шифрування повідомлень, то законний користувач не зможе розшифрувати повідомлення, через те, що він не буде спроможний відтворити ключ шифрування.

Псевдовипадкові числа (ПВЧ) можуть бути відтворені і добре задовольняють потреби користувачів. Проте вибір генератора псевдовипадкових чисел не повинен бути очевидним.

ГПВЧ мають бути відтворюваними, хоча водночас генерують числа, які "здаються випадковими". На основі теорії груп було розроблено кілька типів таких генераторів. Сьогодні найдоступнішими є конгруентні генератори. Визначивши їх, можна зробити математично коректний висновок про те, які властивості мають вихідні сигнали цих генераторів з погляду періодичності та випадковості.

Одним з конгруентних генераторів є лінійний конгруентний ГПВЧ. На основі породжуючого числа T_0 він виробляє послідовність псевдовипадкових чисел $T_1, T_2, \ldots, T_m, \ldots$, використовуючи співвідношення

$$T_{i+1} = (aT_i + c) \bmod m, \qquad (21)$$

де *a* і *c* – константи.

Рівняння (21) генерує ПВЧ з певним періодом повторення, який залежить від вибраних значень *a* і *c*. Значення *m* звичайно беруть таким, що дорівнює 2^b або 2^{b-1}, де *b* – довжина слова в ЕОМ у бітах.

Отримані з рівняння (21) ПВЧ можна використовувати як послідовність, з якої вибираються ключі. Кожен ключ потім об'єднується деяким оборотним способом (наприклад, з використанням логічної операції, виключаючого АБО) з відповідним обсягом тексту.

Отриманий зашифрований текст досить важкий для розкриття, оскільки ключ тепер є змінним. Ключ змінюється випадково для кожного слова тексту. Фактично, якщо період ключа перевищує довжину усіх

посланих повідомлень і якщо жоден вихідний текст не можна викрасти, то шифр теоретично не можна розкрити.

1.4.4.2. Вибір породжуючого числа

Будь-який ГПВЧ може використовувати пароль користувача (файла) або деяку його трансформацію як ініціюючий породжуючий ключ. Отже, кожен користувач (файл) може мати своє власне перетворення секретної інформації, вибране з сім'ї, яка задається рівнянням ГПВЧ.

Для того щоб створити надійний захист від зловмисників при невеликих витратах на систему, послідовність ключа може починатись не раніше, ніж з деякого фіксованого номера *j* з початку циклу. Наприклад, якщо *j*=8, то T_0 (що базується на паролі або імені файла) і $T_1,...,T_7$ будуть генеруватися і відкидатися. В результаті T_8 буде першим елементом послідовності ключа, який реально використовується для шифрування.

Якщо з адміністративних або інших причин бажано використати "непарольне" породжуюче число, воно може бути одержане з ідентифікатора користувача, елементів вихідного тексту, довжини повідомлення або з інших констант.

1.4.4.3. Максимізація довжини послідовності ключа

ГПВЧ мають максимальний період *m* до того, як послідовність почне повторюватись. З причин, про які йшлося раніше, доцільно вибрати *a* і *c* такі, щоб цей період *m* (і, отже, довжина ключа) був максимізований. Доведено, що послідовність (21), де $m = 2^k$ і *k* –ціле число >2, має максимальну довжину *m* тоді, і тільки тоді, коли *c* непарне і $a \bmod 4 = 1$

1.4.5. Методи автентифікації інформації

Автентифікація інформації є життєво важливим питанням для всіх абонентів як комерційних, так і секретних систем зв'язку. Наприклад, особи, які приймають чек, звичайно наполягають на підтвердженні особистості, яка виписала чек – ***автентифікації джерела інформації*** або передавача інформації, а особа, яка виписала чек, проставляє суму не лише цифрами, а й прописом. Крім того, вона може виділити цю частину чека видавлюванням знаків для того, щоб утруднити зловмиснику зміну суми на документі, який має його підпис. Такі найпростіші засоби автентифікації переданої інформації або повідомлення. Цей приклад хоча й ілюструє дві важливі проблеми, з якими стикаються учасники процесу автентифікації інформації, а саме проблему перевірки того, що передача здійснена передбачуваним передавачем, і що інформація не була замінена або змінена, але не розкриває найважливішу характеристику сучасного використання автентифікації. Інформація, транспортована чеком, жорстко пов'язана з фізичним носієм, тобто саме чеком, для якого прийняті протоколи, що встановлюють справжність підпису і цілісність написаного на випадок виникнення згодом суперечок про дійсність чека або справжність підпису, незалежно від змісту записаної на чеку інформації (дата, сума тощо). Тепер найважливіші проблеми автентифікації стосуються ситуацій, за яких відбувається обмін тільки власне інформацією, тобто не існує фізичного носія, який може використовуватись для підтвердження справжності передавача або повідомлення.

Повідомлення, яке позбавлене будь-якого фізичного втілення, подається для автентифікації засобами, які будемо називати ***каналом автентифікації***. Цей канал за визначенням не є безпечним, тобто всі повідомлення,

які через нього передаються, несекретні і можуть бути перехоплені, підмінені або змінені перед тим, як потрапити до пункту призначення.

Обміркуємо спочатку основні принципи, які покладені в основу всіх схем автентифікації. *Автентифікація* – це встановлення санкціонованим одержувачем і, можливо, арбітром того факту, що при існуючому протоколі автентифікації, надіслане повідомлення найімовірніше надіслано санкціонованим передавачем і що воно при цьому не змінене і не спотворене.

У наведеному визначенні мається на увазі, що в будь-якому протоколі автентифікації одержувач буде достовірно отримувати тільки яку-небудь частину можливих повідомлень і що передавач буде використовувати тільки деяку підмножину (можливо, усю) цієї частини при зв'язку з санкціонованим одержувачем. Умови, що визначають множину повідомлень, які приймач може прийняти, а також ту частину цієї множини, яка може використовуватись передавачем, і складають сутність конкретної схеми автентифікації.

У загальноприйнятому в США військовому протоколі автентифікації і передавач, і одержувач мають опечатаний пакет з автентифікатором, який є короткою випадковою послідовністю символів. Ці символи виробляються і розподіляються Агенством Національної безпеки. При автентифікації свого повідомлення передавач розкриває опечатаний пакет, доповнює повідомлення символами автентифікатора і потім шифрує отримане розширене повідомлення, використовуючи криптографічний ключ, який має одержувач. При цьому приєднаний автентифікатор розподіляється по всій довжині отриманого шифртексту. Отриманий шифртекст передається потім як автентифіковане (імітозахищене) повідомлення. Одержувач, після прийняття і розшифрування повідомлення за допомогою своєї копії секретного ключа роздруковує опечатаний текст з автентифікатором і виконує автентифікацію. Повідомлення інтерпретується як справжнє тоді, коли при розшифруванні будуть отримані символи відповідного ідентифікатора. Якщо використовується стійкий криптоалгоритм, то зловмиснику, який не знає секретного ключа, що використовують передавач і одержувач, не залишається нічого іншого, як випадково вибрати шифртекст у надії, що він буде сприйнятий одержувачем як справжній. Якщо автентифікатор містить r бітів інформації, то ймовірність того, що зловмисник обере зашифроване повідомлення і воно буде розшифроване в повідомлення, яке закінчується невідомим йому, але правильним автентифікатором, становитиме лише 2^{-r}.

Передавач і одержувач обмежуються використанням тільки частини загального числа можливих повідомлень, тобто тільки тих повідомлень, які містять надлишкову інформацію. Усі інші повідомлення відхилятимуться одержувачем як помилкові, оскільки передавач не міг їх передавати. Надлишкова інформація тут функціонально не залежить від інформаційного змісту самого повідомлення.

Інший приклад. Інформацію, яка має бути автентифікована, спочатку поділяють на блоки по 64 біти кожен. Перший блок побітно додається за модулем 2 з 64-бітовим початковим вектором, який змінюється кожен день і тримається в секреті в банках даних системи. Отриману суму потім шифрують з використанням секретного ключа алгоритму DES. Отриманий 64-бітовий шифр додають потім за модулем 2 до другого блоку тексту, результат шифрують, отримують другий 64-бітовий шифр тощо. Процедура повторюється, поки не будуть оброблені всі блоки тексту. Очевидно, що останній 64-бітовий шифр є функцією секретного ключа, початкового вектора і кожного біту тексту, незалежно від його довжини. Цей шифр, який зветься ***кодом автентифікації повідомлення*** (КАП), додається до автентифікованої інформації, розширюючи тим самим повідомлення. Отримане розширене повідомлення звичайно передається відкритим, хоча воно може бути і зашифроване, якщо потрібна секретність, але ця операція не залежить від функції автентифікації.

Автентифікатор (КАП) може бути легко перевірений кожним, хто володіє секретним ключем і початковим вектором, повторенням процедури, яку виконав передавач при генеруванні КАП. Стороння особа,

проте, не може ні здійснити генерацію автентифікатора, який міг би сприйнятися одержувачем як справжній, для додання його до фальшивого повідомлення, ні відділити автентифікатор від первісного повідомлення для використання його із зміненим або фальшивим повідомленням. В обох випадках ймовірність того, що фальшиве повідомлення буде інтерпретуватися як справжнє, дорівнює ймовірності "розпізнавання" автентифікатора, тобто, 2^{-64}. Ймовірність вгадування сприйнятого повідомлення, яке пройшло б розглянутий раніше тест, дорівнює 2^{-64}, тобто менше, ніж ймовірність вгадування секретного ключа алгоритму DES, яка дорівнює 2^{-56}.

Термін "автентифікатор" означає додаткову інформацію, яка надається передавачем одержувачу для того, щоб гарантувати правильну інтерпретацію переданого.

1.4.5.1. Практика автентифікації

Раніше ми розглянули ситуацію, коли передавач і одержувач повністю довіряли один одному. Складніший випадок полягає в припущенні, що вони не довіряють один одному або навіть здатні на обман.

Опишемо загальноприйняту комерційну схему автентифікації. Розглянемо вимоги різних учасників системи обробки кредитних карток у пункті продажу. Продавець (автоматичний касовий апарат (АКА) тощо) видає покупцю дещо, що має реальну цінність, тобто деякий товар, гроші, послуги тощо в обмін на деякий запис (інформацію), яка підтверджує платоспроможність останнього. Продавець повинен підозрювати, що покупець не є тим, за кого себе видає, що подана кредитна картка (мандат) є або підробленою, або не належить цьому покупцеві, і що покупець в подальшому відмовиться від того, що робив покупку, або навіть, якщо не заперечуватиме, що робив покупку, стверджуватиме, що сума її менша або покупка була зроблена в інший час тощо. Покупець, у свою чергу, повинен мати можливість переконатися, що запис про зроблену операцію в файлі правильний, що ця сума сплачуватиметься лише один раз, що вона не могла бути завищена і що продавець не зможе надалі, після укладання будь-якої кількості угод з покупцем, видавати себе за нього з метою обманним шляхом зробити покупку, відмінити її тощо за рахунок покупця. Звичайна кредитна операція є класичним прикладом інформаційного обміну між учасниками угод, які не довіряють один одному. Оскільки для прийняття рішення щодо суперечки відносно дійсності зробленої угоди неминуче залучається третя сторона, тобто банк, суд або арбітр, прийняте рішення має відповідати інтересам усіх учасників угоди, і на основі цього рішення має бути логічно визначена сторона, яка повинна нести відповідальність за обман.

Розглянемо, як автентифікація може використовуватися для виконання зазначених вимог на кількох стадіях. Спочатку покажемо, як покупець може бути ідентифікований так, щоб надалі це могло бути перевірено третіми сторонами, які в реальному часі не є учасниками угоди. Для цього можуть бути застосовані два способи. Вибір їх залежить від того, яка ідентифікаційна інформація використовується – внутрішня чи зовнішня. ***Внутрішня інформація*** є сукупністю фізичних ознак індивіда: відбитки пальців, сітківка ока, підпис і (або) динаміка підпису, геометрія руки, зовнішність, зріст, маса, відмітні ознаки тощо. ***Зовнішня інформація*** – це дещо, що має бути відомим законному індивіду: наприклад, паролі доступу до ЕОМ, телефонні номери кредитних карток, номери рахунків відповідних банків, персональні ідентифікаційні номери (PIN), паролі для постів охорони тощо. Для того, щоб мати достатньо стійку схему ідентифікації, що грунтується на зовнішніх ознаках, потрібно створити протокол, який би дав змогу індивіду "довести" , що він знає секретну частину деякої інформації, не розкриваючи всю інформацію, яка могла б допомогти ймовірному зловмиснику видати себе за нього. Схеми ідентифікації залежать від інтерактивних схем, які можна довести і які часто називаються *доведеннями з нульовими знаннями*, у яких індивід відповідає на серію запитань, складених так, що законний користувач може на них відповісти, а зловмиснику зробити це практично неможливо.

Далі ми використовуватимемо добре відомий канал автентифікації, який грунтується на алгоритмі *RSA* як для відкритого (джерело), так і для закритого (покупець) каналу автентифікації. Джерело буде у такий самий спосіб, що і при обчисленні "хорошого" модуля алгоритму *RSA*, вибирати пару простих чисел p і q, обчислювати відповідні показники степеня шифрування-розшифрування, e і d і потім використовувати n і d як відкритий ключ. Джерело буде тримати e (і коефіцієнти p і q) в секреті. Фактично захист системи від нав'язування фальшивих тверджень про справжність не менш надійний, ніж якість захисту, який забезпечує джерело для e.

Центральний пункт і джерело мандатів мають спочатку встановити справжність і точність відповідної інформації для кожного потенційного покупця, потім виробити автентифікаційний запис *ID*, який буде віддаватися покупцеві, як його ***ідентифікаційний мандат***. Він міститиме в собі внутрішню інформацію, яка зашифрована з використанням ключа шифрування двоключової криптосистеми (n і e), а також зовнішні ознаки. Ключі розшифрування мають доставлятися всім продавцям, АКА тощо як автентифіковані, але не обов'язково секретні повідомлення, а ті, в свою чергу, забезпечують цілісність ключа, але не його секретність. Покупець повинен пред'явити зашифрований запис (мандат), який у нього є, і надати можливість обладнанню пункту продажу перевірити його атрибути. Використовуючи ключ розшифрування, продавець спочатку має розшифрувати шифр *ID* і перевірити справжність шифру за надлишковою інформацією. Далі він повинен визначити, чи відповідають тільки що перевірені індивідуальні атрибути розшифрованої інформації внутрішнім атрибутам. Ця інформація міститься в автентифікованому повідомленні. Якщо отримано прийнятну відповідність, особистість покупця буде підтверджена, оскільки шифр міг бути отриманий тільки при використанні секретного ключа шифрування. Зокрема, припускається, що зловмисник не може достатньо точно імітувати внутрішні атрибути інших осіб.

1.4.5.2. Електронний цифровий підпис (ЕЦП)

Автентифікація документів. Безпаперова інформатика дає ряд переваг при обміні документами (наказами, розпорядженнями, листами, постановами тощо) мережею зв'язку або на машинних носіях. У цьому разі витрати часу на роздрукування, пересилання, введення отриманого документа з клавіатури суттєво знижуються. Прискорюється пошук документів. Скорочуються витрати на їх зберігання тощо. Однак при цьому виникає проблема автентифікації автора документа і самого документа (тобто встановлення справжності підпису і відсутності змін в отриманому документі). Ці проблеми у звичайній (паперовій) інформатиці вирішуються за рахунок того, що інформація в документі жорстко пов'язана з фізичним носієм (папером). На машинних носіях такого зв'язку нема.

Проблема автентифікації є актуальною в обчислювальних мережах, електронних системах управління і взагалі там, де треба переконатись у справжності отриманого каналами зв'язку або на машинних носіях повідомлення (документа).

Задачі автентифікації можна поділити на такі типи: автентифікація абонента, автентифікація належності абонента до групи, автентифікація документів, що зберігаються на машинних носіях.

Зупинимося на ***автентифікації документів (або файлів)*** як на найважливішій. Розглядаючи випадок обміну секретними документами (воєнний або дипломатичний зв'язок), з великим ступенем впевненості можна припустити, що обмін здійснюють гідні довіри сторони. Однак можливо, що обмін перебуває під наглядом і управлінням зловмисника, який здатний виконувати складні обчислення і потім або створювати свої власні документи, або перехоплювати і змінювати документи законного джерела. Іншими словами, це випадок, коли захищатись потрібно лише від зловмисника – "свої" підвести не можуть. У комерційному світі справедливим є

майже зворотне твердження, тобто передавач і одержувач, хоча і "свої", але можуть обманювати один одного навіть більшою мірою, ніж сторонні.

У першому випадку ("*свої не обманюють*") схему автентифікації побудувати не важко. Слід забезпечити передаючого і одержуючого абонента надійним шифром і комплектом унікальних ключів для кожного документа, що пересилається, забезпечивши тим самим захищений канал зв'язку. Ця задача висуває високі вимоги до системи шифрування. Так, метод гамірування у цьому разі не підходить, оскільки зловмисник, аналізуючи відкритий і шифрований текст, отримає гаму і зможе нав'язати будь-який потрібний йому текст. Однак існують швидкі алгоритми шифрування, що відповідають цим вимогам.

У другому випадку ("*будь-який з абонентів може обманути*") аналогічний підхід, що грунтується на класичній криптографії, неприйнятний, оскільки є принципова можливість зловмисних дій однієї з сторін, що володіють секретним ключем. Наприклад, приймаюча сторона може згенерувати будь-який документ, зашифрувати його на наявному ключі, спільному для одержувача і передавача, а потім заявити, що він отримав його від законного передавача. Тут слід використовувати схеми, засновані на двохключовій криптографії. У таких випадках у передаючого абонента мережі є свій секретний ключ підпису, а у одержуючого – несекретний відкритий ключ підпису передавача. Цей відкритий ключ можна розглядати як набір перевірочних співвідношень, що дають можливість судити про справжність підпису передаючого абонента, але не дозволяють відновити секретний ключ підпису. Передавач несе одноособову відповідальність за свій секретний ключ. Ніхто, крім нього, не в змозі згенерувати коректний підпис. Секретний ключ передавача можна розглядати як особисту печатку і він повинен всіляко обмежувати доступ до нього сторонніх осіб.

Загальноприйнятою є модель автентифікації, в якій функціонує чотири учасники: *А* – передавач, *В* – одержувач, *С* – зловмисник, *Д* – арбітр. У цьому випадку *А* посилає повідомлення, *В* приймає, *С* намагається скоїти зловмисні дії, а *Д* приймає рішення у спірних випадках, тобто визначає, твердження якої сторони з найбільшою ймовірністю є брехливими. Звичайно, в ролі *С* можуть виступати *А* і *В*. Метою автентифікації є захист від можливих видів зловмисних дій, серед яких виділимо:

1) активне перехоплення – зловмисник, що підключився до мережі, перехоплює документи (файли) і змінює їх;
2) маскарад – абонент *С* посилає документ від імені абонента *А*;
3) ренегатство – абонент *А* заявляє, що не надсилав повідомлення абоненту *В*, хоча насправді надсилав;
4) переробка – абонент *В* змінює документ і стверджує, що цей змінений документ отримав від абонента *А*;
5) підміна – абонент *В* формує новий документ і заявляє, що отримав його від абонента *А*;
6) повтор – абонент *С* повторює раніше переданий документ, який абонент *А* надіслав абоненту *В*.

Ці види зловмисних дій завдають значної шкоди функціонуванню банківських, комерційних структур, державним підприємствам і організаціям, приватним особам, що застосовують у своїй діяльності комп'ютерні інформаційні технології. Крім того, можливість зловмисних дій підриває довіру до комп'ютерної технології. У зв'язку з цим задача автентифікації є дуже важливою.

При виборі алгоритму ***автентифікації повідомлень*** у мережі слід передбачити надійний захист від усіх перелічених раніше видів зловмисних дій. Поряд з такими характеристиками системи автентифікації, як швидкодія і об'єм пам'яті, ступінь захищеності (стійкості) від загроз є дуже важливим параметром.

Технологія застосування електронно-цифрового підпису. Математичні схеми, що використовуються в алгоритмах та реалізують електронний цифровий підпис, грунтуються на односторонніх функціях.

На практиці, як правило, в схемах ЕЦП замість документа x розглядають його хеш-функцію $h(x)$, яка володіє рядом спеціальних властивостей, найважливіша з яких – відсутність "колізій" (тобто практична неможливість створення двох різних документів з однаковим значенням хеш-функції). Найбільш відомі математичні схеми ЕЦП такі: RSA (R.L.Rivest, A.Shamir,L.Adleman), OSS (H.Ong, C.P.Schnorr, A.Shamir), Ель-Гамаля (T.ElGamal), Рабіна (M.Rabin), Окамото-Сараісі (T.Okamoto, A.Shiraishi), Мацумото-Імаі (T.Matsumoto,H.Imai).

Складність задачі підтримки ЕЦП у цих схемах грунтується на обчислювальній складності задач факторизації або дискретного логарифмування. У схемі, запропонованій російським вченим А.А.Грушо (1992р.), її однонаправлена функція, на відміну від перелічених, засновується не на складності теоретико-числових задач, а на складності вирішення систем нелінійних булевих рівнянь.

У прийнятих стандартах США і Росії на ЕЦП (DSS – Digital Signature Standart (FIPS PUB 186), ГОСТ Р34.10-94 і Р34.11-94) використовуються спеціально створені алгоритми. В DSS довжина числа 159-160 біт, у ГОСТ 34.10 – 255-256 біт. В основу цих алгоритмів покладено схеми Ель-Гамаля і Шаміра.

Технологія застосування систем ЕЦП передбачає мережу абонентів, що надсилають один одному електронні документи. Деякі з цих абонентів можуть лише перевіряти підписані іншими повідомлення, інші (назвемо їх абонентами з правом підпису) можуть як перевіряти, так і самостійно підписувати повідомлення. Крім того, можуть бути випадки, коли будь-хто може ставити свій ЕЦП лише як другий підпис після підпису визначеного абонента – начальника (наприклад, директор – бухгалтер).

Далі можливі дві ситуації: або у цій мережі є центр (призначено абонента, що наділений деякими особливими повноваженнями), або всі абоненти з правом підпису рівноправні. Не виключений, однак, і варіант, при якому функції центра розосереджені по кількох локальних центрах. Мережі з центрами можуть бути класифіковані за ступенем довіри абонентів до центру. Інакше кажучи, мережі можуть бути "тоталітарними" і "демократичними". Центри в таких мережах можуть потенційно або повністю контролювати абонента або ж виконувати суто формальні функції адміністрування, скажімо, з приймання в мережу нових абонентів.

Архітектура алгоритмів ЕЦП. Оскільки підпис під важливим документом може мати далекосяжні наслідки, перед підписанням слід передбачити відповідні запобіжні заходи. У разі програмної реалізації, як правило, секретний ключ того, хто підписує, зберігається на його особистій дискеті, захищеній від копіювання. Однак цього буває недостатньо, адже дискету можуть вкрасти або загубити. Отже, потрібен захист від несанкціонованого доступу до секретної інформації (ключа). Природнім рішенням цієї проблеми є парольний захист. Паролем можуть закриватись не лише функції постановки ЕЦП і генерації ключів, але й функції, що змінюють зміст каталогу відкритих ключів абонентів мережі тощо.

Слід перевірити (у разі програмної реалізації, зокрема на ПЕОМ), щоб в системі не було *"криптовірусів*", які можуть завдати суттєвої шкоди. Наприклад, у момент підписування криптовіруси можуть перехопити секретні ключі та скопіювати їх у потрібне місце. Крім того, при перевірці підпису вони можуть змусити систему "сказати", що підпис правильний, хоча насправді він таким не є. Можна уявити собі криптовірус, який, потрапивши в систему лише один раз у момент генерації ключів, "допоможе" системі згенерувати "слабкі" ключі. Наприклад, якщо ключі генеруються на основі датчика псевдовипадкових чисел, який використовує вбудований таймер, вірус може змінити покази таймера, а потім відновити "статус-кво". Ці ключі можуть бути легко відкриті зловмисниками. Надалі цей вірус уже не потрібний. Проти таких криптовірусів є лише один захист – завантаження з чистої системної дискети і використання чистого, "рідного" програмного продукту.

Проставлення і перевірка підпису. Для того, щоб поставити ЕЦП під конкретним документом, треба виконати досить великий обсяг обчислювальної роботи. Ці обчислення розбивають на два етапи: генерація ключів і підпис документу.

Генерація ключів. На цьому етапі для кожного абонента генерується пара ключів: секретний і відкритий. Секретний ключ зберігається абонентом в таємниці і використовується для формування підпису. Відкритий ключ відомий усім іншим користувачам мережі та призначений для перевірки підпису.

Природнім є варіант, коли генерацію ключів абонент може здійснити самостійно. Не виключено, однак, що у певних ситуаціях цю функцію слід передати центру, який вироблятиме пару "секретний – відкритий ключі" для кожного абонента і займатиметься розповсюдженням їх. Цей варіант має ряд переваг адміністративного характеру, однак володіє принциповим недоліком – у абонента нема гарантії, що його особистий секретний ключ є унікальним. Іншими словами, можна сказати, що тут всі абоненти знаходяться під контролем центру, який може підробити будь-який підпис.

Підпис документа. Передусім документ "стискають" до кількох десятків чи сотень байтів за допомогою хеш-функції. Тут термін "стиск" зовсім не аналогічний терміну "архівація", значення хеш-функції тільки складно залежить від документа, але не дає змоги відновити сам документ. Ця хеш-функція має задовольняти ряд умов, а саме:

бути чутливою до всіх можливих змін у тексті, таких, як вставки, вилучення, перестановки тощо;

володіти властивістю необерненості, тобто задача підбору документа, який мав би потрібне значенням хеш-функції обчислювально нездійсненна.

Ймовірність того, що значення хеш-функцій двох різних документів (незалежно від їхньої довжини) збігатимуться, має бути досить незначною.

Тепер розглянемо, які загрози стають можливими, якщо знехтувати хоч би однією з перелічених раніше умов. До отриманого значення хеш-функції застосовують те чи інше математичне перетворення (залежно від обраного алгоритму ЕЦП) і отримують власне підпис документа. Цей підпис може мати можливий для прочитання, " літерний" вигляд, але досить часто його подають у вигляді послідовності довільних символів, що "не читаються". ЕЦП може зберігатися разом з документом, наприклад, на його початку чи наприкінці або в окремому файлі. Природно, що в останньому разі при перевірці підпису треба володіти як самим документом, так і файлом, що містить його підпис.

Перевірка підпису. При перевірці підпису перевіряючий повинен володіти відкритим ключем абонента, що поставив підпис. Цей ключ має бути автентифікованим, тобто перевіряючий повинен бути цілком впевненим, що цей відкритий ключ відповідає тому абоненту, який видає себе за його власника. У разі, коли абоненти обмінюються ключами, ця впевненість може підтверджуватися зв'язком телефоном, особистим контактом або у будь-який інший спосіб. Якщо ж абоненти діють у мережі з виділеним центром, відкриті ключі абонентів підписує (сертифікує) центр, і безпосередній контакт абонентів між собою (при передаванні або підтвердженні справжності ключів) замінюють на контакт кожного з них з центром.

Процедура перевірки ЕЦП складається з двох етапів: обчислення хеш-функції документа і власне математичних обчислень, передбачених у цьому алгоритмі підпису. Останні полягають у перевірці того чи іншого співвідношення, що пов'язує хеш-функцію документа, підпис під ним і відкритий ключ абонента, що підписує. Якщо розглянуте співвідношення виконане, підпис визнають достовірним, а сам документ – справжнім, у протилежному випадку документ розглядають як змінений, а підпис під ним – недійсний.

Користувацькі критерії ЕЦП. Користувачів цікавлять не математичні тонкощі різних схем, а якості, якими мають володіти програмні (або апаратні) комплекси, які здійснюють функції ЕЦП. Найважливіше

значення тут мають криптостійкість і швидкість роботи. Менш важливими можна вважати функціональні можливості та зручність користувача.

Криптостійкість цифрового підпису має бути досить трудомісткою для підробки її будь-якою особою, яка не має доступу до секретного ключа того, хто підписує (як для стороннього, так і для учасника цієї мережі). Трудомісткість не повинна залежати від кількості підписаних документів, перехоплених зловмисником, і на неї не має впливати можливість зловмисника створювати документи "на підпис" відправника. Зокрема комплекс повинен забезпечувати також захист від несанкціонованого доступу до секретного зразка підпису, що зберігається.

Під *швидкістю роботи* розуміють, по-перше, швидкість операції "проставлення підпису", по-друге, швидкість операції "перевірка підпису", по-третє, швидкість операції "генерація ключа підпису".

Крипкостійкість визначається перш за все використаним для створення цифрового підпису криптоалгоритмом з відкритим ключем. Крім того, принципово важливим є правильний вибір хеш-функції та системи захисту програмного комплексу від несанкціонованого доступу. Швидкість роботи залежить передусім від швидкісних якостей криптоалгоритму, що реалізує цифровий підпис. Як правило, чим вища криптостійкість використовуваної схеми цифрового підпису, тим нижчі її швидкісні характеристики. Дуже важливим є вибір алгоритмів багаторозрядної арифметики, що використовуються для обчислення за обраним криптоалгоритмом цифрового підпису, швидкість обчислення хеш-функції, а також тип використовуваного комп'ютера. Для комп'ютерних мереж суттєвим параметром може виявитися довжина підпису. У тих випадках, коли файл, що передається, (наприклад, команда) малий, а кількість таких файлів відносно велика, довжина підпису може вплинути на швидкість обміну інформацією.

Напади на ЕЦП можна класифікувати так:

за видами – найпростіші (підробка, переробка, повтор) і більш тонкі (підбір повідомлення, що подається на "підпис" відправнику, напад на відкритий каталог перевіряючого);

за наслідками (або на одне повідомлення, або на всі повідомлення цього абонента, або на всі повідомлення всіх абонентів у мережі);

за можливостями зловмисника (можливість мати доступ до каналу зв'язку відправник – отримувач, до комп'ютера отримувача, до комп'ютера відправника або брати участь у розробці системи підпису);

за ресурсами, необхідними зловмиснику (за часовими ресурсами – підписана інформація передається в режимі реального часу і застаріває миттєво, або вона зберігається довгі роки і практично не старіє; за ресурсами ЕОМ – порушник має ПЕОМ або ЕОМ типу CRAY).

Розглянута модель автентифікації є досить абстрактною. Оскільки життя завжди різноманітніше у своїх проявах, існують деякі досить "хитрі" види нападів, які важко передбачити теоретично. Зупинимося на трьох різновидах їх.

"Лобові" напади. Так можна назвати найпримітивніші напади, від яких всі в основному і захищаються. Вважається, що зловмисник знає алгоритм поставлення підпису і обчислення хеш-функції та має сильні обчислювальні ресурси.

Напади, в яких бере участь ваша секретарка. Припустімо, що документи вам на підпис готує секретарка, яка (свідомо чи ні) працює в інтересах ваших зловмисників. Останні формували документ, про який ви не підозрюєте і який не маєте бажання підписувати (наприклад, який-небудь дарчий папір від вашого імені). Тепер їм потрібно, щоб під цим документом стояв ваш підпис. Як це зробити? Можна запропонувати спосіб підбору документа з потрібною хеш-функцією. Припустімо, ви дали вказівки секретарці сформувати черговий потрібний документ. Вона передає його зловмисникам, і вони видозмінюють його так, щоб документ,

з однієї сторони, зберіг потрібний зміст, а з іншої – значення хеш-функції для нього збіглося б зі значенням хеш-функції для документа, який сформовано вашими зловмисниками (дарчою). Далі ви підписуєте видозмінений документ, а зловмисники використовують ваш підпис під ним. Ваш підпис можна "відрізати" і "приклеїти" до іншого документа, і якщо значення хеш-функції нового документа збігатиметься зі значенням хеш-функції старого документа, то при перевірці підпису новий документ (дарчу) визнають справжнім.

Ця видозміна може бути зроблена так, що ви ні про що не здогадаєтесь, оскільки, наприклад, поява зайвого пропуску ніяк не позначиться на змісті документа, але може разюче змінити його хеш-функцію. Робота зловмисників для здійснення такого нападу може тривати досить довго (багато місяців). При цьому вони будуть намагатися видозмінити черговий документ, що готується вам на підпис. Якщо цей проміжок часу помножити на швидкодію комп'ютерів, що є у розпорядженні зловмисника, то цифра буде досить значною. Крім того, для розв′язування задач такого типу існує суто алгоритмічний прийом, який в англомовній літературі називають "методом зустрічі посередині". Сутність його полягає в тому, що під одне значення хеш-функції можна "підганяти" одночасно два документи, той, який ви підпишете, і той, до якого ваш підпис потім "приклеять".

Описаний напад з криптографічної точки зору є нападом на хеш-функцію, хоча власне алгоритм з відкритим ключем, що реалізує схему підпису, може бути як завгодно стійким. Факт існування пари документів з однаковим значенням хеш-функції в англомовній літературі прийнято називати "колізією". Для того щоб протистояти описаним нападам, які можна назвати нападами, що грунтуються на підборі підписуваних документів, хеш-функція вибраної схеми підпису має задовольняти жорсткі криптографічні вимоги. В останні роки в англомовній криптографічній літературі значна увага приділяється аналізу хеш-функцій. У деяких хеш-функціях, що здавалися раніше цілком надійними, наприклад SNEFRU, виявлено слабкі місця саме з точки зору описаних нападів.

З погляду можливих наслідків описаний напад є найбільш "вразливим" з усіх можливих, оскільки в розпорядженні зловмисника є лише один підроблений документ. Для підробки інших підписаних вами документів йому знову потрібна значна обчислювальна робота.

Далі, знайомство з секретаркою може виявитись на руку зловмисникам, якщо для підроблення вашого підпису їм будуть потрібні додаткові дані. Кожен документ, який ви підписуєте, може бути підготовлений зловмисниками так, щоб отримати потрібні математичні рівняння відносно невідомих біт секретного ключа вашого підпису.

Напад на перевіряючого. Попередній приклад показує, що для отримання фальшивого документа зловмиснику необов'язково "зламати" секретний ключ підпису. Для досягнення своїх цілей зловмисник може взагалі не вступати в контакт з особою, підпис якої він хоче підробити, і не вдаватися до "злому". Можуть бути застосовані напади на перевіряючу сторону.

Припустімо, що у мережі немає центру, і кожен абонент зберігає на своєму комп'ютері каталог відкритих ключів усіх тих, від кого він може одержати повідомлення. Ця ситуація є цілком реальною і тоді, коли в мережі є центр і кожне підписане повідомлення супроводжується сертифікатом, тобто ще одним повідомленням, підписаним центром, в якому містяться ім'я і відкритий ключ відправника. В останньому випадку, виходячи з витрат часу, найбільш вигідно не перевіряти кожен раз підпис центру на сертифікаті, а робити це лише перший раз, при появі нового абонента. Коли надходить наступне повідомлення цього абонента, можна порівняти цей сертифікат з тим, який зберігається в каталозі і для якого підпис центру уже перевірений.

Зловмисник, якщо, він має хоча б короткочасний доступ до комп'ютера перевіряючого, може просто змінити відповідні записи в каталозі, записавши замість свого прізвища ваше. Якщо тепер він надішле повідомлення, підписане ним, то програма перевірки на комп'ютері із зміненим каталогом покаже, що це повідомлення підписане вами. Певну вигоду від такої операції зловмисник матиме, і вона може виявитися більшою, ніж витрати на неї. Слід зазначити, що необхідність підтримки каталогу відкритих ключів (введення нових абонентів або нових ключів у старих абонентів, знищення ключів абонентів, що вийшли з мережі, перевірка строків дії ключів і сертифікатів, нарешті, переповнення каталогу) створює передумови для нападу, що розглядається.

Звернемо увагу, що описаний напад на каталог відкритих ключів можливий інколи і у тих випадках, коли інформація у ньому зашифрована. (Це може здатися неймовірним навіть для спеціалістів!). Наприклад, у каталозі в зашифрованому вигляді зберігаються відкриті ключі абонентів, причому шифрування здійснено так, що для закриття кожного запису використовується один і той же шифр, нехай дуже стійкий, наприклад, ГОСТ 28147-89 у режимі простої заміни (на одному і тому ж ключі). Такий спосіб шифрування цілком придатний. Він зручний при введенні нових і редагуванні старих записів. Однак зловмиснику для здійснення описаного нападу не обов'язково "зламувати" шифр. Він може просто поміняти місцями шифровані записи відкритих ключів, свого і вашого, залишивши при цьому незмінними решту даних.

Напади, що розглядаються, можна класифікувати за ступенем шкоди, що завдається зловмисником. Найтяжчі для мережі з виділеним центром наслідки має напад, при якому зловмисник може підробляти підпис центру. Це означає, що він може виступати як будь-який абонент мережі, виготовляючи відповідні сертифікати. Далі, якщо порушник зміг "зламати" (або викрасти) секретні ключі якогось абонента, то, очевидно, він може підписати будь-яке повідомлення від імені цього абонента. Нарешті, можливі напади, коли зловмисник може підписати лише одне складене ним повідомлення від імені цього абонента.

Для здійснення своїх планів зловмисник може вдатися до таких заходів:

у певний спосіб заволодіти зразками документів, підписаних його потенційною "жертвою";

готувати "на підпис" документи для "жертви" і використовувати поставлені під ним справжні підписи у своїх цілях;

отримати доступ до комп'ютера абонента, підпис якого він хоче підробити (тут потрібно розрізняти дві ситуації: зловмисник може або змінити програму підпису, наприклад "посадити" криптовірус, або використати якусь інформацію, що стосується цієї програми);

отримати доступ до комп'ютера перевіряючого абонента з тим, щоб змінити програму перевірки підпису у своїх цілях;

виявитися розробником програмного комплексу (іншими словами, в систему закладено потенційні слабкості).

Більша частина розглянутих нападів має сенс лише у тому разі, коли зловмиснику відомі алгоритми обчислення і перевірки підпису, а також алгоритм обчислення хеш-функції. Як правило, в комерційних програмних продуктах ці алгоритми не афішуються, обумовлюється лише метод цифрового підпису (наприклад, RSA, Ель-Гамаля тощо). Більш того, як правило, такі програми захищені від копіювання. Однак, як відомо, якщо існують алгоритми шифрування з гарантованою стійкістю, то говорити про існування алгоритмів захисту від копіювання "з гарантованою стійкістю" не доводиться. Це означає, що кваліфікований зловмисник в принципі може "зняти" захист і мати всю необхідну для власного криптографічного аналізу інформацію. Підкреслимо, що мова йде саме про кваліфікованого зловмисника, у розпорядженні якого є необхідна техніка і достатньо часу. Підсумовуючи викладене, можна зробити такі висновки.

Якщо користувач суворо дотримується норм секретності (зберігання секретних ключів підпису, робота з "чистим" програмним продуктом, що виконує функції підпису) і тим самим виключає можливість викрадення ключів або несанкціонованих змін даних і програм, то стійкість системи підпису визначається винятково криптографічними якостями. Якщо ці умови не виконуються повною мірою, то задача підробки підпису може бути розв′язана. Однак зловмисник повинен мати для цього значні обчислювальні ресурси і високу кваліфікацію як криптоаналітик.

Для виконання більшості з перелічених зловмисних дій потрібні значні обчислювальні ресурси. Важко собі уявити приватну фірму, у розпорядженні якої були б такі ресурси.

Запис і зберігання секретних ключів на жорстких дисках не рекомендується, навіть якщо ваш комп'ютер встановлено в приміщенні, що охороняється. Адже існує велика ймовірність, що зловмисник скористається ними для отримання доступу до вашої інформації та зможе підробити дані, що завдасть вам або вашим клієнтам багато неприємностей. Це стосується не тільки комп'ютерів, якими користуються в різний час кілька людей, а й серверів з вузловими комп'ютерами, ключ з диску яких зловмисник може прочитати, звернувшись до них з мережі.

Отже, існують проблеми, пов'язані з розв′язанням задачі забезпечення надійності ЕЦП.

Слід зазначити, що під стандартом на підпис розуміють лише стандарт на криптографічний алгоритм. Багато досить суттєвих деталей у стандарті не обумовлено (наприклад, способи розповсюдження відкритих ключів, генерації псевдовипадкових чисел тощо). Це може призвести до того, що різні засоби, які здійснюють функцію цифрового підпису (кожна з них за стандартом!), виявляться несумісними між собою.

Можна бути цілком впевненим, що алгоритм із стандарту ГОСТ Р34.10-94 має високу криптографічну стійкість, і більшість з описаних нападів не є для нього небезпечними. Однак користувач має бути переконаний, що його підпис ніхто підробити не зможе, і якщо програма визначила, що якесь повідомлення підписав А.Б.Іванов, то його насправді підписав А.Б.Іванов, і він не зможе від цього відмовитись.

Для досягнення цієї мети слід виконати ряд вимог, однією з яких є криптографічна стійкість алгоритму підпису (саме це і забезпечує стандарт). Прикладами інших вимог є збереження в таємниці секретного ключа підписуючого і забезпечення справжності його відкритого ключа.

Гарантією надійності може бути сертифікація продукту. Сертифікація – це процес, в результаті якого підтверджується відповідність вимогам стандарту. Однак специфіка в цьому випадку полягає в тому, що стандарт прийнято на "Процедуру вироблення і перевірки електронного цифрового підпису", а сертифікується засіб, що реалізує цю процедуру.

При сертифікації слід перевіряти не тільки відповідність вимогам стандарту, а й ряду інших вимог (надійність, відсутність закладок, якість протоколів тощо). Зрозуміло, що робота з сертифікації потребує найвищої кваліфікації, є досить відповідальною і трудомісткою, а тому і тривалою.

У США, наприклад, процес сертифікації займає більше року. Тут потрібно вибирати між надійними сертифікованими і більш сучасними (але які ще не пройшли сертифікацію, а отже і менш надійними) засобами, що реалізують функцію ЕЦП. У зв'язку з тривалістю процесу сертифікації може виникнути ситуація, коли на ринку засобів, що реалізують процедуру виготовлення і перевірки ЕЦП, виявиться невеликий вибір. Це поставить користувачів перед необхідністю купувати не дуже зручний засіб або платити надмірно високу ціну.

Цифровий підпис "Нотаріус". "Нотаріус" – бібліотека програм цифрового підпису і перевірки справжності електронних документів. Вона дає можливість укладати угоди, підписувати контракти, здійснювати платежі, використовуючи персональний комп'ютер і модем [41].

Електронні документи, оформлені “Нотаріусом”, зберігають юридичну силу і не потребують паперових копій. Схема взаємодії двох партнерів-користувачів за допомогою цифрового підпису “Нотаріус”, наведена на рис.3, не потребує особливих пояснень.

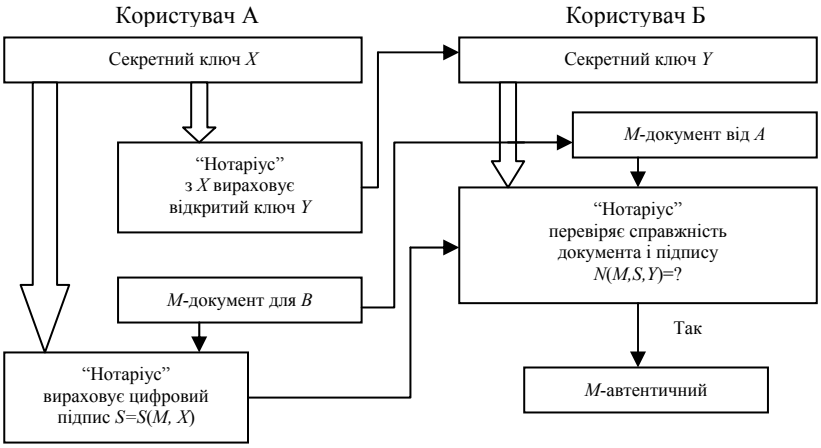

Рис.3. Схема електронного підпису “Нотаріус”

У цифрових підписах реалізуються алгоритми стандартів: ГОСТ Р34.10-94, DES, фірмові алгоритми “ЛАН Крипто”.

Кожен алгоритм бібліотеки “Нотаріус” гарантує стійкість цифрового підпису не менше ніж 10^{20}. Для підробки підпису потрібно більше ніж 250 років роботи суперкомп’ютера потужністю 100 млрд.операцій/с. Швидкодію алгоритмів наведено в табл.1.

Таблиця 1

Час роботи програм підписування / перевірки, с

Тип процесора	Для файлів, кбайт		
	1	10	100
i386SX (33)	0.118/0.245	0.165/0.292	0.641/0.767
i486DX2 (66)	0.052/0.111	0.068/0.126	0.217/0.275
i486DX4 (100)	0.014/0.027	0.024/0.038	0.124/0.138

Використання ЕЦП значно розширює і без того багаті можливості електронної пошти, телефаксу, телексу тощо.

1.4.6. Високошвидкісна арифметика для багатослівних чисел

Внаслідок значного прогресу в створенні алгоритмів факторизації чисел за роки існування криптографії з відкритим ключем, розмір чисел, які використовуються в RSA, постійно зростав. Спочатку мова йшла про стозначні десяткові числа. Вважалось, що стозначні десяткові числа (322 біти) в найближчому майбутньому будуть нерозкладними і що криптографічні системи з більшими модулями на обчислювальній техніці працюють досить повільно. Сьогодні стозначні десяткові числа знаходяться в межах досяжності, і ніхто не говорить про модулі, менші за 512 біт, а то й 1024 біти. Часто згадуються не менш, ніж двохсотзначні десяткові числа: американська корпорація “Cylink” виробляє інтегральні схеми на 1024 біти. Якщо збільшення розмірів модулів викликане досягненнями в розв’язанні задачі розкладання на множники, то успіх корпорації

“Cylink” став можливим завдяки досягненням при виконанні арифметичних операцій над багатослівними числами.

Операція піднесення до степеня, яка використовується при шифруванні, розшифруванні та виконанні допоміжної операції по заготівлі ключів, потребує найбільше обчислень. Причому кожна операція піднесення до степеня виконується за допомогою операції множення. Найменша кількість операцій для піднесення числа до степеня досягається при використанні повторюваного піднесення до квадрату.

Час виконання операції множення на процесорі з фіксованою довжиною слова пропорційний квадрату довжини операндів $O(k^2)$. Якщо ж спеціально для цього сконструювати послідовно паралельне апаратне забезпечення, то цей час може бути зменшений до $O(k)$. У цьому разі потрібна кількість логічних елементів буде пропорційна довжині операндів $O(k)$. Час роботи самих швидкодіючих реалізацій пропорційний $O(\log k)$, але вони потребують порядку $O(k^2)$ логічних елементів.

Тестування алгоритмів і програм багатослівної арифметики для ПЕОМ показує, що ефективними для операцій множення є алгоритми і програми, побудовані на ідеях Карацуби і Шонхаге, Штрассена; для отримання лишку і піднесення до степеня – алгоритми Баррета, Комби і алгоритми з використанням добутку Монтгомері [50].

1.4.7. Методи багаторівневої криптографії

Розглянемо нову парадигму криптографії з секретним ключем, яка може бути корисна при розв’язанні проблем, пов’язаних з експортним (і, можливо, державним) контролем. Як загальну назву використовують термін “багаторівнева криптографія”, оскільки припускається, що криптосистема у межах цієї парадигми може забезпечувати різні рівні секретності. При цьому криптосистема не використовує схему з депонуванням ключів. Різні рівні секретності забезпечуються за рахунок обчислювальної складності алгоритму криптографічного перетворення.

Звернемося спочатку до класичної задачі побудови компромісного рішення для експортної криптографії – обмеження довжини ключа. Стандартний підхід полягає у використанні криптосистеми з фіксованою або змінною довжиною ключа при чітко встановленій згідно з експортними обмеженнями довжині ключа. Типовим є обмеження довжини ключа до 40 бітів.

Такі чіткі обмеження роблять систему вразливою. У зв′язку з цим виникає серйозна проблема – якщо 40 бітів ключа недостатньо для забезпечення належного рівня секретності, то яка має бути “правильна” довжина ключа для криптосистеми з експортними обмеженнями? Під “правильною” мається на увазі довжина ключа, що одночасно задовольняє суперечливі вимоги як національної, так і комерційної безпеки.

Важлива обставина полягає у розумінні суттєвої різниці у витратах при атаці на окремий конкретно взятий шифртекст і множину різних шифртекстів (за умови, що шифрування виконується на різних ключах).

Проблема, пов’язана з основним підходом до експортного контролю через обмеження довжини ключа, пов′язана з тим, що вимоги комерційної безпеки встановлюють таку довжину ключа, при якій витрати на “силову” атаку наближаються до типових можливостей відповідної державної служби, тоді як вимоги самої такої служби спрямовані на обмеження ключового простору з метою мінімізації необхідних витрат.

Принципи багаторівневої криптографії. Ідея вирішення поставленої задачі полягає в тому, що витрати на “силову” атаку при розкритті першого ключа і всіх наступних відрізняються. З обчислювальної точки зору обсяг перебору (перший рівень складності), який потрібно виконати для розкриття першого ключа перевищує обсяг перебору (другий рівень складності) для розкриття будь-якого наступного ключа. Розкриття

першого ключа дає криптоаналітику додаткову інформацію про структуру ключового простору, і всі наступні ключі можуть бути розкриті з меншими витратами.

Конструктивна особливість криптосистем полягає у спеціальному структурованому методі побудови ключів. Так, довільно вибравши початковий ключ певної довжини, користувач обмежується у виборі всіх наступних ключів.

Багаторівнева криптографія подібна до методу "часткового депонування ключів". Основна розбіжність пов'язана з заміною схеми депонування ключів на алгоритмічні методи заданої обчислювальної складності.

Розробка параметричних криптосистем є одним з можливих шляхів розвитку методів багаторівневої криптографії. Наприклад, параметри можуть бути вибрані так, що для розкриття ключів другого рівня складності потрібно розкрити не один, а кілька ключів першого рівня складності. Можливий також варіант криптосистеми з великою кількістю рівнів складності.

Зазначимо, що у разі застосування багаторівневої криптосистеми всередині групи користувачів, розкриття ключа першого рівня складності одного з користувачів не дає змоги розкрити ключі другого рівня складності інших користувачів цієї групи. Це означає, що криптосистема містить множину секретних параметрів, які вибираються користувачами на початковому етапі. Вибраний одного разу параметр не може бути замінений в подальшому. Отже, розкриття одного чи кількох ключів першого рівня складності дає змогу встановити секретний параметр користувача. Очевидно, що будь-яка атака зводиться до розкриття унікального ключа (ключів) першого рівня складності конкретного користувача, оскільки ключі побудовані з застосуванням різних (унікальних) секретних параметрів багаторівневої криптосистеми.

У найпростішому випадку користувач випадково вибирає перший секретний ключ *K:*

$$K=(K_0, K_1).$$

Компоненти K_0 і K_1 є послідовностями n_0 і n_1 двійкових символів (бітів) відповідно. Позначимо загальну довжину ключа *K* як $n = n_0 + n_1$. Усі наступні ключі вибираються аналогічно. Однак побудова їх має бути узгоджена з компонентою K_1. Отже, вибравши перший ключ, користувач встановлює чітку залежність всіх наступних ключів від K_1, тобто n_1 останніх бітів останнього ключа будуть містити компоненту K_1. Назвемо введене обмеження багаторівневим. Вибираючи n =68 *і* n_0 =48 (відповідно, n_1=20), користувач задає параметр багаторівневої криптосистеми "68/48". Назвемо компоненту K_0 короткочасним ключем, або короткочасним ключовим сегментом, а K_1 – довгочасним ключем, або довгочасним ключовим сегментом. Відповідно, ключ *K* складається з короткочасного і довгочасного ключових сегментів. Зазначимо, що компонента K_1 не є відкритою, а є фіксованим секретним параметром, що вибирається користувачем.

Обсяг перебору при "силовій" атаці становить 2^n ключів, оскільки для розкриття ключа першого рівня складності криптоаналітик зловмисника повинен розкрити обидва ключові сегменти K_0 і K_1. Трудомісткість (обсяг перебору) розкриття наступних ключів другого рівня складності складатиме 2^{n_0}, через те, що зусилля криптоаналітика зводяться до визначення короткочасного ключового сегмента K_0.

Цей метод відкриває шлях до досягнення компромісу при узгодженні вимог комерційної та національної безпеки. Вибір двох параметрів (n і n_0) на відміну від одного n_0 дає можливість приймати гнучкі рішення і задовольняти суперечливі вимоги усіх сторін. Хоча службі безпеки доведеться докласти значних зусиль для розкриття *n*-бітного ключа, основна робота зведеться до пошуку n_0-бітного ключа.

Програмна реалізація багаторівневої криптосистеми не може вважатися абсолютно надійною, адже її стратегічні параметри можуть змінитися в результат атаки з боку зловмисника.

Розглянемо один із способів побудови програмної реалізації механізму багаторівневого обмеження.

Метод на основі цифрового підпису. Зміст методу полягає в тому, що криптосистема адекватно сприймає лише підписані копії довгочасних ключів (та інших секретних параметрів). Підпис параметрів виконується або виробником криптосистеми, або відповідним підрозділом експортної служби. Для перевірки підпису розповсюджуване програмне забезпечення повинно містити копію відкритого ключа служби, що підписала параметри криптосистеми. Отже, режим функціонування програмного забезпечення буде визначатися наявністю підпису під довгочасним ключем K_1 (якщо ключ не підписаний, видається попередження або встановлюється $K_1 = 0$).

Користувач може звернутися до підрозділу експортної служби з метою отримання будь-якого необхідного завіреного цифровим підписом електронного документа (який містить ключ K_1 або інший параметр). Користувач повинен довіряти тим, від кого отримує завірені підписом електронні документи.

Підписаний довгостроковий ключ інсталюється в програмне забезпечення і встановлює багаторівневі обмеження в криптосистемі користувача.

Важлива вимога багаторівневої криптографії полягає в тому, що служба, яка виконує підпис довгострокового ключа, не повинна знати, що вона підписує. У разі, коли така вимога є нереальною, багаторівнева криптосистема може бути ефективно замінена схемою з депонуванням ключів [51] або з "напівпрозорою криптографією" [43]. Є два стандартних методи такого підпису.

1. **Хеш-функція**. Користувач передає службі значення $H(R)$, де H – відповідна хеш-функція, а R – випадкове число. Служба підписує значення $H(R)$ і повертає користувачу. Програмне забезпечення користувача для виявлення підміни перевіряє справжність отриманого від служби значення $H(R)$ (заново обчислюючи значення хеш-функції від R і порівнюючи результати) і потім перевіряє підпис. У разі отримання позитивних результатів усіх перевірок користувач як довгостроковий ключ K_1 вибирає n_1 молодших бітів з випадкового числа R.
2. **"Сліпий" (RSA) підпис**. Як і в першому випадку, вибирається відповідна хеш-функція. Потім користувач випадково вибирає "осліплюючий" параметр (число) b і передає службі на підпис результат обчислення $H(R)b^e \pmod n$, де (n,e) – відкритий RSA-ключ служби. У відповідь користувач отримує підпис $(H(R)b^e)^{1/e}$. Поділивши прийняте значення на b, користувач отримує підпис $H(R)^{1/e}$ від $H(R)$. Аналогічно, як довгостроковий ключ вибирається n_1 молодших бітів з випадкового числа R.

Застосування хеш-функції робить задачу отримання R з $H(R)$ обчислювально трудомісткою. У разі застосування "сліпого" підпису визначення $H(R)$ із $H(R)b^e$ неможливе з теоретико-інформаційних міркувань, оскільки для довільного $H(R)$ існує таке b, що обчислення $H(R)b^e$ дає змогу отримати підпис $H(R)$. Скориставшись "сліпим" методом, можна запропонувати на підпис будь-яку інформацію, яка гарантовано не буде розкрита стороною, що підписує документ.

Обчислення значення хеш-функції в "сліпому" методі може бути пропущене, тобто замість підписування $H(R)$ може безпосередньо підписуватися ключ K_1. Проте з підписами $H(R)$ працювати надійніше, ніж з підписами K_1, оскільки для зберігання ключів та підписів може використовуватися різна за рівнем захищеності пам'ять.

Додаткова особливість методу на базі підпису полягає в тому, що підписуюча служба може контролювати число використовуваних ключів K_1 (не зважаючи на те, що ключі невідомі), а також встановлювати, ким вони використовуються.

1.4.8. Основи комп'ютерної стеганографії

Стеганографія (від грецького "тайнопис") має багатовікову історію і за віком суттєво старша за криптографію.

Розглянемо порівняно нові напрями розповсюдження стеганографічних традицій – комп'ютерні технології.

Як відомо, мета криптографії полягає у приховуванні змісту секретних повідомлень. Стеганографія йде принципово далі: її мета – приховати сам факт існування повідомлення. Такі приховані повідомлення можуть включатися в різноманітні зовнішні "невинні" дані і передаватися разом з ними без будь-якої підозри збоку.

Не слід розглядати стеганографію і криптографію як альтернативу одна одній – скоріше це дві сторони однієї медалі. І не лише тому, що ефективність їх тільки зростає від спільного використання, а й у зв'язку з тим, що в їх основі лежить загальна методична та інструментальна база.

Базові принципи комп'ютерної стеганографії такі.

1. Захист має грунтуватися на припущенні, що зловмисник має повне уявлення про стеганографічну систему та деталі її реалізації. Єдиною інформацією, яка залишається невідомою потенційному зловмиснику, є ключ, за допомогою якого лише його власник може встановити факт присутності та зміст прихованого повідомлення.
2. Якщо зловмисник якимось чином дізнається про факт існування прихованого повідомлення, це не повинно дозволити йому довести цей факт третій особі і тим більше виявити подібні повідомлення в інших даних доти, поки ключ зберігається в таємниці.
3. Потенційний зловмисник повинен бути позбавлений будь-яких технічних та інших переваг у розпізнаванні або розкритті змісту таємного повідомлення.

Розглянемо кілька методів приховування повідомлень у цифрових сигнатурах та інших добре визначених, але малоінформативних компонентах цифрового зв'язку, які сьогодні є вже досить поширеними.

Приховування даних у цифрових комунікаціях. Левова частка комп'ютерної інформації "шумить" (наявність помилок у даних, завад та інших випадкових сигналів у каналах зв'язку).

Шум є практично в будь-якому масиві результатів вимірювань, графічному образі, звуковому файлі тощо. Практичні алгоритми стеганографії якраз і засновані на ідеї заміни за певними законами шумових компонент інформації початковим текстом.

Називатимемо таку інформацію, що "шумить" і призначена для приховування таємних повідомлень, **контейнером**, а біти, що "шумлять", – **бітами контейнера**. Біти контейнера, замінені бітами приховуваного повідомлення, дістали назву **прихованих бітів**. Дані контейнера мають бути досить "шумними", щоб невеликі зміни в їх безладді не могли стати помітними. Такий метод відомий як **сурогатна стеганографія**.

Елементи контейнера звичайно є найменш значущими бітами деяких заздалегідь неточних значень і хоча є шумом з точки зору точності вимірювань, можуть мати деякі спеціальні статистичні характеристики.

Припускається, що кодування прихованого повідомлення має відтворювати характеристики шуму контейнера, що є важко досяжною, але реальною метою. Одна з можливостей полягає в генерації великої кількості альтернативних контейнерів, для того щоб вибрати з них найбільш придатний для зберігання таємного коду. Такий підхід називається **селектуючою стеганографією**. Єдина пов'язана з ним проблема

полягає в тому, що навіть оптимально організований, він дає змогу приховати незначну кількість даних при дуже великій обчислювальній роботі. Ще один варіант – моделювання характеристик шуму контейнера. Наслідувана функція має бути побудована так, щоб не тільки кодувати приховувані повідомлення, а й дотримуватися моделі початкового шуму. У граничному випадку ціле повідомлення може конструюватися згідно з моделлю шуму. Подібний підхід можна назвати **конструюючою стеганографією**. Така стратегія має ряд недоліків: її проблематично з'єднати з сильним алгоритмом шифрування, а моделювання шуму – заняття не з легких. Більше того, реальні зразки, створенні на основі цієї моделі, іноді можуть навіть сприяти виявленню таємного повідомлення замість того, щоб збільшувати його безпеку. Якщо зловмисник знає модель, він може з малими витратами знаходити в ній вразливі місця. А оскільки модель шуму при такому підході – це частина приховуючого алгоритму, то ми маємо справу з порушенням правил хорошого тону в криптографічній практиці, що рано чи пізно може стати причиною витоку інформації.

Оскільки спроби наслідування початкового шуму ведуть або до сумнівної безпеки, або до дуже малого діапазону робочих частот для більшості застосувань, то найпривабливішою залишається така базова процедура.

Вибирають клас досить "шумних" контейнерів та ідентифікують біти шуму. Потім наближено визначають, яку порцію шумових бітів контейнера можна замінити псевдовипадковими даними без значної зміни його статистичних характеристик.

Наприклад, якщо контейнер є цифровою фотографією, нас мають цікавити молодші біти сірої шкали або RGB-значень при кольоровому зображенні або коефіцієнти Фур'є в JPEG-форматі стиснутих зображень. У разі видозміни, скажімо, кожного сотого пікселя зображення, один мегабайт нестиснутого зображення може приховати приблизно 1 кілобайт секретних даних.

Типи контейнерів і вибір приховуючих бітів. Контейнери можуть бути потоком неперервних даних, подібно до цифрового телефонного зв'язку (**потокові контейнери**), або файл, подібно растровому зображенню (**контейнери випадкового доступу**).

Про потоковий контейнер не можна попередньо сказати, коли він почнеться, коли закінчиться і наскільки довгим буде. Більше того, об'єктивно немає можливості дізнатися заздалегідь, якими будуть наступні шумові біти. Це призводить до необхідності включати приховуючі повідомлення до потоку в реальному масштабі часу. Приховуючі біти мають вибиратися за допомогою спеціального генератора, який задає відстань між послідовними бітами в потоці. Такий спосіб називають **довільно-інтервальним методом** приховування бітових виборок.

У неперервному потоці даних найскладніше для одержувача – визначити, коли розпочинається приховане повідомлення. Тут не може бути жодної видимої синхронізуючої послідовності. Якщо потік даних має деякі властиві йому сигнали синхронізації або межі пакету, приховане повідомлення розпочинається одразу після одного з них. У цьому разі одержувач повинен намагатися синхронізувати свій генератор випадкових чисел з прихованим повідомленням одразу після таких сигналів.

У найбільш легкому випадку, якщо потік даних має кінцеву тривалість і часто відкривається знову, подібно до телефонних переговорів, таємне повідомлення може завжди починатися з відкриттям сеансу. Для відправника можливі проблеми, якщо він не впевнений у тому, що потік контейнера буде достатньо довгим для розміщення цілого таємного повідомлення. У потокових контейнерах також важко рівномірно розподілити приховуючі біти по всьому потоку.

Файли фіксованої довжини позбавлені розглянутих недоліків потокових контейнерів. Відправник знає заздалегідь розмір файла та його зміст. Приховуючі біти можуть бути рівномірно вибрані з підходящої

псевдовипадкової функції. Головний недолік контейнерів довільного доступу полягає у тому, що їхній розмір часто набагато менший, ніж у потокових, а тому їх інколи важко скоригувати згідно з реальними потребами.

Оскільки контейнер випадкового доступу відомий до використання, він може бути оцінений на ефективність щодо обраного алгоритму приховання інформації.

Слід зазначити, що популярний метод випадкового інтервалу не дуже зручний для контейнерів з довільним доступом. Передусім рівномірний розподіл приховуючих бітів досягається у ймовірнісному змісті. Інакше кажучи, неможливо знати заздалегідь, чи поміститься повідомлення в контейнер. Через це користувачу доводиться самостійно визначати середній інтервал між бітами так, щоб вони розміщувалися всередині файлу.

Інший недолік полягає в тому, що відстань між приховуючими бітами рівномірно розподілена між найкоротшими та найдовшими заданими відстанями, в той час як справжній випадковий шум матиме експоненціальний розподіл довжин інтервалів.

Звичайно, можна згенерувати псевдовипадкові експоненціально розподілені випадкові числа, але цей шлях, як правило, дуже трудомісткий.

Висновки. Можливість ефективного приховування інформації в комп'ютерних системах і мережах має різні практичні наслідки. Не зважаючи на молодість комп'ютерної стеганографії, вже сьогодні будь-який тип даних може бути прихований і переміщений невидимо у місця, де відбувається передача або зберігання великих обсягів "шумних" даних.

Створюючи певні зручності для збереження таємниці, стеганографія одночасно створює умови для виникнення масових неконтрольованих соціально небезпечних каналів. Це є, зокрема, викликом воєнній інформаційній структурі, яка невідворотно має відреагувати на методи стеганографії новим проривом у технологіях інформаційної безпеки. Неспроможність проконтролювати типи переміщених даних справляє глибокий вплив на комерційне використання мереж, що може вплинути на структуру цін на мережеві ресурси. Стеганографія – привабливий засіб для діяльності хакерів.

Стеганографічні програми.

1. *Steganos v.1.4.* – програма, яка може приховувати інформацію, використовуючи стеганографічні методи, і шифрувати її за допомогою технології криптографії. Призначена для роботи в середовищі DOS.

Дає можливість приховувати всі види файлів у графічних файлах формату BMP, у звукових файлах формату WAV і VOC, текстових ASCII. Може не вилучати файл "повідомлення" і створювати резервну копію файла "контейнера". Отриманий в результаті цього перетворення файл формату BMP можна перевести в інші графічні формати, не руйнуючи структуру зображення, наприклад, GIF, і зворотно без втрати закодованої інформації.

2. *Steganos for Windows 95* (Version 1.0a) – програмне забезпечення, що працює в середовищі Windows і поєднує в собі технології криптографії та стеганографії, є "нащадком" Steganos v.1.4.

Дає змогу приховувати всі види файлів у графічних файлах формату BMP і DIB (при цьому краще працювати з 24-бітовим зображенням), звукових файлах формату WAV і VOC, текстових ASPII і HTML. Може не знищувати файл "повідомлення" і створювати резервну копію файла "контейнера".

3. *Hideseek v.5* – програма, що працює під DOS. Може приховувати файл "повідомлення" лише у графічних файлах GIF, а найбільше розширення екрану, з яким вона може працювати, – 320*480 пікселів.

4. *Hideseek v.1.1 for Windows 95* – нова версія Hideseek v.5 для DOS. Приховує файл "повідомлення" лише у графічних файлах формату BMP (256 кольорів).

5. *Hide 4PGP v.1.0* – програма, призначена для роботи в середовищі DOS. Може приховувати всі види файлів у графічних файлах формату BMP (256-кольорове або 24-бітне зображення не повинно бути стиснутим) і звукових файлах формату WAV і VOC.
6. *PGE v.1.0* – програма, що також працює в середовищі DOS. Може приховувати всі види файлів у графічних файлах формату GIF (87,89) і JPG (JFIF).
7. *S-Tools v.4 for Windows* – програмний засіб, що дає можливість приховувати всі види файлів у графічних файлах формату BMP і GIF і звукових файлах формату WAV.

При роботі створює новий файл з закодованою інформацією. Має багатовіконний режим роботи і може одночасно кодувати кілька файлів. Використовує кілька стеганографічних алгоритмів, і користувач може вибрати найбільш придатний.

8. *White Noise Storm*^{TM} – призначений для роботи в середовищі DOS. Може приховувати всі види файлів у графічних файлах формату BMP і GIF і звукових файлах формату VOC.

У ході тестування найпереконливіші результати продемонстрували Steganos for Windows 95 і S-Tools v.4.

РОЗДІЛ 2

БЕЗПЕКА ЕЛЕКТРОННИХ БАНКІВСЬКИХ СИСТЕМ

Банкір одним розчерком пера може вкрасти в 10 разів більше, ніж 10 озброєних грабіжників-нападників.

(Дон Карлеоне)

При створенні більшості автоматизованих систем обробки даних (АСОД) виникає необхідність розв'язувати дві досить суперечливі задачі.

Задача перша полягає в тому, щоб створити АСОД з мінімальною вартістю. Вартість створення подібних систем практично найчастіше пропорційна ступеню використання колективних ресурсів. Це означає, що з метою мінімізації вартості АСОД доцільно створювати колективний ресурс для всіх її користувачів – юридичних і фізичних осіб (банківських установ, підприємств, фірм, компаній, корпорацій), включаючи засоби зберігання інформації, програмні та апаратні засоби її обробки і доступу до інших засобів і систем. Вдало вибрані організація і можливість колективного ресурсу значно знижують вартість створення і експлуатації АСОД при реалізації заданих вимог до її функціонування.

Проте зберігання і обробка інформації з використанням можливостей колективного ресурсу не означає, що кожному користувачу АСОД доступні ці можливості. Доступність визначається правилами (вимогами), що формулюються при створенні АСОД. Саме ці правила, а точніше, дотримання їх при поділі користувачів АСОД на окремі класи і зумовлюють необхідність розв'язання другої задачі, а саме про використання кожним кінцевим користувачем доступного тільки йому ресурсу, включаючи інформацію.

Зрозуміло, що повсюдна індивідуалізація ресурсу для кожного користувача АСОД є оптимальним рішенням для другої задачі, однак значною мірою збільшує вартість створення і експлуатації АСОД. Саме в цьому розумінні цільові установки першої та другої задач суперечать одна одній.

Використання в АСОД ПЕОМ, а також включення до складу їх локальних обчислювальних мереж і підключення до глобальних мереж ускладнили постановку другої задачі: необхідно забезпечити збереження інформації як в пам'яті ПЕОМ так і на носіях, гарантувати достовірність передачі інформації каналами зв'язку, забезпечити ідентифікацію отриманої інформації тощо.

Методи і засоби, які лежать в основі розв'язання другої задачі, а також інші проблеми становлять далеко не повний перелік під загальною назвою "забезпечення безпеки комп'ютерних систем".

З розвитком і розширенням сфери застосування засобів обчислювальної техніки гострота забезпечення безпеки обчислювальних систем і захисту інформації від різних загроз зростає. Для цього є ряд об'єктивних причин.

Головна з них – зростання рівня довіри до АСОІ. Їм довіряють найвідповідальнішу роботу, від якості якої залежить життя і добробут багатьох людей. ЕОМ управляють технологічними процесами на підприємствах і атомних електростанціях, рухом літаків і поїздів, виконують фінансові операції, обробляють секретну інформацію.

Сьогодні проблема захисту обчислювальних систем набуває ще більшого значення у зв'язку з розвитком і розповсюдженням мереж ЕОМ. Розподілені системи і системи з віддаленим доступом висунули на перший план питання захисту інформації, яка передається.

Доступність засобів обчислювальної техніки, і передусім ПЕОМ, призвела до розповсюдження комп'ютерної грамотності в широких колах населення. Це в свою чергу викликало численні спроби втручання в роботу державних і комерційних систем, як зі злим наміром, так із "чисто спортивного інтересу". Багато з цих спроб мали успіх і завдали значної шкоди власникам інформації та обчислювальних систем.

Цілісну картину всіх можливостей захисту створити досить важко, оскільки ще немає єдиної теорії захищених систем. Існує багато підходів і точок зору щодо методології побудови їх. Докладається багато зусиль як у практичному, так і в теоретичному плані, використовуються останні досягнення науки, передові технології. Займаються цими проблемами провідні фірми з виробництва комп'ютерів і програмних забезпечень, провідні університети та інститути.

Відомі різні варіанти захисту – від охоронця на вході до математично вивірених засобів захисту даних. Крім того, можна говорити про глобальний захист та його окремі аспекти: захист ПЕОМ, мереж, баз даних тощо.

Слід зазначити, що абсолютно захищених систем немає. Можна говорити про захист та надійність системи, по-перше, тільки з певною ймовірністю, а по-друге, про захист від певної категорії зловмисників. Захист – це змагання оборони та нападу: хто більше знає та передбачає – той і виграє.

Попри незручності, що заподіюються користувачеві під час роботи, в багатьох випадках засоби захисту можуть бути абсолютно необхідними для нормального функціонування системи. До основних із наведених незручностей потрібно віднести такі:

1. Допоміжні труднощі роботи з більшістю захищених систем.
2. Збільшення вартості захищеної системи.
3. Додаткове навантаження на системні ресурси, що потребує збільшення робочого часу для виконання одного й того ж завдання у зв'язку з уповільненням доступу до даних та виконанням операцій в цілому.
4. Необхідність залучення допоміжного персоналу, який відповідає за підтримку працездатності системи захисту.

Що стосується необхідності застосування захисту, то тут принцип "поки грім не гримне, мужик не перехреститься" абсолютно себе не виправдовує. Часом на карту поставлено надто багато. Інформація може мати занадто велику цінність, щоб нею ризикувати.

Надійний захист АСОІ абсолютно необхідний банкам та іншим великим фінансовим організаціям. Більше того, їм потрібний ретельно спланований та постійно підтримуваний захист. Це зумовлено такими чинниками.

1. Інформація, що зберігається та обробляється в банківських системах, є реальними грошима; на основі інформації комп'ютера можуть здійснюватися платежі, відкриватися кредити, переводитися значні суми. Цілком зрозуміло, що незаконна маніпуляція з такою інформацією може призвести до серйозних збитків.
2. Інформація в банківських системах зачіпає інтереси великої кількості людей та організацій – клієнтів банку. Як правило, вона конфіденційна, і банк несе відповідальність за забезпечення потрібного ступеню секретності перед своїми клієнтами. Природно, клієнти мають право очікувати, що банк має потурбуватися про їхні інтереси, інакше він ризикує своєю репутацією.

Комп'ютер на столі банківського працівника вже давно перетворився з іграшки на звичний та необхідний інструмент. Зв'язок комп'ютерів між собою та з більш потужними комп'ютерами і з ЕОМ інших банків – також необхідна умова успішної діяльності банків (надзвичайно велика кількість операцій, які потрібно виконати протягом короткого періоду часу).

Водночас інформаційні системи стають однією з найвразливіших сторін діяльності сучасного банку, притягуючи до себе зловмисників, як з числа персоналу банку, так і зі сторони. Оцінки збитків від злочинів, пов'язаних з втручанням у діяльність інформаційної системи банків, дуже відрізняються – від 170 млн до 41 млрд. дол. щороку. Середня банківська крадіжка із застосуванням електронних засобів становить приблизно 9

000 дол., а один з найгучніших скандалів пов'язаний із спробою вкрасти 700 млн.дол. (Перший національний банк, Чікаго).

Так потрібно чи не потрібно захищати свої системи? Якщо потрібно, то як? Від кого і від чого? Скільки це коштуватиме? Який це дасть зиск? Як вести себе в критичних ситуаціях?

Багато з пропонованих рекомендацій можуть здатися достатньо очевидними. Проте подані системно та належним чином обгрунтовані вони допоможуть захистити АСОІ.

2.1. Методологія захисту автоматизованих систем обробки інформації (АСОІ)

2.1.1. Безпека АСОІ. Основні уявлення.

Під безпекою АСОІ розуміють здатність протидіяти спробам завдання шкоди її власникам та користувачам при здійсненні різних (навмисних чи ненавмисних) дій на неї.

Безпека АСОІ досягається забезпеченням конфіденційності інформації, що нею обробляється, а також цілісності та доступності компонентів і ресурсів системи.

Конфіденційність – це властивість інформації бути відомою тільки допущеним та тим, які пройшли перевірку (авторизованим) суб'єктам системи (користувачам, програмам, процесам тощо). Для інших суб'єктів системи – ця інформація є закритою.

Цілісність компонента (ресурсу) системи – властивість його бути незмінним (у семантичному розумінні) при функціонуванні системи.

Доступність компонента (ресурсу) системи – властивість його бути доступним для використання авторизованими суб'єктами системи в будь-який час.

Звичайно питання про необхідність захисту комп'ютерної системи не викликає сумнівів. Гарячі дискусії розгортаються при відповідях на такі запитання:

1. Від чого треба захищати систему?
2. Що треба захищати в самій системі?
3. Як треба захищати систему (з допомогою яких методів і засобів)?

Розрізняють зовнішню та внутрішню безпеку АСОІ. **Зовнішня безпека** передбачає захист АСОІ від стихійних лих та від проникнення зловмисників з-зовні з метою розкрадання, одержання доступу до носіїв інформації чи виведення системи з ладу. Предметом **внутрішньої безпеки** є забезпечення надійної та коректної роботи системи, цілісності її програм та даних.

Усі зусилля щодо забезпечення внутрішньої безпеки АСОІ зосереджуються на створенні надійних і зручних механізмів регламентації діяльності всіх її користувачів і обслуговуючого персоналу, дотриманні встановленої в організації дисципліни – прямого або непрямого доступу до ресурсів системи та до інформації.

2.1.1.1. Два підходи до забезпечення безпеки АСОІ

Відомі два підходи до забезпечення безпеки АСОІ – "фрагментарний" і комплексний.

"Фрагментарний" підхід орієнтується на протидію суворо визначеним погрозам за певних умов. Прикладами реалізації такого підходу є, наприклад, спеціалізовані антивірусні засоби, окремі засоби реєстрації та управління, автономні засоби шифрування тощо. Головна особливість "фрагментарного" підходу – відсутність єдиного захищеного середовища обробки інформації.

Перевагою “фрагментарного” підходу є його висока вибірковість щодо конкретної погрози, яка зумовлює також основний його недолік – локальність дії. Навіть невелика зміна погрози призводить до втрати ефективності захисту. Поширити дію таких заходів на всю АСОІ практично неможливо.

Особливістю ***комплексного підходу*** є створення захищеного середовища обробки інформації в АСОІ, яка об’єднує різні заходи протидії погрозам (правові, організаційні, програмно-технічні). Захищене середовище обробки інформації формується на основі розроблених для конкретної АСОІ правил обробки критичної інформації.

Організація захищеного середовища обробки інформації дає змогу гарантувати (в межах розробленої політики безпеки) рівень безпеки АСОІ.

Комплексний підхід застосовують для захисту великих АСОІ або невеликих АСОІ, які обробляють інформацію, що дорого коштує, чи виконують відповідальні завдання.

2.1.1.2. Етапи побудови системи захисту АСОІ

Система захисту АСОІ – це сукупність правових та морально-етичних норм, організаційних, адміністративних і програмно-технічних засобів, спрямованих на протидію загрозам АСОІ з метою зведення до мінімуму можливих втрат користувачів та власників системи.

Етап аналізу можливих погроз АСОІ потрібний для фіксування на певний момент часу стану АСОІ (конфігурації апаратних та програмних засобів, технології обробки інформації) і визначення можливих дій на кожний компонент системи. Із всієї множини можливих дій треба вибрати лише ті, які можуть реально відбутися та завдати значної шкоди користувачам і власникам системи.

Головні етапи побудови системи захисту подано на рис.4:

Рис.4. Схема побудови системи захисту

На етапі планування формується система захисту як єдина сукупність заходів протидії різної природи.

Відомо не так багато універсальних способів захисту АСОІ від різних впливів на неї. Ними є:

ідентифікація і автентифікація суб’єктів АСОІ;

контроль доступу до ресурсів АСОІ;

реєстрація і аналіз подій, що відбуваються в АСОІ;

контроль цілісності об’єктів АСОІ;

шифрування даних;

резервування ресурсів і компонентів АСОІ.

Ці універсальні способи можуть застосовуватись у різних варіаціях та сукупностях в конкретних методах та засобах захисту.

Результатом етапу планування є ***план захисту*** – документ, який містить перелік захищених компонентів АСОІ і можливого впливу на них, вартість захисту інформації в АСОІ, правила обробки інформації в АСОІ, що забезпечують захист її від різних взаємодій, а також опис розробленої системи захисту інформації.

Сутність етапу реалізації системи захисту інформації полягає в налагодженні та розробленні засобів захисту, необхідних для реалізації зафіксованих в плані захисту правил обробки інформації.

Сформувались два основних способи реалізації механізмів захисту.

1. "Доданий" захист, де засоби захисту – це доповнення до основних програмних та апаратних засобів АСОІ. Подібного підходу в забезпеченні безпеки дотримується, наприклад, фірма IBM.
2. "Вбудований" захист, який полягає в тому, що механізми захисту є невід'ємною частиною АСОІ, розробленою та реалізованою з урахуванням певних вимог безпеки. Механізми захисту можуть бути реалізовані у вигляді окремих компонентів АСОІ і розподілені по інших компонентах системи. При цьому засоби захисту становлять єдиний механізм, який відповідає за забезпечення безпеки всієї АСОІ. Цей спосіб використовувався компанією DEC при розробці системи VAX/VMS.

Обидва описані способи мають свої переваги і недоліки. "Доданий" захист більш гнучкий, його механізм можна додавати або вилучати в міру необхідності. У тому разі, коли "додані" засоби захисту не підтримуються "вбудованими" механізмами АСОІ, вони не забезпечать необхідного рівня безпеки.

Основна перевага "вбудованого" захисту – надійність та оптимальність. Засоби захисту розроблялись та реалізовувались одночасно з самою АСОІ. Проте "вбудований" захист має жорстко фіксований набір функцій, не даючи змоги розширювати чи скорочувати його. Деякі функції можна тільки відключити.

Обидва засоби захисту в чистому вигляді зустрічаються рідко. Як правило, використовуються їхні комбінації, що дає змогу об'єднувати переваги та компенсувати недоліки кожного з них.

Комплексний захист АСОІ можна реалізувати як з допомогою "доданого", так і "вбудованого" захисту. Забезпечення захисту АСОІ – це ітеративний процес, що закінчується тільки з завершенням життєвого циклу всієї системи.

2.1.2. Загроза безпеці АСОІ

У 1988 р. втрати від комп'ютерних злочинів досягли 555 млн.дол., 930 років робочого часу і 15,3 року машинного часу [53]. За іншими оцінками [46], втрати фінансових організацій становлять від 173 млн.дол. до 41 млрд.дол. на рік.

2.1.2.1. Класифікація загроз безпеці АСОІ

Загроза безпеці – це потенційно можливий вплив на АСОІ, який може прямо чи опосередковано завдати шкоди користувачам або власникам АСОІ.

Реалізацію загрози надалі назвемо ***атакою***.

Загрози безпеці можна класифікувати за такими 9 ознаками:

1. *За метою реалізації загрози*:

порушення конфіденційності інформації;

порушення цілісності інформації (втрати від таких дій можуть бути набагато більшими, ніж при порушенні конфіденційності);

порушення (часткове чи повне) працездатності АСОІ (порушення доступності).

Відмова в обслуговуванні може суттєво вплинути на роботу користувача.

2. *За принципом впливу на АСОІ*:

з використанням доступу суб'єкта системи (користувача, процесу) до об'єкта (файла даних, каналу зв'язку тощо);

з використанням прихованих каналів.

Доступ – це взаємодія між суб'єктом і об'єктом, яка призводить до виникнення інформаційного потоку від другого до першого.

Під **прихованим каналом** розуміється шлях передачі інформації, який дає змогу двом взаємодіючим процесам обмінюватися інформацією таким способом, що порушує системну політику безпеки.

Вплив, заснований на першому принципі, простіший, більш інформаційний, але від нього легше захиститись. Вплив на основі другого принципу відрізняється трудністю організації, меншою інформаційністю, складністю виявлення і усунення.

3. *За характером впливу на АСОІ*: розрізняють активну і пасивну загрози.

Активна загроза веде до зміни стану системи і може здійснюватись або з використанням доступу (наприклад, до набору даних), або як з використанням доступу, так і з використанням прихованих каналів.

Пасивна загроза здійснюється шляхом спостереження користувачем будь-яких побічних ефектів (наприклад, від роботи програми) та їх аналіз. Прикладом пасивного впливу може бути прослуховування лінії зв'язку між двома вузлами мережі. Пасивний вплив не веде до зміни стану системи. Він завжди пов'язаний тільки з порушенням конфіденційності інформації в АСОІ.

4. *За причиною використовуваної помилки захисту*.

Така помилка може бути зумовлена однією з таких причин:

неадекватністю політики безпеки реальній АСОІ;

помилками адміністративного управління, під якими розуміють некоректну реалізацію або підтримку прийнятої політики безпеки АСОІ;

помилками в алгоритмах, у зв'язках між ними тощо, які виникають на етапі проектування програми або комплексу програм, у зв′язку з чим їх можна використовувати зовсім не так, як це описано в документації;

помилками реалізації алгоритмів (помилками кодування), зв'язками між ними тощо, які виникають на етапі реалізації або відлагодження і які також можуть бути джерелом недокументованості.

5. *За способом впливу на об'єкт атаки* (при активному впливі):

безпосередній вплив на об'єкт атаки, таким діям звичайно легко запобігти з допомогою засобів контролю доступу;

вплив на систему дозволу (в тому числі загарбання привілеїв);

опосередкований вплив (через інших користувачів);

"маскарад", у цьому разі користувач присвоює собі повноваження іншого користувача, видаючи себе за нього;

"користувач наосліп", коли один користувач змушує іншого виконувати необхідні дії, причому останній про них може і не підозрювати; для цього може використовуватись вірус (він виконує необхідні дії та повідомляє тому, хто його впровадив, про результат).

6. *За способом впливу на АСОІ*:

в інтерактивному режимі;

в пакетному режимі.

7. *За об'єктом атаки*.

Впливам можуть піддаватися такі компоненти АСОІ:

АСОІ в цілому (проникнення в систему), для цього, як правило, використовують метод "маскараду", перехоплення або підробки пароля, "злом" або доступ до АСОІ через мережу;

об'єкти АСОІ – дані або програми, самі пристрої системи, канали передачі даних;

суб'єкти АСОІ – процеси і підпроцеси користувачів, частим випадком такого впливу є введення зловмисником вірусу в середовище другого процесу і його виконання від імені цього процесу;

канали передачі даних – пакети даних, які передаються каналами зв'язку і власне канали, прослуховування каналу і аналіз графіка (потоку повідомлень, підміна або модифікація повідомлень у каналах зв'язку і на вузлах-ретрансляторах, зміна топології та характеристик мережі).

8. *За використовуваними засобами атаки* (можна використовувати або стандартне програмне забезпечення, або спеціально розроблені програми).
9. *За станом об'єкта атаки*. Об'єкт атаки може знаходитись в одному із трьох станів:

збереження – вплив на об'єкт, як правило, здійснюється з використанням доступу;

передачі – вплив передбачає або доступ до фрагментів інформації, що передається, або просто прослуховування з використанням прихованих каналів;

обробки – об'єктом атаки є процес користувача.

2.1.2.2. Характеристика найпоширеніших загроз безпеці АСОІ ***Несанкціонований доступ*** *(НСД)*

НСД полягає в отриманні користувачем доступу до об'єкта, на який у нього немає дозволу відповідно до прийнятої в організації політики безпеки. Є два способи реалізації НСД:

перебороти систему захисту, тобто різноманітними впливами зупинити її дію;

поспостерігати за тим, що "погано лежить", тобто які набори даних цінні для зловмисника, відкриті для доступу по недогляду або наміру адміністратора.

У більшості випадків НСД стає можливим через непродуманий вибір засобів захисту, некоректну установку і налагодження їх, а також при неуважному ставленні до захисту своїх особистих даних.

Незаконне використання привілеїв. Зловмисники, використовуючи цей спосіб атаки, як правило, використовують штатне програмне забезпечення. Практично кожна система захисту містить засоби, які використовуються в надзвичайних ситуаціях, або такі, що можуть функціонувати з порушенням існуючої політики безпеки.

Для того щоб зменшити ризик від застосування подібних засобів, більшість систем захисту реалізує такі функції з допомогою набору привілеїв – для виконання певної функції потрібен певний привілей. У такому разі кожен користувач отримує свій набір привілеїв, звичайні користувачі – мінімальний, адміністративні – максимальний (відповідно до принципу мінімуму привілеїв). Несанкціоноване захоплення привілеїв призведе до можливості несанкціонованого виконання певної функції.

Незаконне захоплення привілеїв можливе або при наявності помилок у самій системі захисту, або через халатність при управлінні системою і привілеями.

Атаки "салямі" ("С"). Ці атаки є найхарактернішими для систем, що обробляють грошові рахунки. Принцип атаки "С" побудований на тому факті, що при обробці рахунків використовують цілі одиниці (гривні, копійки), а при нарахуванні відсотків нерідко отримують дробові.

Якщо користувач має доступ до банківських рахунків або програм їх обробки, він може заокруглити суму в інший бік, а різницю в ній записати на свій рахунок. Власник рахунку навряд чи помітить це, а якщо і

помітить, то спише її на похибку обробки і не надасть цьому жодного значення. Якщо зловмисник обробляє 10 000 рахунків за день, то його денний прибуток становить 100 дол. в день, тобто близько 30 000 дол. на рік. Отже, атаки "С" небезпечні в основному для великих банків та інших фінансових організацій.

Причинами атаки "С" є, по-перше, похибки заокруглення, а по-друге, великі обсяги обчислень. Перешкодити таким атакам можна лише забезпечивши цілісність і коректність прикладних програм з обробки рахунків, розмежовуючи доступ користувачів АСОІ до рахунків, а також здійснюючи постійний контроль рахунків.

"Приховані канали" ("ПК") – шляхи передачі інформації між процесами системи, які порушують системну політику безпеки.

"ПК" можуть бути реалізовані різними шляхами, наприклад, за допомогою програмних закладок ("троянських коней").

Атаки з використанням "ПК", як правило, призводять до порушення конфіденційності інформації в АСОІ. За характером впливу вони є пасивними: порушення полягає тільки в передачі інформації. "ПК" можуть бути: кількість пропусків між двома словами, значення будь-якої фіксованої цифри після коми тощо, а також передача інформації про присутність або відсутність певного набору даних, його розмір, дата створення або модифікації.

"***Маскарад***" ("М") – виконання будь-яких дій одним користувачем АСОІ від імені іншого користувача. При цьому другому користувачеві ці дії можуть бути дозволені. Порушення полягає у присвоєнні прав та привілеїв. "М" – це спосіб активного порушення захисту системи. "М", як правило, передує злам системи або перехоплення пароля. Найбільш небезпечний "М" у банківських системах електронних платежів, де помилкова ідентифікація клієнта може призвести до великих збитків.

Для запобігання "М" слід використовувати надійні методи ідентифікації та автентифікації, блокування спроб зламу системи, контроль входу в неї.

"***Збирання сміття***" ("ЗС"). Після закінчення роботи оброблена інформація не завжди повністю знищується в пам'яті ЕОМ. Хоча при спотворенні заголовку файла її прочитати важко, однак, використовуючи спеціальні програми і обладнання, все ж можна. Такий процес дістав назву "Збирання сміття". Він може призвести до витоку важливої інформації.

"ЗС" – активний безпосередній вплив на об'єкт АСОІ з використанням доступу. Для захисту від "ЗС" застосовують спеціальні механізми, які можуть бути реалізовані в ОС або в додаткових програмних засобах.

Прикладами таких механізмів є стираючий взірець і мітка повноти.

"***Злам системи***" ("ЗЛС") – це зумисне проникнення в систему з несанкціонованими параметрами входу, тобто його іменем і його паролем.

"ЗЛС" – навмисний активний вплив на систему в цілому. Основне навантаження по захисту системи від "зламу" несе програма входу. Протистояти "ЗЛС" можна також обмеженням кількості спроб необхідного введення пароля з подальшим блокуванням терміналу та повідомлення оператора у разі порушення.

"***Люки***" ("Л") – прихована, недокументована точка входу в програмний модуль. "Л" уставляють в програму, як правило, на етапі відладки для полегшення роботи: цей модуль можна викликати з різних місць, що дає змогу відладжувати його окремі частини незалежно. Крім того, "Л" може уставлятись на етапі розробки для подальшого зв'язку цього модуля з іншими модулями системи.

Наявність "Л" дає змогу викликати програму нестандартним шляхом, що може серйозно відбитися на стані системи захисту. "Л" належить до категорії загроз, що виникають у випадку помилок реалізації проекту. "Л" можуть з'явитися у програмах з таких причин:

їх забули забрати;

для використання при подальшому налагодження;

для забезпечення підтримки готової програми;

для реалізації таємного контролю доступу до цієї програми після її встановлення.

Велика небезпека “Л”, особливо в програмах операційної системи, пов′язана також з високою складністю їх виявлення. Є лише один захист від “Л”– не допускати появи їх у програмі.

“***Шкідливі програми***” (“ШП”) – програми, які прямо чи непрямо дезорганізують процес обробки інформації чи сприяють її витоку чи спотворенню.

“***Троянський кінь***” (“ТК”) – програма, яка виконує в доповнення до основних (проектних та документованих) додаткові, але не описані в документах, дії. “ТК” належить до активних загроз, що реалізуються програмними засобами. Вона може загрожувати будь-якому об’єкту АСОІ. Найбільш небезпечним є опосередкований вплив, коли “ТК” діє в рамках повноважень одного, але в інтересах іншого користувача, встановити особу якого часто неможливо. “ТК” може спрацьовувати при надходженні деякої умови (дати, часу тощо) або за командою ззовні. Той, хто запустив таку програму, наражає на небезпеку як себе і свої файли, так і всю АСОІ.

Найбільш небезпечні дії “ТК” може виконувати в тому разі, коли користувач, що впровадив її, має поширений набір привілеїв. “ТК” – одна з найнебезпечніших загроз безпеці АСОІ. Радикальним засобом захисту від цієї загрози є створення замкненого середовища виконання програм.

“Вірус” (“В”) – програма, яка може заражати інші програми, включаючи до них свої, можливо модифіковані, копії. Причому останні зберігають здатність до подальшого розмноження.

“В” можна охарактеризувати двома основними особливостями:

здатністю до самовідтворення, ця властивість означає, що за час свого існування на комп’ютері вірус має хоча б один раз відтворити свою копію на довгочасному носії;

здатністю до втручання в обчислювальний процес.

“В” належить до активних програмних засобів.

“Черв’як” (“Ч”) – програма, яка розповсюджується через мережу і не залишає своєї копії на магнітному носії. “Ч” використовує механізми підтримки мережі для визначення вузла, який може бути заражений. Потім з допомогою тих самих механізмів передає своє тіло чи його частину на цей вузол і або активізується, або чекає для цього сприятливих умов.

Найвідоміший представник цього класу – вірус Морріса (“черв’як” Морріса), який зруйнував мережу Internet в 1988 р. Найбільш сприятливим середовищем розповсюдження “Ч” є мережа, всі користувачі якої вважаються дружніми і довіряють один одному.

Найкращий спосіб захисту від “Ч” – вжити запобіжних заходів проти несанкціонованого доступу до мережі.

Для захисту від різновиду шкідливих програм потрібно створити замкнене середовище виконання програм, розмежувати доступ до виконуваних файлів і системних областей, тестувати придбані програмні засоби.

“Жадібні програми” (“ЖП”) – програми, які при виконанні намагаються монополізувати певний ресурс системи, не даючи можливості іншим програмам використовувати його. Використання такими програмами ресурсів системи звичайно призводить до порушення її доступності. Природно, що така атака є активним втручанням в роботу системи. Безпосередній атаці звичайно підлягають об’єкти системи: процесор, оперативна пам’ять, пристрої вводу-виводу.

Багато користувачів, особливо в дослідних центрах, мають фонові програми, які виконуються з нижнім пріоритетом. Проте, при підвищенні пріоритету така програма може блокувати решту програм. Така програма і буде "жадібною".

Безвихідна ситуація виникає тоді, коли "жадібна" програма нескінченна (наприклад, виконує свідомо нескінченний цикл).

Перехоплюючи асинхронні повідомлення про завершення операції вводу-виводу і посилаючи знову запит на новий ввід-вивід, можна отримати по-справжньому нескінченну програму.

Інший приклад "ЖП" – програма, яка захоплює надто велику область оперативної пам'яті. Боротись з захопленням ресурсів можна введенням різних обмежень для виконання програми, а також постійним контролем додержання їх операторами.

"Загарбники паролів" ("ЗП") – програми спеціального призначення для викрадення паролів. "ЗП" – це активний неопосередкований вплив на АСОІ в цілому.

Для запобігання цій загрозі перед входом в систему потрібно впевнитись, що ви вводите ім'я та пароль саме системної програми входу. Крім того, слід обов'язково дотримуватися правил використання паролів та роботи з системою, постійно перевіряти повідомлення про дату і час останнього входу та кількість помилкових входів. Не записувати команди, що містять пароль, до командних процедур, намагатись уникати явного оголошення пароля при запиті доступу до мережі (ці ситуації можна відслідкувати та захопити пароль). Не використовувати один і той самий пароль для доступу до різних вузлів.

Як засвідчує практика, 81,7 відсотка порушень скоюють самі службовці організації, які мають доступ, і лише 17,3 відсотка – сторонні особи (1 відсоток припадає на випадкових осіб).

Отже, несуттєво, чи є у вашої АСОІ зв'язки з зовнішнім світом та чи є зовнішній захист, а внутрішній захист має бути обов'язково.

Три головні причини, що призводять до порушень: безвідповідальність, самоствердження і корисливий інтерес користувачів АСОІ.

Для організації надійного захисту слід чітко усвідомлювати, від яких саме порушень треба передусім позбавитися. Втрати від кожного виду порушень обернено пропорційні його частоті. Від порушень, викликаних недбалістю, потрібний мінімальний захист, від зондування системи – більш жорсткий, від проникнень – найбільш жорсткий, що поєднується з постійним контролем.

Заходи захисту мають бути адекватними ймовірності здійснення і ступеню загрози. Тільки комплексний аналіз загроз та ступеня захищеності АСОІ може забезпечити відносну безпеку.

2.1.3. Аналіз ризику і складання планів

Аналіз ризику (АР) застосовується до різних операцій. Наприклад, при видачі кредиту спеціалісти банку оцінюють ризик його неповернення позичальником. Оцінивши величину ступеню ризику, можна вжити заходів для його зменшення (наприклад, опечатати на складі позичальника високоліквідний товар).

Для чого потрібний АР ?

1. Для підвищення поінформованості персоналу (більш точне виконання інструкцій).
2. Для визначення сильних і слабких сторін існуючих та запропонованих заходів захисту.
3. Для підготовки та прийняття рішення щодо вибору засобів і заходів захисту. Деякі заходи захисту дуже складні та потребують значних витрат коштів. Ступінь ризику визначає рівень і масштаб застосовуваних засобів захисту.

4. Для визначення витрат на захист. Чим менші витрати на захист, тим вища можливість втрати інформації та порушення працездатності АСОІ.

2.1.3.1. Основні етапи аналізу ризику

АР – це процес одержання кількісної чи якісної оцінки збитків у разі реалізації загрози безпеці АСОІ.

Аналіз ризику безпеки АСОІ передбачає.

1. Опис компонентів АСОІ.
2. Визначення вразливих місць АСОІ.
3. Оцінка ймовірності появи загроз безпеці АСОІ.
4. Оцінка очікуваних розмірів втрат.
5. Огляд можливих методів захисту та оцінка їхньої вартості.
6. Оцінка вигоди від застосування передбачуваних заходів.

Опис компонентів АСОІ. Компоненти АСОІ можна розбити на такі категорії:

устаткування – ЕОМ та їхні складові частини, периферійні пристрої;

програмне забезпечення;

вихідна інформація;

співробітники.

Крім того, слід чітко описати технологію обробки інформації в захищеній АСОІ. Стан АСОІ має бути зафіксований як сукупність різних компонентів і технології обробки інформації. Всі подальші етапи аналізу ризику здійснюються саме з цією, зафіксованою на певний момент часу, системою.

Визначення вразливих місць АСОІ. Для всіх перелічених категорій компонентів АСОІ слід визначити, які небезпеки можуть загрожувати кожній з них і що може бути причиною їх.

Небезпечні дії, що можуть призвести до порушення конфіденційності, цілісності та доступності певних компонентів і ресурсів АСОІ, можна згрупувати так.

1. Стихійні лиха.
2. Зовнішні впливи (підключення до мережі, інтерактивна робота, діяння зловмисників);
3. Навмисні порушення.
4. Ненавмисні помилки (введення помилкової команди, даних, використання несправних пристроїв, носіїв, а також нехтування деякими правилами безпеки).

Приклади видів загроз безпеці АСОІ, які можуть з’явитися в результаті небезпечних дій, наведено в табл.2.

Таблиця 2

Приклади видів загроз безпеці АСОІ

Основні шляхи реалізації загроз безпеці				
Вид загрози	Об’єкти дій			
	Устаткування	Програми	Дані	Персонал
Розкриття (витік) інформації	Крадіжка носіїв, підключення, несанкціоноване використання ресурсів	Несанкціоноване копіювання, перехоплення	Крадіжка, копіювання, перехоплення	Передача відомостей про захист, розголошення, халатність
Порушення цілісності інформації	Підключення, модифікація, спеціальні вкладення, зміна режимів, несанкціоноване використання ресурсів	Впровадження “Троянських коней” та “жучків”	Спотворення, модифікація	Вербування, підкуп персоналу, “маскарад”
Порушення	Зміна режимів,	Спотворення,	Видалення,	Звільнення з

працездатності системи	виведення з ладу, руйнування	вилучення, підміна	спотворення	посади, фізичне усунення

Оцінка ймовірностей прояву загроз безпеці АСОІ дає можливість визначити, як часто може виявитися кожна загроза безпеці АСОІ.

Є такі методи оцінки ймовірностей.

1. Емпірична оцінка, наприклад для оцінки ймовірності стихійних лих, обману співробітників, корупції.
2. Безпосередня реєстрація подій (спроби входу в систему, доступ до певного об'єкта тощо).
3. Оцінка частоти виявлення загрози за таблицею.
4. Метод "Дельфійський оракул", (кожний конкретний коефіцієнт одержується з частоти появи певної події).

Огляд можливих методів захисту і оцінки їхньої вартості. Для зменшення розміру збитків слід застосувати (вдосконалювати) різні заходи захисту АСОІ. Захист від вияву тієї чи іншої загрози може бути реалізований різними способами. Наприклад, захистити інформацію на жорсткому диску ПЕОМ від ознайомлення можна так:

організувати контроль за доступом у приміщення, в якому встановлено ПЕОМ;

призначити відповідальних за використання ПЕОМ;

шифрувати інформацію на диску;

використовувати системи розмежування доступу.

Для кожного з цих способів визначають такі характеристики, як вартість та ефективність. При оцінці вартості методу слід враховувати не тільки прямі (закупівля устаткування, навчання персоналу тощо), а й непрямі витрати (уповільнення роботи системи, порушення відповідної технології обробки інформації тощо).

Ефективність методу – це його спроможність протистояти загрозам певного класу. Отримати реальні значення ефективності дуже важко, і в більшості випадків цю характеристику визначають емпірично.

Оцінка вигоди від застосування передбачуваних заходів. На останньому етапі аналізу ризику провадиться оцінка реальних витрат та виграшу від застосування передбачуваних заходів захисту.

Сутність цього етапу полягає в аналізі різних варіантів побудови системи захисту та виборі оптимального з них за деяким критерієм (звичайно за найкращим співвідношенням "ефективність-вартість").

Приклад. Треба оцінити вигоду при захисті інформації від розкриття чи обробки на основі некоректних даних впродовж одного року.

Збитки від реалізації цих загроз оцінимо в 1 000 000 дол. (*C*). Припустімо, що попередній аналіз показав, що в середньому ця ситуація зустрічається один раз на десять років (*P* =0,1). Тоді вартість витрат для цієї загрози (*BB*) становитиме:

$$BB = CP = 1\,000\,000 * 0{,}1 = 100\,000 \text{ дол.}$$

Далі задамо ефективність методів захисту. Для даного абстрактного випадку припустімо, що в результаті експертної оцінки методів захисту було отримано значення 60 відсотків (*EM*) (у шести випадках з десяти захист спрацьовує). Тоді

$$EM = 60\% * BB = 60\,000 \text{ дол.}$$

Витрати на реалізацію цих методів (закупівля засобів захисту, навчання персоналу тощо) становлять 25 000 дол. (*BM*). Тоді вигода дорівнює:

$$PR = EM - BM = 60\,000 - 25\,000 = 35\,000 \text{ дол.}$$

Аналіз ризику дає також змогу експериментувати з деякою моделлю АСОІ для того, щоб з'ясувати, які з наявних методів захисту найефективніші для збереження працездатності системи і конфіденційності оброблюваної в ній інформації.

Гарантії аналізу ризику. АР – добре відомий інструмент планування, який широко використовується в практиці управління. Проте, інколи висуваються аргументи проти його використання, а саме:

неточність. АР визначає ефективний рівень затрат на захист, особливо в умовах обмежених фінансів. Крім цього, надмірна точність може виявитися непотрібною. Наприклад, зовсім неважливо, чи складуть очікувані втрати 100 000 дол., важливо, що вони будуть набагато більші, ніж 20 000 дол.;

швидка змінюваність. Може змінитися склад системи, зовнішні умови тощо і доведеться проводити новий аналіз. Деякі факти могли не враховуватися в минулому році, а деякі могли втратити актуальність;

відсутність наукової бази.

2.1.3.2. Складання плану захисту

Після визначення загроз безпеці АСОІ, від яких здійснюватиметься захист, та вибору заходів захисту, треба скласти ряд документів, що відбивають рішення адміністрації АСОІ щодо створення системи захисту. Це рішення конкретизується в кількох планах: захисту, забезпечення неперервної роботи та відновленні функціонування АСОІ.

План захисту – це документ, що визначає реалізацію системи захисту. Він необхідний:

для визначення загальних правил обробки інформації в АСОІ, мети побудови та функціонування системи захисту і підготовки співробітників;

для фіксації на певний момент часу складу АСОІ, технології обробки інформації, засобів захисту інформації;

для визначення посадових обов'язків співробітників та відповідальності за їх дотримання.

План захисту містить такі групи відомостей:

політика безпеки;

поточний стан системи;

рекомендації щодо реалізації системи захисту;

відповідальність персоналу;

порядок запровадження засобів захисту;

порядок перегляду плану та складу засобів захисту.

Політика безпеки (ПБ). Має бути визначений набір законів, правил та практичних рекомендацій, на основі яких будується управління критичною інформацією в АСОІ, її захист і розподіл.

ПБ повинна передбачати:

мету, яку переслідує реалізація системи захисту в обчислювальній системі (захист даних компанії від НСД, від втрати даних тощо);

заходи відповідальності засобів захисту і нижній рівень гарантованого захисту (в роботі невеликих груп захищених комп'ютерів, у обов'язках кожного службовця тощо);

обов'язки і санкції, пов'язані з захистом (штрафи, персональна відповідальність тощо).

Поточний стан АСОІ. Слід чітко визначити компоненти АСОІ (устаткування, програми, вихідні дані, персонал тощо) і які з них потребують захисту. Далі треба скласти список можливих способів реалізації загроз роботі системи, роль та місце засобів захисту для запобігання кризовим ситуаціям. Після цього фіксують порядок формування та обробки даних в АСОІ, що захищається.

Потрібно також навести відомості про дії засобів захисту у разі виникнення непередбачуваних ситуацій при введенні в дію нової техніки, програм, даних або через помилки в плануванні.

Рекомендації щодо реалізації системи захисту. Всебічний АР має визначати розміри найбільш вірогідних втрат незалежно від ймовірності появи відповідних подій; максимальні розміри очікуваних втрат;

заходи, здійснювані у разі виникнення критичних ситуацій, а також вартість таких заходів. Ці результати використовують при визначенні зон особливого контролю та розподілу засобів для забезпечення захисту.

Деякі ситуації можуть призводити до надто великих збитків (наприклад, аварія системи), а вартість засобів захисту від них може бути надто високою або ці засоби виявляться неефективними. У цьому разі не потрібно враховувати такі ситуації при плануванні захисту, хоч їх і треба відобразити в плані.

Відповідальність персоналу. Можна навести такі приклади обов'язків:

користувач несе відповідальність за фізичну цілісність комп'ютера під час сеансу роботи з АСОІ, а також за нерозголошення власного пароля;

адміністратор баз даних забезпечує конфіденційність інформації в базах даних, її логічну несуперечливість та цілісність;

співробітник керівництва відповідає за розподіл обов'язків у сфері безпеки обробки інформації, попередження можливих загроз та профілактику засобів захисту.

Порядок запровадження систем захисту. Важливою частиною плану захисту є порядок перегляду складу засобів захисту. Склад користувачів, вихідні дані, оточення – все з часом змінюється, з'являються нові програми та апаратні засоби.

Періодично має здійснюватися також аналіз ризику з урахуванням зміни обстановки.

2.1.3.3. План забезпечення неперервної роботи і відновлення функціонування АСОІ

Є кілька способів пом'якшення дії непередбачених ситуацій:

уникати їх;

якщо запобігти якомусь порушенню не можна, слід зменшити ймовірність його появи або пом'якшити його наслідки;

припускаючи, що певні порушення все ж можуть статися, треба передбачити заходи збереження контролю над ситуацією, а також заходи щодо ліквідації наслідків та відновлення інформації.

До плану висуваються такі вимоги:

реальність;

швидке відновлення працездатності системи;

сумісність з повсякденною діяльністю;

можливість практичної перевірки;

забезпечення виконання плану.

Планування має здійснюватися, виходячи з його економічної ефективності. Наприклад, всю інформацію системи в резервних копіях тримати, в принципі, неможливо – її дуже багато і вона занадто часто оновлюється.

Резервне копіювання та зовнішнє збереження програм і даних. Резервні копії роблять з наборів даних, втрата або модифікація яких може завдати значної шкоди. Звичайно в таких копіях зберігають системне програмне забезпечення і набори даних, найважливіше прикладне забезпечення, а також основні набори даних у цій системі (наприклад, база рахунків у банку).

Копії мають зберігатися в надійному місці, де виключена можливість знищення. Інколи зберігають дві і більше копій.

2.1.4. Політика безпеки. Моделі та механізми реалізації політики безпеки

2.1.4.1. Політика безпеки. Моделі політики безпеки.

Політика безпеки (ПБ) – набір законів, правил і практичних рекомендацій, на основі яких здійснюється управління критичною інформацією в системі, її захист та розподіл.

Політика безпеки має бути індивідуальною, залежати від конкретної технології обробки інформації, використовуваних програмних та технічних засобів.

Під "системою" слід розуміти деяку сукупність суб'єктів та об'єктів і відносин між ними.

Суб'єкт – активний компонент системи, який може виявитись причиною потоку інформації від об'єкта до суб'єкта чи зміни стану системи.

Об'єкт – пасивний компонент системи, який зберігає, приймає чи передає інформацію.

Основу ПБ становить спосіб управління доступом, що визначає порядок доступу суб'єктів системи до її об'єктів.

Для вивчення властивостей засобів управління доступом створюється його математична модель. Вона має відбивати стан всієї системи, її переходи з одного стану в інший, а також показувати, які стани і переходи можна вважати безпечними. Для цього застосовують широкий спектр математичних методів (моделювання, теорія інформації, графів, автоматів тощо).

Найбільш вивченими два види політики безпеки: виборча і повноважна. Визначення прав доступу суб'єктів і об'єктів до інформаційних потоків є компетенцією адміністрації системи.

Виборча політика безпеки (ВПБ)

Основою ВПБ є виборче управління доступом (ВУД). Для опису властивостей ВУД застосовують модель системи на основі матриць доступу (МД). Це матриця, в якій об'єкту системи відповідає стовпець, а суб'єкту – рядок. На перетині стовпця і рядка матриці зазначають тип дозволеного доступу суб'єкта до об'єкта. Приклади типів доступу: "доступ на читання", "доступ на запис", "доступ на виконання" тощо. Доступ може бути дозволено в певні дні, години. Крім того, суб'єкт з визначеними повноваженнями може передати їх іншому суб'єкту (якщо це не суперечить політиці безпеки).

Виборче управління доступом є основою вимог класів С1 і С2 (див. 2.1.5.1.)

Повноважна політика безпеки (ППБ). Її основу становить повноважне управління доступом, яке передбачає такі умови:

всі об'єкти і суб'єкти мають бути однозначно ідентифіковані;

кожний об'єкт має мітку критичності, що визначає цінність інформації, яка в ньому міститься;

кожному суб'єкту системи присвоюється рівень прозорості, який визначає максимальне значення мітки критичності об'єктів, до яких суб'єкт має доступ.

Чим важливіший об'єкт чи суб'єкт, тим вища мітка його критичності. Отже, найзахищенішими є об'єкти з найбільш високими значеннями мітки критичності.

Кожний суб'єкт крім рівня прозорості має поточне значення рівня безпеки, яке може змінюватися від деякого мінімального значення до значення його рівня прозорості.

Для прийняття рішення на дозвіл доступу мітку критичності об'єкта порівнюють з рівнем прозорості та поточним рівнем безпеки суб'єкта. Інформація може передаватися тільки "нагору", тобто суб'єкт може читати зміст об'єкта, якщо його поточний рівень безпеки не нижчий, ніж мітка критичності об'єкта, і записувати в нього – якщо не вищий.

Проста умова захисту передбачає, що будь-яку операцію над об'єктом суб'єкт може виконувати тільки в тому разі, якщо рівень його прозорості не нижчий, ніж мітка критичності об'єкта.

Повноважне управління доступом є основою вимог класу B1 (“Оранжева книга”), де воно використовується спільно з виборчим управлінням (див. 2.1.5.1).

Головне призначення ППБ – регулювання доступу з різним рівнем критичності та запобігання втратам інформації з верхніх рівнів посадової ієрархії на нижні, а також блокування можливих проникнень з нижніх рівнів на верхні.

Виборче і повноважне управління доступом, а також управління інформаційними потоками – три своєрідні кити, на яких будується весь захист.

2.1.4.2. Достовірна обчислювальна база (ДОБ)

Усі засоби, які відповідають за реалізацію політики безпеки, самі мають бути захищені від будь-якого втручання в їхню роботу. Їх об’єднують у так звані достовірні обчислювальні бази (ДОБ).

ДОБ – це повністю захищений механізм обчислювальної системи (включаючи апаратні та програмні засоби), який відповідає за підтримку реалізації політики безпеки.

ДОБ виконує подвійне завдання – підтримує реалізацію політики безпеки і гарантує цілісність механізмів захисту, тобто самої себе.

Для підтримки політики безпеки і власної безпеки ДОБ має забезпечити захист суб’єктів (процесів) і об’єктів системи в оперативній пам’яті та на зовнішніх носіях.

Захист ДОБ грунтується на концепції ієрархічної декомпозиції системи. Сутність цієї концепції полягає в тому, що реальна система подається як сукупність ієрархічно впорядкованих абстрактних рівнів. При цьому функції кожного рівня реалізуються компонентами нижчого рівня. Компоненти певного рівня залежать лише від компонентів нижчих рівнів і їхня внутрішня структура вважається недоступною з більш високих рівнів. Зв’язок рівнів здійснюється через міжрівневий інтерфейс.

Множина компонентів усіх рівнів, крім верхнього, а також засоби управління ними і є ДОБ. Вона гарантує неможливість доступу суб’єкта до об’єкта в обхід засобів контролю.

Компоненти верхніх рівнів звичайно описують інтерфейс користувача. Сюди входять різноманітні редактори, компілятори, інтерпретатори командних мов тощо. Середні рівні, як правило, реалізують ввід-вивід на рівні записів, роботу з файлами і віртуальною пам’яттю. Компоненти нижніх рівнів реалізують планування і диспетчеризацію процесів, розподіл ресурсів, ввід-вивід на фізичному рівні, обробку переривань тощо.

Користувачі та їхні програми можуть працювати тільки з віртуальною пам’яттю. Сама база даних є частиною ДОБ. Доступ до неї також контролюється.

2.1.4.3. Механізми захисту

Основою ДОБ є ядро безпеки (ЯБ). ЯБ – це елементи апаратного і програмного забезпечення, захищені від модифікацій і перевірені на коректність, які розділяють всі спроби доступу суб’єктів до об’єктів. ЯБ реалізує концепції монітора посилань – абстрактної концепції механізму захисту. *Монітор посилань* – концепція доступу суб’єктів до об’єктів в абстрактній ЕОМ (рис.4).

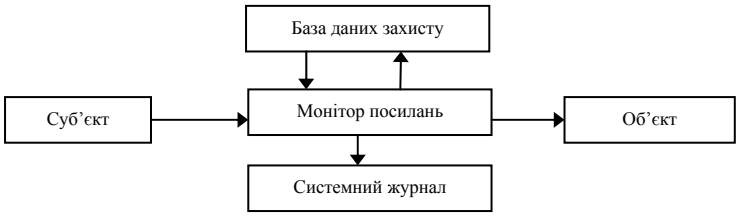

Рис.4. Монітор посилань

Під ***базою даних захисту*** розуміють базу даних, яка зберігає інформацію про права доступу суб'єктів системи до об'єктів. Її основою є матриця доступу.

Функції монітора посилань такі:

перевірка права доступу кожного суб'єкта до будь-якого об'єкта на основі інформації, що міститься в базі даних захисту, і положень політики безпеки;

при необхідності реєструвати факт доступу і його параметри в системному журналі.

ЯБ, що реалізує монітор посилань, має такі властивості:

контролює всі спроби доступу суб'єктів до об'єктів;

має захист від модифікації, підробки і нав'язування;

протестоване та верифіковане для отримання гарантій надійності;

має невеликий розмір і компактну структуру.

Основними функціями, які виконує ЯБ разом з іншими службами ОС, є такі.

1. Ідентифікація, автентифікація і авторизація суб'єктів і об'єктів системи.
2. Контроль входу користувача в систему і управління паролями.
3. Реєстрація і протоколювання.
4. Протидія "збиранню сміття".
5. Контроль цілісності (КЦ) суб'єктів – попередження його несанкціонованої модифікації.
6. Контроль доступу (КД).

Авторизація – надання суб'єкту прав на доступ до об'єкта. Ці функції використовуються як в процесі роботи, так і при вході в систему.

Системний журнал (audit trail) є складовою частиною монітора посилань і призначений для контролю додержання безпеки. Він є одним з основних засобів контролю, який допомагає адміністратору попереджувати можливі порушення у зв'язку з тим, що:

спроможний оперативно фіксувати події, які відбуваються в системі;

може допомогти виявити засоби і апріорну інформацію, які використані зловмисниками для порушення;

може допомогти визначити, наскільки значні порушення, підказати метод розслідування і способи виправлення ситуації.

Для захисту від "ЗС" використовують спеціальні засоби, які можуть входити до ядра безпеки ОС або встановлюються додатково.

КЦ забезпечується процедурами ядра безпеки. Основну роль відіграють такі механізми, як підтримка віртуальної пам'яті та режим виконання процесу.

Під КД розуміють обмеження можливостей використання ресурсів системи програмами, процесами чи іншими системами (для мережі) згідно з політикою безпеки.

Під доступом розуміють виконання суб'єктом деякої операції над об'єктом з багатьох дозволених для цього типу, наприклад, читання, відкриття, записування набору даних, звертання до пристрою тощо.

Контроль даних здійснюють при доступі до:

оперативної пам'яті;

розділених пристроїв прямого доступу;

розділених пристроїв послідовного доступу;

розділених програм та підпрограм;

розділених наборів даних.

Основним об’єктом уваги засобів контролю доступу є спільні набори даних і ресурси системи.

Існує 4 основних способи розділення суб’єктів по відношенню до об’єктів, що використовуються сумісно:

фізичне;

тимчасове;

логічне (під контролем засобів розмежування доступу);

криптографічне – всі об’єкти зберігаються в закодованому вигляді, права доступу визначаються наявністю ключа для розшифрування об’єкта.

2.1.4.4. Принципи реалізації політики безпеки

Розглянемо загальні принципи налагодження механізмів захисту.

1. Групування (об’єднання користувачів у групи).
2. Правила замовчування (суб’єкт, що створив об’єкт і є його власником; по замовчуванню отримує всі права на нього).
3. Мінімум привілеїв.
4. “Треба знати” (доступ дозволений тільки до тієї інформації, яка потрібна для роботи).
5. Об’єднання критичної інформації. Простіше захистити одним і тим же способом великий масив інформації, ніж організувати індивідуальний захист для кожного набору даних.
6. Ієрархія привілеїв. Контроль об’єктів системи може мати ієрархічну організацію. При цьому схема контролю має вигляд дерева, в якому вузли – суб’єкти системи, ребра – право контролю привілеїв згідно з ієрархією, корінь – адміністратор системи, який має право змінювати привілеї будь-якого користувача.
7. Привілеї власника: кожному об’єкту відповідає єдиний суб’єкт з виключним правом контролю об’єкта, як правило, це його творець. Такий принцип звичайно використовують при захисті особистих об’єктів користувачів.
8. Вільна передача привілеїв. Використовується в основному в дослідницьких групах, що працюють над одним проектом.

Набір повноважень кожного користувача має бути ретельно продуманий, виключати можливі протиріччя і дублювання, оскільки велика кількість порушень виникає в основному через це. Можливий витік інформації без порушення захисту, якщо погано була спроектована або реалізована політика безпеки.

Політика безпеки і механізми підтримки її реалізації утворюють єдине захищене середовище обробки інформації. Це середовище має ієрархічну структуру, де верхні рівні представлені вимогами політики безпеки, далі іде інтерфейс користувача, потім – кілька програмних рівнів захисту (включаючи рівні ОС). І, нарешті, нижній рівень цієї структури містить апаратні засоби захисту. На всіх рівнях, окрім верхнього, мають реалізовуватися вимоги політики безпеки, за що, власне, і відповідають механізми захисту.

2.1.5. Оцінка безпеки систем

2.1.5.1. Основні критерії оцінки безпеки систем

Задається ієрархія функціональних класів безпеки. Кожному класу відповідає певна сукупність обов’язкових функцій. Конкретний засіб розмежування доступу належить до такого класу безпеки, в якому реалізовані всі відповідні йому функції безпеки, якщо воно не може бути віднесене до більш високого класу.

Система документів США. У період з 1983 по 1988р. в США Міністерством оборони і Національним Центром Комп'ютерної Безпеки була розроблена система документів щодо комп'ютерної безпеки. До неї належать:

"Критерій оцінки безпеки комп'ютерних систем" ("Оранжева книга" (ОК)).

Областю дій ОК є операційні системи і програмно-апаратні засоби, які змінюють функції операційних систем.

ОК необхідна:

користувачам, для оцінки ступеня довіри системи, яка вибирається для обробки конфіденційної інформації;

виробникам, щоб знати вимоги, які висуваються до систем захисту інформації, та враховувати це в своїх комерційних продуктах;

розробникам стандартів для забезпечення основи розробки інших документів у галузі безпеки.

Виділено 6 головних вимог до безпеки: 4 з них стосуються управління доступом до інформації (політика безпеки, маркування, ідентифікація, облік), а 2 – наданих гарантій (впевненість в системі та неперервність захисту).

Клас захищеності присвоюють системі при проходженні нею сертифікації.

Сертифікації підлягає вся система в цілому, а клас захищеності присвоюють тільки в тому випадку, коли "найслабший" показник задовольняє його вимоги.

Клас Д: підсистеми безпеки. Він присвоюється тим системам, які не пройшли випробовування на більш високому рівні захищеності, а також системам, що використовуються для захисту лише окремої функції (підсистеми) безпеки.

Клас С1: виборчий захист. Засоби захисту систем класу С1 задовольняють вимоги виборчого управління доступом, забезпечуючи розмежування користувачів і даних. У системах цього класу обов'язковими є ідентифікація і автентифікація суб'єкта доступу, а також підтримка зі сторони обладнання.

Клас С2: керований доступ. До вимог класу С1 додається вимога унікальної ідентифікації суб'єкта доступу, захисту по замовчуванню і реєстрація подій. Унікальна ідентифікація означає, що будь-який користувач системи повинен мати унікальне ім'я. Захист по замовчуванню припускає призначення повноважень доступу користувача за принципом "все, що не дозволено, заборонено".

Системи класу В. Характеризуються реалізацією повноважного управління доступом, при якому кожний суб'єкт і об'єкт мають мітки конфіденційності, а рішення на доступ суб'єкта до об'єкта приймаються за певним правилом на основі зіставлення інформації, яка міститься в обох мітках.

Клас В1: міточний захист. Доступ до об'єкта всередині системи дозволяється тільки тим суб'єктам, мітки яких задовольняють певний критерій щодо мітки об'єкта. Прикладом такого критерію є проста умова безпеки та *- властивість у моделях Белла-Лападула [18;Д]. Мітка безпеки на дані, які вводяться, запитується у користувача.

Клас В2: структурований захист. Додатково до вимог класу В1 додається вимога наявності добре визначеної та документованої формальної моделі політики безпеки, яка вимагає дії виборчого і повноважного управління доступом до всіх об'єктів системи.

Вводиться вимога управління інформаційними потоками відповідно до повноважної політики безпеки.

Висуваються також додаткові вимоги до захисту механізмів автентифікації. Інтерфейс з ДОБ має бути добре продокументований.

Клас B3: області безпеки. Має бути реалізована концепція монітора посилань. Усі взаємодії суб'єктів з об'єктами контролюються цим монітором. Дії мають виконуватись у межах областей безпеки, які мають ієрархічну структуру і захищені один від одного за допомогою спеціальних механізмів.

Із системи захисту слід вилучити код, який не вимагається для забезпечення підтримки політики безпеки. Механізм реєстрації подій безпеки повинен також сповіщати адміністратора і користувача про порушення безпеки.

Клас A1: верифікаційована розробка. Відрізняється від класу B3 тим, що для перевірки специфікацій застосовуються методи формальної верифікації – аналізу специфікацій системи щодо неповноти або суперечності, які можуть призвести до появи виломів безпеки.

Сертифікація продукції може тривати від півроку до 2-3 років, тому при продажу продукції звичайно стверджують, що продукція розроблена згідно з вимогами до певного класу.

Для присвоєння класу захищеності система повинна мати посібник адміністратора системи, посібник користувача, тестову і конструкторську (проектну) документацію.

Вартість сертифікації можна порівняти з вартістю розробки засобів захисту.

Потенційним споживачам з комерційного сектора сертифікат на засоби захисту попри гарантування впевненості завдає таких незручностей:

значне збільшення вартості порівняно з несертифікованими аналогами;

труднощі підтримки і супроводження придбаних засобів захисту.

Після сертифікації засобів захисту розробки зміни до програм вносити не можна, в протилежному випадку втрачається сертифікат.

Докорінні зміни відбудуться, якщо сертифікаційні центри не займатимуться розробкою засобів захисту інформації та знизять розцінки на свої послуги.

2.1.5.2. Стандарти в галузі криптографічного захисту інформації

За рубежем найбільш відомими стандартами є такі.

1. DES (Data Encryption Algorithm). Введений в дію у 1977 р., блочний алгоритм з секретним ключем. Довжина ключа – 56 біт (див.1.1.5).

Криптоалгоритм DES в 1994 р. було замінено алгоритмом SKIPJACK (Clipper+Capstone). Вхід – 64 біти, вихід – 80 бітів, довжина ключа – 80 бітів, 4 режими (подібні до режимів DES і ГОСТ28147-89), 32 цикли шифрування, розробку було почато в 1985 р., тестування алгоритму завершено в 1990 р. Відомо, що він DES-подібний. Фахівці стверджують, що цей алгоритм буде стійким впродовж 30-40 років.

2. RSA (Rivest, Shamir, Adleman) – криптосистема з відкритими ключами, опублікована в 1978 р. (див.1.2.3). Швидкість роботи значно менша, ніж у DES, тому використовується спільно з більш швидкими алгоритмами. Ефективний для цифрового підпису.
3. MAA (Message Autentification Algorithm) – розроблений у Великій Британії стандарт для захисту цілісності даних (ISO 8731-2/ ANSI X9.8)/ Використовується для захисту фінансових повідомлень від махінацій.
4. MAC (Код перевірки достовірності даних – Message Autentification Code ISO 8730 і 9807/ ANSI X9.9 і X9.19). Використовується в банківських системах для підтвердження достовірності повідомлень спільно з MAA.

Призначення MAC полягає в доведенні, що під час передачі повідомлення воно не було замінене або підмінене навіть тією людиною, яка також має секретний ключ.

5. Стандарт криптографічного перетворення інформації (ГОСТ 28147-89) було введено в дію у Росії 3 липня 1990 р. Він визначає правила шифрування даних та виготовлення імітовставки. Це блочний алгоритм з секретним ключем. Довжина ключа – 265 біт, довжина блоку підстановки – 512 біт, розмір мінімального блоку для шифрування – 64 біти. Висока криптостійкість - 10^{75}, а також більший набір режимів функціонування, ніж у DES. Суттєвим недоліком є складність його програмно-технічної реалізації і, як наслідок, низька швидкість шифрування. Наприклад, програми реалізації режиму гамірування зі зворотнім зв'язком цього алгоритму на PC/AT-286/16 MHz має швидкодію 12-15 Кб/сек. Існуючі апаратні реалізації цього алгоритму трохи швидші (50 – 150 Кб/сек).

6. Стандарт цифрового підпису (ГОСТ Р34.10-94 і Р34.11-94).

Докладніша інформація щодо стандартів по захисту інформації міститься в [53].

2.1.6. Управління захистом АСОІ

Засоби захисту слід настроювати у такий спосіб, щоб всі вимоги щодо політики безпеки виконувалися так, як було спроектовано (і зафіксовано у плані захисту). Крім того, потрібно контролювати роботу АСОІ.

Спільне використання будь-яких ресурсів створює умови для порушення безпеки.

Принципи організації захисту і контролю функціонування системи. Управління системою захисту полягає в періодичному внесенні змін до бази даних захисту, які містять відомості про користувачів, допущених до роботи в системі, їхні права доступу до різних об'єктів системи тощо.

Особливу увагу при управлінні системою захисту треба звернути на:

документованість усіх змін у базі даних захисту;

періодичне резервне копіювання бази даних з метою запобігання втрати їх актуальної копії у разі збою обладнання.

Контроль за функціонуванням АСОІ полягає в слідкуванні за небезпечними подіями, аналізі причин, які призвели до їх виникнення, та ліквідації наслідків.

Задачі управління та контролю розв'язує адміністративна група. Звичайно до неї входять: адміністратор безпеки, менеджер безпеки і оператор.

Небезпечні події та попередження їх. Для більшості АСОІ причинами загроз є такі:

перехоплення інформації з ліній зв'язку;

перехоплення паролів;

спроба проникнення в систему;

створення чи заміна записів бази даних захисту;

несанкціоноване одержання та використання привілеїв;

несанкціонований доступ до набору даних;

встановлення неперевірених програм і командних процедур, які можуть містити "троянських коней", "черв'яків" тощо;

"збирання сміття" на диску чи в оперативній пам'яті;

використання вузлів мережі або портів для проникнення в інші вузли мережі ЕОМ.

Інформацію про будь-які способи атакувати систему можна отримати з кількох джерел:

від користувачів – про стан захисту особистого набору даних окремих користувачів;

при моніторингу функціонування АСОІ – про стан загальних характеристик системи;

з системного журналу – про стан захисту різних наборів даних.

Заходи, яких слід вжити після встановлення факту проникнення:

убезпечити базу даних захисту (інформацію про користувачів, їхні повноваження, а також про захист об'єктів системи);

змінити паролі (хоча б для привілейованих користувачів);

повністю або частково оновити системні модулі з резервних копій;

зробити захист більш жорстким (застосувати додаткові заходи захисту набору даних, системні паролі, їхні генератори).

Прикладом додаткових засобів контролю є контроль банківських операцій. Можна автоматично слідкувати за сумами, які пересилаються, номерами рахунків, місцем призначення, часом платежу. Якщо окремий параметр, який використовується, чи їхня комбінація, перейдуть в область заборонених (наприклад, розмір платежу перевищує встановлений), надходить сигнал тривоги.

2.1.7. Безпека комп'ютерних мереж

Перед передачею даних каналами зв'язку виникає необхідність попереднього перетворення їх. Для цього використовують додаткову інформацію, без якої її неможливо передати абоненту, та відновлення до початкового варіанту. Так створюють ***комп'ютерні мережі***.

Комп'ютерна мережа – це об'єднання фізичних та логічних незалежних систем в єдине середовище, в якому для передачі інформації від системи до системи вона проходить ланцюг певних перетворень. Незалежні системи, що входять до складу мережі, називають ***вузлами.***

2.1.7.1. Особливості захисту інформації в мережах ЕОМ

Головні проблеми організації захисту мереж ЕОМ такі:

розподілення ресурсів, які використовуються спільно (значно зростає ризик несанкціонованого доступу – в мережі його можна здійснити простіше і непомітніше);

розширення зони контролю (інші держави);

комбінація різних програмно-апаратних засобів;

невідомий периметр мережі;

множина точок атаки (модеми, лінії зв'язку);

складність управління та контролю доступу до системи (з віддалених точок).

Захист мереж, як і захист окремих систем, переслідує три мети: підтримка конфіденційності інформації, що передається та обробляється в мережі, цілісності та доступності ресурсів мережі.

Як і для АСОІ, захист мережі має плануватися як єдиний комплекс заходів, що охоплюють всі особливості обробки інформації. Проте слід враховувати, що кожен вузол мережі повинен мати індивідуальний захист залежно від функцій, які виконуються, і від можливостей мережі. При цьому захист окремого вузла має бути частиною загального захисту.

На кожному вузлі потрібно організувати:

контроль доступу до всіх файлів та інших наборів даних, доступних із локальної мережі та інших мереж;

контроль процесів, активізованих з віддалених вузлів;

контроль мережевого трафіка;

ефективну ідентифікацію і автентифікацію користувачів, що отримують доступ до цього вузла мережі;

контроль доступу до ресурсів локального вузла, доступного для використання користувачам мережі;

контроль за розповсюдженням інформації у межах локальної та пов'язаних з нею інших мереж.

Захист мережі як єдиної системи, передбачає заходи захисту кожного окремого вузла і функцій захисту протоколів цієї мережі.

Програмне забезпечення мережі має входити до складу довірчої обчислювальної бази (ДОБ) вузла, в протилежному разі можливе порушення роботи мережі та її захисту в результаті заміни програм або даних. Тоді захист інформації в мережі здійснюватиме мережа ДОБ. Вона складається з ДОБ окремих вузлів, пов'язаних захисними протоколами.

Класифікація погроз, характерних для мереж (погрози нижчого рівня).

1. Пасивні погрози (порушення конфіденційності даних, що циркулюють у мережі):

   перегляд і (чи) запис даних, що передаються лініями зв'язку;

   перегляд повідомлень;

   аналіз трафіка.

2. Активні погрози (порушення цілісності або доступності ресурсів (компонентів) мережі):

   несанкціоноване використання пристроїв, що мають доступ до мережі для зміни окремих повідомлень;

   відмова служб передачі повідомлень – зловмисник може знищувати або затримувати окремі повідомлення чи потік повідомлень;

   "Маскарад" – зловмисник може присвоїти своєму вузлу чи ретранслятору чужий ідентифікатор і відправляти або отримувати повідомлення від чужого імені;

   впровадження мережевих вірусів – передача по мережі тіла вірусу з його наступною активізацією користувачем віддаленого чи локального вузла;

   модифікація потоку повідомлень – зловмисник може вибірково знищувати, модифікувати, затримувати, перевпорядковувати та дублювати повідомлення, а також вставляти підроблені повідомлення.

2.1.7.2. Методи і механізми захисту мереж

До механізмів захисту відносять такі:

1. Механізми шифрування, які забезпечують конфіденційність даних, що передаються. Розрізняють два способи шифрування: канальний та кінцевий. У разі канального шифрування захищається вся інформація, що передається каналами зв'язку, включаючи службову (для кожної пари вузлів є свій ключ). Кінцеве шифрування дає можливість забезпечувати конфіденційність даних, що передаються між двома об'єктами (захищеним у цьому разі буде тільки зміст повідомлення, вся службова інформація залишається відкритою).
2. Механізми цифрового підпису, які містять процедури закриття блоків даних та перевірки закритого блоку даних. Сформувати непідробний блок може тільки користувач, що має відповідний ключ.
3. Механізми контролю доступу. Здійснюють перевірку повноважень об'єкта мережі на доступ до ресурсів (відповідно до правил політики безпеки та механізмів, які їх реалізують).
4. Механізми забезпечення цілісності даних, що передаються. Цілісність забезпечується об'єктами, що передають і приймають. Виявлення змін може потягти за собою дії щодо відновлення даних.
5. Механізми автентифікації об'єктів мережі. Використовують паролі, перевірку характеристик об'єкта, криптографічні методи (аналогічні цифровим підписам).
6. Механізми заповнення тексту використовують для забезпечення захисту від аналізу трафіка.
7. Механізми керування маршрутами (в обхід небезпечних ділянок).
8. Механізми засвідчення (арбітр).
9. Виявлення і обробка подій (аналогічно до засобів контролю небезпечних подій).

10. Звіт щодо перевірки небезпеки (аналогічно до перевірки з використанням системного журналу) на відповідність цій ПБ.

2.1.7.3. Особливості захисту різних класів мереж

Захист має відповідати принципам організації мережі: якщо мережа централізована, то і захист повинен бути централізований, якщо мережа розподілена, то і захист повинен бути розподілений.

Для централізованої обробки найкраще підходить топологія "зірка"; для розподіленої – "загальна шина", що характеризується високою швидкістю передачі даних і порівняно швидким доступом до вузла.

Доступ до мережі за допомогою комутованих ліній зв'язку вважають потенційно найбільш небезпечним. Потрібно автентифікувати будь-який вхід через комутовані лінії зв'язку (парольний захист, перевірка за описом списку дозволених номерів).

Є сенс використовувати цю методологію захищених АСОІ в тому разі, якщо витрати на реалізацію менші, ніж вартість інформації, що може бути втрачена. Найреальнішим об'єктом використання цієї методології є великі АСОІ чи АСОІ, що обробляють дорогу інформацію або розв'язують відповідальні задачі.

2.2. Електронні платежі: організація і захист

2.2.1. Вплив інформаційних технологій на розвиток банківської індустрії

Метою цього розділу є визначення зовнішніх та внутрішніх чинників, що мають вплив на розвиток банківської індустрії, ступінь впливу, а також напрям вдосконалення діяльності банків.

Проблеми банківської індустрії. Законодавчі акти Спільного ринку та поява нових інформаційних технологій починають впливати на розробку політики банків. До того ж на діяльність банків впливають і внутрішні чинники, такі як зміни запитів клієнтів, необхідність зменшення часу обслуговування, розширення використання високих технологій.

У жорстких умовах сучасного ринку банки мають дати чітку відповідь на такі запитання.

1. Що впливає на мій бізнес ?
2. Що впливає на бізнес моїх клієнтів?
3. Як я буду конкурувати на Європейському та інших світових ринках ?
4. Як я можу збільшити кількість моїх клієнтів ?
5. Чи можу я збільшити надходження з допомогою розширеного набору послуг?
6. На яких ринках мені потрібно бути?
7. Де і як виникають найбільші витрати і як я можу їх зменшити?
8. Як я можу збільшити кількість моїх акціонерів?

Зовнішні та внутрішні чинники. Зовнішніми називають чинники, які справляють вплив на формування середовища функціонування банку (зміна політичної та економічної ситуації, розвиток технологій). Внутрішні чинники відносять до сфери впливу самого банку.

Зовнішні чинники:

спільний ринок;

друга банківська директива (стандарти контролю і регулювання діяльності банків, ліцензії на діяльність банків);

глобалізація ринку послуг;

спільний ринок, Європейський економічний простір, єдина грошова політика;

Східна та Центральна Європа;

зміни в законодавстві;

достатня кількість капіталів (мінімальний рівень власних капіталів банку, збільшення вимог щодо ліквідності та депозитних резервів банку);

збільшення вимог клієнтів;

технології (електронні платежі та засоби розрахунку в точці продажу).

Внутрішні чинники:

акціонерний капітал (збільшення обороту потребує збільшення акціонерного капіталу для захисту капіталу банку);

витрати на управління (55 відсотків – службовці, 30 відсотків – витрати на підтримку інформаційних технологій);

зміни в управлінні (слід використовувати гнучкі технології, перебудувати свою структуру відповідно до сучасних потреб);

борги країн, що розвиваються.

Банківська індустрія: ланцюг пріоритетів. Різні типи банків (роздрібні, інвестиційні, міжнародні) мають різний склад ланцюга пріоритетів. Проте всі вони включають в свою діяльність 5 основних напрямів.

1. Використання залучених вкладів.
2. Розробка продукції для задоволення потреб клієнтів.
3. Управління ризиком.
4. Обробка транзакцій.
5. Розподіл товарів і послуг.

Все більшого значення набуває віддалене банківське обслуговування за допомогою автоматичних касових апаратів, систем електронних платежів, розрахунку в точці продажу. Воно здійснюється за допомогою інтелектуальних та інших електронних банківських карт, клієнтних терміналів і телефонного обслуговування.

Роль інформаційних технологій у діяльності банку. Інформаційні технології впливають на розмір отримуваних доходів, а також на їх склад та розподіл.

Одна з основних проблем банків сьогодні – це управління інвестиціями в електронних банківських системах з тим, щоб останні повністю відображували зміни в банківській індустрії та сучасні уявлення про банківську діяльність. Успіх на стратегічних напрямах бізнесу цілком залежить від реалізації нових систем.

2.2.2. Автоматизація банківських операцій і їхній захист

З часу своєї появи банки незмінно притягували до себе злочинців. У наші дні банки перетворились на обладнані за останнім словом техніки бастіони, що ховають в своїх надрах мільярди. Проте прогрес у техніці злочинців йшов не менш швидкими темпами, ніж розвиток банківських технологій. У наші дні значна частка всіх злочинів пов’язана з використанням АСОІ банку. Отже, при створенні АСОІ банку потрібно приділяти велику увагу забезпеченню їхньої безпеки.

Необхідність захисту банківських систем: тенденції та факти. Комп’ютерні системи – джерело абсолютно нових, раніше невідомих загроз, а саме [2]:

втрати банків від впливу на їхні системи обробки близько 3 млрд. дол. на рік;

обсяг втрат, пов’язаних з використанням пластикових карток, приблизно дорівнює 2 млрд. дол. на рік, що становить 0,5–10 відсотків від загального обсягу платежів.

Захист АСОІ банку – складний захист, що потребує значних витрат. Так, “Bar clays Bank” витрачає на захист своєї автоматизованої системи близько 20 млн. фунтів стерлінгів щороку.

2.2.2.1. Загрози безпеці автоматизованих банківських систем

Опитування* за 1153 анкетами дало змогу згрупувати основні проблеми, з якими стикались менеджери інформаційних систем, у табл.3, у відсотках.

Таблиця 3

Статистика по основних проблемах

Опис загроз	1991	1992
Втрата зв'язку:		
стихійне лихо	14	8
інші причини	42	36
недбалість користувачів	–	15
несправність в АТС	–	21
несправність в мережах передачі даних	–	46
помилки програмних засобів	–	39
Злочини, пов'язані з комп'ютерами:		
за допомогою програми (включаючи віруси)	22	44
розкриття пароля	28	30
зсередини системи	4	5
зовні системи	2	2
займання комп'ютерів	2	1
втрати інформації	9	11
Втрата живлення:		
стихійні лиха	29	22
інші причини	53	50
несправність обладнання	–	28
вимикання електрики	–	71
недбалість персоналу	–	10
вихід генератора з ладу	–	15

Аналіз таблиці показує:

за 1992 р. різко зріс (в 2 рази) рівень злочинності з використанням програмних засобів;

найбільших неприємностей менеджерам систем завдало розкриття пароля і несанкціонований доступ (НСД) до інформації.

Варто також звернути увагу на значне збільшення вірусних загроз і числа НСД до інформації, яка спільно використовується в мережі ЕОМ. 10 відсотків порушень скоєні скривдженими та невдоволеними службовцями АСОІ банку, 10 – з корисливих мотивів персоналом системи, 50–55 відсотків – результат ненавмисних помилок.

Особливості злочинів у фінансовій сфері такі.

1. Більшість комп'ютерних злочинів є дрібними. Збитки від них становлять 10 000 – 50 000 дол.
2. Комп'ютерні злочини, як правило, потребують великої кількості банківських операцій (до кількох сотень). Проте великі суми можуть пересилатися всього лише за кілька транзакцій.
3. Більшість злочинців – клерки.
4. Комп'ютерні злочини не завжди високо технологічні.
5. Багато зловмисників пояснюють свої дії тим, що вони начебто беруть позику в банку з наступним поверненням.

* Опитування в 1992 р. проводила Datapro Information Services Group

2.2.2.2. Особливості захисту інформації в електронних банківських системах (ЕБС)

В АСОІ зберігається і обробляється конфіденційна інформація. Її підробка або витік можуть призвести до серйозних наслідків. Через це електронні банківські системи приречені залишатися відносно закритими, працювати під керуванням специфічного програмного забезпечення і приділяти більше уваги своїй безпеці.

Другою особливістю ЕБС є підвищення вимогливості та надійності апаратного і програмного забезпечення. Це дає змогу здійснювати безперервну обробку інформації.

Можна виділити два класи задач, які розв'язує ЕБС.

1. Аналітичні (прогнозування, планування, аналіз рахунків тощо). Результати їхнього розв'язання можуть справляти вплив на політику банків. Внаслідок цінності результатів їхній захист має бути постійним.
2. Щоденні (виконання платежів і коригування розрахунків). Для їхнього розв'язання звичайно потрібно набагато більше ресурсів, ніж для аналітичних задач. Звичайно досить забезпечити захист безпосередньо в момент його здійснення. При цьому захист самого процесу обробки інформації та кінцевих результатів має бути постійним.

Політику безпеки мають 82 відсотки опитаних організацій. Різні організації все більше уваги приділяють захисту інформації, що зберігається і обробляється. Лише 66 відсотків організацій з числом співробітників менше 100 чол. мають політику безпеки, тоді коли для організацій з числом співробітників більше 5000 чол., частка таких організацій досягає 94 відсотки. У 88 відсотків організацій, що мають політику безпеки, існують спеціальні підрозділи, які відповідають за її реалізацію.

У плані захисту особливу увагу приділяють захисту великих ЕОМ (82 відсотки), відновленню інформації після аварій і катастроф (73 відсотки), захисту від комп'ютерних вірусів (72 відсотки), захисту персональних ЕОМ (69 відсотків).

До особливостей організації захисту мереж ЕОМ в фінансових установах можна віднести широке використання комерційного програмного забезпечення для управління доступом до мережі (82 відсотки, в державному секторі – 71 відсоток), захист точок підключення до систем через комутовані лінії зв'язку (69 відсотків, в державному секторі – 51 відсоток). Інші способи захисту, такі як використання антивірусних засобів, кінцеве канальне шифрування даних, що передаються, автентифікація повідомлень, використовуються менше, ніж у 50 відсотках організацій. Велика увага приділяється захисту приміщень, у яких розміщені комп'ютери.

Захист ЕБС має розроблятися для кожної системи індивідуально відповідно до загальних правил і включати:

аналіз ризику, що завершується розробкою проекту системи захисту і планів захисту, безперервної роботи і відновлення;

реалізацію системи захисту (СЗ) на основі результатів аналізу ризику;

постійний контроль за роботою СЗ і АСОІ в цілому.

Кожну систему обробки інформації потрібно розробляти індивідуально, враховуючи такі особливості:

організаційну структуру банку;

обсяг і характер інформаційних потоків (усередині банку в цілому, усередині відділів, між відділами, зовнішніх);

кількість і характер виконуваних операцій: аналітичних і щоденних (один з ключових показників активності банку – число банківських операцій за день);

кількість і функціональні обов'язки персоналу;

кількість і характер клієнтів;

графік добового навантаження.

2.2.2.3. Зовнішній ресурс

Банківський бізнес належить до найбільш ризикованих. Конкуренція між окремими банками, ризик при фінансуванні проектів, непередбачувана політична та економічна ситуація змушують багато банків використовувати будь-які заходи, що сприяють економії коштів. Одним з таких заходів, які стосуються проектування інформаційної системи, є використання зовнішніх ресурсів (ЗР), тобто ресурсів іншої організації (постачальника).

Розрізняють два види ЗР.

1. Сервіс-бюро. Банк укладає контракт з постачальником (або з іншим банком) на надання обчислювальних ресурсів для обробки інформації в центрі постачальника.
2. Послуги з управління. Постачальник керує роботою центру обробки банку, використовуючи при цьому обладнання самого банку.

Правильно вибрана політика використання ЗР дає можливість зекономити значні суми: 10 – 50 відсотків порівняно з обробкою у власній системі.

2.2.3. Електронні платежі

Специфічною рисою електронних банківських систем є спеціальна форма обміну електронними даними – електронними платежами.

2.2.3.1. Обмін електронними даними (ОЕД) і електронні платежі

ОЕД – це міжкомп'ютерний обмін діловими, комерційними, фінансовими електронними документами. Наприклад, замовленнями, платіжними документами, контрактними пропозиціями, накладними, квитанціями тощо.

ОЕД забезпечує оперативну взаємодію торгових партнерів на всіх етапах підготовки торгової угоди, укладання контрактів та реалізації поставки. На етапі оплати контракту і переказу грошових засобів ОЕД може приводити до електронного обміну фінансовими документами. При цьому створюється ефективне середовище для здійснення торгово-платіжних операцій:

можливі ознайомлення торгових партнерів з пропозиціями товарів і послуг, вибір потрібного товару (послуги), уточнення комерційних умов (вартості та термінів поставки, торгових знижок, гарантійних і сервісних зобов'язань) у реальному масштабі часу;

замовлення товару (послуги) або запит контрактної пропозиції в реальному масштабі часу;

оперативний контроль поставки товару, отримання електронною поштою супроводжуючих документів;

підтвердження завершення поставки товару (послуги), виставлення і оплата рахунків;

виконання банківських кредитних і платіжних операцій.

До переваг ОЕД треба віднести:

зменшення вартості операцій за рахунок переходу на безпаперову технологію. Виграш від використання ОЕД оцінюється, наприклад, в автомобільній промисловості США більш як 200 дол. на один виготовлений автомобіль;

прискорення розрахунку й обороту грошей;

підвищення зручності розрахунків.

Існує дві ключові стратегії розвитку ОЕД.

1. Як перевага в конкурентній боротьбі.
2. Для підвищення ефективності взаємодії різних комерційних об'єднань.

Основною перешкодою поширенню ОЕД є розмаїття документів при обміні ними каналами зв'язку. Для подолання цієї перешкоди були розроблені стандарти представлень документів у системах ОЕД.

Частковим випадком ОЕД є ***електронні платежі*** (ЕП) – обмін фінансовими документами між клієнтами і банками, між банками та іншими фінансовими та комерційними організаціями.

Сутність концепції ЕП полягає в тому, що повідомлення, які пересилаються лініями зв'язку, певним чином оформлені та передані, є основою для виконання однієї або кількох банківських операцій. На основі такого повідомлення можна пересилати або отримувати гроші, відкривати кредит, оплачувати покупки або послуги, виконувати будь-які інші банківські операції. Такі повідомлення називають ***електронними грошима***. Природно, що весь процес здійснення ЕП потребує надійного захисту. Інакше банк і його клієнтів чекають серйозні неприємності.

Для здійснення ОЕД слід реалізувати такий набір основних послуг:

електронна пошта за стандартом X.400;

передача файлів;

зв'язок "крапка–крапка";

доступ до баз даних в режимі "on-line";

поштова скринька;

перетворення стандартів представлення інформації.

Міжбанківські розрахунки бувають 3-х видів.

1. Клірингові розрахунки з використанням потужної обчислювальної системи банку-посередника (клірингового банку) і кореспондентських рахунків банків – учасників розрахунків у цьому банку. Система заснована на заліку взаємних грошових вимог і зобов'язань юридичних осіб з наступним переказом сальдо.
2. Прямі розрахунки, при яких два банки здійснюють зв'язок безпосередньо між собою. Звичайно така система об'єднує кілька банків. При цьому кожна пара може зв'язуватись між собою, обходячи посередників.
3. Обробка електронних чеків.

2.2.3.2. Загальні проблеми безпеки ОЕД

Одним з найвразливіших місць ОЕД є пересилання платіжних та інших повідомлень між банком і банкоматом або між банком і клієнтом.

При цьому виникають такі проблеми: взаємодія одержувача і відправника документів здійснюється опосередковано – через канал зв'язку. Це породжує 3 типи проблем:

взаємного розпізнавання абонентів (проблема автентифікації при з'єднанні);

захист документів, які передаються каналами зв'язку (забезпечення їхньої цілісності та конфіденційності);

захист самого процесу обміну документами (проблема доведення факту відправки (отримання) документа).

У системах ОЕД мають бути реалізовані механізми, що забезпечують реалізацію функцій захисту на окремих вузлах системи ОЕД, та на рівні протоколів високого рівня:

автентифікація абонентів;

неможливість відмови від авторства повідомлення;

контроль цілісності повідомлення;

забезпечення конфіденційності повідомлення;

управління доступом на кінцевих системах;

гарантії доставки повідомлення;

неможливість відмови від вжиття заходів за отриманим повідомленням;

реєстрація послідовності повідомлень;

контроль цілісності послідовності повідомлень;

забезпечення конфіденційності потоку повідомлень.

Повнота вирішення перелічених проблем значною мірою залежить від правильного вибору системи шифрування. **Система шифрування (або криптосистема)** – це сукупність алгоритмів шифрування і методів розповсюдження ключів.

Правильний вибір системи шифрування допомагає:

приховати зміст документа від сторонніх осіб завдяки шифруванню його змісту;

забезпечити спільне використання документа групою користувачів системи ОЕД в результаті криптографічного розмежування інформації та відповідного протоколу розповсюдження ключів. При цьому для осіб, які не входять до групи, документ є недоступним;

своєчасно виявити перекручення, підробку документа введенням криптографічної контрольної ознаки (імітовставки);

переконатися в тому, що абонент, з яким відбувається взаємодія в мережі, є дійсно тим, за кого себе видає (автентифікація абонента / джерела даних).

Слід зазначити, що при захисті ОЕД (і для електронних платежів зокрема) велике значення має не стільки шифрування документа, скільки забезпечення його цілісності та автентифікації джерела даних при проведенні сеансу зв'язку.

Надійність криптосистеми в цілому залежить від механізму розсилання (розподілу) ключів між учасниками взаємодій. Основні підходи до розсилання ключів такі:

метод базових (сеансових) ключів (master / session keys). Вводиться ієрархія ключів (головний ключ (ГК), ключ шифрування ключів (КК), ключ шифрування даних (КД)). Ієрархія може бути дворівневою (КК /КД), або трирівневою (ГК /КК /КД). При цьому старший ключ в ієрархії розповсюджується між учасниками взаємодії неелектронним шляхом, що виключає його перехоплення та (або) компрометацію. Стандарт визначає 3 способи розповсюдження ключів: безпосередня, з використанням центру розповсюдження, з використанням центру трансляції ключів. Стандарт не застосовується для розповсюдження ключів між спеціалізованими банківськими пристроями, такими як банкомати і пристрої розрахунків у точці продажу;

метод відкритих ключів (public keys). Базується на односторонніх перетвореннях, за яких частина ключа залишається відкритою і може бути передана лініями зв'язку у відкритому вигляді. Це звільняє від дорогої процедури розповсюдження ключів як шифрування неелектронним способом;

метод виведеного ключа (derived key). Застосовується для захисту інформації, яка передається між терміналом системи розрахунку в точці продажу і комп'ютером банку. При цьому методі ключ для шифрування кожної наступної трансакції обчислюється одностороннім перетворенням попереднього ключа і параметрів трансакцій;

метод ключа трансакцій (transaction key). Також застосовується для захисту інформації, що передається між терміналом системи розрахунку в точці продажу і комп'ютером банку. Він відрізняється від методу виведеного ключа тим, що при обчисленні ключа для наступної трансакції не застосовуються її параметри.

2.2.3.3. Захист міжбанківських платежів

Особливу увагу слід звернути на захист терміналів, підключених до систем електронних платежів.

Якщо банк виконує операції підвищеного ризику, здійснювані процедури забезпечення безпеки мають включати парольний захист, багаторівневу авторизацію користувачів, контроль операцій, ведення системного журналу. Треба також здійснювати розмежування доступу користувачів до терміналів та інших зовнішніх пристроїв, які мають бути захищені фізично.

Для забезпечення безпеки даних, що передаються лініями зв'язку, слід використовувати криптографічні методи.

Система безпеки центральної АСОІ має включати багаторівневий контроль доступу до периферійних пристроїв і центральної бази даних.

Задачі з безпеки визначаються для кожного конкретного випадку індивідуально в процесі аналізу ризику.

Найвідоміша система електронних платежів SWIFT (The Society for Worldwide inter – bank Financia / Telecommunication) – безприбуткове кооперативне міжнародне співтовариство, метою якого є організація міжнародних банківських розрахунків по всьому світу. Вона об'єднує 3200 користувачів з 84 країн світу, прямий доступ користувачів до своїх кореспондентів по всьому світу 20 хв., доставка термінового повідомлення – 5 хв.

2.2.4. Персональні платежі та їхній захист

Розглянемо способи розрахунку фізичних осіб з фінансовими закладами – так звані персональні платежі, а також способи їх захисту.

2.2.4.1. Персональні платежі: форми організації

Домашнє (телефонне) обслуговування. Розпорядження можуть бути віддані як голосом спеціальному службовцю банку або електронній системі, так і в електронній формі безпосередньо банківському комп'ютеру.

Введення даних для платежу (ідентифікатор, номер рахунку, розмір платежу) здійснює клієнт з клавіатури телефона.

Особливу увагу приділяють початковій ідентифікації та перевірці абонента. Для ідентифікації може бути використаний, наприклад, десятисимвольний пароль, який встановлюється клієнтом і відомий лише йому. Перевірка абонента може здійснюватися при взаємодії з оператором. На початку роботи оператор запитує навмання одну або кілька літер з пароля користувача. Додатково клієнт забезпечується кодовим словом, яке використовується при цій процедурі.

Майбутнє цього виду послуг залежить від прогресу в галузі розпізнавання мови і створення надійних і порівняно недорогих пристроїв з прийнятними характеристиками такого розпізнавання.

Автоматичні касові апарати *(АКА).* АКА (банкомат) – спеціалізований пристрій, призначений для обслуговування клієнта за відсутності банківського персоналу. Він призначений в основному для видачі готівки. Крім цієї функції, АКА може виконувати ряд додаткових, а саме:

перевірка стану рахунку клієнта;

зміна параметрів рахунку клієнта;

здійснення різноманітних платежів;

надання інформації про страховий поліс клієнта, котирування цінних паперів на фондовому ринку, купівлю й продаж акцій, обмінні курси валют тощо.

Взаємодія клієнта з АКА здійснюється за допомогою пластикової картки, на якій записана потрібна інформація, виносної клавіатури і мікродисплея. Фактично АКА являють собою ПЕОМ, яка має до 16 Мбайт ОП, до 100 Мбайт дискової пам'яті, нагромаджувач на гнучких магнітних дисках, дисплей, принтер та інші периферійні пристрої. Шифрування конфіденційної інформації при передачі каналами зв'язку або записуванні на диск здійснюється на основі стандарту DES. Станом на 1989 р., у різних країнах світу встановлено понад 200000 АКА, загальні вклади в індустрію АКА становили 3 млрд. дол.

Розрахунок у точці продажу *(POS).* В основному всі термінали, підключені до цих систем, розміщені на підприємствах торгівлі. Більшість таких терміналів встановлено в супермаркетах, на автозаправних станціях тощо.

Системи POS забезпечують такі послуги:

перевірку і підтвердження чеків;

перевірку і обслуговування дебетових і кредитних карток;

використання системи електронних розрахунків.

Дані, необхідні для платежу, передаються через термінали системи POS банківському комп'ютеру, проводиться платіж і гроші переводяться з рахунку покупця на рахунок продавця.

2.2.4.2. Персональний ідентифікатор (PIN)

PIN – це послідовність цифр (звичайно 4-6, але може бути до 12), яка використовується для ідентифікації клієнта. За способом призначення можна виділити такі типи PIN:

призначені виведені (derived);

призначені випадкові (random);

вибрані користувачем.

У зв'язку з тим, що PIN призначений для ідентифікації та автентифікації клієнта, його значення має бути відомим тільки клієнту.

Алгоритм ідентифікації клієнта. Є два основні способи перевірки PIN: алгоритмічний і неалгоритмічний.

Алгоритмічний спосіб перевірки полягає в тому, що у користувача запитується персональний ідентифікатор PIN, який перетворюється за певним алгоритмом з використанням таємного ключа, а потім порівнюється з значенням PIN, що зберігається на картці. Переваги цього методу:

відсутність копії PIN на головному комп'ютері, що виключає його розкриття персоналом банку;

відсутність передачі PIN між АКА та головним комп'ютером банку, що виключає його перехоплення зловмисниками чи нав'язування результатів порівняння.

Генерація PIN з номера рахунку. Спочатку номер рахунку клієнта доповнюється нулями або іншою константою до 16 шістнадцятиричних цифр (8 байтів). Потім одержані 8 байтів шифруються з використанням таємного ключа за алгоритмом DES. З одержаного шифртексту (8 байт), починаючи з молодших байтів, виділяються по 4 біти. Якщо значення числа, утвореного цими бітами, менше за 10, то одержана цифра включається в PIN, інше значення відкидається. Отже, обробляються всі 8 байтів (64 біти). Якщо в результаті обробки не вдалося одержати необхідну кількість десяткових цифр, з невикористаних комбінацій віднімається 10.

2.2.4.3.Огляд технологій електронних карток

Використання систем POS і АКА поставило вимогу появи деякого носія інформації, який би міг ідентифікувати користувача та зберігати деякі облікові дані. У ролі таких носіїв стали виступати пластикові картки.

Тепер у світі випущено 600 млн. пластикових карток. Найбільш відомими з них є такі:

кредитні картки VISA (більше ніж 200 млн.) та Master Card (148 млн.);

міжнародні чекові гарантії Eurochegue і Postchegue;

картки для оплати подорожей і розваг American Expresse (40 млн.) і Diners Club.

За принципом дії можна виділити пасивні та активні пластикові картки. ***Пасивні*** лише зберігають інформацію на тому чи іншому носії. Особливість ***активних*** карток – наявність вбудованої в них мікросхеми. Картка з мікропроцесором називається ***інтелектуальною.***

За характером розрахунків, що провадяться з допомогою пластикових карток, можна виділити кредитні та дебітні картки.

За характером використання картки поділяють на корпоративні та особисті.

Інтелектуальні картки *(ІК).* Цей тип карток винайдений та запатентований Роланом Мореном у Франції і набув найбільшого поширення в США. Серцем таких карток є не просто мікропроцесор, а мікроЕОМ, оскільки в постійний запам'ятовуючий пристрій, встановлений на картці, "прошивається" спеціальний набір програм, що називається Операційною Системою Картки.

Ці картки забезпечують різноманітний набір функцій:

можливість роботи із захищеною файловою системою (доступ до файлів потребує повноважень по читанню (запису) інформації);

шифрування даних з використанням різних алгоритмів;

ведення ключової системи тощо.

Деякі картки забезпечують режим "самоблокування" при спробі НСД.

ІК дає змогу суттєво спростити процедуру ідентифікації клієнта. Для перевірки PIN використовується алгоритм, що реалізується мікропроцесором на картці.

Водночас ІК мають і суттєві недоліки, які зумовили обмежене поширення їх:

висока вартість виготовлення картки;

збільшена, порівняно з стандартом, товщина, через що вона не може бути прочитана звичайним АКА. Для читання таких карток потрібна установка спеціальних зчитувачів.

Кредитні картки *(КК).* КК – найпоширеніший тип пластикових карток. До них належать VISA та Master Card, American Exprese та AmEx'S Optima, картки Discovery Card фірми Sears, місцеві та регіональні картки універсальних магазинів. КК пред'являється для оплати товарів і послуг. При оплаті з допомогою КК банк відкриває покупцю кредит на суму покупки і потім через деякий час (звичайно 25 днів) надсилає рахунок поштою. Покупець повертає оплачений чек назад до банку.

Дебітові картки *(ДК).* Це пластикові картки, що використовуються для дебітових розрахунків. Вони багато в чому аналогічні кредитним. Для дебітових трансакцій найчастіше використовується АКА. Дебітові картки призначені для заміни готівки та персональних чеків.

Головна її відмінність від КК полягає в тому, що з її допомогою можна вносити гроші на свій рахунок.

ДК в основному застосовуються для одержання готівки через АКА.

У 1993 р. Акціонерна компанія "Дизайнцентр-"ИДИС" представила перші російські пластикові картки. Сьогодні такі картки використовуються для безготівкової оплати телефонних переговорів. Уже кілька

російських банків обслуговують картки VISA (Кредобанк, Столичний, Мост-банк, Автобанк, Інкомбанк тощо). Координатором діяльності російських членів Master Card є АО "Кард-центр". Майже всі російські картки дебетові.

Лідером в галузі карбованцевих карток є STB-Card. Сума готівки, що знімається, не повинна перевищувати еквівалента 200 дол.

Захист пластикових карток від підробки. До банківських карток висуваються дві головні вимоги: унікальність і необоротність.

Перша вимога означає, що серед усіх випущених банком карток не повинно бути однакових за характеристиками.

Згідно з другою вимогою не може бути відновлена первісна інформація на картці.

Є два основних способи захисту від підробки – метод магнітних водяних знаків і метод "сендвіча".

Метод магнітних водяних знаків передбачає нанесення на магнітну стрічку, розташовану на картці, спеціального малюнка.

Метод "сендвіча" полягає в тому, що одна стрічка містить ділянки з різними рівнями намагнічення.

Сучасні пластикові картки мають кілька ступенів захисту. Наприклад, у картки VISA їх 7.

Порушення, пов'язані з використанням кредитних карток. За деякими даними втрати від використання пластикових карток становлять 2 млрд. дол. щороку. Головною причиною втрат є неправильне використання карток їхніми законними власниками.

Статистика втрат для Visa і Master Card (США, 1987 р.) у відсотках:

шахрайство продавця – 22,6;

крадіжки – 17,2;

підробка карток – 14,3;

зміна рельєфу карток – 8,1;

загублені картки – 7,5;

неправильне застосування – 7,4;

шахрайство по телефону – 6,3;

шахрайство при пересиланні поштою – 4,5;

поштове шахрайство – 3,6;

крадіжки при виробництві та пересиланні – 2,9;

зговір з власником картки – 2,1;

інші – 3,5.

2.2.4.4. Автоматичні касові апарати (АКА)

На АКА покладають такі завдання:

ідентифікація і автентифікація клієнта;

видача готівки;

сповіщення про стан рахунку клієнта;

переказ коштів клієнта з одного рахунку на інший;

реєстрація всіх здійснених операцій і видача квитанцій.

Основне завдання АКА – видача грошей клієнту.

Є два режими роботи АКА.

1. Off-line (автономний режим) – АКА функціонує незалежно від комп'ютерів банку, а запис інформації про трансакції провадиться на внутрішній магнітний диск і виводиться на вбудований принтер.
2. On-line (режим реального часу) – АКА має бути приєднаний до головного комп'ютера банку, і реєстрація трансакцій здійснюється безпосередньо на головному комп'ютері, хоча підтвердження про трансакцію видається на принтер АКА.

Перевага автономного режиму АКА полягає в його відносній дешевизні та незалежності від якості ліній зв'язку. Водночас низька вартість установки зумовлює високу вартість експлуатації цих апаратів (щоденне оновлення списків загублених карток).

Складності виникають також при ідентифікації (автентифікації) клієнта. Компрометація ключа хоча б на одному АКА призведе до порушення захисту на всіх АКА.

Режим реального часу дає можливість клієнту не тільки одержати готівку, а й здійснювати маніпуляції зі своїм рахунком. Централізована ідентифікація (автентифікація) дає змогу значно підвищити стійкість системи до компрометації ключів шифрування. Централізована перевірка ідентифікатора користувача робить можливим швидке оновлення списків заборонених для використання карток, а також введення обмежень на кількість готівки, яку може отримати клієнт протягом одного дня (для захисту від використання украдених карток).

Наявність каналу зв'язку породжує й інші загрози безпеці порівняно з автономним режимом. Це аналіз трафіка та імітація роботи головного комп'ютера. При першій загрозі аналізуються дані, що передаються АКА головному комп'ютеру і на їх основі отримується інформація про рахунки, суми, умови платежів тощо. При другій загрозі головний комп'ютер може бути імітований комп'ютером зловмисника і на запит АКА про результати ідентифікації (автентифікації) видавати позитивну відповідь.

У разі, коли АКА працює в режимі реального часу, для здійснення ідентифікації він обмінюється з головним комп'ютером трьома повідомленнями.

Для АКА, що працюють в режимі реального часу, такий захист організувати досить просто. Якщо три спроби вводу PIN виявилися невдалими, в платежі клієнту відмовляється.

Розподілені мережі АКА. Крім окремих АКА експлуатуються і мережі АКА, в яких беруть участь кілька банків. Учасники такої мережі переслідують такі цілі:

розподіл витрат і ризику при розробці нових видів послуг між учасниками мережі;

зменшення вартості операцій для учасників;

надання послугам загальнонаціонального характеру;

можливість негайно одержати вигоду від лібералізації законодавства.

У США функціонує 3 загальнонаціональні мережі – Master Card Cirrus, Plus System, VISA USA.

При спільному використанні банками мережі АКА з'являється нова проблема – захист конфіденційної інформації банків один від одного (ключі шифрування, списки номерів, заборонених для використання карток тощо). Для її успішного вирішення було запропоновано схему централізованої перевірки PIN кожним банком у своєму центрі зв'язку з АКА. При цьому також ускладнюється система розподілу ключів між всіма учасниками мережі. Для захисту взаємодії комп'ютерів банків між собою і з АКА використовується кінцеве (абонентське) шифрування інформації, що передається лінією зв'язку.

Найчастіше використовується такий метод: вся мережа АКА розбита на зони і в кожній з них використовується свій головний зональний керуючий ключ. Він призначений для шифрування ключів при обміні між мережним маршрутизатором і головним комп'ютером банку. Ключ індивідуальний для всіх учасників мережі. Звичайно він випадково генерується маршрутизатором і неелектронним способом

передається до банку. Розкриття ключа призведе до розкриття всіх PIN, які передаються між маршрутизатором та головним комп'ютером банку.

Для шифрування інформації, що надходить від головного комп'ютера емітента (учасника мережі) на маршрутизатор використовується робочий ключ емітента. Його повідомляє головному комп'ютеру банку маршрутизатор у зашифрованому вигляді. Ключ може змінюватися за запитом користувача в процесі роботи. Аналогічний за призначенням ключ для обміну між одержувачем і маршрутизатором називають ***робочим ключем одержувача***. Для шифрування інформації при передачі від АКА до головного комп'ютера банку використовується ***комунікаційний ключ одержувача***.

У нерозподіленій мережі АКА достатньо на всіх АКА використовувати один відкритий ключ, а на головному комп'ютері банку – закритий ключ.

У мережі спільно використовуваних АКА застосування системи шифрування з відкритим ключем дає змогу відмовитись від зональних ключів і дорогої процедури їх заміни. Проте в цьому разі схема ідентифікації АКА за паролем не працюватиме. Ця проблема може бути вирішена в тому разі, коли кожний АКА разом з запитом буде пересилати і свій відкритий ключ, завірений банком.

2.2.4.5. Особливості розрахунку в точці продажу

Системи POS призначені для скорочення витрат з обробки паперових грошей і для зменшення ризику покупця і продавця, пов'язаного з цією обробкою.

Покупець для оплати покупки пред'являє дебетову або кредитну картки і для підтвердження особи вводить PIN. Продавець, зі свого боку, вводить суму, яку потрібно заплатити за покупку чи за послуги.

Запит на переказ грошей надходить до банку продавця. Той для перевірки справжності картки, пред'явленої покупцем, переадресує запит до банку покупця. Якщо картка справжня, і покупець має право використовувати її для оплати товарів і послуг, банк покупця переводить гроші до банку продавця на його рахунок. Після переказу грошей банк продавця надсилає повідомлення на термінал POS, у якому повідомляє про завершення трансакції. Після цього продавець видає покупцеві повідомлення.

Для захисту системи POS потрібно додержуватись таких вимог:

перевірка PIN, введеного покупцем, має здійснюватися системою банку одержувача. При пересиланні каналами зв'язку PIN повинні бути зашифровані;

повідомлення, що містять запит на переказ грошей (або підтвердження про переказ), слід перевіряти на справжність для захисту від внесення змін та заміни при проходженні лініями зв'язку до обробних процесорів.

Найвразливішим місцем системи POS є її термінали. Первісно припускається, що термінал системи POS незахищений від зовнішнього впливу.

У зв'язку з цим припущенням виникають нові типи загроз для терміналу. Вони пов'язані з розкриттям таємного ключа, який знаходиться в терміналі POS і призначений для шифрування інформації, що передається терміналом до банку продавця. Ці загрози одержали такі назви:

"*обернене трасування*" – зловмисник одержить ключ шифрування, він намагатиметься відновити значення PIN, використане у попередніх трансакціях;

"*пряме трасування*" – зловмисник одержить ключ шифрування, він намагатиметься відновити PIN, що використовуються в трансакціях, які відбудуться після того, коли він одержить ключ.

Для захисту від цих загроз використовують 3 методи: метод ключа трансакції, метод виведеного ключа і метод відкритих ключів.

Метод ключа трансакції *(transaction key)* був запропонований в 1983 р. Н.Бекером та іншими. Інформація, що передається між кожним терміналом та кожним емітентом карток, має бути зашифрована на унікальному ключі, який, у свою чергу, повинен змінюватися від трансакції до трансакції. Проте використання цього методу для великої кількості терміналів і емітентів карток ускладнює управління ключами. Через це на практиці він переважно застосовується не до зв'язку "термінал–емітент карток", а до зв'язку "термінал–одержувач", оскільки кожен одержувач має обмежений набір обслуговуваних терміналів.

При генерації нового ключа використовуються такі складові: однонаправлена функція від значення попереднього ключа; зміст трансакції та інформація, одержана з картки. При цьому мається на увазі, що попередня трансакція завершилась успішно. Така схема захищає як від оберненого, так і від "прямого трасування". Розкриття одного ключа не дає можливості зловмисникам розкрити всі попередні або наступні трансакції. Метод передбачає також окрему генерацію двох ключів – одного для шифрування PIN, другого – для одержання коду автентифікації повідомлення. Це необхідно для розподілу функцій банків продавця та одержувача. Недоліком схеми є її складність.

Метод виведеного ключа *(derived key).* Цей метод є більш простий, але менш надійний, ніж попередній Він забезпечує зміну ключа при кожній трансакції незалежно від її змісту. Для генерації ключа використовується однонаправлена функція від поточного значення ключа та деяке випадкове значення. Метод забезпечує захист лише від "оберненого трасування". Одностороння функція реалізована на основі алгоритму DES.

Метод застосування відкритих ключів дає змогу надійно захиститися від будь-яких видів трасування і забезпечити надійне шифрування інформації, яка передається. Термінал POS забезпечується таємним ключем, на якому шифрується запит до банку продавця.

Цей ключ генерується при ініціалізації терміналу. Після генерації таємного ключа термінал надсилає пов'язаний з ним відкритий ключ на комп'ютер продавця. Обмін між учасниками взаємозв'язку відбувається з використанням відкритого ключа кожного з них. Підтверджує справжність учасників спеціальний центр реєстрації ключів з використанням своєї пари відкритого і закритого ключів.

Недоліком методу є його порівняно мала швидкодія.

2.2.4.6. Електронні чеки

Електронний чек – еквівалент банківського чеку, який застосовується для платежу. Чек може бути застосований як в точках купівлі, так і в АКА.

Електронний чек складається з трьох частин, які включають відомості про банк, про клієнта і про чек.

Для організації платежів з використанням електронних чеків використовуються так звані електронні папірці, реалізовані на базі інтелектуальних карток. Термінал збирає всі пред'явлені йому чеки за певний період і звертається до банку, подаючи їх до оплати.

Сучасним банкам потрібні розроблені за останнім словом техніки інформаційні системи, а ті, в свою чергу, потребують постійного захисту.

На Заході створена ціла індустрія захисту економічної інформації, яка включає розробку і виробництво безпечного апаратного і програмного забезпечення, периферійних пристроїв, наукові дослідження тощо. Мета цих робіт – зробити обробку комерційної інформації якомога безпечнішою.

Статистика показує таке:

більшість організацій має план з правилами доступу до інформації, а також план її відновлення після аварій;

більшість користувачів більш за все бояться несанкціонованого доступу із мережі або з внутрішньої частини системи;

як превентивні засоби захисту більшість користувачів ставлять на перше місце зовнішнє зберігання резервних копій найважливіших даних і наявність плану відновлення після аварій.

Є одна особливість, яка виділяє банківські системи серед решти систем. Вона зумовлює необхідність високопродуктивного і надійного банківського захисту. Це електронні платежі, без яких жоден сучасний банк не може існувати. Сутність концепції електронних платежів полягає в тому, що належним чином оформлені та передані мережами зв'язку повідомлення є основою для виконання банківських операцій.

Для банківських систем особливе значення має не стільки кодування даних, скільки надійна автентифікація і підтримка цілісності.

Для кожного окремого виду електронних платежів чи інших способів обміну конфіденційною інформацією існують свої специфічні особливості захисту.

2.3. Програмні та апаратні засоби для автоматизації банківських систем

Висновки, одержані в результаті оцінки ринку систем автоматизації банків, можна узагальнити так:

якщо за рубежем автоматизація здійснюється від великих централізованих систем до розподілених ("згори-донизу"), то у нас –поступовим нарощуванням можливостей ПК ("знизу-догори");

найближчим часом, широкого використання банківських систем іноземного виробництва очікувати не варто. Це пояснюється відсутністю чітких концептуальних поглядів на автоматизацію банків, дороговизною іноземних банківських систем. Найімовірніше застосування іноземних ЕОМ і розробка власного програмного забезпечення;

тривалий час як основні засоби автоматизації застосовуватимуться IBM PC-сумісні комп'ютери;

використання IBM PC-сумісних комп'ютерів зумовлює посилену увагу захисту інформації незалежно від типу головних машин (серверів);

у запропонованих на вітчизняному ринку системах автоматизації банківської діяльності проблеми захисту враховуються досить слабо, а якщо і враховуються, то фрагментарно. Це утруднює забезпечення належного захисту інформації на етапах її охорони, передачі та обробки;

найчастіше захищається та інформація, яка виходить за межі банку. Внутрішня система банку, як правило, незахищена. Це зумовлено неочевидністю внутрішніх погроз і відсутністю статистики злочинів, скоєних службовцями банків.

Банківські системи докорінно відрізняються від обчислювальних систем взагалі. Основні відмінності їх можна згрупувати у такий спосіб.

1. Банківські системи будуються звичайно на базі мультипроцесорних або розподілених систем (потрібно опрацьовувати великий потік інформації);
2. Система має бути надійно захищена і відокремлена, зв'язок з іншими системами здійснюється через спеціальні "шлюзи";
3. Система має продовжувати роботу навіть у разі виходу з ладу окремих вузлів.

Можна припустити, що моделями базових ЕОМ, які найбільше підходять для банківських систем, є такі.

1. Для середніх і великих комп'ютерних систем банків, які розширюються – моделі, які забезпечують розв'язання широкого кола задач і відрізняються можливістю швидкого розширення до більш потужної системи, модульною архітектурою, можливістю інтеграції у відкриті системи, надійністю і високою ефективністю, а також забезпечуючих гарантовану безпеку процесу обробки і зберігання інформації: серії

Cyclone і CLX компанії Tandem Computers Inc., серія A компанії Unisys (моделі A6, A11, A12, A16), серії VAX 6000 і 9000, для невеликих систем – VAX 3000 і 4000 корпорації DEC.

2. Для середніх комп'ютерних систем банків, які розширюються –моделі, орієнтовані на ОС UNIX, які забезпечують потрібну безпеку процесу обробки і зберігання інформації: серія U компанії Unisys, сімейство DPX/20 компанії Bull, серія 3000 компанії NCR.
3. Для малих і середніх комп'ютерних систем банків, які не потребують розширення і потужних мережних функцій, – середовище моделей класу міні ЕОМ, які забезпечують високий рівень безпеки – серія AS/400 компанії IBM.

Можна виділити 3 основні підходи до створення захищених комп'ютерних систем: адміністративний, криптографічний і програмно-технічний.

Характерною особливістю нашої дійсності є практично повна відсутність кваліфікованих кадрів і організованих колективів у сфері створення захищених комп'ютерних систем за наявності великої кількості кваліфікованих програмістів і математиків.

Проблема захисту має ще один аспект. Справа в тому, що його планування і реалізацію здійснювати власними силами (силами організації) можливо, з залученням консультантів. Захист – це ключ до системи, а отже, і до інформації, яка в ній зберігається. Навіщо відкривати її будь-кому? Це по-перше. А по-друге, навіщо копіювати чужі помилки, краще робити свої. В усякому разі про них не швидко стане відомо, і вони не стануть "троянським конем" вашої системи.

Непрофесійний підхід до захисту, що спостерігається у нашій країні, може призвести до сумних наслідків, спричинити значні збитки як матеріальні, так і моральні. Становище, що склалося, треба виправляти уже сьогодні, інакше немає жодних підстав дивитися у майбутнє з оптимізмом.

2.4. Безпека банківських технологій (досвід України)

2.4.1. Захист інформації в електронних системах

Інформація – одне з найважливіших джерел процвітання будь-якої держави, банку чи фірми. Недарма кажуть: "Хто володіє інформацією, той володіє світом". Будь-яке управлінське рішення базується і коштує тієї інформації, на основі якої воно прийняте.

Витік інформації може завдати серйозної шкоди банку, його економічному становищу та іміджу, часто дозволяючи конкурентам зайняти провідні позиції на ринку, а іноді призводить і до банкрутства.

За законами бізнесу попит породжує пропозицію. Саме тому на сучасному ринку засобів захисту інформації з'являються все різноманітніші та потужніші засоби. Особливо цей процес активізувався в останні роки.

Помітно різке вторгнення на цей ринок іноземних фірм – виробників таких засобів і систем.

Розглянемо окремі проблеми інформаційної безпеки і доцільність використання в Україні іноземних програмних засобів безпеки інформації.

У 1990 р. тодішній директор Агентства Національної Безпеки (АНБ) США Уільям Студеман заявляв, що його агентству доведеться в найближчий час змінити напрям діяльності, зробивши своїм пріоритетом не військове, а економічне шпигунство. При цьому "під ковпаком" у АНБ виявиться багато країн–союзників США, не говорячи вже про країни колишнього СРСР, чиї банки, торговельні і промислові компанії виходять на світовий ринок та стають конкурентами американцям.

Мова йде про цілеспрямоване електронне слідкування за конкретними банками і компаніями, що мають найбільші перспективи розвитку з метою добування відомостей про їхні нові товари, технології, фінансові та

торгові операції, які плануються. Одним із способів отримання такої інформації є контроль каналів обміну інформацією. Незалежність держави багато в чому залежить від незалежності та надійності її інформаційних баз і каналів. Контроль їх ставить державу, її банки і компанії в залежність від того, хто контролює і знає всі ходи наперед. Одним із способів контролю інформаційних каналів є електронні та програмні "закладки".

"Електронні закладки" ("жучки" тощо) вже давно використовуються спецслужбами для промислового шпигунства. За допомогою цих "жучків" можна перехопити не лише акустичну, але і спеціальну електронну інформацію. Припустимо, одна фірма продала іншій комп'ютер, ксерокс, телефон, факс, і "продавець" тепер знає все, що робиться у "покупця". "Жучок" справно поставляє своєму господарю інформацію радіоканалом чи, наприклад, через комп'ютерну мережу. І звичайно ж, продавець точно знає, кому дістанеться ця техніка. Отже, витрати на "жучка" швидко відшкодовуються.

Як дешевший, але не менш ефективний спосіб отримання інформації з комп'ютерів використовують зняття з них електромагнітного випромінювання. Окремі види навіть побутової телевізійної техніки дають змогу отримати "картинку" з екрана дисплея комп'ютера на своїх екранах. Уявіть собі, що в машині, припаркованій недалеко від банку сидять "електронні хакери" і спостерігають по телевізору, що відбувається на банківському комп'ютері. Однак таке можливе лише з звичайним, незахищеним від випромінювання комп'ютером.

Фірми, які надають подібні послуги зі "зняття" інформації, уже з'явилися в Києві, Москві, і успіх їхньої діяльності зумовлений тим, що у нас поки що або зовсім не захищаються, або захищаються непрофесійно.

Іншим ефективним способом ведення промислового шпигунства є проникнення в комп'ютерні мережі, електронні бази даних банків, фірм тощо. У розвинених країнах збитки від подібних акцій становлять до кількох десятків міліардів доларів.

Якщо ж такі проникнення плануються заздалегідь, то для полегшення роботи "зломщику" до програми, яка поставляється клієнтові, розробник вносить "програмну закладку", яка дає можливість легко увійти в комп'ютерну систему того, у кого вона буде стояти. У зв'язку з цим у воєнній галузі з'явився новий термін – "інформаційна зброя".

Існує багато прикладів впровадження "програмних закладок" в інформаційні системи різних фінансових та комерційних структур. Ефективність дії лише однієї такої закладки може бути такою, що призведе до повного розорення власника інформаційної системи або за рахунок витікання конфіденційної інформації, або за рахунок несанкціонованого впливу розробника на саму систему. Особливо широко подібні впливи застосовуються в країнах з дуже розвиненими комп'ютерними системами, коли розробник може продовжувати впливати на роботу своєї програми "дистанційно", зв'язуючись з нею через мережу. Однак і в наших умовах уже з'являються повідомлення про подібні випадки.

Уряд США вважає за потрібне взяти розповсюдження криптосистем під свій контроль. У зв'язку з цим в середині квітня 1993 р. президент США запропонував прийняти за стандартну для США шифрсистему Clipper замість стандарту DES. Уряд США закріплює за собою управління криптоключами шифрсистеми Clipper. Ключ розділяється на дві частини і кожна частина зберігається в окремій організації, яку вибирає генеральний прокурор. При отриманні дозволу суду на підслуховування правоохоронні органи отримують обидві частини ключа і можуть розшифровувати інформацію, що передається.

Основою нової системи шифрування стане секретний криптоалгоритм Skipjack АНБ США. Секретність ключа шифрування системи Clipper заснована на принципі розділеного і депонованого ключа.

Крипточип Capstone є розширеним варіантом крипточипа Clipper і містить, крім інших елементів, додатково схему реалізації алгоритму цифрового підпису DSA (Digital Signature Algorithm), запропоновану

національним інститутом стандартів і технологій NIST (США). Цей алгоритм використовуватиметься замість алгоритму цифрового підпису RSA.

Слід замислитись про доцільність використання в Україні іноземних програмних засобів безпеки інформації та створення і використання вітчизняних систем захисту.

2.4.2. Захист інформації в системах "клієнт–банк"

На сьогоднішній день саме в банківській сфері спостерігається як позитивний ефект, пов'язаний з впровадженням сучасних автоматизованих технологій обробки інформації та пов'язаного з цим розширення спектру послуг, що надаються, і прискоренням оборотності коштів, так і неминучі негативні вияви, а саме:

частішають спроби крадіжок грошових коштів, в тому числі за допомогою засобів комп'ютерної техніки*;

не завжди ефект від впровадження передових технологій адекватний витратам;

не всі послуги надаються на досить якісному рівні.

Уже сьогодні потребують негайного вирішення такі проблеми:

забезпечення безпеки обміну інформацією між відділами банків, що працюють в режимі єдиного кореспондентського рахунку в Національному банку України. Оскільки більше ніж 70 відсотків платежів у таких банках становлять внутрішньосистемні (міжфілійні) платежі, очевидно, наскільки актуальна ця задача. За Промінвестбанком України, що працює в цьому режимі, на нього будуть переходити й інші банки (організація взаємодії за принципом "кожен з кожним");

безпеки інформації, що циркулює у відомчих мережах передачі даних. Уже існує відомча мережа передачі даних банку "Україна";

відсутності нормативно-правової бази, яка дає змогу вирішувати питання електронного грошового обігу як між відділами банків, так і між банками і їхніми клієнтами (в системах "Клієнт–Банк");

відсутності єдиних стандартів галузі як найпоширеніших алгоритмів, так і термінології;

на сьогоднішній день ніякими засобами, крім досить слабких, які входять до складу найпопулярніших мережевих операційних систем, не забезпечується безпека інформації, що обробляється всередині відділу банку. Водночас 70–90 відсотків усіх крадіжок грошових коштів в автоматизованих системах здійснюють співробітники банків;

сертифікації програмних і апаратних засобів. З однієї сторони, НБУ справедливо вимагає використання для захисту банківської інформації лише сертифікованих програмних і апаратних засобів, з іншої – система державної сертифікації таких засобів ще реально не функціонує, а спроби НБУ виступати в ролі сертифікаційної організації не зовсім законні.

Без комплексного вирішення цих та інших питань створити надійну систему електронних розрахунків і зробити доступ до неї простим і зручним для всіх її учасників – завдання недосяжне.

У наш час спостерігається сповільнення темпів зростання кількості банків, що працюють на території України. Цей процес замінюється процесом зростання якості та обсягу послуг, що надаються, у тому числі в області автоматизації електронного грошового обігу. Як приклад можна навести застосування у ряді банків кредитних карток, активний обмін фінансовою інформацією між відділами банків з використанням засобів телекомунікації, впровадження різноманітних автоматизованих систем обробки фінансової інформації всередині банків. Не останнє місце серед таких нововведень займають системи електронних платежів "Клієнт–Банк", що дають змогу клієнтам банку – юридичним особам виконувати операції зі своїм банківським рахунком

безпосередньо з офісу. Проаналізуємо проблеми забезпечення захисту інформації, яка обробляється в таких системах, а також дамо деякі рекомендації щодо реалізації їх.

Для цього слід проаналізувати всі стадії процесу взаємодії клієнта з банком, виявити можливі загрози безпеці і вибрати методи, що дадуть змогу захиститись від цих загроз.

Одну з можливих технологічних схем функціонування системи "Клієнт–Банк" наведено на рис. 5.

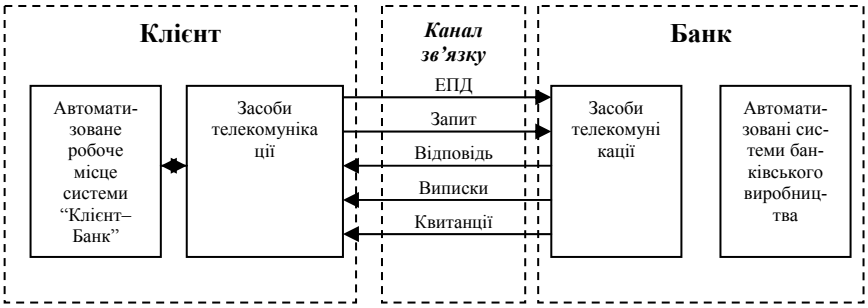

Рис. 5 Технологічна схема роботи системи "Клієнт–Банк"

Така схема використовується, наприклад, в АПБ "Україна", подібна – в кількох інших банках. Клієнт на своєму автоматизованому робочому місці (АРМ) виконує підготовку електронних платежів документів (ЕПД). ЕПД за допомогою програмно-технічних засобів телекомунікації (модему і відповідного програмного забезпечення) передаються до банку, де приймаються також через телекомунікаційні засоби, що функціонують на спеціально впровадженому комп'ютері (зв'язному сервері), включеному до локальної обчислювальної мережі (ЛОМ) банку. У цій ЛОМ функціонує програмний комплекс автоматизованої системи банківського виробництва (АСБВ), який називають ***комплексом операційного дня банку*** *(ОДБ)*. Прийняті зв'язним сервером (ЗС) електронні платежі документів каналами ЛОМ передаються в АСБВ, де здійснюється їх подальша обробка. Після прийняття ЕПД і обробки АСБВ формує квитанцію і передає її на ЗС для наступної передачі клієнту. Протягом операційного дня і після його завершення АСБВ формує і передає на ЗС повідомлення про рух на рахунку клієнта (поточні та кінцеві виписки).

З точки зору забезпечення безпеки в цій технології можна виділити три групи проблем.

1. Такі, що виникають при обробці інформації всередині організації-відправника ЕПД.
2. Пов'язані з забезпеченням захисту ЕПД при пересиланні їх між клієнтом і банком.
3. Ті, що виникають у процесі обробки документа в банку і прийняття рішень про зміну стану рахунку клієнта (про переказ коштів).

Проблеми першої групи пов'язані в основному з такими причинами:

необхідністю забезпечення юридичної значимості сформованого документа для установи банку (проблема автентифікації виконавця документа);

блокуванням можливості внесення зловмисником змін в уже сформовані та підготовлені до відправки ЕПД (проблема автентифікації або захисту цілісності документа);

захистом цілісності використовуваних при підготовці ЕПД програмних засобів для блокування можливостей несанкціонованого формування (відправки) ЕПД (проблема автентифікації або захисту цілісності програмних засобів).

---

[*] 23 жовтня 1998 року з рахунків резервного фонду Вінницького обласного управління Національного банку України, несанкціоновано проникнувши до комп'ютерних мереж банку, невідомий хакер викрав 80,4 млн. грн. Майже вісім місяців праці співробітників служби по боротьбі з організованою злочинністю закінчилися успіхом [Факты и коментарии. №126 (0457), 13.07.1999р.].

Одне з вразливих місць – пересилання документів між клієнтом і банком. Це породжує три типи проблем, пов'язаних з необхідністю:

взаємного розпізнавання абонентів (проблема автентифікації при встановленні зв'язку);

захист документів, які передаються каналами зв'язку (забезпечення цілісності та конфіденційності документів);

захист самого процесу обміну документами (проблема доведення факту відправлення (доставки) документа).

У банку в процесі обробки прийнятого ЕПД можуть виникнути такі проблеми:

підтвердження цілісності та юридичної значимості прийнятого документа (ідентифікація та автентифікація відправника, а також автентифікація повідомлення);

забезпечення захисту від несанкціонованої модифікації вже прийнятого ЕПД або від нав'язування хибної інформації зловмисником всередині відділення банку;

захист цілісності використовуваних при обробці ЕПД в банку програмних засобів для блокування можливостей несанкціонованого доступу і модифікації інформації про стан рахунків клієнта;

оскільки клієнт і банк юридично незалежні, існує проблема недовіри – чи будуть вжиті щодо прийнятого документа відповідні дії.

Отже, для забезпечення надійності роботи системи "Клієнт–Банк" засоби захисту мають забезпечувати:

ідентифікацію та автентифікацію клієнта–відправника ЕПД з однозначною авторизацією документа;

автентифікацію ЕПД;

автентифікацію програмного забезпечення, яке функціонує у клієнта в банку;

автентифікацію абонентів у процесі встановлення зв'язку і передачі повідомлення;

приховування смислового змісту повідомлення, що передається;

захист сформованих ЕПД від несанкціонованого доступу (НСД) як у клієнта, так і в банку;

фіксацію фактів прийому (передачі) документів з веденням відповідних архівів і журнальних файлів;

чітку регламентацію обов'язків клієнта і банку стосовно один одного.

Розглянемо методи і алгоритми, за допомогою яких можуть бути вирішені описані задачі.

Способом ідентифікації та автентифікації відправника ЕПД, а також авторизації самого документа є застосування цифрового підпису документа, що виконується за допомогою несиметричних криптоалгоритмів. Існує кілька алгоритмів для виконання цифрового підпису. Серед них алгоритм RSA і алгоритм Ель-Гамаля. У Росії діє набір стандартів (ГОСТ РФ 34.10, ГОСТ РФ 34.11), які визначають алгоритм формування цифрового підпису, а також алгоритм хешування (стиснення) повідомлень, що підписуються. В Україні стандарту на алгоритм цифрового підпису поки що немає.

Для автентифікації та приховування смислового змісту повідомлень звичайно застосовують симетричні криптоалгоритми, наприклад, DES, Clipper або діючий на території колишнього СРСР, в тому числі в Україні, ГОСТ 28147-89.

Розв'язок задачі автентифікації абонентів при встановленні зв'язку може виконуватися двома процедурами: простої та строгої автентифікації. Процедура простої автентифікації полягає, загалом, в обміні паролями. У процедурі строгої автентифікації застосовують несиметричні криптоалгоритми. При цьому зникає необхідність у попередньому обміні секретними паролями, що значно підвищує стійкість системи.

Захист ЕПД в процесі обробки їх у клієнтській і банківській автоматизованих системах не може бути реалізований без контролю повноважень операторів щодо запуску програмних засобів і доступу до даних.

Для фіксації процесів приймання (передачі) повідомлень засобами системи захисту слід підтримувати ведення архівів прийнятих і переданих документів, причому доступ до цих архівів має бути обмеженим як програмно, так і організаційно. Всі повідомлення про спроби НСД до інформації, виявлені засобами системи захисту, повинні фіксуватися в спеціальних журнальних файлах.

Починати використовувати систему "Клієнт–Банк" можна тільки після укладання між клієнтом і банком угоди, в якій чітко зафіксовані зобов'язання сторін стосовно одна одної, а також їхня згода підкорятися вимогам, викладеним у "Положенні про порядок використання засобів цифрового підпису", вирішувати всі спірні питання у відповідній експертній організації та підкорятися її рішенням.

Звідси випливає, що система захисту "Клієнт–Банк" має бути комплексом програмно-апаратних засобів, що функціонують у банку і у клієнта. Можливі схеми включення цих засобів до поданої на рис.5 технології наведено на рис.6,7.

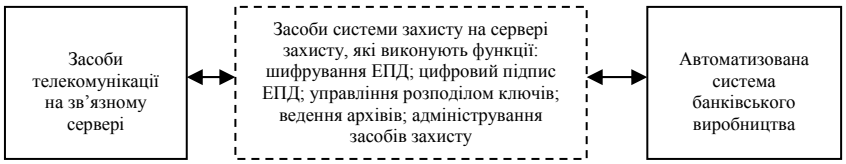

Рис. 6 Схема включення засобів захисту банку

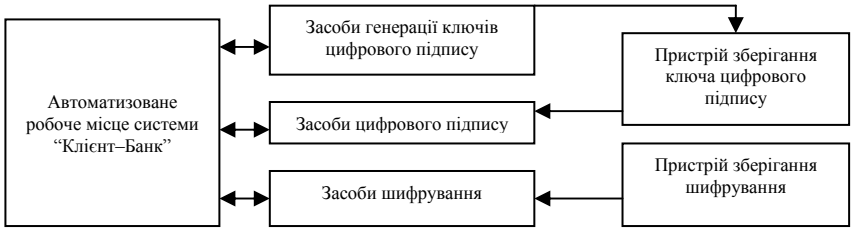

Рис.7. Схема включення засобів захисту у клієнта

Засоби захисту в клієнта містять програмні або апаратні засоби шифрування інформації, цифрового підпису, генерації ключів цифрового підпису.

Неодмінний компонент системи захисту – програмно-апаратні засоби захисту комп'ютерів від НСД, які обов'язково мають встановлюватися в банку, але можуть бути встановлені також у клієнта.

Слід зазначити, що, на жаль, сьогодні на ринку України практично немає систем, які задовольняють наведені вимоги. Є лише окремі їх компоненти, що реалізують, як правило, функції шифрування і цифрового підпису. При цьому абсолютно не продумані питання інтеграції засобів захисту з АСБВ і забезпечення надійного і безпечного їх взаємозв'язку. Мабуть, єдиним винятком з цього правила є система "Піраміда-К", розроблена на замовлення банку "Україна".

РОЗДІЛ 3

КОМЕРЦІЙНА ТАЄМНИЦЯ ТА ЇЇ ЗАХИСТ

Ринком володіє той,
хто володіє інформацією
(Головна заповідь менеджера)

3.1. Комерційна таємниця

На даний час існує поділ таємниці на державну та комерційну. Отже, з області права виділяють інститут приватного права, який захищає інтереси підприємців.

Державна таємниця – вид таємної інформації, що охоплює відомості у сфері оборони, економіки, зовнішніх відносин, державної безпеки і охорони правопорядку, розголошення яких може завдати шкоди життєво важливим інтересам України і які визначені у порядку, встановленому Законом "Про державну таємницю", та підлягають охороні з боку держави.

Законодавство України про державну таємницю базується на Законі України "Про інформацію" та інших актах законодавства, прийнятих відповідно до нього.

Дія законодавства України про державну таємницю не поширюється на відносини, пов'язані з охороною комерційної банківської таємниці, іншої конфіденційної та таємної інформації, якщо остання одночасно не є державною таємницею.

Власник інформації, що віднесена до державної таємниці або її матеріальних носіїв, здійснює своє право власності із врахуванням обмежень, встановлених відповідно до Закону "Про державну таємницю".

Порядок та умови охорони державної таємниці, включаючи встановлення спеціального режиму користування і розпорядження інформацією, що віднесена до державної таємниці, та її носіями, визначають відповідно до вищезгаданого закону договором між власником інформації або її носіїв та Державним комітетом України з питань державних секретів.

Якщо зазначені в договорі обмеження права власності на інформацію, що віднесена до державної таємниці, та її носії завдають шкоди їх власнику, ця шкода йому компенсується повним обсягом, включаючи неодержані доходи, за рахунок держави.

Віднесення інформації до державної таємниці здійснюють мотивованим рішенням Державного експерта з питань таємниць.

Інформацію вважають державною таємницею з часу включення її до Переліку відомостей, що становлять державну таємницю.

Перелік відомостей, що становлять державну таємницю, формує та публікує в офіційних державних виданнях Державний комітет України з питань державних секретів на підставі рішень державних експертів з питань таємниць.

Засекречування інформації, що віднесена до державної таємниці, здійснюють шляхом надання відповідному документу, виробу чи іншому матеріальному носію інформації грифа секретності.

Гриф секретності є обов'язковим реквізитом кожного матеріального носія інформації, що віднесена до державної таємниці. Він має містити відомості про ступінь секретності цієї інформації ("особливої важливості", "цілком таємно", "таємно"), строк засекречування інформації та посадову особу, яка надала зазначений гриф.

Якщо гриф секретності неможливо нанести безпосередньо на носій інформації, він має бути зазначений у супровідних документах.

Забороняється надавати грифи секретності, передбачені Законом про державну таємницю, носіям іншої таємної та конфіденційної інформації, яка не становить державної таємниці.

Строк засекречування інформації залежить від ступеня її секретності та встановлюють у рішенні Державного експерта з питань таємниць. Він не може перевищувати для інформації "особливої важливості" 30 років, для інформації "цілком таємно" – 10 років, для інформації "таємно" – 5 років.

Після закінчення встановлених строків засекречування інформації та у разі зниження ступеня секретності інформації та скасування рішення про віднесення її до державної таємниці посадові особи, які здійснювали засекречування інформації, зобов'язані забезпечити зміну грифа секретності або розсекречення інформації.

Чим відрізняється комерційна таємниця від державної?

Відомості, які складають державну таємницю, встановлені відповідним законодавчим актом та підлягають захисту зі сторони держави. Комерційна таємниця законодавчо не визначена, оскільки вона завжди різна залежно від фірм чи підприємств, до яких вона належить. Інша відмінність полягає в тому, що державну таємницю захищають силами держави в особі відповідних органів, тоді коли комерційну – службами безпеки фірми. При цьому слід мати на увазі, що комерційні секрети можуть бути і державними секретами, проте державні – не можуть бути комерційною таємницею, оскільки в цьому випадку йшла б торгівля державними інтересами.

У повсякденному житті комерційна таємниця завжди виступає у формі комерційних секретів. Тому будь-яка таємниця є секретом, але не усякий секрет є таємницею. Виходячи з цього, спробуємо дати визначення комерційної таємниці і комерційного секрету.

Комерційна таємниця – це економічні інтереси, що приховуються з комерційних міркувань, та відомості про різні сторони і сфери фінансової, виробничо-господарської, управлінської, науково-технічної діяльності банківських установ, фірми, підприємства, компанії, корпорації (в подальшому фірми), охорона яких зумовлена інтересами конкуренції і можливою загрозою економічної безпеки фірми. Комерційна таємниця виникає тоді, коли вона становить інтерес для комерції.

Комерційні секрети – форма прояву комерційної таємниці. Вони є інформацією у вигляді документів, схем, виробів, що належать до комерційної таємниці фірми, і підлягають захисту з боку служби безпеки від можливого посягання шляхом викрадення, вивідування тощо витоку інформації.

Їх розрізняють за такими ознаками:

природою комерційної таємниці (технологічні, виробничі, організаційні, маркетингові, інтелектуальні, рекламні);

належності власнику (власність фірми, групи підприємств, окремої особи, групи осіб тощо);

призначенням.

Документам, що містять комерційні секрети, надають гриф "конфіденційно", "суворо конфіденційно", "конфіденційно лише адресату" тощо).

Під носієм секрету розуміють особу, обізнану про комерційні секрети фірми (керівників і допущених до комерційних секретів виконавців).

Носіїв комерційних секретів слід відрізняти від джерел закритої комерційної інформації ("ноу-хау", схем, документів, технологій, виробів, зразків).

Секретність в умовах ринкового господарювання захищає виробника від недобросовісної конкуренції, до якої належать різні протиправні дії у вигляді прихованого використання торгової марки, підроблення

продукції конкурента, обманної реклами, підкупу, шантажу тощо. Не останнє місце в цьому ряді займає несанкціонований доступ до секретної інформації (промислове шпигунство)[*].

Сьогодні стало вже масовим явищем безсоромне запозичення інтелектуальної і промислової власності: співробітники підприємств, які є одночасно членами кооперативів, малих і спільних підприємств, використовують методики, програми і технології, розроблені на вітчизняних підприємствах і які є їх інтелектуальним капіталом. Західні партнери прагнуть законним шляхом отримати закриту інформацію, що є економічним інтересом для них. Тому забезпечення економічної безпеки фірми чи будь-якої іншої форми господарювання в умовах ринкової економіки вимагає захисту комерційної таємниці.

У США, ФРН, КНР, Японії й інших країнах захист комерційної таємниці забезпечують системою фінансово-промислової секретності, яка базується на відповідній правовій базі. При цьому основну роль у забезпеченні її збереження відіграють самі фірми, а не державні органи.

У Сполучених Штатах, які мають найбільш досконале законодавство в області захисту інформації, Закон про комерційну таємницю або, за їхньою термінологією, "фірмових секретів" ("секретів виробництва") був прийнятий лише в 1979 р. і то не всіма штатами. Згідно з цим законом комерційною таємницею є інформація, яка: має самостійну економічну вартість завдяки тому, що не є загальновідомою або доступною людям, які можуть використати її в комерційних цілях; є об'єктом розумних зусиль по захисту.

Якщо щось названо комерційною таємницею, то це дійсно повинно нею бути, що інколи непросто довести юридично. Тому закон рекомендує:

вказати цінність інформації (які кошти затрачені на отримання інформації і у що обійдеться вам її несанкціоноване обнародування);

назвати, які заходи захисту даного секрету були зроблені.

У ФРН діє закон про недобросовісну конкуренцію, в якому виділяють два види таємниць – виробничу і комерційну. Цей закон встановлює карну відповідальність до трьох років тюремного ув'язнення за повідомлення виробничої або комерційної таємниці стороннім особам або за її вивідування.

До виробничої таємниці в ФРН належать відомості організаційного і технічного характеру, які мають відношення до способу виробництва, технології, організації праці, а також технічні відкриття, винаходи або інформація про характер і цілі дослідницької роботи тощо.

Комерційною таємницею, на відміну від виробничої, вважають відомості, які стосуються торгових відносин фірм: організація і розміри обороту, стан ринків збуту, банківських операцій, інформація про постачальників і споживачів.

Держрада КНР у 1988 р. затвердила Положення про комерційні служби безпеки, які не входять до структури державних правоохоронних органів. Комерційні служби безпеки є госпрозрахунковими організаціями і виконують певний вид робіт і послуг згідно з контрактами, що укладаються з держустановами, кооперативами, приватними підприємствами, а також підприємствами, заснованими на змішаному китайському та іноземних капіталах. Рішення про те, які секрети слід захищати на кожній фірмі, в кожній організації приймається на основі домовленості та спирається на економічний розрахунок.

---

[*] ***Несанкціонований доступ до секретної інформації*** – незаконне збирання інформації, що складає комерційну таємницю, незаконне використання секретної інформації особою або підприємством, неуповноваженим на це її власником. Об'єктом промислового шпигунства можуть виступати будь-які матеріальні чи нематеріальні об'єкти, що містять комерційну таємницю підприємства: документи, креслення, зразки продукції, неоформлені патенти, технічні проекти, інформація про ціни, контракти постачальників, маркетингові дослідження та інші відомості, що представляють підприємницький інтерес.

У Японії немає ні законів, ні будь-яких інших нормативних актів, що передбачають відповідальність за розголошування комерційної таємниці. Там ця проблема вирішується так: на департаменти кадрів, що є в кожній японській фірмі, покладають контроль за неухильним дотриманням режиму секретності, який базується на кодексі поведінки працівників. У ньому містяться положення, які забороняють:

передавати стороннім особам інформацію, що містить комерційну таємницю;

укладати угоди, які можуть підірвати довіру до фірми з боку клієнтів;

влаштовуватися без дозволу керівництва на роботу за сумісництвом;

навмисно наносити економічний збиток;

давати і отримувати хабарі.

Слід відмітити, що японський бізнес менш за все страждає від витоку інформації. Це пов'язано з властивою у цій країні системою "довірчого найму" і вихованням у співробітників почуття патерналізму, коли вони вважають себе членами однієї сім'ї.

Керівник фірми "Соні" Акио Моріта стверджує, що коли немає відданості, яку набувають з довгостроковою зайнятістю, неможливо покласти кінець витокам інформації і крадіжкам, від яких постійно страждає бізнес на Заході.

Поняття "комерційна таємниця" з'явилося в законодавстві Росії в 1990 р. у тексті Закону про підприємства і підприємницьку діяльність. Згідно з ст. 139 Цивільного кодексу Російської Федерації, прийнятого Державною Думою 21 жовтня 1994 року, "інформація складає службову або комерційну таємницю у випадку, коли ця інформація має дійсну або потенційну комерційну цінність внаслідок невідомості її третім особам, до неї немає вільного доступу на законній основі і власник інформації вживає заходів з охорони її конфіденційності".

Розголошування комерційної таємниці може погіршити економічне становище підприємства або фірми. Щоб цього уникнути, слід перевести таку інформацію в розряд "інформація, що охороняється". Це роблять наказом керівника фірми, в якому перераховують відомості, що належать до комерційної таємниці, оскільки вони мають свій, спеціальний режим охорони. Зокрема керівник фірми не може віднести до комерційної таємниці інформацію про види діяльності фірми, оскільки це може призвести до приховання відомостей про забруднення навколишнього середовища й іншої негативної діяльності, здатної нанести збиток суспільству.

Методика віднесення тих чи інших відомостей до комерційної таємниці в нашій країні ще не розроблена, тому, спираючись на досвід зарубіжних країн, обмежимося лише деякими рекомендаціями.

1. При засекреченні інформації слід виходити з принципу економічної вигоди і безпеки фірми. Причому, оголошуючи ту чи іншу інформацію комерційною таємницею, важливо дотримуватися "золотої середини". Надмірне засекречення діяльності фірми може призвести до втрати прибутків, оскільки умови ринку вимагають широкої реклами вироблюваної продукції і надання послуг. Ті самі результати може викликати зневажливе ставлення до комерційної таємниці, оскільки ринок – це завжди конкуренція. Американські підприємці вважають, що втрата 20 відсотків інформації призводить до розорення фірми протягом місяця.
2. Інформація типу "ноу-хау", безумовно, має бути віднесена до розряду комерційної таємниці. ЇЇ треба охороняти і від власного персоналу, бо завжди існує небезпека, що той чи інший співробітник звільниться і влаштується на роботу в конкуруючу фірму. Інформація ж, якою він володіє, не може бути у нього вилучена, і є ймовірність її розголошення чи продажу.

У деяких країнах існує практика підписання з співробітниками угоди, за якою йому після звільнення забороняється працювати в конкуруючій фірмі. Проте такого роду угоди (див. додатки до 3 розділу) діють

лише протягом певного терміну після розірвання договору з найму. Зокрема, під час дії цього обмеження співробітнику слід виплачувати винагороду. У нашій практиці такі угоди поки що невідомі.

3. Інформація про раціоналізаторську пропозицію, винахід тощо, що знаходиться у стадії розробки, безсумнівно, належить до комерційної таємниці.

Раціоналізаторська пропозиція навіть після її оформлення і видачі авторського свідоцтва може залишатися комерційною таємницею, оскільки є технічним розв'язанням задачі, новим для даної фірми.

Винахід після видачі на нього патенту має спеціальну правову охорону і тому не потребує захисту за допомогою комерційної таємниці. Інша справа, якщо за угодою з автором винаходу фірма ухвалить рішення не подавати заявку в Держпатент України. Тоді охорона інформації цілком покладається на фірму. Слід підкреслити, не подавати заявку на винахід на патентоспроможне технічне рішення можливо лише за домовленістю з автором.

За даними російських літературних джерел донедавна 90 відсотків авторських свідоцтв отримували гриф "для службового користування". Замість авторського свідоцтва тепер видають патент*. Основним принципом патенту є його обов'язкова відкритість, що сприяє прискоренню науково-технічного прогресу. Патент – товар винахідника, але держава, при необхідності, може засекречувати патенти.

4. Особливу увагу слід приділити охороні договорів, що укладаються фірмою. Більшість, безумовно, належить до комерційної таємниці. Причому у певних випадках охороні підлягає не лише текст договору, але і сам факт його укладання.

Керівник фірми має встановити суворий порядок зберігання перших примірників договорів і роботи з ними. Їх слід зберігати у певному місці у відповідальної особи і видавати лише під розписку з письмового дозволу керівника фірми. На особи, відповідальні за зберігання договорів і роботу з ними, покладають персональну відповідальність за втрату договорів або витік інформації з них. Все це необхідно тому, що діяльність комерційних структур будують здебільшого на договірних засадах, і конкурент або партнер на переговорах, володіючи інформацією у цій сфері, може скласти досить повну картину виробничого і фінансового стану фірми. Пропажа (крадіжка) перших примірників договорів веде до значних ускладнень і навіть неможливості доведення тих або інших положень при виникненні суперечки і її вирішення в судовому порядку. При підписанні договору рекомендують, щоб представники сторін ставили підписи не лише в кінці договору, але і на кожному листі, щоб уникнути заміни одного тексту іншим.

Слід відмітити, що витрати зарубіжних фірм на охорону своєї комерційної таємниці становлять 10-15 відсотків усіх витрат на процес виробництва. Тому найбільш ощадливі підприємці намагаються на цьому зекономити, переклавши витрати на плечі держави. Яким чином? Шляхом отримання держзамовлень оборонного характеру. Крім інших переваг держзамовлення дають змогу користуватися захистом державних правоохоронних органів і, насамперед, контррозвідки.

Допускаючи працівників фірми до держсекретів, контррозвідка з властивою їй ретельністю перевіряє благонадійність кожного з них.

Традиційна перевірка громадян США, що отримують доступ до секретної інформації, звичайно включає:

обов'язкову перевірку на детекторі брехні (поліграфі). У число тих, що перевіряються, включають також співробітників служб безпеки і персонал фірм-підрядчиків. Відмова від проходження перевірки на детекторі брехні веде до автоматичного позбавлення допуску або звільнення з роботи;

глибоке і всебічне вивчення досьє кандидата на роботу, перевірка його біографічних даних за останні 10 років, з'ясування цілей і обставин поїздок за кордон, дослідження фінансового стану.

У ході перевірки працівників отримані відомості зіставляють з даними Національного банку інформації про секретоносії, де на кожного існує електронне досьє. У ньому містяться дані попередніх перевірок, фотокартка працівника, фонограма його голосу, інформація про зміни в його фінансовому положенні, про його поїздки за кордон.

Крім перевірки на благонадійність співробітників комерційної фірми, що отримують доступ до державних секретів, контррозвідувальні органи формують систему безпеки фірми, включаючи програму захисту, вводять в її штат своїх співробітників.

Наша економіка знаходиться на етапі становлення ринкових відносин, тому для комерційних структур, не пов'язаних з виконанням оборонних замовлень, стан захисту від промислового шпигунства гнітючий.

Що можна рекомендувати керівнику, який починає створювати систему безпеки на своїй фірмі? Передусім, знати, що це обійдеться недешево. Доручити створення системи безпеки професіоналам, і лише їм. Відразу ж слід подумати про безпеку найважливіших секретів, витік яких здатний нанести збиток, що значно перевищує витрати на їхній захист. При цьому треба встановити: яка інформація потребує захисту; кого вона може зацікавити; який "термін життя" цих секретів; у що обійдеться їхній захист.

Потім треба підготувати план з охорони комерційної таємниці. Як свідчить зарубіжний досвід, він повинен складатися з двох розділів: запобігання викраденню секретної інформації і запобігання витоку секретної інформації. Для цього потрібно:

визначити, яка комерційна інформація є секретом фірми;

встановити місця її нагромадження;

виявити потенційні канали витоку інформації;

отримати консультацію з перекриття цих каналів у фахівців;

проаналізувати співвідношення витрат на використання різних систем, що забезпечують захист секретної інформації, і вибрати найприйнятнішу;

призначити людей, відповідальних за кожну частину цієї системи;

скласти графік перевірки стану справ на дільницях.

Система забезпечення безпеки фірми охоплює такі організаційні заходи:

контроль приміщень і обладнання (забезпечення безпеки виробничих і конторських приміщень, охорона фото- та іншого копіювального обладнання, контроль за відвідувачами);

робота з персоналом (бесіди при прийомі на роботу, інструктаж щойно прийнятих працівників з правилами захисту інформації, навчання збереженню комерційної таємниці, стимулювання дотримання комерційної таємниці, робота з співробітниками, що підозрюються в розкраданні секретної інформації, бесіди з тими, що звільняються);

організація роботи з конфіденційними документами (встановлення порядку діловодства, контроль за походженням секретних документів, контроль за публікаціями, розсекречення і знищення конфіденційних документів, охорона секретів інших фірм);

робота з конфіденційною інформацією, нагромадженою в комп'ютерах фірми (створення системи захисту електронної інформації від несанкціонованого доступу, забезпечення контролю за користуванням ЕОМ);

захист комерційних таємниць фірми в процесі укладання контрактів (тут важливо чітко визначити коло осіб, що мають відношення до цієї роботи).

---

* Перший патент на винахід був виданий у 1791 р.

Викладений вище план є наближеним. Однак, у всіх випадках захисту комерційної таємниці слід звернути особливу увагу на документи, оскільки в нашій країні основні обсяги комерційної інформації зберігають в документах.

Керівник має впорядкувати процеси фіксації секретної інформації в ділових паперах і організувати їх рух так, щоб викрадення конфіденційних документів було ускладнено настільки, щоб воно ставало економічно невигідним для викрадача.

При роботі з документами, що містять комерційну таємницю, слід дотримуватися певних правил, а саме:

суворого контролю (особисто або через службу безпеки) за допуском персоналу до секретних документів;

призначення відповідальних осіб за контролем секретного діловодства і наділення їх відповідними повноваженнями;

розроблення інструкції (пам'ятки) роботи з секретними документами, ознайомлення з нею відповідних співробітників фірми;

контроль за прийняттям працівниками письмових зобов'язань про збереження комерційної таємниці фірми;

особистий контроль з боку керівника фірми за службами внутрішньої безпеки і секретного діловодства.

Існують різні способи ведення секретного діловодства, спрямовані на запобігання витоку комерційних секретів, що містяться в документах. Як вже було вказано, документи, що містять комерційну таємницю, поділяють у міру секретності інформації, що є в них, і забезпечують відповідним грифом секретності.

Для роботи з секретними документами відводять спеціальні приміщення з надійною звукоізоляцією. У ті приміщення не допускають не лише сторонніх осіб, але і співробітників, що не мають дозволу (допуску) на роботу з секретами фірми. Ці приміщення повинні мати капітальні стіни, надійні перекриття, міцні двері із замками та засувами, захист на вікнах від проникнення сторонніх осіб, а також надійно охоронятися, в тому числі системою охоронної сигналізації, електронно-механічними пристосуваннями із застосуванням кабельного телебачення тощо.

Чернетки секретних документів треба готувати в зошитах з пронумерованими аркушами. Після підготовки документів "начисто" чернетки знищують уповноважені на те співробітники. Слід вести облік кількості копій секретних документів і забезпечувати секретні машини лічильником копій і ключем, що запускає машини в дію.

Копіювальний папір і фарбувальна стрічка друкарських машин – предмет особливих турбот, оскільки з них можна зняти секретну інформацію. Тому використаний копіювальний папір і стрічку знищують під контролем відповідальних осіб.

Ймовірність витоку секретної інформації з документів особливо велика в процесі їх пересилання. Якщо немає можливості користуватися послугами воєнізованого фельдзв'язку, то доставку секретних документів і цінностей слід організувати своїми силами із залученням співробітників власної служби безпеки або ж звернутися в спеціалізовані фірми, які такі послуги надають за плату.

Працівники фірми, що відповідають за збереження, використання і своєчасне знищення секретних документів, мають бути захищені від спокуси торгівлі секретами фірми простим, але вельми надійним способом – високою зарплатою.

У процесі зберігання і пересилання секретних документів можуть застосовати засоби захисту і сигналізації при несанкціонованому доступі до них. Одна з новинок – світлочутливе покриття, нанесене на

документи, яке може проявитися під впливом світла, вказуючи тим самим на факт ознайомлення з документами або їх фотографування сторонніми особами.

З цією метою використовують і електроніку. Електронний пристрій величиною з сірникову коробку реагує на світло. Варто його включити і вмісити у сейфі, під паперами на робочому столі – і у вашому розпорядженні надійний сторож. Електронний пристрій спрацьовує при попаданні на нього світла і подає пронизливий звуковий сигнал. Цей пристрій, який коштує 10 доларів США, називають "Хоум детективом" (домашнім детективом). "Хоум детектив" забезпечують радіопередавачем, який включає на значній відстані інші захисні системи і зовнішню сигналізацію.

Фахівцям з питань комерційної інформації відомі й інші технології і системи охорони конфіденційних документів від несанкціонованого доступу або можливого витоку з них відомостей, що охороняються.

З комерційною таємницею пов'язане таке поняття як інтелектуальна власність, яке в широкому розумінні може бути визначене як комерційно цінні ідеї. Не обов'язково, щоб це було щось нове або запатентоване. Головне, щоб інформація не належала до числа загальновідомої.

Поняття "інтелектуальна власність" існує з 1967 р., коли на Стокгольмській конференції була створена Всесвітня організація інтелектуальної власності, до якої приєдналася недавно і наша держава. До цього власністю вважали лише те, що можна взяти в руки, поторкати або на що можна подивитися. Слід задуматися над тим, яку справді безцінну інтелектуальну власність має в своєму розпорядженні країна, і що берегти її треба не менше, ніж золотий запас. Цьому свідчить ряд гірких уроків. Одним з них став метод безперервного розливання сталі, що був винайдений у нас, а використаний у всьому світі, і для його повернення на батьківщину довелося заплатити чималі кошти. У країні створена велика кількість лікарських препаратів, секрети яких витекли за кордон, і зараз ми змушені купувати патенти на їх виробництво. Японський бізнесмен тепло подякував журналу "Юний технік" за його додаток "Зроби сам". Використовуючи креслення, вміщені в цьому виданні, він заробив мільйони доларів. І таких прикладів дужу багато.

Нові ідеї – специфічний товар, що має комерційну вартість. На відміну від матеріальних речей, які постійно мають вартість, скільки б разів їх не виробляли, вартість ідей одноразова (ніхто не платитиме за вже відомі відомості).

Інтелектуальна власність має не лише реальну вартість, в яку входять витрати на отримання інформації та її захист, але і потенційну вартість (можливий прибуток при її реалізації). У якості дещо несподіваного прикладу інформації, що має потенційну вартість, можна привести "негативну" інформацію (про те, що не слід робити), яка дає можливість запобігти витратам коштів на тупикові розробки.

Сьогодні рівень конкурентоздатності чималою мірою залежить від уміння захистити свою ділову, виробничу, фінансову і технічну інформацію від розкрадання, несанкціонованого використання, зміни або знищення. Як це робиться, ми розглянемо в подальшому.

3.2. Забезпечення захисту комерційної таємниці

Хороша ідея цінніша за гаманець, набитий золотом, а вкрасти її легше. Тому промислове шпигунство набуло справді гігантського розмаху[*]. За оцінками експертів, на початку 80-х років щорічні втрати американського бізнесу від крадіжки виробничих і торгових секретів перевищують двадцять мільярдів доларів[*].

[*] Воно знаходить все більш широке застосування в науці, техніці, економіці і ведеться на всіх рівнях: державами, міжнародними організаціями, фірмами, окремими особами.

[*] Духов В.Е. Экономическая разведка и безопасность бизнеса. – К.: ИМСО МО Украины, НМФ «Студцентр», 1997. – 175с.

Крім прямого викрадення можна використати і витік інформації, при цьому найбільш вірогідними джерелами є: персонал, що має доступ до інформації; документи, що містять цю інформацію; технічні засоби і системи обробки інформації, у тому числі лінії зв'язку, якими вона передається.

Отже, персонал – один з головних каналів витоку інформації. Знаючи це, треба ретельніше вивчати біографію особливо важливих співробітників. Варто звернути пильну увагу як на знову прийнятих на роботу, так і на тих, хто підлягає звільненню. Ці люди знаходяться в ситуаціях, найсприятливіших для витоку інформації. Можливими джерелами витоку інтелектуальної власності можуть стати конгреси, конференції, симпозіуми, торговельні виставки, демонстрації створеної техніки, ярмарки, реклама тощо. Професіоналів промислового шпигунства приваблюють різні з'їзди фахівців, тому що вони знають: найкращі джерела комерційної і науково-технічної інформації – базіки.

Витік інформації охоплює широке коло різних дій. Це і втрата інформації з комп'ютера, і пропажа документів. Втратою вважають і таємне копіювання інформації конфіденційного характеру з дискети на дискету, знятої "особисто для себе" копія документа, що містить комерційну таємницю.

Існує три загально прийнятих методи захисту інтелектуальної власності: патент, авторське право і комерційна таємниця.

Патентом оформляють право винахідника "законно монополізувати" використання винаходу протягом встановленого періоду. Патент є методом захисту промислової, а не комерційної інформації.

Авторське право, навпаки, захищає лише форму, в якій виражена ідея, а не саму ідею. Це відрізняє авторське право і від патенту, і від комерційної таємниці, які належать до суті, змісту ідеї. Оригінальні думки, що містяться в книгах і наукових статтях, після їх прочитання вже належать кожному. Ними можна вільно користуватися. Однак при використанні цих ідей в нових публікаціях слід робити посилання на конкретного автора, інакше будуть порушені авторські права. Це стосується здебільшого літературної творчості, музики, програмного забезпечення.

Комерційна таємниця як форма інтелектуальної власності в нашій країні не охоплена правовим регулюванням, тому для захисту комерційної інформації застосування законів значно ускладнене, і тут великого значення набувають інші заходи захисту.

Важливу роль у захисті інформації грають морально-етичні норми, які не є обов'язковими, однак їх недотримання веде до втрати авторитету (престижу) людини, групи осіб або всієї організації.

При охороні інформації від прямого розкрадання або знищення нерідко вдаються до заходів фізичного захисту. Це – замки на дверях, грати на вікнах, різні механічні, електромеханічні і електронні пристрої охорони будівлі, лабораторії, інших приміщень фірми.

Фізичні заходи захисту, як правило, застосовують в сукупності з адміністративними заходами, до яких належать: організація відповідного режиму секретності, пропускного і внутрішнього режиму, створення служби безпеки, навчання й інструктаж персоналу.

Технічні системи охорони охоплюють електромеханічні, акустичні, ємнісні, радіотехнічні, магнітометричні засоби.

Як було сказано в попередніх розділах, криптографічні засоби захисту дають можливість шифрувати інформацію так, щоб її зміст міг стати доступним лише при пред'явленні специфічної інформації (ключа). Фахівці вважають криптографічне закриття інформації найефективнішим і найнадійнішим засобом.

Як потенційна загроза безпеці інформації можуть виступати стихійні лиха, несприятливе зовнішнє середовище, катастрофи, політична нестабільність, помилки і несправності комп'ютерних програм, комп'ютерна злочинність. Виходячи з властивостей загрози, вибирають різні заходи протидії.

Для захисту комерційних секретів слід дотримуватися таких правил:

забезпечення безпеки скрізь і завжди – справа професіоналів, тому що для цього потрібні спеціальні знання;

превентивні заходи мають передбачати спеціальну програму дезинформації промислових шпигунів;

система превентивних заходів має включати такий найважливіший елемент, як організація руху інформації, що охороняється, виключивши при цьому можливість її витоку;

система превентивних заходів має базуватися на матеріальній зацікавленості співробітників, а для цього треба пристойно оплачувати їхню працю.

Таку систему превентивних заходів по захисту комерційної таємниці можуть дозволити собі лише деякі приватні фірми.

Об'єктивні потреби фірми, банку страхової компанії тощо в забезпеченні збереження комерційної таємниці визначаються рядом чинників, а саме: загостренням конкурентної боротьби на ринку товарів і послуг; важливістю збереження секретної інформації протягом деякого проміжку часу; можливістю перевірити кожний з вірогідних каналів витоку інформації і, насамперед, конкретних працівників.

Останні два чинники мають бути ретельно прораховані за витратами.

На початковій стадії створення фірми, коли її штат обмежений кількома співробітниками, а фінансові можливості не дають змоги здійснити весь комплекс заходів по захисту інформації, складається ситуація, при якій будь-які дії конкурентів несуть реальну загрозу існуванню фірми. На цій стадії слід здійснити хоча б мінімальний комплекс заходів:

постановити, щоб працівники в заявах про прийом на роботу, в трудових угодах і контрактах брали на себе чітко виражені письмові зобов'язання не розголошувати таємниці фірми та іншу інформацію, що нею охороняється;

визначитися з потоками інформації і всі документи, що містять комерційну таємницю, позначити відповідним грифом, що відображає міру їх секретності. Сюди належать, передусім, документи з планами майбутньої діяльності фірми, технологічна документація, списки постачальників і покупців;

передбачити питання захисту комерційної таємниці в типових угодах із замовниками, покупцями виробів і послуг фірми, продавцями, торговими агентами тощо.

У промислово розвинених країнах основою захисту комерційної таємниці є законодавчі акти і контракти найму-звільнення, які укладає фірма з працівниками. Навіть при наявності відповідних законів більшість фірм йде на те, щоб підписувати контракти зі своїми працівниками про нерозголошування довірених їм секретів або з моменту встановлення трудових відносин, або коли співробітник отримує доступ до комерційних секретів.

В умовах, коли правове регулювання охорони комерційної таємниці вже існує, слід обумовити прийняття на себе працівником фірми, прийнятим за контрактом, зобов'язання про нерозголошування комерційних секретів. При цьому даний документ має прямо передбачати право роботодавця розірвати трудову угоду (контракт) із співробітником, що порушив назване зобов'язання, а також вживати інших заходів, передбачених законом.

У країнах, де норми права досить детально регламентують охорону комерційної таємниці, використовують загальновживані форми угод (контрактів) про її нерозголошування.

Приклад форми документа, рекомендованої для захисту ділової інформації подано в додатку 1 до 3-го розділу.

Звичайно, працівник фірми, підписуючи такого роду документ, повинен чітко уявляти, *що* конкретно з ділової інформації і технологічних розробок є таємницею фірми. Якраз з цієї причини і вважають обов'язковою

вимогу про те, щоб вся секретна інформація була відособлена від інших відомостей, і документи, що її містять, носили відповідний гриф.

На практиці для охорони комерційної таємниці фірми її працівниками як під час роботи в ній, так і після звільнення використовують більш детально розроблені угоди. Важливо, щоб умови збереження комерційної таємниці колишнім співробітником фірми були реальними за часом, залишаючи йому можливість підшукати гідно оплачувану роботу.

Використання контрактів про збереження комерційної таємниці дає можливість забезпечити формальний юридичний захист комерційної інформації, до якої має або мав доступ персонал фірми.

Однак, комерційні таємниці цілком або частково можуть стати відомими діловим партнерам вашої фірми в процесі обміну з ними необхідною для спільної роботи інформацією. Отже, вони мають взяти на себе зобов'язання по захисту ваших комерційних таємниць, так само як і вам слід вчинити з ними. Це традиційна для ділового світу практика, але і вона має підкріплюватися письмовими зобов'язаннями (див. додаток 2 до 3-го розділу).

Готуючи документи на придбання яких-небудь товарів чи послуг, розміщуючи замовлення на них, слід у відповідних угодах або договорах обов'язково вказати, що продавець (постачальник) зобов'язується зберігати в секреті всю надану йому в зв'язку із замовленням вашу інформацію. Після виконання замовлення всі документи фірми, що містять секретну інформацію, він зобов'язується повернути у зазначені терміни.

Рекомендують на документах з конфіденційною інформацією, що адресується постачальникам фірми, ставити штамп, який свідчив би про те, що викладені в документі відомості є приватною власністю фірми і вимагають охорони і своєчасного повернення власнику.

Угоду про збереження конфіденційної інформації слід підписати і з тими діловими партнерами, які надають фірмі різного роду сервісні послуги (ремонт обладнання, прибирання приміщень тощо).

Якщо фірма вдається до послуг торгових посередників і наймає торговий персонал, то і в цьому разі єдиною можливістю збереження комерційних секретів буде підписання з ними відповідного контракту.

Немає інших шляхів для збереження комерційних секретів продукції (товарів), що виробляє (реалізовує) фірма в спілкуванні з контрагентом, крім укладання відповідної угоди про збереження комерційної таємниці. Такі відомості можуть бути потрібні контрагенту, наприклад, для того, щоб оцінити ваші можливості нарощування виробництва даного виду продукції (товару), коротка угода про збереження таємниці змусить його берегти отриману інформацію.

Так само охороняють комерційні таємниці третьої сторони, зокрема, вашого постачальника.

Ділові партнери можуть висловити побажання про надання їм всієї комерційної інформації для оцінки реального стану ваших справ. На попередній стадії обговорення операції слід уникати детального обговорення вашої секретної інформації. Це можливо лише після підписання угоди про збереження комерційної таємниці.

Загалом же захист комерційних таємниць фірми в спілкуванні з дружніми, лояльними особами або ж тими, що займають нейтральну позицію щодо вашого бізнесу, здійснюють на основі укладання відповідних угод, прямо вказаних у нормах або заснованих на них.

Навіть ті таємниці фірми, що ретельно охороняються, можуть стати відомими вашим конкурентам із звичайних публікацій для широкої публіки, якщо пустити цю справу на самоплив. Тому один із співробітників має заздалегідь переглядати рекламні оголошення, брошури, що готують до друку, прес-релізи та інші матеріали, призначені для симпозіумів, конгресів, виставок, а також виступи, наукові та інші публікації співробітників вашої фірми. Він має керуватися простим, але досить ефективним правилом, суть якого полягає в тому, щоб максимально роздрібнити, роз'єднати за часом і авторами ту секретну комерційну інформацію, без

якої неможливе опублікування згаданих вище робіт. Все це істотно перешкоджає збору секретної інформації про фірму конкурентами або недоброзичливцями. Звичайно, цей бар'єр можна подолати, але лише за допомогою значних витрат.

Важко знайти золоту середину між прагненням зберегти комерційну таємницю і бажанням використати в рекламних цілях найбільш вражаючі дані з секретної інформації, особливо ті з них, які, безсумнівно, допомогли б розширити збут вироблюваних товарів і послуг.

Розглянемо тепер питання про те, як і де підприємець може отримати необхідні йому відомості про клієнтів і конкурентів, що дають йому можливість нормально працювати в умовах ринкової економіки. Відомо, що володіння такими відомостями за своєю суттю є одним з елементів системи превентивних заходів по боротьбі з промисловим шпигунством.

У капіталістичних країнах інформацію про клієнтів прийнято вважати не комерційною таємницею фірми, а швидше, її капіталом. Тому список клієнтів фірми та інші відомості про них складає, перш за все, керівник, і цю інформацію не довіряють навіть його найближчому оточенню.

На кожного клієнта фірми нагромаджують інформацію, де відбивають його звички, характерні риси поведінки, інтереси особистого життя, надані йому фірмою привілеї. Тут зберігають відомості про його вимоги до кількості товарів і послуг, застосовувані режиму доставки товарів, періодичність доставок, особливості платні та інші специфічні риси контрактів з даним клієнтом. Тут відбивають ті відомості, які визначають прибутковість всієї операції з клієнтом, передбачення об'ємів операцій, частота поставок.

Інформацію про діяльність фірми і її керівників збирають в різних економічних журналах і газетах, довідниках, випитують у біржовиків, купують у приватних детективів.

Обізнаність про найбільш вигідних клієнтів конкурента дає шанс перемогти в змаганні з ним, якщо вам вдасться "переманити" його клієнтуру. Тут на перший план виступає персоніфікована інформація про клієнтів, відомості про симпатії і антипатії, їхню прихильність, дружні зв'язки в середовищі підприємців і їхніх конкурентів, які впливають на прийняття ними рішень про підтримку ділових відносин з вашою фірмою або їх припинення.

Збір інформації про клієнтів і конкурентів має бути впорядкований найретельніше, і цю інформацію слід зберігати лише у керівництва фірми.

Співробітники фірми, що просувають на ринок її продукцію, мають надати письмові звіти про конкретних клієнтів за кожним фахом продажу. У цих звітах слід відобразити перспективи майбутніх операцій.

Якщо вашій фірмі під силу витрати на утримання аналітичного відділу, що вивчає кон'юнктуру ринку, клієнтів, конкурентів, то і в цьому випадку слід розподіляти такого роду конфіденційну інформацію серед співробітників.

Документація на це має бути суворо секретною, а персонал, який працює з нею, – дотримуватися правил поводження з секретними документами. Всі працівники, що працюють безпосередньо з клієнтами, повинні дати письмові зобов'язання про зберігання комерційних таємниць фірми.

Аналітичний відділ або відділ маркетингу, вивчаючи клієнтів, має одночасно збирати і аналізувати відомості про конкурентів. Для цього треба розробити програму дій кожного співробітника відділу. Слід чітко знати, які відомості треба мати і де вони концентруються, хто, як і де може добути ці відомості з найменшими витратами, які труднощі можуть виникнути і як їх подолати. Обов'язково слід фіксувати: де, коли і як отримана інформація, ким конкретно і що з нею зроблено*.

* Наприклад, в Європі існує аналітична структура «Єврогейт», заснована найбільшими банками, таких як англійський «Ротшильд», французький «Кафас», німецький «Гермес». Її задачі полягають у зборі даних на всі зареєстровані фірми: їхній оборот, статутний капітал,

У наших умовах добування достовірної інформації про клієнтів та конкурентів – предмет постійного головного болю. Ринок, його інформаційні структури – ще в стадії формування, причому на найнижчих рівнях. З цієї причини можна розв'язати проблему так:

власними силами (створення відділів маркетингу, вивчення попиту тощо);

отриманням за плату потрібної інформації у тих комерційних структур, які мають її в своєму розпорядженні (банки, страхові компанії, біржі, приватні детективні агентства тощо);

звертання за допомогою, зрозуміло, платою, до служб промислової контррозвідки, до приватних розшукних агентств тощо.

Підприємець здійснює вибір сам, але в будь-якому випадку цей вибір слід зробити тому, що система превентивних заходів, що забезпечує безпеку фірми, без вичерпної інформації про її клієнтів і конкурентів існувати не може, а сама фірма в таких умовах приречена на програш в конкурентній боротьбі.

Добуваючи життєво важливу комерційну інформацію, не слід забувати, що ваші конкуренти думають про те саме. У Франції, наприклад, за промисловими секретами полюють десятки тисяч промислових шпигунів і на оплату їхньої праці французькі бізнесмени щорічно тратять понад один мільярд доларів.

Для постійного спілкування з представниками засобів масової інформації (ЗМІ) і громадськості слід призначити компетентного, тямущого співробітника, що вміє спілкуватися з людьми, приваблювати їх до себе, швидко реагувати на зміну обставин. Він готує програму, що відображає такі питання: в яких засобах масової інформації, коли і як часто мають освітлюватися узгоджені з керівництвом фірми теми або проблеми; в якому напрямі слід орієнтувати громадськість з поточних питань життя фірми; які теми піднімати в пресі.

Виходячи з **Закону України "Про друковані засоби масової інформації (пресу) в Україні" від 16.11.1992р.**, не допускається використання засобів масової інформації "… для розголошування відомостей, що складають державну або іншу спеціальну таємницю, що охороняється законом". Зокрема **Закон України "Про інформацію" від 2.10.1992р.** наголошує, що не підлягають розголошенню такі відомості: що становлять державну або іншу передбачену законодавством таємницю; що стосуються лікарської таємниці, грошових вкладів, прибутків від підприємницької діяльності, усиновлення, листування, телефонних розмов і телеграфних повідомлень, крім випадків, передбачених законом (ст.46). Порушення законодавства України про інформацію тягне за собою дисциплінарну, цивільно-правову, адміністративну або кримінальну відповідальність згідно з законодавством України (ст.47). Крім того, цей закон передбачає відповідальність за можливість нанесення навіть неістотної матеріальної та моральної шкоди через розголошування комерційних таємниць (ст.49).

При проведенні різного роду зустрічей з представниками ЗМІ цей працівник має бути наділеним правом розпоряджатися представницькими коштами. Природно, що після кожної зустрічі подається фінансовий звіт. У ході зустрічей з журналістами не слід забувати про збереження комерційних секретів.

Працівників слід проінструктувати так, щоб кожний з них, уникаючи спілкування з представниками ЗМІ з питань своєї службової діяльності, відсилав їх до спеціально підготовленого для цих цілей співробітника.

Робочі приміщення, службові кабінети мають бути закритими для відвідування сторонніми особами. Всіх відвідувачів, крім клієнтів і ділових партнерів, повинні зустрічати і супроводжувати по території фірми працівники відділу кадрів, служби внутрішньої безпеки або охорони. Прийом відвідувачів і роботу з ними здійснюють у спеціально обладнаних технічними засобами охорони і сигналізації приміщеннях.

У багатьох фірмах промислово розвинених країн відвідувачам видають разові картки (перепустки) гостя, що розміщуються на грудях або на лацкані піджака. Картки забарвлені в яскраві кольори. Доступ у ті чи

нерухомість, точність в розрахунках, відносини з податковими, адміністративними, судовими інстанціямиУ Росії представником є фірма «РУСС-ИГК». За помірну плату вона надає своїм клієнтам необхідну інформацію.

інші приміщення фірми визначають кольором гостьової картки. Переміщення гостя, таким чином, контролюють не лише супроводжуючі його особи, а й інший персонал фірми.

Деякі приміщення в будь-якому випадку слід залишати недоступними для відвідувань всіма без виключення сторонніми особами, а також співробітниками фірми, недопущеними до роботи з її секретами. Ці приміщення – "свята святих" – сховища секретних документів, кімнати для роботи з ними, певні підрозділи фірми, такі як: відділ маркетингу, служба внутрішньої безпеки, аналітичний відділ. Всі приміщення знаходяться в зоні безпеки, забороненій для доступу сторонніх осіб, яку суворо охороняють і періодично перевіряють на можливу наявність у ній технічних засобів промислового шпигунства. Ця зона – об'єкт особливих турбот для служби внутрішньої безпеки. Її стерильність від електронних засобів, призначених для промислового шпигунства, багато в чому забезпечує економічну безпеку і конкурентоздатність фірми, її виживання в умовах ринкової економіки.

Сьогодні електронні засоби, призначені для промислового шпигунства, досягли високого рівня досконалості в своєму розвитку. Вже багато років підряд не вимагає великих зусиль запис розмови в приміщенні по вібрації віконного скла з вулиці з досить великої відстані. Записують і розмову в машині з машини, що йде паралельно, трохи позаду або спереду, обладнаної відповідними електронними системами. За даними преси, на "чорному ринку" вартість одного "жучка" для підслухування коливається від 300 до 1000 доларів. Задоволення дороге, але доступне. Попит є, але поки невеликий, що дає можливість сподіватися на декілька років спокійного життя для вашої фірми, але не більше.

Отже, що ж належить до комерційної таємниці і потребує захисту?

І. Ділова інформація:

фінансові відомості;

дані про ціну (вартість) продукції і послуг, технології;

ділові плани і плани виробництва нової продукції;

списки клієнтів і продавців, контракти, преференції і плани;

інформація про маркетинг;

угоди, пропозиції, квоти;

списки персоналу, організаційні схеми й інформація про співробітників (їх характеристики).

ІІ. Технічна інформація:

науково-дослідні проекти;

конструкторські розробки по виробництву якої-небудь продукції і її технічні параметри;

заявки на патенти;

дизайн, ефективність і можливості виробничих методів, обладнання і систем;

інформаційний процес;

програмне забезпечення ЕОМ[*].

Аналізуючи зарубіжний досвід по створенню механізму захисту комерційної таємниці, можна виділити основні блоки, з яких він складається:

норми права для захисту інтересів її власників;

норми, встановлені керівництвом фірми, фірми тощо (накази, розпорядження, інструкції);

[*] В Японії для захисту комп'ютерних програм використовують патенти, у США такі програми розглядаються як інтелектуальна, а не промислова власність. Деякі юристи ряду країн вважають, що комп'ютерні програми є унікальнними і вимагають якоїсь нової форми захисту. Вони вважають, що ні закон про патенти, ні закон про авторське право тут не годяться.

спеціальні структурні підрозділи, що забезпечують дотримання цих норм (підрозділ режиму, служби безпеки тощо).

Все вищевказане має бути тісно пов'язане між собою. Так, наприклад, фірма може мати найдосконаліші права й інструкції, що стосуються внутрішнього порядку поводження з конфіденційними матеріалами, але при відсутності державно-правового регулювання навряд чи зможе захистити свої секрети. Так само навряд чи вдасться зберегти секрети при наявності правового регулювання, але при відсутності професіоналів, які втілюватимуть норми права й інструкції на практиці. А не знаючи основних напрямків захисту секретів, не вдасться зберегти свою конфіденційну інформацію навіть при наявності державної підтримки і спеціального структурного підрозділу в штатному розкладі.

Сьогодні, коли повною ходою йде процес становлення нових господарських форм і відносин, у підприємств виникають проблеми, пов'язані з необхідністю захисту власної секретної інформації. Спроби, що робляться для автоматичного перенесення системи організації державних секретів в область комерційної таємниці, напевне, приречені на невдачу.

Світовий досвід в області захисту виробничих секретів показує, що суто адміністративні заходи не гарантують результат, тому підприємці, не відмовляючись від адміністративних заходів, переходять до поєднання їх з активним залученням в процес захисту конфіденційної інформації всіх співробітників фірми.

Головне місце в організації надійного захисту секретної інформації відводять роботі з кадрами. Фахівці вважають, що збереження секретів на 80 відсотків залежить від правильного підбору, розміщення і виховання кадрів. І цю роботу слід починати від дня прийому людини на роботу.

Другим за важливістю заходом є обмеження доступу до секретної інформації. Робота має бути організована так, щоб кожний співробітник мав доступ лише до тієї інформації, яка необхідна йому в процесі виконання прямих службових обов'язків. Ця міра не зможе цілком захистити від можливого її витоку, але дасть змогу звести можливий збиток до мінімуму.

Третім напрямком у роботі з кадрами є проведення виховної роботи. Фахівці області протидії промисловому шпигунству дають такі рекомендації:

використовувати будь-яку можливість для пропаганди програм забезпечення режиму секретності;

різнобічно стимулювати зацікавленість робітників у виконанні режиму секретності;

не забувати періодично винагороджувати співробітників за успіхи в захисті секретної інформації.

Слід мати на увазі, що самі заклики не дають позитивних результатів, тому значне місце у виховній роботі відводять навчанню, цілями якого є:

чітке знання співробітником обсягів інформації, що охороняється, за безпеку якої він несе особисту відповідальність;

розуміння виконавцем секретних робіт, характеру і цінності даних, з якими він працює;

навчання правилам зберігання і захисту секретних даних.

При цьому жодне правило або процедуру не рекомендують вводити без роз'яснення їхньої суті, доцільності і необхідності. Кожний керівник, доводячи такі правила до відома своїх підлеглих, зобов'язаний підкреслити, що вони є невід'ємною частиною їхньої роботи.

Водночас не слід обмежуватися лише виховною роботою і навчанням. Співробітник, що порушив правила роботи з секретною інформацією, має знати, що у нього будуть серйозні неприємності і він буде покараним керівництвом.

Такі підходи до роботи з кадрами дають непогані результати і можуть застосовуватися на фірмах різного профілю діяльності.

Важливим напрямком в організації роботи по захисту конфіденційної інформації є встановлення порядку поводження з її носіями, такими як документи, креслення, дискети, комп'ютерні програми тощо. При цьому слід враховувати, що:

фахівці ставлять обов'язковою умовою наявність на носіях конфіденційної інформації відмітних поміток, що розрізняють залежно від рівня секретності, але вони мають відрізнятися від тих, що застосовуються в сфері захисту державних секретів;

в умовах фірми забезпечити кожному виконавцеві роботу в спеціально виділеному приміщенні буває практично неможливо, тому слід дотримуватися "політики чистих столів", суть якої полягає в тому, що при відсутності працівника на робочому місці не має бути жодних документів.

У нас існує міф про те, що в західних фірмах на кожному кроці стоять ксерокси і зробити копію з будь-якого документа не складає труднощів для будь-якого бажаючого. Це абсолютно не відповідає дійсності: в будь-якій фірмі, що має справу з конфіденційною інформацією, існує суворо встановлений порядок розмноження документів. З метою утруднити або навіть унеможливити копіювання закритих матеріалів вживають додаткових заходів захисту. Так, американська фірма "Ксерокс" розробила спеціальний барвник, який наносять на текст документу, що виключає можливість несанкціонованого копіювання – копія стає нечитабельною.

Як показує практика, значний витік комерційної інформації відбувається у ході ведення переговорів. Це пояснюється різними причинами: невірно зрозумілий престиж, невміння правильно рекламувати свою продукцію тощо. Велику роль відіграє вміння ведення переговорів. Співробітник повинен чітко знати, яку інформацію він має право повідомити партнеру по переговорах, а яку – ні. Слід вчити проведенню реклами за методом "чорного ящика", тобто можна повідомити параметри вибору, отриманий результат, а як він отриманий – секрет фірми. Співробітник має розуміти, що від успішно проведених переговорів залежить не лише процвітання фірми, але і його особисте благополуччя.

Ключову роль у структурі підрозділу, що займається захистом комерційної таємниці, відводять комерційній службі. Сучасна фірма, що функціонує в умовах ринкової економіки, зрозуміло, не зможе дозволити собі засекречувати всю інформацію. Це дуже дорого і невигідно: певну частину інформації використовують в рекламі, до того ж велика кількість засекречених матеріалів створює перешкоди в роботі.

Водночас фахівці в області стратегічного планування і виробництва відносять збір інформації про конкурентні фірми і компанії до звичайного маркетингу, як і інформацію про потенційних споживачів, репутацію фірми, державне регулювання на ринку тощо.

Є три основних напрямки збору інформації:

І. Інформація про ринок

ціни, умови договорів, специфікація продукту, знижки;

об'єм, тенденція і прогноз збуту конкретного продукту;

частка на ринку і тенденція її зміни;

ринкова політика і плани;

відносини із споживачами і репутація;

чисельність і розміщення торгових агентів;

канали, політика і методи збуту;

постановка реклами.

ІІ. Інформація про виробництво продукції:

оцінка якості й ефективності;

номенклатура виробів;

технологія і обладнання;

рівень витрат;

виробничі потужності;

спосіб упаковки;

доставка;

розміщення і розмір виробничих підрозділів і складів;

можливості проведення науково-дослідних робіт.

III. Інформація про організаційні особливості і фінанси

виявлення осіб, що приймають ключові рішення;

філософія осіб, що приймають ключові рішення;

програми розширення і придбань;

головні проблеми і можливості їх вирішення;

програма проведення науково-дослідних та проектно-конструкторських робіт.

Наведені напрямки охоплюють основні аспекти діяльності фірми, і намагатися захистити комерційну таємницю, накладаючи обмеження на доступ до інформації у перерахованих напрямках, навряд чи можливо, але слід надавати протидію суперникам по конкурентній боротьбі на ринку. Тут аналітичні підрозділи мають зіграти свою роль у визначенні ключової інформації, виявленні можливих каналів витоку, пошуків шляхів її захисту.

Аналіз літературних джерел показує, що на даний час об'єктом найпильнішої уваги розвідки стають технологічно розвинені виробництва і їхні керівники. Так, наприклад, американська компанія Ай-бі-ем оголосила себе жертвою шпигунських операцій з боку французьких і японських секретних служб, що заподіяли їй збиток на один мільярд доларів. Разючу картину показало дослідження, проведене одним спеціалізованим агентством серед менеджерів і підприємців: 56 відсотків опитаних упевнені, що деякі їхні важливі і не призначені для сторонніх вух розмови по телефону прослуховують*. Більше ніж 28 відсотків опитаних заявили про дивний витік інформації із захищених традиційними способами робочих приміщень. Більшість з них повідомили про викрадення даних з комп'ютерів, терміналів, блоків пам'яті.

Промислове шпигунство існує відтоді як з'явилася на світ сама промисловість. Чарівна дівчина, що "підчепила на гачок" керівника фірми, – підкуплений службовець, розкриття чемоданів з документами, залишеними безтурботними ділками в готельному номері, – все це технічні прийоми, які відомі давно і з успіхом використовуються досі, хоча в наш час мікроелектроніки й інформатики все ж значно рідше. Сьогодні перевагу віддають "жучкам" (мікрофонам і телекамері), які стають все мініатюрнішими і продаються за цінами, доступними для всіх бажаючих.

"Жучок", величина якого може бути меншою за 1 мм^3, а вага – від декількох грамів, можна сховати де завгодно – в авторучці, попільничці, спинці крісла, квітковому горщику, люстрі, пачці сигарет, кредитній картці, склянці для води тощо. Його ціна – дрібниця порівняно з прибутком, який дає здобута з його допомогою інформація. Однак, на думку фахівців, у нього є і недолік – блок живлення. Батарейка "електронного вуха" швидко зношується і до того ж є його найбільшою деталлю. Проте безвихідних становищ не буває: "жучок"

* Тому, перш ніж зняти телефонну трубку, прикиньте вартість того, про що Ви матимете намір розмовляти.

можна вмонтувати в електророзетку[**], вимикач, телефонну розетку, телефонний апарат так, щоб він постійно заряджався від електромережі. А той, кому треба підслухати розмови (телефонні і нетелефонні) з відстані півкілометра, навіть може не витрачати часу і сидіти в навушниках – досить залишити в автомобілі, припаркованому поблизу будівлі, де засідає адміністративна рада якої-небудь фірми, магнітофон або радіоприймач, приєднаний до електронного підслухувального пристрою, що вмикається лише тоді, коли об'єкт підслухування говорить.

Якщо проникнення на об'єкт є обмеженим, "жучки" вмонтовують у кулі, стріли. Оскільки модель JIPE-PS можна вмонувати в стрілу, то безшумним пістолетом її прицільно вистрілюють на віддаль до 25 м. Модель STG-301, яка передає інформацію на відстань до 100 м., вмонтовують в стрілу арбалета[*].

Нарівні із звичайними "жучками", пристосованими для перехоплення інформації в невеликих приміщеннях, на телефонних лініях чи телефаксах, існують і складніші пристрої з використанням інфрачервоних променів і які приводяться в дію в потрібний момент мікрохвилями, спрямованими з відстані. Нерідко такі "жучки" замуровують в стіни, і тому їх називають пасивними. Створені системи, здатні з відстані в кілька десятків метрів зчитувати інформацію з екранів комп'ютерів, а також мікрофони, що записують стукіт друкарської машинки, а згодом "переводять" кожний звук або набір звуків у літери алфавіту, відтворюючи необхідний текст.

Така техніка як лазерні системи, що дають змогу записувати виступ доповідача на нараді або розмову за вібрацією віконного скла, поки що є лише у розпорядженні секретних служб країн, високо розвинених у технічному відношенні. Проте і у приватного агента в розпорядженні є засоби, які ще декілька років тому не можна було й уявити: мініатюрні телекамери, що поміщуються у корпусі наручного годинника або в запальничці.

За даними публікацій існують телевізори (в основному, фірми "Панасонік") величиною з сигаретну пачку. Хоча вони чорно-білі, але телекамери можуть працювати навіть при світлі полум'я свічки і передавати сигнал на відстань 300-500 метрів. Блискуча операція "Зелений лід", внаслідок якої італійській та американській поліції вдалося виявити мережу торговців наркотиками в Італії і Колумбії, була проведена за допомогою саме таких телекамер.

Навіть розмови так званими "сотовими" телефонами, які широко застосовують, можуть легко перехопити, якщо не використовувати кодифікатор звуків. Проте і вони можуть виявитися даремними. На заході випускають спеціалізовану апаратуру для автоматичного контролю за переговорами "сотовими" телефонами.

Паралельно із службами промислового шпигунства існують й агентства по контршпигунству, які допомагають очистити від сторонніх "очей" і "вух" приміщення і телефони. Плату ці фірми беруть помірну, і до їхніх послуг вдається все більше зацікавлених осіб.

"Спорядження несанкціонованого доступу до інформації" використовують іноді в абсолютно несподіваних цілях, наприклад, для визначення ринкової кон'юнктури. Кінець XX століття відзначився тим, що завершується перехід від індустріального суспільства до суспільства інформатики. Наша цивілізація вступає в

[**] На даний час для збільшення тривалості роботи "жучків" з автономним живленням, а також для вирішення проблем приховування (зменшення часу "холостої" роботи передавача, знижує ймовірність його виявлення) розробляють моделі з дистанційним вмиканням (TRM-1530 і TRM-1532), а також із автоматичним вмиканням при виникненні звуку – музики, мови – і з вимиканням при його щезанні (STG-4001).

[*] Адрианов В., Бородин В., Соколов А. Шпионские штучки и устройства для защиты объектов информации. Справочное пособие. – С.-Пб.: Лань. 1996.

нову еру, де інформація є стержнем розвитку економіки*. Вже сьогодні 75 відсотків працівників у Сполучених Штатах, а в Японії – близько 80 відсотків займаються обробкою інформації. Скоро ви, сидячи вдома за комп'ютером, зможете отримати будь-яку інформацію з будь-якої точки планети. Але це – в майбутньому. А поки що фірмам, зацікавленим в своїй конкурентоздатності, слід забезпечити ефективний захист своєї інформації і встановити контроль за її використанням. Тому урядові і комерційні організації ряду держав приступили до реалізації програм наукових досліджень і проектно-конструкторських робіт в області захисту інформації, створення з цією метою спеціальних технічних і програмних засобів.

3.3. Захист від технічних засобів несанкціонованого доступу до інформації

Будь-яка юридична чи фізична особа (в подальшому "об'єкт") має різноманітні технічні засоби, призначені для прийому, передачі, переробки та зберігання інформації. Фізичні процеси, які відбуваються в таких пристроях, при їхньому функціонуванні створюють в оточуючому просторі побічні випромінювання, які можна виявити на досить значних відстанях (до декількох сотень метрів), і, як наслідок, перехоплювати.

Фізичні явища, які лежать в основі випромінювань мають різний характер, але витік інформації за рахунок побічних випромінювань відбувається від передавача (джерела випромінювань), середовища, в якому ці випромінювання розповсюджуються, та приймача. Таку "систему зв'язку" називають технічним каналом витоку інформації.

До ***технічних*** каналів витоку інформації можна віднести:

- радіоканали (електромагнітні випромінювання);
- електричні (напруга і точки в різних струмопровідникових комунікаціях);
- акустичні (поширення звукових коливань в будь-якому звукопровідниковому матеріалі);
- оптичні (електромагнітні випромінювання у видимій, інфрачервоній і ультрафіолетовій частинах спектру).

Джерелами випромінювань у технічних каналах є різноманітні технічні засоби, а саме ті, в яких циркулює конфіденційна інформація. Ними вважають:

- мережі електроживлення і лінії заземлення;
- автоматичні мережі телефонного зв'язку;
- системи факс, телекодового і телеграфного зв'язку;
- засоби гучномовного зв'язку;
- засоби звуко- і відеозапису;
- системи звукопосилення;
- електронно-обчислювальна техніка;
- електронні засоби оргтехніки;
- голос людини (середовищем поширення акустичних випромінювань у цьому випадку є повітря, а при зачинених вікнах і дверях – повітря і різні звукопровідникові комунікації. Якщо для перехоплення використовують спеціальні мікрофони , то утворюється акустичний канал витоку інформації).

Технічні засоби не лише самі випромінюють у простір сигнали, що містять оброблювану ними інформацію, але й вловлюють за рахунок мікрофонів, антенних властивостей інших випромінювань (акустичних, електромагнітних), які існують в безпосередній близькості від них. Вловивши, вони

* Є розрахунки, згідно з якими чоторикратне збільшення обсягу інформації веде до подвоєння виробництва.

перетворюють прийняті випромінювання в електричні сигнали, безконтрольно передають їх своїми лініями зв'язку на значні відстані. Це ще більше підвищує небезпеку витоку інформації. До числа технічних пристроїв, що мають властивість утворювати електричні канали витоку належать телефони, датчики охоронної та пожежної сигналізації, їх лінії, а також мережі електропроводки.

Для створення системи захисту об'єкта від витоку інформації технічними каналами слід здійснити ряд заходів. Перш за все, –проаналізувати специфічні особливості розміщення споруд, приміщень у спорудах, територію навколо них і підведені комунікації, а також виділити ті приміщення, всередині яких циркулює конфіденційна інформація і врахувати технічні засоби, що в них використовуються. Далі здійснюють такі технічні заходи:

- перевірку техніки, що використовується, на відповідні величини побічних випромінювань допустимих рівнів;
- екранування приміщення з технікою або техніку в приміщеннях;
- перемонтування окремих ланок, ліній, кабелів;
- використання спеціальних пристроїв і засобів пасивного та активного захисту.

Слід відмітити, що на кожний метод отримання інформації технічними каналами її витоку існує метод протидії, часто не один, який може звести загрозу витоку до мінімуму. При цьому успіх залежить від двох чинників – вашої компетентності в питаннях захисту інформації (чи то компетентності тих осіб, яким цю справу доручено) та наявності необхідного обладнання. Перший чинник важливіший, оскільки найдосконаліша апаратура стає мертвим вантажем в руках дилетанта.

У яких випадках доцільно проводити міри захисту від технічного проникнення? Перш за все, таку роботу слід здійснювати превентивно.

Здійснюючи комплекс захисних заходів, не варто прагнути забезпечити захист усього об'єкту. Головне – обмежити доступ у тих місцях і до тієї техніки, де зосереджена конфіденційна інформація (не забуваючи про можливості і методи її дистанційного отримання). Зокрема, використання кодових замків, засобів сигналізації, звукоізоляції стін, дверей, стелі і підлоги, звукового захисту вентиляційних каналів, труб, які проходять через ці приміщення, демонтаж незадовільної проводки, а також застосування спеціальних пристроїв (генератора шуму, засекреченої апаратури зв'язку (ЗАЗ) та інше вищевказане) серйозно ускладнять або зроблять беззмістовними всі спроби впровадження спецтехніки.

Отже, для розробки та реалізації заходів щодо захисту інформації від витоку технічними каналами слід доручати кваліфікованим спеціалістам або готувати власних за відповідними програмами у навчальних закладах.

Методи і засоби отримання інформації із закритого приміщення

На рис. 3.1. показано схему з різними варіантами "проникнення" в закрите приміщення з метою несанкціонованого доступу до інформації[*]:

1) лазерна установка підслухування розмови за вібрацією скла;
2) магнітофон, що приймає сигнали від "жучка", вмонтованого у вікно;
3) телекамера, з'єднана з оптичними волокнами в стіні;
4) "жучок", пов'язаний з вікном напряму;
5) система зчитування даних з комп'ютера;

[*] За даними публікацій вартість захисту інформації на час написання цієї книги в Москві: шифратор – 450 доларів, програма шифрування – 50 доларів, захист телефону – 3500 доларів, захист телефаксу – 3500 доларів. Є спеціальні системи для «прорахування» підслухування. Ви можете дізнатися, що хтось до Вас підключився, але не знатимете, хто саме.

6) “жучки” в телефонній мережі;
7) приймач сигналів від “жучка”, що реагує на стукіт друкарської машинки;
8) джерело та приймач “пасивних” мікрохвиль;
9) “жучок” у вимикачі світла”;
10) мікрофон вузькоспрямованої дії.

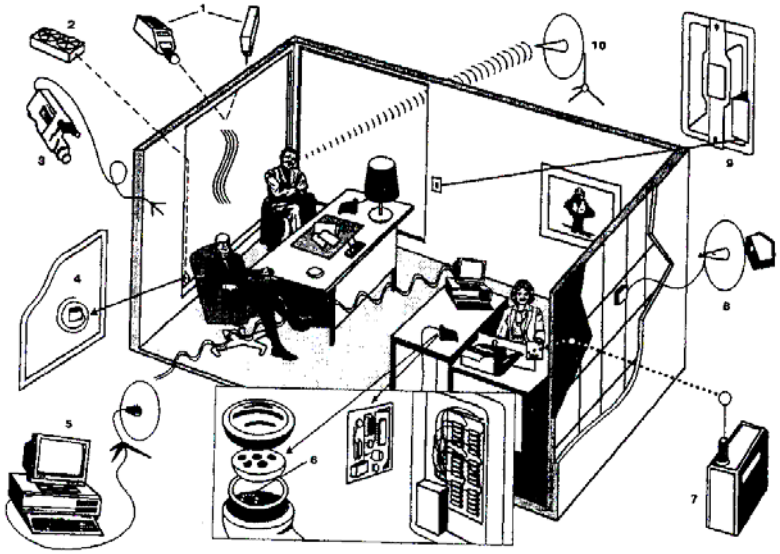

Рис. 3.1. Схема “проникнення” в закрите приміщення з метою несанкціонованого доступу до інформації

Заземлення технічних засобів переробки та передачі інформації (ТЗППІ). Однією з важливих умов захисту ТЗППІ є правильне заземлення цих пристроїв. На практиці найчастіше доводиться мати справу з радіальною системою заземлення, яка має менше загальних ділянок для протікання сигналів та струмів живлення у зворотному напрямку (від ТЗППІ до сторонніх суб’єктів).

При встановленні заземлення ТЗППІ не варто застосовувати природні заземлювачі: металічні конструкції споруд, з’єднані із землею, прокладені в землі металічні труби, металічні оболонки підземних кабелів. При розрахунку конкретних заземлюючих пристроїв слід використовувати спеціальні формули та таблиці.

Мережеві фільтри. Виникнення проблем у мережах живлення ТЗППІ найчастіше пов’язані з тим, що вони підключені до загальних ліній живлення. Тому мережеві фільтри виконують дві функції з метою живлення ТЗППІ: захисту апаратури від зовнішніх імпульсивних перешкод і захисту від наводок, які створює сама апаратура. При цьому однофазну систему розподілу електроенергії має створювати трансформатор із заземленою середньою точкою, трифазну – високовольтний понижуючий трансформатор.

При виборі фільтрів слід враховувати: номінальну величину струмів та напруг у ланцюгах живлення, а також, допустимі значення спаду напруги на фільтрі при максимальному навантаженні; допустимі значення реактивної складової струму на основній частоті напруги живлення; необхідне затухання фільтра; механічні характеристики фільтра (розмір, вага, тип корпусу, спосіб встановлення); ступінь екранування фільтра від сторонніх полів.

Екранування приміщень. Для повного усунення наводок від ТЗППІ у приміщеннях, лінії яких виходять за межі контрольованої зони, слід не лише “подавити” їх у проводах, що відходять від джерела, а й обмежити сферу дії електромагнітного поля, яке створює система внутрішньої електропроводки. Це вирішують шляхом екранування. Розміри екранованого приміщення вибирають, виходячи з його призначення.

Захист телефонів та факсів. Як будь-який електронний пристрій, телефон, факс, а також їх лінії зв'язку випромінюють у відкритий простір високорівневі поля в діапазоні частот до 200 мГц. Щоб цілком подавити всі види випромінювань від цих ТЗППІ, слід відфільтрувати випромінювання у проводах мікротелефону, в проводах, що відходять від апарату, а також забезпечити достатнє екранування внутрішньої схеми апарату. Усього цього можна досягти лише шляхом значної переробки конструкцій апаратів і зміни їхніх електричних параметрів. Тобто, треба захистити ланцюг мікрофона, ланцюг дзвінка і двопровідну лінію телефонного зв'язку. Зрозуміло, що здійснити вказані заходи можуть лише спеціалісти з використанням відповідного обладнання і стандартних схем. Це ж саме стосується і проблеми захисту ліній зв'язку, що виходять за межі приміщень з апаратами.

Загалом, це дуже серйозна проблема, оскільки подібні лінії практично завжди безконтрольні і до них можна підключити різноманітні засоби знімання інформації. Тут є два шляхи: по-перше, застосувати спеціальні проводи (екранований біфіляр, трифіляр, коаксильний кабель, екранований плоский кабель). По-друге, систематично перевіряти спеціальною апаратурою на факт підключення засобів знімання інформації. Виявлення наведених сигналів проводять на межі контрольованої зони або комутаційними пристроями в кросах чи розподільчих шафах. Потім або визначають конкретне місце підключення, або (якщо таке визначення неможливе) влаштовують шумову завісу.

Але найефективніший спосіб захисту інформації, яку передають телефоном або факсом, – це використання ЗАЗ.

Захист від вмонтованих та вузькоспрямованих мікрофонів. Мікрофони, як відомо, перетворюють звук в електричний сигнал. У сукупності з спеціальними підсилювачами і фільтрами їх можна використовувати як підслуховуючі пристрої. Для цього створюють приховану лінію зв'язку, яку можна виявити лише фізичним пошуком або (що важче) шляхом контрольних вимірів сигналів в усіх проводах, наявних у приміщенні. Методи радіоконтролю, ефективні для пошуку радіозакладок, у цьому разі не мають змісту.

Окрім перехоплення звукових коливань, спеціальні мікрофони-стетоскопи дуже добре сприймають звуки, які поширюються у конструкціях споруд. З їх допомогою здійснюють підслухування через стіни, двері та вікна. Існує ряд модифікацій вузькоспрямованих мікрофонів, що сприймають і підсилюють звуки, які йдуть тільки з одного напряму, і послаблюють при цьому решту звуків. Такі мікрофони мають вигляд довгої трубки, батареї трубок або параболічної тарілки з конусом концентратора. Вони вловлюють звуки людського голосу на відстані до одного кілометра.

Для захисту від вузькоспрямованих мікрофонів можна рекомендувати:

- конфіденційні переговори проводити в кімнатах, ізольованих від сусідніх приміщень, при зачинених дверях, вікнах і квартирках, закритих цупких шторах. Стіни також мають бути ізольовані від сусідніх будинків;
- підлогу та стелю варто ізолювати від підслухування мікрофонами та іншою апаратурою;
- не слід вести важливих розмов на вулиці, у парках та інших відкритих просторах, незалежно від того, сидите ви чи прогулюєтеся;
- у закритому приміщенні поза офісом у випадку необхідності обміну конфіденційною інформацією, несподівано для тих, хто стежить за вами, змініть приміщення на те, яке знаходиться під надійним контролем вашої служби безпеки;
- спробуйте завадити підслухуванню розмови звуками води, що ллється з крану (або з фонтану), хоча й це є малоефективним;

- якщо вам обов'язково потрібно щось повідомити або почути, а гарантій від підслухувань немає, говоріть один одному пошепки прямо у вухо або пишіть повідомлення на папері, який відразу після прочитання знищуйте.

Захист від лазерних підслуховуючих пристроїв. Лазери – це пристрої, в яких передачу і отримання інформації здійснюють в оптичному діапазоні. Вони малогабаритні і економні, тим більше, що в якості приймача нерідко виступають фотооб'єктиви з великою фокусною відстанню, які дають змогу вести перехоплення сигналів з далеких відстаней.

Принцип дії лазерного пристрою полягає в посиланні зондуючого променя в напрямі джерела звуку і прийманні цього променя після відображення від будь-яких предметів. Цими предметами, що вібрують під дією оточуючих звуків як своєрідні мембрани, можуть бути скло вікон, шаф, дзеркала, посуд і т.п. Своїми коливаннями вони модулюють лазерний промінь, який, після прийому приймачем, здатний відновити звуки мови. Лазерні пристрої дають можливість вільно підслуховувати людську мову через зачинені вікна з подвійними рамами на відстані до 300 метрів.

Найпростішим і в той самий час досить надійним способом захисту від лазерних пристроїв є створення перешкод для модулювання за допомогою п'єзоелемента. П'єзоелемент коливає скло з більшою амплітудою, ніж голос людини, тому амплітуда вібрації скла виключає ведення прослуховування.

Радіозакладки. Радіозакладки ("жучки") займають чільне місце серед засобів технічного несанкціонованого доступу до інформації. Вони бувають різних конструкцій – від самих простих до дуже складних (що мають дистанційне керування, системи нагромадження та передачі сигналів у стислому вигляді короткими серіями).

Для підвищення секретності роботи потужність передавача радіозакладки роблять невеликою, але достатньою для перехоплення високочутливим приймачем з невеликої відстані. Робочу частоту для підвищення скритності часто вибирають поблизу потужної радіостанції. Мікрофони застосовують як вмонтовані, так і виносні. Вони бувають двох типів: акустичні (тобто чутливі до людських голосів) або вібраційні (які перетворюють в електричні сигнали коливання, що виникають від людської мови в різноманітних жорстких конструкціях). Радіозакладки найчастіше працюють на високих частотах (вище 300кГц).

Однак є й такі пристрої, які працюють у низькочастотному діапазоні (50-300кГц). В якості каналу зв'язку використовують мережі електропроводки або телефонні лінії. Такі радіозакладки практично не випромінюють сигналів в оточуючий простір, тобто мають властивість підвищеної скритності. Якщо їх вмонтувати в світильник, розетку, подовжувач, фільтр-розетку, будь-який електроприлад, що працює від мережі змінного струму, то вони, живлячись від мережі, будуть довгий час передавати нею інформацію в будь-яку точку будинку і навіть за його межі.

Для виявлення радіозакладок застосовують спеціальні вимірювальні приймачі, які автоматично сканують за діапазоном. За їх допомогою здійснюють пошук і фіксацію робочих частот радіозакладок, а також визначають їх місцезнаходження. Дана процедура досить складна, вона вимагає відповідних теоретичних знань, практичних навиків роботи з різноманітною, досить складною вимірювальною апаратурою.

Якщо радіозакладки виключені в момент пошуку і не випромінюють сигнали, за яким можна їх виявити радіоприймальною апаратурою, то для їхнього пошуку (а також для пошуку мікрофонів підслуховуючих пристроїв та мінімагнітофонів) застосовують спеціальну рентгенівську апаратуру і нелінійні детектори з вмонтованими генераторами мікрохвильових коливань низького рівня. Такі коливання проникають крізь стіни, стелі, підлогу, меблі, портфелі та інші предмети – в довільне місце, де може бути захована радіозакладка, мікрофон, магнітофон. Коли мікрохвильовий промінь стикається з транзистором, діодом чи

мікросхемою, він відбивається назад до пристрою. Принцип дії в даному випадку схожий на міношукач, що реагує на присутність металу.

У випадках, коли немає пристроїв для пошуку радіозакладок, або немає часу на їхній пошук, можна скористатися генераторами перешкод для приймачів. Вони досить прості, надійні і цілком знімають інформацію з радіозакладок у широкому діапазоні частот.

Захист ПЕОМ. ПЕОМ, в яких зберігають конфіденційну інформацію, треба розміщувати в спеціально обладнаних (захищених від систем несанкціонованого доступу до інформації) приміщеннях. Якщо ПЕОМ використовує лише один користувач, то важливо, по-перше, попередити несанкціонований доступ до комп'ютера інших осіб тоді, коли в ньому знаходиться інформація, яку потрібно захищати, і, по-друге, забезпечити захист даних на зовнішніх носіях інформації від викрадання. Якщо ж ПЕОМ використовує група осіб, то окрім вказаних моментів захисту, може виникнути необхідність попередити несанкціонований доступ цих користувачів до інформації один одного. Ні в якому разі не слід підключати ПЕОМ, в якій знаходиться конфіденційна інформація до глобальної мережі Internet та інших глобальних та локальних мереж.

Щодо безпеки Windows та Internet професіонали вважають, що в мережевій операційній системі Windows 98 передбачено заходи з управління правами доступу до вмісту жорсткого диску локального ПК. А.Зеленін з цього приводу пише: "Хотів сказати – зовсім без мого відому оновлювати системні файли немає можливості… Я завжди намагаюся знати, що робить моя машина. Виявити те, що робить WIN-98 без вашого відому, на мою думку, досить просто. Вішаєш sniffrra на сегмент – і спокійно розбираєш "логи". Один-два користувачі зроблять це і проголосять цілому світові про результати. Однак протокол один – TCP/IP, і його ніхто не відмінював". Загалом, вірно. Проте це все – захист від іншого користувача, а не від Глобального Системного Адміністратора. Припустимо, наприклад, користувач Windows 98 забороняє доступ до деяких директорій або сегментів жорсткого диску. Але кому він забороняє? Очевидно, що іншому користувачеві, але не самій операційній системі і не Глобальному Системному Адміністратору з абсолютними правами доступу. Адже саме система Windows контролює на основі вказівок користувача кому дозволити доступ, а кому ні[*].

Водночас слід захищати інформацію від пошкодження в результаті помилок працівників, програм і обладнання, зараження комп'ютерними вірусами. Однак проведення страхових заходів обов'язкове для всіх без виключення користувачів ПЕОМ і не належить безпосередньо до проблеми захисту інформації від конкурентів.

Для забезпечення безпеки інформації використовують такі методи:

- засоби захисту обчислювальних ресурсів, що обмежують доступ несанкціонованого користувача;
- застосування різних шифрів, що не залежать від контексту інформації.

Однією з необхідних запорук успіху у зручному та надійному зборі, передачі, переробці, зберіганні, тиражуванні інформації ПЕОМ та засобами комунікацій є добре сплановані структура та доступ до даних. Неспланові чи погано сплановані вищезгадані фактори можуть призвести як до значного збільшення матеріальних затрат, так і до прямого витоку інформації[*].

---

[*] Інформація з мережі Internet.

[*] Сьогодні в комп'ютерних блоках використовуються вже не просто маяки, а цілі ретранслятори, які нагромаджують і ретранслюють за стіни об'єкта управління інформацію, що обробляють комп'ютером.

Як повідомляли "Московские новости" в 1992 році подібна закладка була знайдена в ЕОМ "Вакс" американської фірми "ТЭК". Перевірка 200 комп'ютерів цього типу, закуплених свого часу Мінавіапромом СРСР, показала, що з 8 із них було 20 закладок. Виявилось це випадково, коли на одному з підмосковних підприємств вийшов з ладу комп'ютер "Вакс". Російські Кулібіни розібрали цю машину і знайшли в ній закладку, яка нагромаджувала інформацію. За задумом "продавців" при поломці комп'ютера повинен був мати місце виклик "спеціаліста", який би й списав інформацію, що містилася в блоці. А після цього через деякий час у закладці повинна була спрацювати програма на самознищення комп'ютера. Підприємство врятувало несанкціоновані дії (не за інструкцією) персоналу, коли обслуговуючий персонал чи то за браком коштів чи з власної цікавості вирішив самостійно полагодити комп'ютер, за який у свій час було оплачено 3 млн. доларів. Виявлена комп'ютерна закладка надійшла сигналом до загальної перевірки комп'ютерів цього типу, закуплених в США [Батурин Ю., Жодзишский А. Компьютерная преступность и компьютерная безопастность. М.: Юридическая литература. – 1991].

Важливим аспектом у системі управління інформацією є персонал (системні та прикладні програмісти, інженери з апаратного забезпечення, оператори тощо). Наявність неетичних, несумлінних (тобто з будь-яких причин), некомпетентних осіб призводить до витоку інформації та значних матеріальних затрат.

Нагадаємо, що в ПЕОМ в якості обчислювальних ресурсів виступають оперативна пам'ять, процесор, вмонтовані нагромаджувачі на жорстких або гнучких магнітних дисках, клавіатура, дисплей, принтер, периферійні пристрої. Захист оперативної пам'яті і процесора передбачає контроль за появою в оперативній пам'яті так званих резидентних програм, захист системних даних, очистку залишків секретної інформації в невикористовуваних областях пам'яті. Для цього слід мати в своєму розпорядженні програму перегляду оперативної пам'яті для контролю за складом резидентних програм та їх розміщенням.

Значно важливіший захист вмонтованих нагромаджувачів. Є кілька типів програмних засобів, які можуть вирішити це завдання:

- захист диску від запису і читання;
- контроль за звертаннями до диску;
- засоби знищення залишків секретної інформації.

Але найнадійнішим методом захисту є, безумовно, шифрування, оскільки у цьому разі оберігається безпосередньо сама інформація, а не доступ до неї (наприклад, зашифрований файл не можливо прочитати навіть у випадку викрадання дискети). Однак у ряді випадків використання шифрування є складним або неможливим, тому слід використовувати обидва методи в сукупності. Більшість засобів захисту реалізують у вигляді програм або пакетів програм. Це розширює можливості стандартних операційних систем, а також систем управління базами даних.

ДОДАТКИ ДО 3-ГО РОЗДІЛУ

Додаток 1

Угода про нерозголошення комерційної таємниці

Приступаючи до виконання своїх обов'язків як працівник Фірми, я, П.І.П., розумію, що отримаю доступ до інформації, що стосується її бізнесу. Я також розумію, що під час виконання своїх обов'язків буду займатися аналізом, складанням схем, таблиць, креслень, доповідей та інших конфіденційних документів, що мають відношення до справ Фірми.

У зв'язку з цим, даю зобов'язання, що ні під час моєї роботи, ні після звільнення не буду обговорювати з будь-ким або розкривати (за винятком випадків виконання обов'язків як працівник Фірми) будь-яку інформацію або комерційні секрети, отримані або розроблені мною. Я також погоджуюся з тим, що всі аналітичні розробки, схеми, креслення, доповіді й інші документи, підготовлені особисто мною, або у співпраці з іншими працівниками, є власністю Фірми. Зобов'язуюся, що не буду сам і не дозволю нікому іншому знімати копії і робити анотації з вищезазначених документів.

Ознайомлений із змістом статті 148^6 та 148^7 КК України про кримінальну відповідальність за розголошення комерційної таємниці і попереджений про те, що в разі умисного чи неумисного розголошення комерційної таємниці несу повну матеріальну відповідальність по відшкодуванню нанесеної Фірмі шкоди.

Я підтверджую, що не маю перед будь-ким ніяких зобов'язань, які входять у суперечність з цією Угодою, або обмежують мою діяльність у Фірмі.

Дата *Підпис працівника*

Дата *Підпис свідка*

Додаток 2

Угода про збереження комерційної таємниці

Тут і далі “Довіритель” або ваше ім’я, тут і далі “Довірений” з метою _____, для чого необхідно, щоб довірений мав доступ до інформації про _____ .

Ця інформація складає комерційну таємницю Довірителя і розкривається лише в заздалегідь обумовлених цілях. Довірений зобов’язується зберігати в секреті цю інформацію і не використовувати її в інших цілях. Довірений зобов’язується ознайомити під розпис з цією Угодою всіх своїх співробітників, які отримають доступ до даної інформації. Після закінчення переговорів (або співробітництва) Довірений відразу поверне всі матеріали, що містять дану інформацію, Довірителю.

Ця Угода не стосується інформації, законним власником якої є Довірений, або інформації, отриманої ним від третіх осіб.

Дата, *Підписи*

Додаток 3

Угода про секретність*

Тут і далі ***"Довіритель",*** тут і далі ***"Довірений"*** бажають розглянути можливість … (наприклад, інвестування Довіреного в корпорації, створення спільного підприємства, відношення покупець-продавець тощо). Тому необхідно, щоб Довірений мав доступ до певної інформації про … (дається відповідний загальний опис матеріалу, що складає комерційну таємницю).

Ця інформація складає комерційну таємницю Довірителя і розкривається лише в заздалегідь обумовлених цілях. Довірений зобов'язується зберігати в секреті цю інформацію і не використовувати її в інших цілях. Довірений зобов'язується взяти підписи від своїх працівників, які отримають доступ до даної інформації про її нерозголошення. Після закінчення переговорів Довірений відразу ж повертає всі матеріали, що містять дану інформацію, Довірителю.

Ця Угода не стосується інформації, законним власником якої є Довірений, або інформації, отриманої ним у третіх осіб.

Дата *Підписи*

* Підписується з потенційними інвесторами, партнерами, клієнтами або покупцями

Додаток 4

Угода про припинення роботи

Я, П.І.П., що підписався нижче, підтверджую, що був проінструктований стосовно комерційних секретів Фірми і її приватної інформації, до якої мав доступ під час моєї роботи. При прийомі на роботу я підписав угоду про нерозголошування комерційної таємниці і пізніше мене неодноразово попереджали, що я не можу використати приватну інформацію і комерційні секрети Фірми.

Я підтверджую, що повернув Фірми всі доповіді, креслення, схеми, таблиці, інші письмові матеріали і матеріали, що містяться в пам'яті ЕОМ і не маю більше в своєму розпорядженні або будь-де ще таких документів або їхніх копій.

Дата *Підпис працівника*

Дата *Підпис свідка*

Додаток 5

Заява працівника, що звільняється

Я, П.І.П., що підписався нижче, підтверджую свої зобов'язання перед Фірмою про нерозголошування комерційної таємниці і її приватної інформації. За час моєї роботи я ніколи не порушував прийнятих на себе зобов'язань, не використовував у своїх цілях і не розкривав будь-яку приватну або конфіденційну інформацію, за винятком випадків виконання моїх зобов'язань в інтересах Фірми.

Підтверджую, що я передавав Фірмі всі винаходи і всю інформацію, які розробив або дізнався, тобто все, що може бути корисним для бізнесу Фірми.

Зі всією відповідальністю заявляю, що я не брав участь в якій-небудь діяльності, що складає конкуренцію Фірмі або суперечить моїм обов'язкам як працівника.

Дата *Підпис працівника*

Дата *Підпис свідка*

КОРОТКИЙ СЛОВНИК ТЕРМІНІВ БЕЗПЕКИ ІНФОРМАЦІЇ[*]

Автентифікація (*authentication*) – перевірка належності суб'єкта доступу пред'явленого ним ідентифікатора. Ознакою наявності повноважень у суб'єкта доступу є знання пароля.

Автентифікація даних (*data association*) – визначення джерела даних.

Автентифікація користувача (*authentication of user*) – перевірка відповідності ідентифікатора користувача, що ним пред'являється.

Автентифікація повідомлень (*authentication of messages*) – додання до блоку даних контрольного поля для виявлення будь-якої зміни в даних. При обчисленні значень цього поля використовується ключ, відомий тільки одержувачу даних.

Авторизація (*authorization*) – надання певних повноважень системі обробки даних.

Адміністратор бази даних (*database administrator*) – спеціальна посадова особа (група осіб), що має уявлення про базу даних і відповідає за її ведення, використання та розвиток. Функції: підтримка цілісності бази даних, необхідного рівня захисту даних.

Адміністратор системи (*system administrator*) – особа, що відповідає за експлуатацію системи та підтримання її в робочому стані.

Антивірус – в обчислювальній техніці – програма, що виявляє або виявляє та знищує комп'ютерні віруси.

Атака (*attack*) – спроба подолання системи захисту. Атака може бути активною і пасивною. Міра "успіху" атаки залежить від вразливості системи захисту та ефективності захисних заходів.

Атестація засобів захисту (*endorsment*) – засвідчення ступеня відповідності вимогам певного класу засобів захисту.

База даних (*database*) – пойменована структурована сукупність даних, що належать до конкретної предметної області.

Безпека (*security, safety*) – властивість системи, яка полягає в тому, що ризик одержання негативних наслідків у процесі функціонування системи мінімальний. Поняття безпеки пов'язане з поняттями цілісності та захисту.

Безпека даних (*data security*) – властивість організації доступу до даних, що забезпечує захист їх від несанкціонованого використання, розкриття, навмисного чи ненавмисного спотворення або руйнування. Безпека даних досягається за рахунок застосування апаратних, програмних та криптографічних методів і засобів захисту, а також комплексу організаційних заходів. Одним з показників безпеки даних є безпечний час.

Безпека комп'ютерних (обчислювальних) систем (*computer security*) – властивість комп'ютерних систем протистояти спробам несанкціонованого доступу до інформації, що обробляється та зберігається, витоку інформації, що призводить до деструктурних дій, та нав'язування фальшивої інформації.

Біт (*bit*) – мінімальна одиниця кількості інформації в ЕОМ.

Боротьба з комп'ютерною злочинністю – профілактика та попередження комп'ютерних злочинів. Боротьба з комп'ютерною злочинністю передбачає: створення, сертифікацію, ліцензування і впровадження необхідних засобів технічного та програмного захисту інформації; створення спеціалізованих організаційних структур , задачею яких є забезпечення постійного функціонування засобів захисту, засобів генерації ключів та паролів, їх розподілу, контролю за використанням, зміни та знищення.

[*] Короткий словник складений з використанням робіт [4],[7].

Витік інформації (*information leakage*) – неконтрольоване поширення інформації, яке призводить до його несанкціонованого одержання. Може бути результатом дії зловмисника або недосконалістю системи захисту інформації.

Відновлення даних (*data recovery*) – процес копіювання даних з носія, що містить захисну копію даних, на носій-оригінал у випадку порушення на ньому цілісності даних.

Вірус (*virus*) – спеціальна програма, що здатна самочинно розмножуватись, створюючи свої копії, і поширюватись, модифікуючи (заражаючи) інші програми шляхом приєднання до них, для наступного одержання управління та відтворення нових копій. При запуску заражених програм вірус може виконувати різні небажані дії, що порушують цілісність інформації та (або) режим роботи засобів обчислювальної техніки: псування файлів та каталогів, модифікування програмного забезпечення, спотворення результатів обчислень, засмічування або стирання пам'яті, створення завад при роботі ЕОМ, наприклад, різних аудіо- та відеоефектів. Переноситься при копіюванні програм через заражені дискети або по обчислювальній мережі.

Генератор випадкових паролів (*random-password generator*) – програмно-апаратний засіб, що являє собою генератор випадкових чисел, які використовуються як паролі.

Дані закриті (захищені) (*restricted data*) – дані, що доступні обмеженому колу користувачів.

Дешифратор (*decipherer*) – пристрій, призначений для перетворення шифрограм у вихідні повідомлення. Зворотну функцію виконує шифратор.

Дешифрування (*decipherement, decryption*) – процес перетворення шифртексту у вихідний текст без знання ключа; процес зворотний процесу шифрування.

Джерело інформації (*information source*) – матеріальний об'єкт, який володіє певними відомостями, що мають конкретний інтерес для зловмисників або конкурентів.

Достовірність даних (*data validity*) – ступінь відповідності даних, що зберігаються у пам'яті ЕОМ або документах, реальному стану відображених ними об'єктів предметної області.

Доступ (*access*) – 1) взаємодія між суб'єктом і об'єктом доступу, що забезпечує обмін даними між ними; 2) в обчислювальній техніці – процедура встановлення зв'язку із запам'ятовуючим пристроєм і файлом для записування або читання даних.

Доступ за ключем (*Keyed access*) – спосіб доступу, при якому для звернення для запису файла необхідно вказати його ключ.

Доступ несанкціонований (неавторизований) (*unauthorized (illegal) access*) – навмисне звернення користувача до даних, доступ до яких йому не дозволений, з метою їх читання, оновлення або руйнування.

Живучість (*viability*) – властивість системи залишатись працездатною в умовах зовнішніх впливів.

Журнал системний (*system log*) – набір даних, в яких операційна система записує інформацію, що характеризує хід обчислювального процесу (виконання завдань, опис подій, заміну носіїв, повідомлення операторів тощо).

Загроза (*threat*) – потенційна можливість порушення захисту від несанкціонованого доступу; будь-яка дія, спрямована на подолання захисту інформації.

Закладка (*bug*) – потай встановлений технічний або програмний засіб, що являє загрозу для інформації.

Засоби криптографічні захисту інформації (*cryptographic information protection facility*) – засоби, що здійснюють криптографічні перетворення інформації для забезпечення її безпеки.

Захист (*protection, security, lock out*) – засіб для обмеження доступу чи використання всієї або частини обчислювальної системи; юридичні, організаційні та технічні, в тому числі програмні, заходи запобігання несанкціонованого доступу до апаратури, програм і даних.

Захист криптографічний (*cryptographical security*) – захист інформації за допомогою її криптографічного перетворення.

Захист інформації технічний (*technical protection of information*) – діяльність, спрямована на запобігання порушенню цілісності інформації та її витоку технічними каналами.

Зловмисник – фізична або посадова особа, що навмисно чи ненавмисно здійснює неправомірні дії по відношенню до обчислювальної системи та інформації, що міститься в ній.

Злочин комп'ютерний – дії, що суперечать законодавству в галузі обробки інформації в автоматизованих системах.

Ідентифікатор (*identifier*) – лексична одиниця, що використовується як ім'я для елементів мови; ім'я, що присвоюється даним і являє собою послідовність латинських літер і цифр, яка починається з літери.

Ідентифікація (*identification*) – операція розпізнавання обчислювальною системою суб'єктів та об'єктів доступу за унікальною ознакою–ідентифікатором, яка необхідна для управління доступом; після ідентифікації, як правило, проводиться перевірка повноважень (див. Автентифікація).

Інформація закрита (*private information*) – інформація, яка з тих чи інших міркувань є таємницею, і розповсюдження якої можливе лише за згодою органів, уповноважених контролювати питання, пов'язані з цією інформацією.

Інформація з обмеженим доступом (*limited access information*) – інформація, право доступу до якої обмежене встановленими правовими нормами та (або) правилами.

Інформація конфіденційна (*confidental (sensitive) information*) – інформація з обмеженим доступом, що містить відомості, які перебувають у володінні, користуванні чи розпорядженні окремих фізичних чи юридичних осіб або держави, і порядок доступу до якої встановлюється ними.

Інформація таємна (*secret information*) – інформація з обмеженим доступом, що містить відомості, які становлять державну та іншу передбачену законом таємницю, і розголошення яких завдає шкоди особі, суспільству та державі.

Інформація фальшива (*false information*) – свідомо сформована інформація, що неправильно, помилково відображає характеристики та ознаки об'єкта, або інформація про неіснуючий реально об'єкт.

Канал витоку інформації (*channel of information leakage*) – сукупність носія інформації, середовища його поширення та технічного засобу розвідки.

Категорія доступу (*access category*) – атрибут об'єкта доступу, що визначає рівень повноважень, який повинен мати суб'єкт доступу для одержання права доступу до даних об'єкта (наприклад, категорія таємності і службові повноваження).

Ключ (*key*) – 1) сукупність символів, що використовується для ідентифікації елемента множини, наприклад, запису у файлі або запису бази даних; 2) сукупність символів, що використовується для підтвердження повноважень на доступ до деякої інформації; 3) значення деяких параметрів алгоритму криптографічного перетворення даних, яке забезпечує вибір одного варіанту криптоперетворення із сукупності можливих для даного алгоритму.

Ключ системний (*system key*) – ключ, що забезпечує захист системних засобів від несанкціонованого доступу.

Код автентифікації (*authentication code*) – контрольне поле, що додається до блоку даних для автентифікації повідомлень.

Кодування (*coding, incoding*) – ототожнення даних з їхніми кодовими комбінаціями; встановлення відповідності між елементами даних та кодовою комбінацією (словом коду).

Контроль доступу (за доступом) (*access control*) – високонадійний процес, що забезпечує визначення і обмеження доступу користувачів, програм або процесів до ресурсів та об'єктів обчислювальної системи згідно з моделлю механізму захисту. Може бути реалізований організацією звернення до таблиці, що зберігається в пам'яті і в якій перелічені права суб'єктів доступу. У ході виконання процесу може здійснюватися реєстрація всіх спроб несанкціонованого доступу в системному журналі.

Конфіденційність (*privacy*) – 1) право на захист даних, що належать окремим особам або організаціям; 2) право окремих осіб контролювати доступ інших осіб (користувачів) до інформації; право контролю, наприклад, має адміністратор банку даних, що відповідає за розмежування доступу.

Користувач (*user, substriber*) обчислювальної системи – 1) фізична або посадова особа, яка має право використання ресурсів обчислювальної системи для виконання своїх службових обов'язків (для одержання інформації або вирішення різних задач); 2) програма або система, що використовує ресурси іншої системи.

Криптоаналіз (*cryptanalysis*) – 1) наука, що займається вивченням і розробкою методів, способів та засобів дешифрування; 2) процес обробки шифрограми з метою визначення застосованого шифру та відповідного ключа, що потрібні для виділення вихідної інформації.

Криптографія (*cryptography*) – наука, що займається вивченням і розробкою методів, способів та засобів тайнопису.

Криптологія (*cryptology*) – наука, складовими якої є криптографія та криптоаналіз.

Криптосистема (*cryptosystem*) – система для криптографічного перетворення інформації; що містить у собі п'ять компонентів: множину вихідних (відкритих) текстів, множину шифртексів, множину ключів, сім'ю шифруючих перетворень, сім'ю розшифровуючих перетворень.

Криптосистема асиметрична *(криптосистема, з відкритим ключем)* – криптосистема, у якій ключі шифрування і розшифрування розрізняються у такий спосіб, що за допомогою обчислень практично неможливо вивести один ключ з іншого.

Криптосистема симетрична – криптосистема, у якої ключі шифрування і розшифрування або однакові, або легко виводяться один з одного, забезпечуючи спільний ключ.

Криптостійкість – характеристика шифру, що показує його стійкість до дешифрування і визначається часом, необхідним для дешифрування.

"Маскарад" – вид атаки, при якій один об'єкт системи видається за інший. Прикладом такої атаки може бути перехоплення процедури автентифікації об'єкта і використання в подальшому одержаних даних для здійснення незаконної авторизації.

Мережа обчислювальна (*computer network*) – сукупність мережі передавання даних, взаємозв'язаних нею ЕОМ та необхідних для реалізації цього зв'язку програмного забезпечення і (або) технічних засобів, що призначені для розподіленого оброблення даних (інформації).

Метод захисту (*protection method*) – система принципів і прийомів, спрямованих на реалізацію функції захисту. Метод захисту може бути реалізований програмним, програмно-апаратним або апаратним способом.

Метод захисту криптографічний (*cryptographical method*) – інформаційний метод захисту, що полягає у криптографічному перетворенні інформації.

Модель Белла-Лападула (*Bell-LaPadula model*) – формальна автоматна модель політики безпеки, що описує множину правил управління доступом. У цій моделі компоненти системи розподіляються на об'єкти і суб'єкти доступу. Вводиться поняття безпечного стану і доводиться, що коли кожен перехід зберігає безпечний

стан (тобто переводить систему із безпечного стану в безпечне), то згідно з принципом індукції система є безпечною.

Модель політики безпеки (*security policy model*) – формальне подання політики безпеки, що розроблена для системи. Модель політики безпеки містить формальний опис чинників та правил, що визначають управління, розподіл і захист критичної інформації.

Об'єкт доступу (*access object*) – пасивна сутність (запис, файл, блок пам'яті тощо), що містить або одержує інформацію. Доступ до об'єкта доступу здійснюється суб'єктами доступу за допомогою набору операцій, які надаються об'єктом доступу.

Пароль (*password*) – ідентифікатор суб'єкта доступу, що є його секретом і використовується в процедурі автентифікації.

Підпис цифровий (*digital signature*) – цифрова послідовність, що додається до повідомлення (даних) для забезпечення цілісності та підтвердження авторства і формується із застосуванням асиметричних криптосистем.

Політика безпеки (*security policy*) – сукупність законів, правил та практичного досвіду, на основі яких будується управління, захист та розподіл конфіденційної інформації.

Режим забезпечення безпеки (*security processing mode*) – опис всіх категорій допуску усіх користувачів у прив'язці до всіх категорій захисту інформації, що має зберігатись і оброблятись в системі.

Рівень повноважень (*subject privilege*) – сукупність прав доступу суб'єкта доступу.

Розмежування доступу – сукупність методів, заходів та засобів, що забезпечують захист даних від несанкціонованого доступу.

Розшифрування – процес перетворення шифртексту на вихідний текст при відомому ключі; процес, зворотний процесу шифрування.

Сертифікація (*certification*) – офіційна атестація.

Система захисту інформації – система правничих та організаційних заходів, технічних та програмних засобів, що забезпечують певні умови для управління доступом до інформаційних ресурсів з урахуванням вимог до захисту даних і для контролю за доступом до тих частин інформаційної системи, які охоплені засобами захисту.

Скремблер *(scrambler*) – пристрій, що реалізує динамічні аналого-цифрові засекречені перетворення з застосуванням шифрування.

Стандарт забезпечення захисту (*security standart*) – 1) опис послідовності оцінок, які потрібно виконати, щоб вважати цю характеристику безпеки підтвердженою з точки зору атестації захисту; 2) множина характеристик безпеки, які має забезпечити система захисту, щоб її можна було використовувати в цьому конкретному режимі забезпечення безпеки або у відповідності з загальною стратегією захисту.

Стратегія захисту (*security strategy*) – формальне визначення критеріїв, якими слід керуватися при забезпеченні захисту систем від відомих загроз.

Таємність інформації (*information privacy*) – обмеження, що накладається автором на доступ до його інформації інших осіб. Оформляється присвоєнням інформації певного грифа таємності та досягається закриттям її паролем, шифруванням та іншими методами захисту.

"***Троянський кінь***" (*trojan horse*) – програма, яка на доповнення до основних (проектних та документованих) надає додаткові, але не описані в документації функціональні можливості, спрямовані на те, щоб обійти контроль доступу. Найбільш небезпечним є опосередкований вплив, при якому "троянський кінь"

діє в межах повноважень одного користувача, але в інтересах іншого користувача, встановити особу якого інколи неможливо.

Управління системою захисту інформації – процес, який забезпечує організацію спільної роботи всіх елементів системи захисту інформації та реалізацію виробленої стратегії захисту, а також надає засоби реалізації організаційно-розпорядчих заходів щодо захисту інформації в обчислювальній системі.

Хакер (*hacker*) – користувач, який намагається вносити зміни до системного програмного забезпечення, часто не маючи на це права; програміст-фанатик, який займається досконалим вивченням обчислювальних систем з метою розширення їхніх можливостей, створенням більш-менш корисних допоміжних програм, які здебільшого погано документовані та інколи спричиняють небажані побічні результати.

Цілісність (*integrity*) – стан даних або комп'ютерної системи, в якій дані та програми використовуються встановленим чином, що забезпечує: стійку роботу системи; автоматичне відновлення у випадку виявлення системою потенційної помилки; автоматичне використання альтернативних компонентів замість тих, що вийшли з ладу.

Час безпечний (*security time-lag*) – математичне сподівання часу розкриття системи захисту статистичним апробуванням можливих варіантів доступу до даних.

Шифр (*cipher*) – метод криптографічного перетворення даних, за допомогою якого відкритий текст перетворюється на шифртекст з метою захисту від несанкціонованого доступу.

Шифратор (*encipherer, encrypter*) – пристрій, призначений для перетворення вихідних повідомлень на шифрограми.

Шифрограма (*ciphergram*) – зашифрована форма вихідного повідомлення.

Шифртекст (*ciphertext*) – вихідний текст після виконання над ним процедури шифрування.

Шифрування (*encipherement, encryption*) – процес перетворення відкритого тексту до виду, незрозумілого несанкціонованому користувачу.

Шифрування блочне (*block encryption*) – спосіб шифрування, при якому кожен блок, що передається, шифрується незалежно.

Шифрування поточне (*stream encryption*) – спосіб шифрування даних, при якому кожен знак шифрується незалежно.

Ядро безпеки (*security kernel*) – атестований процес, що інтегрує механізми захисту згідно з визначеною моделлю механізму захисту.

СПИСОК ЛІТЕРАТУРИ

ОСНОВНИЙ

1. Акушский И.А., Юдицкий Д.И.. Машинная арифметика в остаточных классах. – М.:Сов. Радио. – 1968. – 439 с.
2. Артехин Б.В. Стеганография // Конфидент, № 4, 1996, с.47-50
3. Березовський А.І., Данильченко Л.С., Задірака В.К., Шевчук Л.Б. Оптимізація алгоритмів виконання операцій з багаторозрядними числами. Праці симпозіума “Питання оптимізації обчислень. – Київ, 22-24.11.1993. – Вид. ІК НАНУ, 1993,с.23.
4. Богуш В.М., Кудін А.М. Інформаційна безпека “від А до Я”. 3000 термінів та понять. – К.: Техніка, 1999. – 300 с.
5. Боровиков А.М., Тимошенко А.А. Системы защиты информационного обмена «Клиент-Банк»// Безопасность информации, № 1, 1995. – с.53-60.
6. Бухштаб А.А. Теория чисел.-М.: Просвещение, 1966. – 384с.
7. Гайкович В., Першин А. Безопасность електронных банковских систем. – М.: Единая Европа. – 1994. – 364 с.
8. Диффи У., Хеллмэн М.Э. Защищенность и имитостойкость: Введение в криптографию // ТИИЭР, т.67, №3, 1979. – с. 71-103.
9. Задирака В.К., Мельникова С.С. Цифровая обработка сигналов. – К.: Наукова думка, 1993. – 294с.
10. Ивченко И.С., Новак И.Н. К вопросу об информационной безопасности платежных систем коммерческих банков Украины и снижению системных рисков.// Безопасность информации, № 2 (5), 1996. – с.48-56.
11. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки Электронной цифровой подписи на базе асимметричного криптографического алгоритма: ГОСТ Р34. 10-94.
12. Клопов В.А., Мотуз О.В. Основи компьютерной стеганографии// Конфидент, 4, 97, с.43-48.
13. Кнут Д.Е. Искусство программирования для ЭВМ. Т.2.- М.: Мир, 1977. – 724с.
14. Конхейм А.Г. Основы криптографии /пер. с англ. – М.: Мир, 1987.- 412с.
15. Лагутин В.С., Петраков А.В. Утечка и защита информации в телефонних каналах. М.: Енергоатомиздат, 1996. – 296с.
16. Макклеллан Дж.Х., Рейдер Ч.М. Применение теории чисел в цифровой обработке сигналов.-М.: Радио и связь, 1983.- с. 17-21.
17. Малый тематический выпуск “Защита информации” // ТИИЭР, т.76, №5, 1988, с.24-125.
18. Мафтик С. Механизмы защиты в сетях ЭВМ.-М.: Мир, 1993.- 216 с.
19. Першиков В.И., Савенков В.М. Толковый словарь по информатике. – 2-е изд., доп. – М.: Финансы и статистика, 1995. – 544 с.
20. Райвест Р.Л. Многоуравневая криптография// Конфидент, 1, 97, с.65-70.
21. Саломаа А. Криптография с открытым ключом / Пер. с англ.- М.: Мир, 1996.- 318с.
22. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования: ГОСТ 28147-89.
23. Сравнение практических схем цифровой подписи // Передача информации: Экспресс-информация .- 1993, №6.- с.19-27.
24. Сяо Д., Керр Д., Медник С. Защита ЭВМ. – М.: Мир, 1982. – 263 с.

25. Тимошенко А.А. Защита информации в системах «Клиент-Банк» // Безопасность информации,№ 1, 1995. – с.39-44.
26. Уолкер Б.Дж., Блейк Я.Ф. Безопасность ЭВМ и организация их защиты. – М.: Связь, 1980. – 142 с.
27. Хоффман Л.Д. Современные методы защиты информации, - М.: Сов.радио, 1980.-264с.
28. Шеннон К.Э. Теория связи в секретных системах. В работах по теории информации и кибернетики. – М.:И.Л., 1963. – 830 с.
29. Denning D.E. Cryptography and data security. – M.: Addison-Wesley, 1982. – 393 p.
30. Diffi W., Hellman M. New directions in cryptography// IEEE Trans. on Informat.Theory. VIT-22, 1976. – p. 644-654.

ДОДАТКОВИЙ

31. Анисимов А.В. Методы быстрой модулярной редукции//Безопасность информации, №2,1996. – с.10-17.
32. Данильченко Л.С. О некоторых эффективных алгоритмах вычисления остатка и возведения в степень многоразрядных чисел// Кибернетика и системный анализ, №3, 1996. – с.145-151.
33. Задирака В.R., Мельникова С.С. Быстрое умножение многоразрядных чисел с использованием БПФ// Кибернетика и системный анализ, №3, 1996. – с.63-68.
34. Задирака В.К. Теория вычисления преобразования Фурье. – К: Наукова думка, 1983. – 216с.
35. Качко Е.Г., Свинарёв А.В., Горбенко И.Д., Мельникова О.А. Программирование операций многократной точности//Безопасность информации, №1, 1995, с. 18-21.
36. Коваленко Н.И., Никитин А.И., Пилипчук С.И., Фаль А.М. Стандарты по защите информации, требующие использования криптографических методов // Безопасность информации, № 3(6), 1996. – с. 18-23.
37. Кудин А.М. Анализ современных методов формирования ключей с использованием принципов ассиметричной криптографии// Безопасность информации, №4(7), 1996. – с.6-10.
38. Моисеенков И.Э. Основы безопасности компьютерных систем//Компьютер Пресс. – 1991. №11. – с.7-21.
39. Охрименко С.А. Защита от компьютерных вирусов. – Кишинев: Штеминица, 1991. – 102с.
40. Плотников В. Алгоритмическая реализация криптографического метода RSA на ПК// Монитор, №2, 1994.
41. Проспекты фирм “Ноумедж экспресс”, “Маском”, “Защита информации”, “Videosys”, “Сконтек”, “Анкад”, “Лан-Крипто”… на выставках “Interpolitex-95”, “Банк и офис-95”, “Безопасность-96”, “CEBIT-96”.
42. Barrett P.D. Implementing the Rivest Shamir and Adleman Public Key Encryption Algorithm on a Standart Digital Signal Processor// Advances in Cryptology. Eurocrypt’86.Lect. Notes Comput. Sci. № 263, 1987. – p. 311-323.
43. Bellare M., Rivest R. Translucent cryptography – an alternative to key escrow and its implementation via fractional oblivious transfer// Version February 18,1996. Available from http://theory.ins.mit.edu.
44. Cordon D.M. Discrete logarithms in GF(P) using the number field sieve, presented at the Workshop on Number Theory and Algorithms, Mathematical Sciences Research Institute (Berkeley, CA), March 26-29, 1990.
45. Datapro Reports on Banking Automation, 1990-93.
46. Datapro Reports on Information Security, vol.1-3, 1990-93.
47. Lenstra A.K., Manasse M.S. Factoring with two large primes. Advances in Cryptology//Eurocrypt’90. – Springer – Verlag, Berlin, 1991. – p. 72-82.
48. McLean J. Reasoning about Security Models. – Proc.of the 1987 IEEE Symp. On Security and Privacy, pp.123-131.

49. Menezes A.,Okamoto T. and Vanstone S. Reducing elliptic curve logarithms to logarithms in a finite field (Unpublished manuscript, Sept. 1990).
50. Montgomery P.L. Modular Multiplication Without Trial Division// Math. Comp.T.44,№ 170, 1985. – p.519-521.
51. NIST FIPS PVB 185 Escrowed encryption standart. – V.S. Department of Comerce, Feb. 1994.
52. Odlizko A.M. Discrete logarithms in finite fields and their cryptographic significance" in lecture Notes in Computer science 209; Advances in Cryptology: Proc. Eutocrypt'84, T.Beth, N.Cot and I.Indemarsson, Eds. Paris, France, April 9-11, 1984, hh.224-314. Berlin: Springer – Verlag, 1985.
53. Richard H. Baker. Computer Security Handbook. – TAB Professional and Reference Books, 1991.