**Зміст**

I модуль Безпека і захист даних

1. Мета вивчення та структура курсу "Технології захисту інформації". Лiтература для самостiйної роботи над курсом…………………………………………………………...2
2. Огляд безпеки системи……………………………………………………………………5
3. Механізми і політики розмежування прав доступу……………………………………..16
4. Методи та пристрої забезпечення захисту і безпеки…………………………………..35
5. Захист, доступ та аутентифікація……………………………………………………….41
6. Моделі захисту. Захист пам'яті………………………………………………………….50
7. Шифрування даних……………………………………………………………………….70
8. Управління відновленням……………………………………………………………….87
9. Основні напрямки розвитку сучасної криптографії……………………………………94
10. Механізми та протоколи керування ключами в ІВК інформаційної системи……….123

II модуль Мережева безпека

11.Основні види атак, принципи криптоаналізу. Основи криптографії………………….149

12. Алгоритми з секретним ключем………………………………………………………..164

13.Алгоритми з відкритим ключем………………………………………………………...165

14.Протоколи аутентифікації………………………………………………………………..166

15.Цифрові підписи………………………………………………………………………….173

16.Використання паролів і механізмів контролю за доступом……………………………185

17.Питання безпеки та брандмауери………………………………………………………203

**Модуль №1**

**1) Мета вивчення та структура курсу "Технології захисту інформації". Лiте­ра­тура для самостiйної роботи над курсом.**

**1. Мета та завдання курсу**

    Навчальна дисципліна «Захист даних у інформаційних системах» вивчає методи та засоби захисту інформації в комп’ютерних системах, основні засади інформаційної безпеки, класифікацію та принципи побудови систем захисту.

**1.2 Мета**

    Метою викладання курсу є надання студентам знань про загальні відомості щодо захисту інформації, потенційних загроз та проблем захисту даних в локальних системах та комп’ютерних мережах.

**1.3.Завдання**

    Студенти при вивченні дисципліни отримують знання про загальні відомості щодо захисту інформації, класифікацію загроз інформації та міри протидії ним, класифікацію та особливості комп’ютерних вірусів, основи захисту інформації в комп’ютерних мережах. У них повинні сформуватись вміння класифікувати, ідентифікувати і захищати засоби обробки інформації від несанкціонованого доступу та комп’ютерних вірусів, захищати інформацію персонального комп’ютера, управляти доступом та адмініструванням мереж, використовувати системи кодування інформації та її стискування, розробляти індивідуальні системи управління доступом і захистом інформації

НАВЧАЛЬНО-ТЕМАТИЧНИЙ ПЛАН

вивчення дисципліни

“ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ

Назва теми

1 Основні положення теорії захисту інформації

2 Законодавча база в галузі захисту інформації

3 Технологія реалізації атак на комп’ютерну систему та мережу

4 Методологія захисту інформації в комп’ютерних системах і

мережах

5 Системи захисту на основі мережових екранів

6 Основи криптографії та криптоаналізу

7 Системи визначення атак і системи реакції на атаку.

Моніторинг систем інформаційної безпеки

8 Захист програмного продукту

ПРОГРАМНИЙ МАТЕРІАЛ

до вивчення дисципліни

“ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ”

Тема 1. Основні положеннятеорії захисту інформації.

Основні означення та поняття теорії захисту інформації. Технічний захист інформації. Історія розвитку. Сфера застосування. Тер-мінологія. Мета й завдання курсу. Місце дисципліни серед інших дисциплін.

Види загроз та їх системна класифікація. Зловмисники та випадкова втрата даних. Поняття атаки на комп’ютерну систему.

Проблема забезпечення безпеки інформації. Високонадійна обчислювальна база. Формальні моделі захищених інформаційних систем. Особливості моделей Белла-Ла Падулі та Біба. Визначення політики безпеки.

PDF created with FinePrint pdfFactory Pro trial version http://www.fineprint.com5

Тема 2. Законодавча база в галузі захисту інформації

Вітчизняні державні стандарти з технічного захисту інформації. Закони України “Про інформацію” та “Про захист інформації в автоматизованих системах”. Вимоги вітчизняних стандартів із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах. Порядок проведення робіт із технічного захисту інформації. Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу.

Закордонна нормативна база в галузі технічного захисту інформації. “Оранжева книга” безпеки. Критерії, вимоги та категорії систем безпеки “Оранжевої книги”.

Тема 3. Технологія реалізації атак на комп’ютерну системутамережу

Характеристика та класифікація атак на комп’ютерні системи та мережі. Загальна методика та розповсюджені засоби реалізації атак. Атаки на комп’ютерну систему “із середини”: “троянський кінь”, фальшиві програми реєстрації, використання “логічних бомб”, “таємних дверей” і помилок у програмному забезпеченні.Зовнішні атаки на комп’ютерну систему: віруси, Інтернет-хробаки, мобільні програми.Використання особливостей програмних технологій для реалізації атак. Особливості атак на комп’ютерні мережі, інтегровані з Інтернет.

Тема 4. Методологія захисту інформації в комп’ютерних системах і мережах

Побудова комплексної системи захисту інформації. Критерії оцінювання рівня безпеки інформації. Механізми захисту: аутентифікація й авторизація користувачів, домени захисту, визначення прав доступу. Аутентифікація користувачів за допомогою паролів,з використанням фізичних об’єктів і біометричних даних. Система захисту від несанкціонованого доступу Kerberos. Методика забезпечення захисту програмних технологій Java, ActiveX, Flach, Php, COM, DCOM, COM+. Захист операційних систем Windows і Linux. Захист Web-серверів Apache та IIS. Обмеження доступу до вмісту Web-сторінки за допомогою паролю. Політика безпеки в разі опрацювання електронної пошти.

Тема 5. Системи захистуна основі мережевихекранів

Проблема гарантування безпеки комп’ютерної мережі, інтегрованої з Інтернет. Принципи функціонування Інтернет. Протокол TCP/IP. Поняття мережевого екрана (брандмауера). Типові компоненти. Обмеження функціонування мережі, пов’язані з використанням брандмауерів. Класифікація брандмауерів. Визначення політики

використання брандмауерів. Особливості інсталяції, настроювання та використання популяр-

них брандмауерів.

Тема 6. Основи криптографії та криптоаналізу

Основні терміни та визначення в галузі криптографії та криптоаналізу. Задачі, розв’язувані за допомогою криптографії та криптоаналізу. Актуальність проблеми надійності чинних криптосиситем. Класична модель симетричної системи секретного зв’язку за К. Шенноном. Елементарні шифри. Поняття ключевого потоку. Основні типи шифрів. Загальні алгоритмічні проблеми, пов’язані зі стійкістю сучасних криптоалгоритмів. Недоліки симетричних систем секретного зв’язку. Загальна ідея односторонньої функції з лазівкою. Асиметричні криптосиситеми, основні поняття та означення.

Недоліки та переваги. Використання цифрового підпису. Криптографічні протоколи. Числові алгоритми в симетричній й асиметричній криптографії.

PDF created with FinePrint pdfFactory Pro trial version http://www.fineprint.com7

Тема 7. Системивизначенняатакісистемиреакціїнаатаку.

Моніторинг систем інформаційної безпеки. Передумови побудови та використання систем визначення атак і реакції на атаку. Класифікація та типові компоненти. Системи виз-

начення атак на базі методів визначення аномалій і зловживань. Порівняльна характеристика. Приклади реалізації. Принципи функціонування систем реакцій на атаку. Класифікація, типові компоненти. Приклад реалізації та використання.

Технологія та завдання моніторингу системи інформаційної безпеки. Обґрунтування переліку контрольованих параметрів. Модель оптимізації режиму моніторингу. Критерії оптимізації. Визначення оптимального періоду контролю та допуску на контрольовані пара-метри. Характеристика програмних продуктів призначених для реалізації моніторингу.

Тема 8. Захистпрограмного продукту

Нормативна база в галузі захисту програмних продуктів від несанкціонованого використання. Критерії та методика визначення потрібного рівня захисту. Методика захисту програмних продуктів від несанкціонованого копіювання. Технологія прив’язки програм до клієнтського апаратного та програмного забезпечення. Розробка прикладної реалізації прив’язки програм до конкретної обчислювальної системи. Підходи до аналізу програмних реалізацій. Захист програм від вивчення. Особливості захисту текстової інформації. Приклади реалізації.

**2) Огляд безпеки системи**

**Попереджувальна безпека для надійного захисту даних**

Мережна безпека — це основа працездатної ІТ-інфраструктури. Кожен елемент мережі використовує передачу даних, а це одна з причин вразливості мережі до зловмисних атак.

Розташовуючи елементи безпеки у критичних точках мережі, можна надавати належним користувачам доступ до ресурсів, які їм потрібні, й одночасно захищати корпоративні дані й ІТ-системи.

* [**Технологічна проблема**](http://www.microsoft.com/ukraine/infrastructure/capabilities/securityandnetworking.mspx#technology)
* [**Рішення**](http://www.microsoft.com/ukraine/infrastructure/capabilities/securityandnetworking.mspx#solution)
* [**Бізнес-переваги**](http://www.microsoft.com/ukraine/infrastructure/capabilities/securityandnetworking.mspx#benefits)

*Технологічна проблема*

Оскільки мережні служби є найбільш фундаментальними елементами інфраструктури, ІТ-фахівці мають бути напоготові, щоб допомогти захистити корпоративні активи від атак. Атака може мати форму вірусів, хробаків або зловмисних користувачів, яким потрібні конфіденційні дані. Мережі також можуть бути вразливими до зловмисних атак, спрямованих на пошкодження служб, які заважають користувачам працювати та завдають компаніям великих збитків.

Визнання загроз безпеки та розгортання рішень для боротьби з ними — це основна сфера відповідальності сучасних ІТ-відділів. Нижче перелічені деякі з проблем, з які постають перед ІТ-фахівцями під час забезпечення захисту та надійності роботи служб.

**Запобігання проникненню вірусів і зловмисного вмісту.**У разі проникнення до корпоративної мережі комп’ютерні віруси можуть пошкодити роботу комп’ютерних систем, оскільки вони заважають операціям, заражають дані та навіть сприяють викраданню цінних активів компаній. Незалежно від того, як комп’ютерні віруси потрапляють до мережі, вони в результаті спричиняють пошкодження та збитки.

**Забезпечення функціонування та доступності мережі.**Оскільки це служба основної ІТ-інфраструктури, мережа має бути доступною. Сучасні мережі включають велику кількість різноманітних систем і пристроїв, тому керування доступом може бути складною нестандартною задачею. Надійні інструменти безпеки можуть зменшити складність і покращити безпеку, не порушуючи доступність.

**Баланс доступу та безпеки.** Розрізнення загроз для мережі та припустимих запитів на доступ є основною задачею. Найбільш безпечна система у світі — це та, до якої ніхто немає доступу, але на практиці вона не приносить користі. Таким чином, загрози безпеці мають розпізнаватися й усуватися без порушення роботи служб.

*Рішення*

Визначення загроз, їх нейтралізація та запровадження надійних методів керування може забезпечити доступність мережних служб. Більш захищена мережна інфраструктура підтримує бізнес-служби, забезпечуючи надійну основу. Коли мережа працює, компанія теж працює. Коли мережа не працює, робота компанії зупиняється.

Ключові елементи більш захищених мережних служб

* **Брандмауери.** Централізовані брандмауери та брандмауери окремих комп’ютерів можуть запобігати проникненню зловмисного мережного трафіку до мережі, яка підтримує діяльність компанії.
* **Антивірусні засоби.** Більш захищена мережа може виявляти загрози, що створюють віруси, хробаки та інше зловмисне програмне забезпечення, і боротися з ним попереджувальними методами, перш ніж вони зможуть заподіяти шкоду.
* **Надійність мережі.** Знаряддя, які відстежують стан мережі, грають важливу роль під час визначення мережних загроз.
* **Захищений віддалений доступ і обмін даними.**Безпечний доступ для всіх типів клієнтів із використанням різноманітних механізмів доступу грає важливу роль для забезпечення доступу користувачів до потрібних даних, незалежно від їх місцезнаходження та використовуваних пристроїв.

**Керування конфігурацією.** Хоча це і не елемент безпеки, у строгому значенні цього слова, керування конфігурацією дає змогу визначити відповідну конфігурацію систем на основі політик безпеки.

*Бізнес-переваги*

Створення оптимізованої та більш захищеної мережі може допомогти вашій компанії наступним чином.

* Забезпечення більш стабільної та захищеної інфраструктури.
* Забезпечення стандартів для політик, які дають змогу створити більш стандартизоване середовище.
* Швидке та надійне розповсюдження оновлень безпеки для усунення певних вразливих місць у програмних ресурсах.
* Створення шарів захисту на рівні периметра, сервера, ПК та застосунків, що забезпечує кероване й ефективне середовище, яке може протистояти зловмисним атакам.
* Зниження складності операцій з обладнанням і програмним забезпеченням, що підвищує зручність процесів керування змінами.
* Запобігання конфліктам ІР-адрес завдяки ефективній і надійній мережній конфігурації ТСР/ІР (служби DHCP), яка забезпечує фіксоване використання ІР-адрес за допомогою централізованого керування призначенням адрес.
* Зменшення кількості звернень до служби підтримки через вразливі місця системи захисту.

Корпорація Майкрософт пропонує комплексний, інтегрований і відкритий підхід до створення рішень безпеки, які допоможуть вам усунути загрози безпеці ІТ-інфраструктури, перш ніж вони стануть проблемою. Комплексні галузеві продукти для безпеки Microsoft Forefront забезпечують посилений захист і керування завдяки інтеграції з наявною ІТ-інфраструктурою та спрощеному розгортанню, керуванню й аналізу.

**2. Огляд безпеки системи**

**Огляд стандартів з захисту інформації**

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

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

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

* політика безпеки; вимога 1 (політика безпеки) – система має підтримувати точно визначену політику безпеки, можливість доступу до об'єктів повинна визначатися на основі їх ідентифікації і набору правил керування доступом; вимога 2 (мітки) – кожен об'єкт повинний мати мітку, яка використовується в якості атрибуту контролю доступу;
* аудит; вимога 3 (ідентифікація та автентифікація) – всі суб'єкти повинні мати унікальні ідентифікатори, контроль доступу здійснюється на основі ідентифікації та автентифікації суб'єкта й об'єкта доступу; вимога 4 (реєстрація й облік) – всі події, що мають відношення до безпеки, мають відстежуватися і реєструватися в захищеному протоколі;
* коректність; вимога 5 (контроль коректності функціонування засобів захисту) – засоби захисту знаходяться під контролем засобів перевірки коректності, засоби захисту незалежні від засобів контролю коректності; вимога 6 (безперервність захисту) – захист повинний бути постійним і безперервним в будь-якому режимі функціонування системи захисту і всієї системи в цілому.

Запропоновано також чотири групи критеріїв рівня захищеності. Мінімальний захист (група D), містить один клас (D); дискреційний захист (група С), містить два класи (С1, С2); мандатний захист (група В), містить три класи (В1, В2, В3); верифікований захист (група А), містить один клас (А). Усі групи і класи в них характеризуються зростаючим вимогами безпеки для системи захисту.  
  
 У подальшому виявилося, що ряд положень документа застарів і він був розвинутий (було створено більш чотирьох десятків допоміжних документів – «Райдужна серія»). Значення «Оранжевої книги» важко переоцінити – це була перша спроба, фактично прорив, створення єдиного стандарту безпеки і це був справжній прорив в області безпеки інформаційних технологій. Цей документ став відправною точкою для подальших досліджень і розробок. Основною його відмінністю є орієнтація на системи військового застосування, причому в основному на ОС.

Історично другими були розроблені «Критерії безпеки інформаційних технологій» (Information Technology Security Evaluation Criteria, далі «Європейські критерії»). Вони були розроблені Францією, Німеччиною, Нідерландами та Великобританією і вперше опубліковані в 1991 році.

«Європейські критерії» розглядають наступні основні задачі інформаційної безпеки:

* захист інформації від НСД з метою забезпечення конфіденційності;
* забезпечення цілісності інформації шляхом захисту її від несанкціонованої модифікації або знищення;
* забезпечення працездатності систем за допомогою протидії загрозам відмови в обслуговуванні.

Для забезпечення вимог конфіденційності, цілісності і працездатності в системі необхідно реалізувати відповідний набір функцій безпеки, таких як ідентифікація й автентифікація, керування доступом, аудит і т.д. Ступінь впевненості в правильності їх вибору і надійності функціонування визначається за допомогою адекватності (assurance), яка включає до собі два аспекти: ефективність (відповідність засобів безпеки задачам безпеки) і коректність (правильність і надійність реалізації функцій безпеки). Загальна оцінка рівня безпеки системи складається з функціональної потужності засобів захисту і рівня адекватності їх реалізації.  
  
 Ефективність визначається функціональними критеріями, які розглядаються на трьох рівнях деталізації: перший – цілі безпеки, другий – специфікації функцій захисту, третій – механізми захисту. Специфікації функцій захисту розглядаються з точки зору наступних вимог

* ідентифікація й автентифікація;
* керування доступом;
* підзвітність;
* аудит;
* повторне використання об'єктів;
* цілісність інформації;
* надійність обслуговування;
* безпечний обмін даними.

Набір функцій безпеки специфікується за допомогою визначених класів-шаблонів. Всього визначено десять класів (F-C1, F-C2, F-B1, F-B2, F-B3, F-IN, F-AV, F-DI, F-DC, F-DX) за зростаючими вимогами.

«Європейські критерії» визначають також сім рівнів адекватності – від Е0 до Е6 (за зростанням вимог при аналізі ефективності та коректності засобів захисту).

Головне досягнення цього документа – введення поняття адекватності засобів захисту і визначення окремої шкали для адекватності. Крім того, були визначені основні властивості захищеної інформації – конфіденційність, цілісність.

У 1992 р. Держтехкомісія (ДТК) при Президенті Російської федерації опублікувала п'ять Керуючих документів з питань захисту інформації від НСД:

1. Захист від несанкціонованого доступу до інформації. Терміни і визначення.
2. Концепція захисту ЗОТ і АС від НСД до інформації.
3. Автоматизовані системи. Захист від несанкціонованого доступу до інформації. Класифікація автоматизованих систем і вимоги по захисту інформації.
4. Засоби обчислювальної техніки. Захист від несанкціонованого доступу до інформації. Показники захищеності від НСД до інформації.
5. Тимчасове положення при організації розробки, виготовлення й експлуатації програмних і технічних засобів захисту інформації від НСД в автоматизованих системах і засобах обчислювальної техніки.

Найбільшу цікавість представляють другий, третій та четвертий документи.  
  
 Ідейною основою цих документів є другий документ, який містить систему поглядів ДТК на проблему інформаційної безпеки й основні принципи захисту комп'ютерних систем. З точки зору розробників даних документів основна задача засобів безпеки – це забезпечення захисту від НСД до інформації. Якщо засобам контролю і забезпеченню цілісності деяка увага і приділяється, то про підтримку працездатності систем обробки інформації взагалі не згадується.  
  
Керуючі документи ДТК розглядають дві групи критеріїв безпеки – показники захищеності ЗОТ від НСД і критерії захищеності АС обробки даних. Перша група дозволяє оцінити ступінь захищеності окремих компонентів АС, а друга – повнофункціональні системи обробки даних.

Встановлено сім класів захищеності ЗОТ від НСД до інформації. Найнижчий клас сьомий, найвищий – перший. Для кожного з класів визначено певні вимоги для ЗОТ.  
  
 Для оцінки рівня захищеності АС від НСД встановлено дев'ять класів. Клас підрозділяються на три групи, які відрізняються специфікою обробки інформації в АС. Група АС визначається на основі наступних ознак:

* наявність в АС інформації різного рівня конфіденційності;
* рівень повноважень користувачів АС на доступ до конфіденційної інформації;
* режим обробки даних в АС (колективний або індивідуальний).

Наведемо склад кожної групи за зростанням рівня захищеності. Отже, третя група включає АС, у яких працює один користувач допущень до всієї інформації АС, що розміщена на носіях один рівня конфіденційності. Група містить два класи – 3Б і 3А.

Друга група включає АС, у яких користувачі мають однакові повноваження доступу до інформації, яка обробляється на носіях різного рівня конфіденційності. Вона має два класи – 2Б і 2А.

Перша група включає багатокористувацьки АС, у яких водночас обробляється інформація різних рівнів конфіденційності. Користувачі мають різні права доступу. Група містить п'ять класів – 1Д, 1М, 1В, 1Б, 1А.

Розробка стандарту із ІБ ДТК було дуже важливим новим кроком для тогочасного рівня розвитку інформаційних технологій Росії. Великий вплив на нього зробила «Оранжева книга», оскільки і той і другий стандарти були орієнтовані на системи військового застосування. До недоліків даного стандарту слід віднести відсутність вимог до захисту від загроз працездатності, орієнтація тільки на захист від НСД, відсутність вимог до адекватності реалізації політики безпеки. Поняття політики безпеки трактується виключно як підтримка секретності і відсутність НСД, що принципово неправильно.

«Федеральні критерії безпеки інформаційних технологій» (Federal Criteria for Information Technology Security) розроблялись як одна зі складових «Американського федерального стандарту по обробці інформації» (Federal for Information Processing Standard) і мала замінити «Оранжеву книгу». Розробниками стандарту виступили Національний інститут стандартів і технологій США (National of Snandards and Technology – NIST) та Агенство національної безпеки США (National Security Agency – NSA). Перша версія документа була опублікована в грудні 1992 р.

Цей документ розроблений на основі результатів численних досліджень в області забезпечення інформаційних технологій 80-х - початку 90-х років, а також на основі досвіду використання «Оранжевої книги». Документ являє собою основу для розробки і сертифікації компонентів інформаційних технологій з погляду забезпечення безпеки. Створення документа переслідувало наступні цілі:  
  
1. Визначення універсального й відкритого для подальшого розвитку базового набору вимог безпеки до сучасних інформаційних технологій. Вимоги до безпеки і критерії оцінки рівня захищеності повинні відповідати сучасному рівню розвитку інформаційних технологій і враховувати його прогрес у майбутньому.  
2. Удосконалювання існуючих вимог і критеріїв безпеки. У зв'язку з розвитком інформаційних технологій назріла необхідність перегляду фундаментальних принципів безпеки з урахуванням появи нових областей їхнього застосування як у державному так і в приватному секторах.

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

4. Нормативне закріплення основних принципів інформаційної безпеки. Стандарт є узагальненням основних принципів забезпечення безпеки інформаційних технологій, розроблених у 80-і роки, і забезпечує наступність стосовно них з метою збереження досягнень в області захисту інформації.

Основними об'єктами вимог безпеки «Федеральних критеріїв» є продукти ІТ, під якими розуміється сукупність апаратних і/чи програмних засобів, яка являє собою готовий до використання засіб обробки інформації і поставляється споживачу. Як правило, ІТ-продукт експлуатується не автономно, а інтегрується в систему обробки інформації, що представляє собою сукупність ІТ-продуктів, об'єднаних у функціонально повний комплекс, призначений для рішення прикладних задач. З погляду безпеки принципове розходження між ІТ-продуктом і системою обробки інформації визначається середовищем їхньої експлуатації. Продукт ІТ звичайно розробляється в розрахунку на те, що він буде використовуватися в багатьох системах обробки інформації, і, отже, розроблювач повинний орієнтуватися тільки на самі загальні припущення про середовище експлуатації свого продукту, що включають умови застосування і загальні загрози. Навпроти, системи обробки інформації розробляється для рішення прикладних задач у розрахунку на вимоги кінцевих споживачів, що дозволяє враховувати специфіку впливів з боку конкретного середовища експлуатації.

«Федеральні критерії» містять положення, що відносяться тільки до окремих продуктів ІТ. Положення стосуються тільки власних засобів забезпечення безпеки ІТ-продуктів, тобто механізмів захисту, убудованих безпосередньо в ці продукти у виді відповідних програмних, апаратних чи спеціальних засобів. Для підвищення ефективності їх роботи можуть використовуватися зовнішні системи захисту і засоби забезпечення безпеки, до яких відносяться як технічні засоби, так і організаційні заходи, правові і юридичні норми. У кінцевому рахунку, безпека ІТ-продукту визначається сукупністю власних засобів забезпечення безпеки і зовнішніх засобів, що є частиною середовища експлуатації.

Ключовим поняттям «Федеральних критеріїв» є поняття профілю захисту – нормативного документа, що регламентує всі аспекти безпеки ІТ-продукту у виді вимог до його проектування, технології розробки і кваліфікаційного аналізу.  
  
 «Федеральні критерії» представляють процес розробки інформації у виді трьох основних етапів:

1. Розробка й аналіз профілю захисту. Вимоги, викладені в профілі захисту, визначають функціональні можливості ІТ-продукта по забезпеченню безпеки. Профіль безпеки аналізується на повноту, несуперечність і технічну коректність.  
  
2.Розробка і кваліфікаційний аналіз ІТ-продукта.

3. Компонування і сертифікація система обробки інформації в цілому.

«Федеральні критерії» регламентують тільки перший етап цієї схеми - розробку й аналіз профілю захисту, наступні етапи залишаються поза рамками цього стандарту.

«Федеральні критерії» є першим стандартом ІБ, у якому визначаються три незалежні групи вимог: функціональні вимоги до засобів захисту, вимоги до технології розробки і до процесу кваліфікаційного аналізу. Вперше запропонована концепція профілю захисту, що містить опис усіх вимог безпеки як до самому ІТ-продукту, так і до процесу його проектування, розробки, тестування і кваліфікаційного аналізу. В документі не використовувався підхід до єдиної оцінки рівня безпеки ІТ-продукта, а запропоновано незалежне ранжування вимог кожної групи.«

Канадські критерії безпеки комп'ютерних систем» (Canadian Trusted Computer Product EvaluationCriteria) були розроблені в Центрі безпеки відомства безпеки зв'язку Канади (Canadian System Security Centre Communication Security Establishment) для використання в якості національного стандарту безпеки комп'ютерних систем. Першу версію стандарту було опубліковано в 1992 р.  
 При розробці «Канадських критеріїв» переслідувалися наступні цілі:  
 1. Запропонувати єдину шкалу критеріїв оцінки безпеки КС для порівняння систем по ступені забезпечення безпеки.

2. Створити основу для розробки специфікацій безпечних КС, яка могла б використовуватися розроблювачами при проектуванні систем як керівництво.

3. Запропонувати уніфікований підхід і стандартні засоби для опису характеристик безпечних КС.

Базовим поняттям стандарту є об'єкт, що може знаходитися в трьох станах: об'єкт-користувач, об'єкт-процес, пасивний об'єкт.

Функціональні критерії розділяються на чотири групи: критерії конфіденційності, цілісності, працездатності й аудита. Кожна з цих груп (крім аудита) відбиває функціональні можливості системи по відображенню відповідного класу загроз. В кожній групи критеріїв визначені рівні безпеки, що відбивають можливості засобів захисту за рішенням задач даного розділу. Ранжування за рівнями здійснюється на підставі потужності використовуваних методів захисту і класу відбиваних загроз. Рівні з великим номером забезпечують більш високий ступінь безпеки.

Адекватність реалізації визначається тим, наскільки точно і послідовно засоби, що забезпечують захист, реалізують прийняту в системі політику безпеки. Критерії адекватності відбивають рівень коректності реалізації політики безпеки й охоплюють усі стадії проектування, розробки й експлуатації комп'ютерної системи.

У такий спосіб «Канадські критерії» визначають ступінь безпеки комп'ютерної системи як сукупність функціональних можливостей використовуваних засобів захисту, що характеризується приватними показниками забезпечуваного рівня безпеки, і одного узагальненого параметра - рівня адекватності реалізації політики безпеки.

«Канадські критерії» з'явилися першим стандартом ІБ, у якому на рівні структури документа функціональні вимоги до засобів захисту відділені від вимог адекватності і якості реалізації політики безпеки. Вперше багато уваги приділяється взаємній відповідності і взаємодії всіх систем забезпечення безпеки. Прогресивними також є вимоги доказу коректності реалізації функціональних вимог і їх формальної відповідності політиці і моделі безпеки.

«Єдині критерії безпеки інформаційних технологій» (Common Criteria for Information Technology Security Evaluation) є результатом сумісних зусиль авторів Європейських «Критеріїв безпеки інформаційних технологій», «Федеральних критеріїв безпеки інформаційних технологій» і «Канадських критеріїв безпеки комп'ютерних систем», спрямованих на об'єднання основних положень цих документів і створення єдиного міжнародного стандарту безпеки інформаційних технологій. Робота над цім самим масштабним в історії стандартів інформаційної безпеки проектом почалася в червні 1993 року з метою подолання концептуальних і технічних різниць між вказаними документами, їх узгодження і створення єдиного міжнародного стандарту. Перша версія «Єдиних критеріїв» була опублікована в січні 1996 р. Розробниками документа виступили США, Великобританія, Канада, Франція і Нідерланди. Розробка цього стандарту переслідувала наступні основні мети

* уніфікація національних стандартів в області оцінки безпеки ІТ;
* підвищення рівня довіри до оцінки безпеки ІТ;
* скорочення витрат на оцінку безпеки ІТ на основі взаємного визнання сертифікатів.

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

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

У травні 1998 року була опублікована версія 2.0 документа і на її основі в червні 1999 року був прийнятий міжнародний стандарт ІСО/МЕК 15408. Офіційний текст стандарту виданий 1 грудня 1999 року. Зміни, внесені в стандарт на завершальній стадії його прийняття, враховані у версії 2.1, ідентичної початковій. В даний час на підставі отриманого досвіду практичного застосування стандарту готується версія 3.0, що вийде в 2002 році.

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

В єдиних критеріях проведена класифікація широкого набору функціональних вимог і вимог довіри до безпеки, визначені структури їхнього групування і принципи цільового використання.

Основними відмітними рисами стандарту є:

1. Насамперед, стандарт – це визначена методологія і система формування вимог і оцінки безпеки ІТ. Системність просліджується, починаючи від термінології і рівнів абстракції представлення вимог і закінчуючи їх використанням при оцінці безпеки на всіх етапах життєвого циклу виробів ІТ.
2. Єдині критерії характеризуються найбільш повною на сьогоднішній день сукупністю вимог до безпеки ІТ.
3. В єдиних критеріях проведений чіткий поділ вимог безпеки на функціональні вимоги і вимоги довіри до безпеки. Функціональні вимоги відносяться до сервісів безпеки (ідентифікації, автентифікації, керуванню доступом, аудиту і т.д.), а вимоги довіри – до технології розробки, тестуванню, аналізу уразливостей, експлуатаційної документації, постачанню, супроводу, тобто до всіх етапів життєвого циклу виробів ІТ.
4. Єдині критерії включають шкалу довіри до безпеки (оцінні рівні довіри до безпеки), що може використовуватися для формування різних рівнів впевненості в безпеці продуктів ІТ.
5. Систематизація і класифікація вимог по ієрархії «клас»-«сімейство»-«компоненти»-«елемент» з унікальними ідентифікаторами вимог забезпечує зручність їхнього використання.
6. Компоненти вимог у сімействах і класах ранжовані за ступенем повноти і жорсткості, а також згруповані в пакети вимог.
7. Гнучкість у підході до формування вимог безпеки для різних типів виробів ІТ і умов їхнього застосування забезпечуються можливістю цілеспрямованого формування необхідних наборів вимог у виді визначених стандартизованих структур (профілів захисту і завдань по безпеці).
8. Єдині критерії мають відкритість для наступного нарощування сукупності вимог.

Як показують оцінки фахівців в області інформаційної безпеки [ЗИ], за рівнем систематизації, повноті і можливостям деталізації вимог, універсальності і гнучкості в застосуванні стандарт являє собою найбільш розроблений з існуючих в даний час стандартів. Причому, що дуже важливо, в силу особливостей побудови, він має практично необмежені можливості для розвитку, являє собою не функціональний стандарт, а методологію завдання, оцінки і каталог вимог безпеки ІТ, що може нарощуватися й уточнюватися. Основними документами, що описують всі аспекти безпеки ІТ-продукта, з погляду користувачів і розроблювачів є відповідно профіль захисту і проект захисту. Профіль захисту визначає вимоги безпеки до визначеної категорії ІТ-продуктів і не уточнює методи і засоби їхньої реалізації. Це дуже докладний документ, що містить такі розділи: уведення, опис ІТ-продукта, середовище експлуатації, задачі захисту, вимоги безпеки, додаткові зведення, обґрунтування задач захисту і вимог безпеки.

Проект захисту містить вимоги і задачі ІТ-продукта, а також описує рівень функціональних можливостей реалізованих у ньому засобів захисту, їхнє обґрунтування і підтвердження ступеня їхньої адекватності. Проект захисту, з одного боку є відправною крапкою для розроблювача системи, а з іншого, являє собою еталон системи в ході кваліфікаційного аналізу. Документ містить наступні розділи: вступ, опис ІТ-продукта, середовище експлуатації, задачі захисту, вимоги безпеки, загальні специфікації ІТ-продукта, заявка на відповідність профілю захисту, обґрунтування.

Профіль і проект захисту вичерпним образом регламентують взаємодію споживачів, виробників і експертів по кваліфікації в процесі створення ІТ-продукта. Фактично ці документи визначають технологію розробки захищених систем. Найважливішим елементом цієї технології є вимоги безпеки.

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

Функціональні вимоги регламентують функціонування компонентів ІТ-продукта, що забезпечують безпеку, і визначають можливості засобів захисту. Функціональні вимоги представляються у виді складної, але добре проробленої формальної ієрархічної структури, що складається з класів, розбитих на розділи.  
  
 Адекватність являє собою характеристику ІТ-продукта, що показує, наскільки ефективно забезпечується заявлений рівень безпеки, а також ступінь коректності реалізації засобів захисту. Вимоги адекватності жорстко структуровані і регламентують всі етапи проектування, створення й експлуатації ІТ-продукта з погляду надійності роботи засобів захисту і їхньої адекватності функціональним вимогам, задачам захисту і погрозам безпеки. Є сім стандартних рівнів адекватності, причому рівень вимог адекватності зростає від першого рівня до сьомого. Кожен рівень характеризується набором вимог адекватності, що регламентують застосування різних методів і технологій розробки, тестування, контролю і верифікації ІТ-продукта:

Рівень1. Функціональне тестування

Рівень2. Структурне тестування

Рівень3.Методичне тестування і перевірка

Рівень4.Методична розробка, тестування й аналіз.

Рівень5.Напівформальні методи розробки і тестування.

Рівень 6. Напівформальні методи верифікації розробки і тестування.

Рівень7.Формальні методи верифікації розробки і тестування.

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

Даний стандарт ознаменував собою новий рівень стандартизації інформаційних технологій, піднявши його на міждержавний рівень. За цим проглядається реальна перспектива створення єдиного безпечного інформаційного простору, у якому сертифікація систем безпеки обробки інформації буде здійснюватися на глобальному рівні, що надасть можливості для інтеграції національних інформаційних систем, що у свою чергу відкриє зовсім нові сфери застосування інформаційних технологій.

**3)** **Механізми і політики розмежування прав доступу**

РЕАЛІЗАЦІЯ АНТИВІРУСНОГО ЗАХИСТУ НА ОСНОВІ РОЗМЕЖУВАЛЬНОЇ ПОЛІТИКИ ДОСТУПУ ДО РЕСУРСІВ

Національний технічний університет України «Київський політехнічний інститут»

Фізико-технічний інститут

Більшість антивірусних засобів захисту містять у своїй основі механізми контролю (контроль сигнатур і поведінкові аналізатори). Разом з тим, відомо, що основу ефективного захисту інформації становить реалізація розмежувальної політики доступу до ресурсів, механізми контролю (наприклад, контролю цілісності), як правило вторинні, вони використовуються в тому випадку, коли неможливо коректно вирішити завдання механізмами розмежування прав доступу до ресурсів. І це цілком зрозуміло, механізми контролю не тільки дуже ресурсомісткі, але і в принципі не можуть ефективно вирішити завдання захисту. Наприклад, розглянемо сучасні сигнатурні аналізатори.

По-перше, вони можуть виявляти лише відомі віруси, для яких розробниками виявлена сигнатура. Розповсюдженні антивірусні програми блокують лише близько 20 відсотків недавно з'явившихся шкідливих програм. При цьому популярні антивіруси пропускають до 80 відсотків нових троянів, шпигунів і інших шкідливих программ. Це означає, що у восьми з десяти випадків вірус, який нещодавно з'явився може проникнути на комп'ютер користувача.По-друге, бази сигнатур вже давно «перевалили» за сотні тисяч. Контроль тільки системного диска може складати кілька годин. У результаті, з одного боку, немає ніякої гарантії виявити знову створений вірус, з іншого боку, використання засобів ускладнено: рідко – неефективно, часто – неможливо. Тому проблема ефективного антивірусного захисту і до цього дня залишається однією з ключових проблем інформаційної безпеки [1]. Тому, давно назріла необхідність у використанні принципово інших підходів до антивірусного захисту одним з яких є реалізація розмежувальної політики доступу до ресурсів за допомогою якої можна ефективно вирішити такі ключові завдання антивірусного захисту:

• Запобігання запуску будь-якого стороннього процесу;

• Захистити від несанкціонованої модифікації системні комп'ютерні ресурси (як

системні файлові об'єкти, так і об'єкти реєстру ОС);

• Істотно знизити ймовірність вірусної атаки на інформаційні ресурси, які

зберігаються на комп'ютері.

При цьому зазначимо, що дані завдання антивірусного захисту вирішуються в загальному вигляді, не вимагають виявлення будь-яких сигнатур, що забезпечує можливість ефективної протидії як відомим вірусам, так і потенційно можливим вірусам. Найважливішою властивістю даних підходів до вирішення завдання антивірусного захисту, на відміну від підходів, в основу яких покладена реалізація механізмів контролю, є мінімальний вплив засобів захисту на завантаження обчислювального ресурсу. Все це дозволяє нам зробити висновок про перспективність саме такого підходу до комплексного об’єднання механізмів і засобів для вирішення задачі антивірусного захисту в корпоративних додатках.

Перелік посилань:

1. Компьютерная безопасность. Деструктивные и шпионские программы, эксплойты, трояны, вирусы и прочее. Существуют ли средства эффективного противодействия? – [Электронный ресурс] / ЗАО «НПП «Информационные технологии в бизнесе»;. – ред. д.т.н., проф. Щеглов А.Ю. – Электрон. дан., 2008 – Режим доступа: http://www.npp-itb.spb.ru/publications/4.html, свободный. – Яз. рус.

Розмежування доступу до ресурсів ОС

Мережна операційна система (ОС) – це пакет програм, що забезпечує реалізацію та управління мережею, дає змогу клієнтам користуватись мережним сервісом. Основними завданнями мережної ОС є забезпечення сумісного використання та розподілу ресурсів мережі; надання клієнтам мережного сервісу; адміністрування мережі; обміну повідомленнями між вузлами мережі; взаємодії процесів у мережі; надійного зберігання даних та інших завдань, пов’язаних з функціонуванням мережі. Важливою функцією мережної ОС є забезпечення системи захисту – конфіденційності зберігання даних, розмежування прав доступу до ресурсів, парольний захист, виявлення спроб несанкціонованого доступу, трасування дій користувачів, ведення журналів системних подій тощо.  
 Мережна ОС забезпечує підтримку різноманітних периферійних пристроїв, мережних адаптерів, протоколів та можливість їх конфігурування.

Програмне забезпечення клієнтської частини перетворює запити прикладної програми на використання мережних ресурсів у відповідні мережні формати, забезпечує їх пересилання через середовище передавання та здійснює зворотні перетворення. Клієнтська частина залежить від ОС, що встановлена на робочій станції (DOS, Windows’95’98, Unix, Macintosh, OS/2), та типів мереж.

У мережах з централізованим управлінням (виділеним сервером) мережна ОС є головною (або єдиною) системою, що управляє ресурсами серверу. Такі системи, звичайно, мають високу продуктивність та функціональні можливості, використовують власні дискові та файлові системи, що оптимізовані для роботи в мережі (NetWare, Windows’NT’2000).  
Однорангові мережі дають змогу кожному вузлу мережі одночасно виступати в ролі сервера та клієнта. Тут мережна ОС може бути процесом, що виконується під управлінням ОС вузла (NetWare Lite, LANtastic, Windows for Workgroups), або складовою частиною ОС (Personal NetWare, Windows’95’98, Windows’NT’2000).

Клієнтська частина реалізується у вигляді оболонки (редиректора), що обслуговує мережні запити та працює під управлінням вихідної ОС вузла (DOS, Unix, OS/2), або є органічною частиною ОС (Windows’95’98’NT’2000). Звичайно, клієнт може мати одночасний доступ до ресурсів різних мереж, що використовують спільне середовище передавання.

I. Огляд систем доступу в Unix- та Windows-подібних системах

**Права доступу до файлів в Unix-системах.**

Розрахована на багато користувачів система UNIX підтримує механізм, відомий, як система прав доступу до файлів. Цей механізм дозволяє вказати для кожного файлу власника і забезпечити захист файлів від доступу інших користувачів. UNIX дозволяє також спільно використовувати файли декільком користувачам і групам користувачів. У більшості систем, за замовчуванням, іншим користувачам дозволяється читати ваші файли, але забороняється вносити зміни у файли або видаляти їх. Отже, кожен файл має конкретного власника, але, крім того файлами, також можуть володіти конкретні групи користувачів, які визначаються при реєстрації користувачів у системі. Кожен користувач стає членом як мінімум однієї групи користувачів (своєї або який-то із загальних груп). Системний адміністратор (суперкористувач, зазвичай root) може забезпечити користувачеві доступ більш, ніж до однієї групи. Групи зазвичай визначаються типами користувачів цієї машини, наприклад, в університетському UNIX користувачі можуть бути розбиті на групи студент, викладач, керівництво, гість, або користувачі віртуального хостингу одного і того ж сервера можуть належати до групи www. Права доступу підрозділяються на три типи: читання (read), запис (write) і виконання (execute). Ці типи прав доступу можуть бути надані трьом класам користувачів: власнику файлу, групі, в яку входить власник, і всім іншим користувачам цієї машини. Дозвіл на читання (read) дозволяє користувачеві читати вміст файлів, а у разі каталогів - переглядати перелік імен файлів у каталозі. Дозвіл на запис дозволяє користувачеві писати в файл і змінювати його.Для каталогів це дає право створювати в каталозі нові файли і каталоги, або видаляти файли та каталоги у поточному каталозі. Нарешті дозвіл на виконання дозволяє користувачеві виконувати файли (як бінарні програми, так і командні файли). Дозвіл на виконання стосовно до каталогів дозволяє пользовотелю увійти до каталогу або, по іншому кажучи, змінити значення змінної оточення $ PWD командної оболонки на значення, відповідне місцю розташування цього каталогу від кореня файлової системи UNIX (повний шлях). При цьому, якщо біт читання (read) для даного каталогу не встановлений, то користувач зможе тільки увійти до каталогу, але не зможе прочитати імена файлів, що містяться в цьому каталозі - для користувача каталог буде порожній. Невеликий приклад, що демонструє роботу з правами доступу. Використовуючи команду ls з опціями-al можна отримати на екрані перелік всіх файлів даного каталогу (навіть прихованих) у "довгому" форматі, що включає й інформацію про права доступу.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| drwx --- --- | 4 | user | user | 4096 | Вересні 1912 19:11 | . / |
| drwx --- --- | 9 | user | user | 4096 | 7 червня 1:14 | .. / |
| -Rw-r - r - | 1 | user | user | 11282 | 25 лютого 2003 | data-type0.5.4.txt |
| -Rw-r - r - | 1 | user | user | 20897 | 6 липня 16:43 | data-type0.5.4.txt.html |
| drwx --- --- | 2 | user | user | 4096 | Березень 1914 18:17 | test / |
| drwx rx rx | 2 | user | user | 4096 | 6 березня 2003 | todo / |

Сім полів, зліва направо, позначають буквально наступне: атрибути об'єкта, кількість посилань на об'єкт, ім'я власника, група до якої належить власник, розмір об'єкта, дата і час останньої модифікації, ім'я об'єкта. Перше поле - поле атрибутів. Воно складається з 10 полів, разділених на 4 секції:

1. У першій секції, яка складається з одного поля, перебуває або - (прочерк), або d. Наявність букви d говорить про те, що даний об'єкт є директорією.Прочерк позначає,      що  об'єкт - звичайний файл.
2. Друга секція, як і всі наступні, складається з 3-х полів ... Вона визначає права доступу для власника (u) об'єкта до цього об'єкта. Перше поле означає право на читання (r), тобто на відкриття та читання вмісту цього файлу; або перегляд вмісту директорії, якщо це директорія. Друге поле визначає право на запис (w), тобто на модифікацію, видалення цього файлу; або, якщо це директорія, на створення і видалення в ній файлів і директорій; третє поле - право на виконання (x), тобто система буде вважати, що цей файл - програма або скрипт, коли ж це директорія - то наявність даного атрибуту дозволить у неї "зайти".
3. Третя секція, аналогічна першій, але визначає права для групи (g), яка встановлена для цього об'єкту.
4. Четверта секція, аналогічна першій, але визначає права для всіх інших (o)користувачів системи.

Крім того, система прав доступу має також і числове подання. Права представляють із себе число вигляду XYZ, що складається з цифр X, Y і Z, що визначають права для власника (X), групи (Y) і інших (Z), відповідно.Складається X, Y або Z за однаковими правилами: праву на читання відповідає цифра 4, праву на запис - 2, праву на виконання - 1. Якщо ви дозволяєте якісь з цих прав просто сумміруете, відповідні ним цифри. Таким чином, якщо ваш файл має право читати, змінювати і запускати тільки власник, то, відповідні значення для числового представлення обчислюються наступним чином: X = 4 +2 +1 = 7, Y = 0 +0 +0 = 0, Z = 0 +0 +0 = 0. Тепер давайте звернемося до питання про те, як же змінювати права доступу. Тут все залежить від способу вашого доступу до системи. Якщо ви маєте unix shell, то ви можете скористатися командою chmod (change mode) приблизно так chmod 0644 file.txt або навіть так chmod og-x file.txt Для одержання більш докладної інформації про команду chmod зверніться до сторінки довідкового керівництва - man chmod. Якщо ж ви маєте доступ до системи по протоколу FTP (наприклад, доступ до вашого сайту), то і тут ви зможете працювати з правами доступу, якщо це "дозволяє" сервер. Сучасні клієнти FTP, як для Windows, так і для Unix, надають таку можливість. Причому найчастіше, ви маєте можливість працювати як з буквеним, так і числовим представленням прав доступу, як вам зручніше. Можна встановлювати права доступу як заманеться, але треба пам'ятати, що небажано давати право на запис у своїй директорії та файли всім іншим (other) користувачам системи, і в деяких випадках, користувачам, які входять до своєї групи. Можна взагалі заборонити будь-які дії зі своїми файлами і директоріями для користувачів із своєї групи і всіх інших користувачів, встановивши права для директорій drwx --- --- і для невиконуваних файлів-rw---- ---.

**Мережевий доступ до Windows XP Pro**

Система Windows XP поставляється на продаж у двох варіантах - Home і Professional Edition. З точки зору мережевих параметрів між ними є два важливих відмінності.  
У Home Edition відсутня можливість тонкої настройки мережевого доступу внаслідок того що мається на увазі використання цієї ОС виключно в домашніх мережах. Тому ряд вимог безпеки для таких мереж кілька знижений. У ній існує тільки один, простий спосіб надання ресурсів комп'ютера в загальне користування (Simple File Sharing). Далі по тексту для скорочення я буду іноді застосовувати слово «розшарити» (від слова "Share") для поняття «надання ресурсів комп'ютера в загальне користування» (так коротше). Простий загальний доступ в Home Edition включений за замовчуванням, не вимагає особливих налаштувань і , як правило, працює без втручання користувача. Home Edition не може працювати в домені, який, за великим рахунком, для домашніх мереж є зайвою розкішшю (без застосування спеціальних трюків ).

Мережевий доступ до системи Windows XP заснований на аналогічних системах Windows NT і Windows 2000, тому користувачі систем Windows 95, 98, і Me будуть стурбовані новими особливостями. Ці особливості виражені у введенні деяких обмежень для підвищення рівня безпеки. Зокрема, у свіжовстановленій системі мережевий доступ до XP-комп'ютера заборонений і його треба налаштовувати. У Windows 95/98/Me можна обмежити доступ до спільного диска або папки на парольному рівні і лише той, хто його знає, зможе отримати доступ до загального ресурсу.

Windows XP Pro пропонує на заміну парольного системі доступу дві альтернативи:

* Простий спільний доступ Simple File Sharing, який дозволений за замовчуванням для учасників робочих груп (звичайна структура для невеликих мереж). При використанні цього методу немає ніяких обмежень у доступі різним користувачам і кожен Розшарені ресурс доступний будь-якому учаснику цієї мережі. Нагадаю, що Простий спільний доступ це єдиний метод розшарювання ресурсу в Windows XP Home Edition.
* «Простий спільний доступ» включений за замовчуванням і не вимагає тонкої настройки. Потрібно тільки включити саму можливість мережевого доступу до XP-комп'ютера.

Після заборони використання Простого загального доступу ви зможете використовувати Список управління доступом Access Control List, ACL для кожного спільного диска або папки і при цьому отримаєте можливість Налаштувати Список управління доступом \*\* для кожного користувача.

***Дозвіл мережевого доступу Гостям*** Щоб дозволити доступ мережевим гостям (його іноді називають анонімним входом), треба виконати наступне:   
Створити спільний ресурс. Для цього на папці, яка стане загальною, правою кнопкою викликаємо меню і вибираємо пункт Загальний доступ і безпека. На вкладці Доступ читаємо попередження («Якщо ви розумієте потенційну небезпеку ...»), клікаєм по ньому, переставляємо крапку в полі« Просто включити загальний доступ до файлів »і натискаємо ОК. Після цього у вікні властивостей папки з'явиться новий розділ - «Мережевий загальний доступ і безпека». У ньому треба поставити галочку в полі Відкрити спільний доступ до цієї папки. У полі «Ім'я загального ресурсу» вводимо ім'я під яким ця папка буде видно в мережі або (краще) залишаємо його як є, щоб не плутатися. Натискаємо «Застосувати» і потім натискаємо на лінк «Перегляд параметрів брандмауера Windows» для переходу до його настройки. Далі налаштувати Брандмауер Windows, включений за замовчуванням. У вікні налаштування брандмауера переходимо на вкладку «Винятки» і ставимо галочку в полі Загальний доступ до файлів і принтерів, натискаємо ОК.

***Заборона «Простого загального доступу»***

Заборонити «Простий загальний доступ» потрібно для того, щоб отримати набагато більш широкі та гнучкі можливості по управлінню доступом до вашого XP-комп'ютера через створення та застосування Списку управління доступом для Розшарені дисків і файлів.

***Створення облікового запису користувача***

Цю операцію іноді називають «завести користувача». Крім уже наявних, нам знадобиться завести на своєму комп'ютері нових, тих, кому ми будемо давати доступ до своїх ресурсів. Саме на підставі даних цих облікових записів ваш комп'ютер буде ідентифікувати користувачів і вирішувати кого і куди пускати.

***Паролі***

Безпарольний обліковий запис означає, що будь-який користувач може сісти за ваш комп'ютер, включити його і увійти в систему (отримати локальний доступ) без введення пароля. Зовсім інша справа - мережевий доступ. За замовчуванням Windows XP не допускає до себе мережних користувачів і вхід в систему без пароля. А ми як раз і збиралися зайнятися саме мережевим доступом і для цього слід визначитися з подальшою політикою.

У вас є два варіанти політики:

Вхід з паролем забезпечує високий рівень безпеки. Якщо ви хочете підвищити рівень безпеки (рекомендовано), задайте користувачам пароль. Пам'ятайте, що це зажадає від користувачів, що бажають зайти по мережі на ваш комп'ютер, спочатку входити на свій з тим же паролем. Якщо ці комп'ютери однокористувацький, то ви можете встановити автоматичний вхід (автологін) в систему з використанням програми TweakUI в 98-х системах або її аналога з комплекту PowerToys for Windows XP для XP. У XP можна також автоматизувати вхід в систему .

Багато користувачів з Windows 95/98/Me вважають за краще встановлювати на своїх комп'ютерах вхід в мережу способом Вхід в Windows і без пароля, це дозволяє їм просто і гладко входити в свою систему без відповіді на запит пароля, але при цьому до ваших Розшарені ресурсів вони доступу не отримають. Якщо ви не хочете напружувати їх «зайвої» операцією при завантаженні їх системи, то вам слід змінити політику безпеки на вашому Windows XP комп'ютері так, щоб дозволити вхід до вас по мережі користувачам без коду (не рекомендується)

***Дозвіл мережевого входу без пароля***

Щоб все-таки дозволити користувачам входити на свої комп'ютери без пароля і потім заходити по мережі на ваш комп'ютер теж без пароля ви повинні змінити вашу політику безпеки і дозволити вхід до вас без пароля.

Цим самим ви дозволяєте локальний і мережевий вхід на ваш комп'ютер без пароля. Інші користувачі зможуть при завантаженні заходити без пароля прямо на свою Робочий стіл і коли їм знадобиться зайти на ваш комп'ютер, вони зможуть зайти під пов'язаної з їх ім'ям обліковим записом на XP без пароля.

Зауважте, що іноді використовується термін «порожній пароль» не зовсім технічно правильний. Є різниця між паролем, що містить один або більше порожніх знаків (типу пробіл) та відсутністю пароля взагалі. Виконана установка дозволяє доступ без пароля взагалі. Увага! Дозвіл доступу без пароля відкриває доступ з порожніми паролями і до так званим «адміністративним» ресурсів, що розділяються, що зовсім не безпечно.   
Можна переглянути облікові записи по-іншому: Панель управління - Адміністрування - Управління комп'ютером - Локальні користувачі та групи - Користувачі. Тут знаходяться всі ваші облікові записи! Ви можете звідси змінити налаштування для кожного користувача і навіть створити новий запис натиснувши Дія - Новий користувач.

II. Журнали порушення безпеки операційних систем

Повідомлення в журналі брандмаура необхідні для визначення атак, пошуку проблем в правилах, а також для визначення незвичайної активності у вашій мережі. Щоб активувати журнал вам необхідно включити відповідні правила в конфігурацію вашого міжмережевого екрану, більше того, ці правила повинні бути задані раніше всіх застосованих завершальних правил (це правила з метою, яка визначає подальшу долю пакету, такі як ACCEPT, DROP або REJECT). Наприклад,

sudo iptables-A INPUT-m state - state NEW-p tcp - dport 80-j LOG - log-prefix "NEW\_HTTP\_CONN:"

Тоді запит на порт 80 з локальної машини буде генерувати повідомлення в dmesg подібне наступному:

[4304885.870000] NEW\_HTTP\_CONN: IN = lo OUT = MAC = 00:00:00:00:00:00:00:00:00:00:00:00:08:00 SRC = 127.0.0.1 DST = 127.0.0.1 LEN = 60 TOS = 0x00 PREC = 0x00 TTL = 64 ID = 58288 DF PROTO = TCP SPT = 53981 DPT = 80 WINDOW = 32767 RES = 0x00 SYN URGP = 0

Повідомлення вище, буде також записано у файли / var / log / messages, / var / log / syslog, і / var / log / kern.log. Дану поведінку можна змінити відповідними настройками у файлі / etc / syslog.conf або за допомогою установки і настройки ulogd (при цьому потрібно використовувати мета ULOG замість LOG). Демон ulogd - це сервер користувацького робочого простору, який очікує від ядра інструкцій для запису в журнал, специфічних для брандмауерів, і може зберігати їх у будь-який файл на ваш смак, і навіть до бази даних PostgreSQL або MySQL. Розібратися в журналі брандмауера може допомогти використання утиліт аналізу журналів подій, таких як fwanalog, fwlogwatch, або lire.

**syslog** - стандарт відправки повідомлень про події (логи), що відбуваються в системі, який використовується в комп'ютерних мережах, що працюють за протоколом IP.   
Протокол syslog простий: відправник посилає коротке текстове повідомлення, розміром менше 1024 байт одержувачу повідомлення. Одержувач при цьому носить ім'я «syslogd», «syslog daemon», або ж, «syslog server». Повідомлення можуть відправлятися як по UDP, так і по TCP. Як правило, таке повідомлення надсилається у відкритому вигляді. Тим не менш, використовуючи спеціальні засоби (такі, як Stunnel, sslio або sslwrap), можливе шифрування повідомлень і відправлення їх по SSL / TLS.

Syslog використовується для зручності адміністрування та забезпечення інформаційної безпеки. Він реалізований під безліч платформ і використовується в безлічі пристроїв.Тому, використання syslog дозволяє забезпечити збір інформації з різних місць і зберігання її у єдиному сховищі.

Командний інтерфейс до syslog - logger

**Реалізації**

***UNIX-подібні ОС***

* [sysklogd](http://www.infodrom.org/projects/sysklogd/)
* [rsyslogd](http://sourceforge.net/projects/rsyslog/): Implements syslog over TCP and [RFC 3195](http://tools.ietf.org/html/rfc3195) support
* [syslog-ng](http://www.balabit.com/network-security/syslog-ng/)
* [metalog](http://metalog.sourceforge.net/)
* [msyslog](http://sourceforge.net/projects/msyslog/)
* [socklog](http://smarden.org/socklog/)

***Microsoft Windows NT5.x***

* [syslog-win32](http://sourceforge.net/projects/syslog-win32/) реалізація клієнта і сервера (BSD/GPL/public domain)
* [Kiwi Syslog Daemon](http://www.kiwisyslog.com/)
* [MonitorWare Products: MonitorWare Agent, WinSyslog](http://www.monitorware.com/en/Product/product_comparision.php)
* [NetDecision LogVision](http://www.netmechanica.com/products/?prod_id=1016)
* [NTsyslog](http://ntsyslog.sourceforge.net/)
* [EvtSys](https://engineering.purdue.edu/ECN/Resources/Documents/UNIX/evtsys/index_html) — syslog клієнт, що відправляє на syslog сервер інформацію із EventLog Windows.
* [Syslog Watcher](http://www.snmpsoft.com/syslogwatcher/)
* [SL4NT](http://www.netal.com/sl4nt.htm) — найпростіший syslog-сервер, пише прийняті повідомлення в системний журнал подій Windows.
* [Small Syslog Server](http://www.mt-team.ru/forum/index.php?topic=6.0) — Маленький і продуктивний Syslog сервер під ОС Windows XP/2003/7.

***Крос-платформна***

* [Weird Solutions Syslog](http://www.weird-solutions.com/)
* [SyslServe](http://www.syslserve.com/)

**RFC**

[RFC 3164](http://tools.ietf.org/html/rfc3164) - The BSD syslog Protocol

[RFC 3195](http://tools.ietf.org/html/rfc3195) - Reliable Delivery for syslog (гарантована доставка)

**Питання:**

1. Визначення політики інформаційної безпеки
2. Предмет політики
3. Принципи політики безпеки
4. Види політики безпеки
5. Організація секретного діловодства

Література:

1. Закон України "Про захист інформації в автоматизованих системах";
2. НД ТЗІ Загальні положення щодо захисту інформації в КС від несанкціонованого доступу
3. НД ТЗІ Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу
4. НД ТЗІ Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі
5. НД ТЗІ 1.1-003-99. Термінологія у галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.

**Визначення політики інформаційної безпеки (003)**

При прийнятті рішень адміністратори ІС зіштовхуються з проблемою вибору варіантів рішень по організації ЗИ на основі обліку принципів діяльності організації, співвідношення важливості цілей і наявності ресурсів. Ці рішення включають визначення того, як будуть захищатися технічні й інформаційні ресурси, а також як повинні поводитися службовці в тих чи інших ситуаціях.

***Політика інформаційної безпеки***— набір законів, правил і практичних рекомендацій і практичного досвіду, що визначають управлінські і проектні рішення в області ЗИ. На основі ПІБ будується керування, захист і розподіл критичної інформації в системі. Вона повинна охоплювати всі особливості процесу обробки інформації, визначаючи поводження ІС у різних ситуаціях.

Відповідно до запропонованого в книзі підходом політика (ЗАХОДИ) інформаційної безпеки (003) реалізується відповідною СТРУКТУРОЮ органів (002) на основі нормативно-методичної БАЗИ (001) з використанням програмно-технічних методів і ЗІСОБІВ (004), що визначають архітектуру системи захисту.

Для конкретної ІС політика безпеки повинна бути індивідуальної. Вона залежить від технології обробки інформації, використовуваних програмних і технічних засобів, структури організації т.д.

**Предмет політики (003) [12]**

Для того щоб описати ПІБ для конкретної ІС, адміністратори спочатку повинні визначити саму область обмежень і умов у зрозумілих усьому термінах. Корисно вказати чи мета причини розробки ПІБ – це допоможе домогтися дотримання політики.

Інформація, що циркулює в рамках ІС, є критично важливої. ІС дозволяє користувачам розділяти програми і дані, що збільшує ризик. Отже, кожний з комп'ютерів, що входять у мережу, має потребу в більш сильному захисті.

ПІБ переслідує двох головні цілі - продемонструвати співробітникам важливість захисту мережного середовища, описати їхня роль у забезпеченні безпеки, а також розподілити конкретні обов'язки по захисту інформації, що циркулює в мережі, так само як і самої мережі.

У відношенні політики безпеки в Internet організації може знадобитися уточнення, чи охоплює ця політика всі з'єднання, через які ведеться робота з Internet( чи прямо опосредованно) чи власне з'єднання Internet. Ця політика також може визначати, чи враховуються інші аспекти роботи в Internet, що не мають відносини до безпеки, такі як персональне використання з'єднань з Internet.

**Принципи політики безпеки (003) [11]**

Політика безпеки визначається як сукупність документованих управлінських рішень, спрямованих на захист інформації й асоційованих з нею ресурсів.

При розробці і проведенні її в життя доцільно керуватися наступними засадами:

1. неможливість минати захисні засоби;
2. посилення самої слабкої ланки;
3. неприпустимість переходу у відкритий стан;
4. мінімізація привілеїв;
5. поділ обов'язків;
6. багаторівневий захист;
7. розмаїтість захисних засобів;
8. простота і керованість інформаційної системи;
9. забезпечення загальної підтримки заходів безпеки.

Пояснимо зміст перерахованих принципів.

1. Стосовно до межмережевих екранів принцип неможливості минати захисні засоби означає, що всі інформаційні потоки в мережу, що захищається, і з її повинні проходити через екран. Не повинно бути "таємних" модемних чи входів тестових ліній, що йдуть в обхід екрана.
2. Надійність будь-якої оборони визначається самою слабкою ланкою. Часто самою слабкою ланкою виявляється не чи комп'ютер програма, а людина, і тоді проблема забезпечення інформаційної безпеки здобуває нетехнічний характер.
3. Принцип неприпустимості переходу у відкритий стан означає, що при будь-яких обставинах (у тому числі позаштатних), СЗІ або цілком виконує свої функції, або повинна цілком блокувати доступ.
4. Принцип мінімізації привілеїв наказує виділяти користувачам і адміністраторам тільки ті права доступу, що необхідні їм для виконання службових обов'язків.
5. Принцип поділу обов'язків припускає такий розподіл ролей і відповідальності, при якому одна людина не може порушити критично важливий для організації процес. Це особливо важливо, щоб запобігти зловмисні чи некваліфіковані дії системного адміністратора.
6. Принцип багаторівневого захисту наказує не покладатися на один захисний рубіж, яким би надійним він ні здавався. За засобами фізичного захисту повинні випливати програмно-технічні засоби, за ідентифікацією й аутентификацией - керування доступом і, як останній рубіж, - протоколювання й аудит. Ешелонована оборона здатна принаймні затримати зловмисника, а наявність такого рубежу, як протоколювання й аудит, істотно утрудняє непомітне виконання злочинних дій.
7. Принцип розмаїтості захисних засобів рекомендує організовувати різні за своїм характером оборонні рубежі, щоб від потенційного зловмисника було потрібно оволодіння різноманітними і, по можливості, несумісними між собою навичками подолання СЗІ.
8. Принцип простоти і керованості інформаційної системи в цілому і СЗІ особливо визначає можливість формального чи неформально доказу коректності реалізації механізмів захисту. Тільки в простій і керованій системі можна перевірити погодженість конфігурації різних компонентів і здійснити централізоване адміністрування.
9. Принцип загальної підтримки заходів безпеки - носить нетехнічний характер. Рекомендується із самого початку передбачити комплекс заходів, спрямований на забезпечення лояльності персоналу, на постійне навчання, теоретичне і, головне, практичне.

**Види політики безпеки (603)**

Основу політики безпеки складає спосіб керування доступом, що визначає порядок доступу суб'єктів системи до об'єктів системи. Назва цього способу, як правило, визначає назва політики безпеки.

Для вивчення властивостей способу керування доступом створюється його формальний опис — математична модель. При цьому модель повинна відбивати стану всієї системи, її переходи з одного стану в інше, а також враховувати, які стани і переходи можна вважати безпечними в змісті даного керування. Без цього говорити про яких-небудь властивості системи, і тим більше гарантувати їх, щонайменше некоректно.

В даний час найкраще вивчені два види політики безпеки: виборча і повноважна, засновані, відповідно на виборчому і повноважному способах керування доступом.

Крім того, існує набір вимог, що підсилює дію цих політик і призначений для керування інформаційними потоками в системі.

Слід зазначити, що засобу захисту, призначені для реалізації якого-небудь з названих способу керування доступом, тільки надають можливості надійного керування чи доступом інформаційними потоками. Визначення прав доступу суб'єктів до об'єктів і/чи інформаційним потокам (повноважень суб'єктів і атрибутів об'єктів, присвоєння міток критичності і т.д.) входить у компетенцію адміністрації системи.

**Виборча політика безпеки (603)**

Основою виборчої політики безпеки є виборче керування доступом, що має на увазі, що:

- усі суб'єкти й об'єкти системи повинні бути ідентифіковані;

- права доступу суб'єкта до об'єкта системи визначаються на підставі деякого правила (властивість вибірковості).

Для опису властивостей виборчого керування доступом застосовується модель системи на основі матриці доступу (МД), іноді неї називають матрицею контролю доступу. Така модель одержала назву матричної.

Матриця доступу являє собою прямокутну матрицю, у якій об'єкту системи відповідає рядок, а суб'єкту стовпець. На перетинанні стовпця і рядка матриці вказується тип дозволеного доступу суб'єкта до об'єкта. Звичайно виділяють такі типи доступу суб'єкта до об'єкта, як “доступ на читання”, “доступ на запис”, “доступ на виконання” і ін.

Безліч об'єктів і типів доступу до них суб'єкта може змінюватися відповідно до деяких правил, що існують у даній системі. Визначення і зміна цих правил також є задачею МД.

Рішення на доступ суб'єкта до об'єкта приймається відповідно до типу доступу, зазначеним у відповідній осередку матриці доступу. Звичайно виборче керування доступом реалізує принцип “що не дозволено, те заборонено”, що припускає явний дозвіл доступу суб'єкта до об'єкта. Матриця доступу — найбільш простий підхід до моделювання систем доступу.

Виборча політика безпеки найбільше широко застосовується в комерційному секторі, тому що її реалізація на практиці відповідає вимогам комерційних організацій по розмежуванню доступу і підзвітності, а також має прийнятну вартість і невеликі накладні витрати.

**Повноважна політика безпеки (603)**

Основу повноважної політики безпеки складає повноважне керування доступом, що має на увазі, що:

- усі суб'єкти й об'єкти системи повинні бути однозначно ідентифіковані;

- кожному об'єкту системи привласнена влучна критичності, що визначає цінність інформації, що міститься в ньому;

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

У тому випадку, коли сукупність міток має однакові значення, говорять, що вони належать до одного рівня безпеки. Організація міток має ієрархічну структуру і, таким чином, у системі можна реалізувати ієрархічно спадний потік інформації (наприклад, від рядових виконавців до керівництва). Ніж важливіше чи об'єкт суб'єкт, тим вище його мітка критичності. Тому найбільш захищеними виявляються об'єкти з найбільш високими значеннями мітки критичності.

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

Основне призначення повноважної політики безпеки — регулювання доступу суб'єктів системи до об'єктів з різним рівнем критичності і запобігання витоку інформації з верхніх рівнів посадової ієрархії на нижні, а також блокування можливого проникнення з нижніх рівнів на верхні. При цьому вона функціонує на тлі виборчої політики, додаючи її вимогам ієрархічно упорядкований характер (відповідно до рівнів безпеки).

Споконвічно повноважна політика безпеки була розроблена в інтересах МО США для обробки інформації з різними грифами таємності. Її застосування в комерційному секторі стримується наступними основними причинами:

- відсутністю в комерційних організаціях чіткої класифікації збереженої й оброблюваної інформації, аналогічної державної класифікації (грифи таємності зведень);

- високою вартістю реалізації і великих накладних витрат.

**Організаційно-технічні заходи (603)**

***Приведемо перелік основних організаційно-технічні заходи щодо ЗИ:***

- розробка і твердження функціональних обов'язків посадових осіб служби інформаційної безпеки;

- внесення необхідних змін і доповнень в усі організаційно-розпорядницькі документи (положення про підрозділи, обов'язок посадових осіб, інструкції користувачів системи і т.п.) з питань забезпечення безпеки програмно-інформаційних ресурсів ІС і діям у випадку виникнення кризових ситуацій;

- оформлення юридичних документів (договору, накази і розпоряджень керівництва організації) з питань регламентації відносин з користувачами (клієнтами), що працюють в автоматизованій системі, між учасниками інформаційного обміну і третьою стороною (арбітраж, третейський суд) про правила дозволу споровши, зв'язаних із застосуванням електронного підпису;

- створення науково-технічних і методологічних основ захисту ІС;

- виключення можливості таємного проникнення в приміщення, установки апаратури, що прослухує, і т.п.);

- перевірка і сертифікація використовуваних у ІС технічних і програмних засобів на предмет визначення заходів для їхнього захисту від витоку по каналах побічних електромагнітних випромінювань і наведень;

- визначення порядку призначення, зміни, твердження і надання конкретним посадовим особам необхідних повноважень по доступі до ресурсів системи;

- розробка правил керування доступом до ресурсів системи, визначення переліку задач, розв'язуваних структурними підрозділами організації з використанням ІС, а також використовуваних при їхньому рішенні режимів обробки і доступу до даних;

- визначення переліку файлів і баз даних, що містять зведення, що складають комерційну і службову таємницю, а також вимоги до рівнів їхньої захищеності від НСД при передачі, збереженні й обробці в ІС;

- виявлення найбільш ймовірних погроз для даної ІС, виявлення уразливих місць процесу обробки інформації і каналів доступу до неї;

- оцінка можливого збитку, викликаного порушенням безпеки інформації, розробка адекватних вимог по основних напрямках захисту;

- організація надійного пропускного режиму;

- визначення порядку обліку, видачі, використання і збереження знімних магнітних носіїв інформації, що містять еталонні і резервні копії програм і масивів інформації, архівні дані і т.п.;

- організація обліку, збереження, використання і знищення документів і носіїв із закритою інформацією;

- організація і контроль за дотриманням усіма посадовими особами вимог по забезпеченню безпеки обробки інформації;

- визначення переліку необхідних заходів для забезпечення безупинної роботи ІС у критичних ситуаціях, що виникають у результаті НСД, збоїв і відмовлень СВТ, помилок у програмах і діях персоналу, стихійних лих і т.п.

- контроль функціонування і керування використовуваними засобами захисту;

- явний і схований контроль за роботою персоналу системи;

- контроль за реалізацією обраних заходів захисту в процесі проектування, розробки, введення в лад і функціонування ІС;

- періодичний аналіз стану й оцінка ефективності заходів захисту інформації;

- розподіл реквізитів розмежування доступу (паролів, ключів шифрування і т.п.);

- аналіз системних журналів, уживання заходів по виявлених порушеннях правил роботи;

- складання правил розмежування доступу користувачів до інформації;

- періодичне з залученням сторонніх фахівців здійснення аналізу стану й оцінки ефективності заходів і застосовуваних засобів захисту. На основі отриманої в результаті такого аналізу інформації вживати необхідних заходів по удосконалюванню системи захисту;

- розгляд і твердження всіх змін в устаткуванні ІС, перевірка їх на задоволення вимогам захисту, документальне відображення змін і т.п.;

- перевірка прийнятих на роботу, навчання їхнім правилам роботи з інформацією, ознайомлення з заходів відповідальності за порушення правил захисту, навчання, створення умов, при яких персоналу було б невигідно порушувати свої обов'язки.

**Захист даних адміністративними методами (603)**

До таких заходів захисту можна віднести організаційно-технічні й організаційно-правові заходи, здійснювані в процесі створення й експлуатації системи обробки і передачі дані чи фірми банку з метою забезпечення захисту інформації.

Наскільки важливі організаційно-режимні заходи в загальному арсеналі засобів захисту, говорить уже хоча б той факт, що жодна ІС не може функціонувати без участі обслуговуючого персоналу. Крім того, організаційно-режимні заходи охоплюють усі структурні елементи системи захисту на всіх етапах їхнього життєвого циклу: будівництво приміщень, проектування системи, монтаж і налагодження устаткування, іспити і перевірка в експлуатації апаратури, оргтехніки, засобів обробки і передачі даних.

З одного боку, ці заходи повинні бути спрямовані на забезпечення правильності функціонування механізмів захисту і виконуватися адміністратором безпеки системи. З іншого боку, керівництво фірми повинне регламентувати правила обробки і захисту інформації, а також установити заходів відповідальності за порушення цих правил.

Нижче перерахований ряд дуже простих дій, що можуть значно підвищити ступінь захисту корпоративної мережі без великих фінансових уливань.

1. Більш ретельний контроль за персоналом, особливо за самими низько­оплачу­вани­ми працівниками, наприклад прибиральниками й охоронцями.

2. Акуратна непомітна перевірка послужного списку найманого працівника, що допоможе уникнути виникнення проблем у майбутньому.

3. Ознайомлення найманого співробітника з документами, що описують політику компанії в області інформаційної безпеки, і одержання від нього відповідної розписки.

4. Зміна умісту всіх екранів для входу в систему таким чином, щоб вони відбивали політику компанії в області захисту даних (ця заходів настійно рекомендується Міністерством юстиції США).

5. Підвищення рівня фізичного захисту.

6. Блокування всіх дисководів гнучких дисків в організаціях, у яких установлена мережа, – це дозволить мінімізувати ризик комп'ютерних крадіжок і зараження вірусами.

7. Визнання за співробітниками визначених прав при роботі з комп'ютерами, наприклад організація дощок оголошень, дотримання конфіденційності електронної пошти, дозвіл використовувати визначені комп'ютерні ігри.

Співробітники компанії повинні бути союзниками, а не супротивниками адміністратора системи в боротьбі за безпеку даних.

**Організація секретного діловодства (063)**

Під час роботи з захисту комерційної таємниці необхідно звернути особлива увага на документи фірми, оскільки більшість комерційних структур у нашій країні основні обсяги комерційної інформації, у тому числі конфіденційної, зберігають у документах.

Керівник фірми повинний упорядкувати відповідним чином процеси фіксації секретної інформації в ділових паперах і організувати їхній рух таким чином, щоб викрадення конфіденційних документів було б утруднене настільки, щоб воно ставало економічно невигідним для викрадача.

При роботі з документами, що містять охоронювану фірмою інформацію, слід дотримуватися наступних правил:

-строгий контроль ( чиособисто через службу безпеки) за допуском персоналу до секретних документів;

- установлення конкретних облич з керівництва і фірми, що служить, організуючих і

контролюючих секретне діловодство фірми; наділення їхній відповідними повноваженнями;

- розробка інструкції (пам'ятки) по роботі із секретними документами, ознайомлення з нею відповідних працівників фірми;

- контроль за прийняттям відповідними службовцями письмових зобов'язань про збереження комерційної таємниці фірми;

- уведення системи матеріального й іншого стимулювання фірми, що служить, що мають доступ до її секретів;

- впровадження в повсякденну практику механізмів і технологій захисту комерційної таємниці фірми;

- особистий контроль з боку керівника фірми служби внутрішньої безпеки і секретного діловодства.

Імовірність витоку секретної інформації з документів особливо велика в процесі їхнього пересилання. Очевидно, що в комерційних структур немає можливостей користатися послугами воєнізованої фельдсвязи. Тому доставку секретних документів і цінностей приходиться здійснювати власними силами з залученням охоронців чи фірми звертатися в спеціальні фірми.

Фірми, що служать, відповідальні за схоронність, використання і своєчасне знищення секретних документів, повинні бути захищені від спокуси торгівлі секретами фірми простим, але радикальним способом — гарною платою за роботу.

У процесі збереження і пересилання секретних документів фірми можуть бути застосовані засоби захисту і сигналізації про несанкціонований доступ до них. Одна з новинок — невидиме світлочутливе покриття, наносимо на документи, що виявляється під впливом світла, указуючи тим самим на факт несанкціонованого ознайомлення з чи документами їхнього фотографування.

Фахівцям з питань захисту комерційної інформації відомі й інші технології і системи охорони конфіденційних документів фірми від несанкціонованого до неї чи доступу можливого витоку охоронюваних зведень. За інформацією з даного питання варто звертатися в організації і служби, що спеціально займаються даною проблемою. Для ведення секретного діловодства повинні залучатися люди, що пройшли спеціальну перевірку, і в чесності яких немає сумнівів. Крім того, ці люди повинні бути відповідним чином підготовлені і навчені, тому що професійні недоліки і відступ від правил у їхній роботі можуть занадто дорого коштувати фірмі.

Приміщення, у яких ведеться робота із секретними документами, повинні добре охоронятися, а доступ туди повинний бути закритий для сторонніх облич. Ці приміщення повинні мати міцні перекриття і стіни, посилену металеві двері, міцні віконні рами з подвійними стеклами і ґратами, щільні штори. Сховище повинне бути обладнане охоронною і пожежною сигналізацією і ретельно охоронятися силами внутрішньої охорони. Доступ у сховище строго обмежений. Не рекомендується розташовувати таке приміщення на першому й останньому поверхах будинку. Секретні документи храняться в чи сейфах несгараемых металевих шафах з надійними замками і запорами.

Різні прийоми ведення секретного діловодства спрямовані на запобігання витоку комерційних секретів. Наприклад, документи, що містять комерційну таємницю, підрозділяються по ступені таємності відображеної в них інформації і забезпечуються відповідним грифом таємності.

Навіть ретельно охоронювані таємниці фірми можуть стати надбанням конкурентів зі звичайних публікацій, якщо пустити ця справа на самоплив. Тому один зі службовців фірми обов'язково повинний бути наділений самими широкими владними повноваженнями, щоб займатися попередньою цензурою брошур, що готуються, рекламних объвлений, прес-релізів і інших матеріалів для симпозіумів, виставок, конгресів, а також виступів, наукових і інших публікацій співробітників фірми.

Інтереси охорони секретів фірми найчастіше знаходяться у важко розв'язному протиріччі з особистими амбіціями, самолюбством, академічною незалежністю співробітників фірми, що бажають професійно само затверджуватися в ученому світі, серед своїх колег, у суспільній чи груповій думці.

Не менш легкий для дозволу конфлікт між прагненням зберегти комерційні таємниці фірми і бажанням використовувати в рекламних цілях деякі найбільш вражаючі дані зі строго охоронюваної інформації, особливо ті з них, що, безсумнівно, допомогли б розширити збут вироблених товарів і послуг.

Співробітник, що здійснює цензуру відкритих публікацій рекламного, наукового і популяризаторського характеру, що готуються персоналом чи фірми по її замовленнях, повинний керуватися простим, але ефективним правилом. Суть його в тім, щоб у максимально можливому ступені роздрібнити, роз'єднати за часом, у просторі і по авторах ту строго охоронювану комерційну інформацію, без якого неможливе опублікування згаданих робіт. Звичайно, усе це утрудняє здійснення персоналом фірми науково-дослідних і дослідно-конструкторських робіт, але зате істотно перешкоджає збору секретної інформації про фірму конкурентами і недоброзичливцями.

Цей бар'єр переборний лише за допомогою великих витрат.

**4) Методи та пристрої забезпечення захисту і безпеки**

***1. Поняття інформаційної безпеки.***

***2. Методи забезпечення інформаційної безпеки.***

***3. Інструментальні засоби аналізу захищеності інформаційних систем.***

**1. Поняття інформаційної безпеки.**

Підключення організації до глобальної мережі, такий як Internet, вимагає створення системи захисту інформаційних ресурсів, від тих, хто схоче їх використовувати, модифікувати або просто знищити. Не дивлячись на свою специфіку, система захисту організації при роботі в глобальних мережах повинна бути продовженням загального комплексу зусиль, направлених на забезпечення безпеки інформаційних ресурсів. Під інформаційною безпекою розуміється "стан захищеності інформації, оброблюваної засобами обчислювальної техніки або автоматизованої системи від внутрішніх або зовнішніх загроз". Захист інформації - це комплекс заходів, направлених на забезпечення інформаційної безпеки. На практиці під цим розуміється підтримка цілісності, доступності і, якщо необхідно, конфіденційності інформації і ресурсів, що використовуються для введення, зберігання, обробки і передачі даних. Комплексний характер, проблеми захисту говорить про те, що для її вирішення необхідне поєднання законодавчих, організаційних і програмно-технічних заходів.

Знання можливих загроз, а також вразливих місць інформаційної системи, необхідне для того, щоб вибирати найефективніші засоби забезпечення безпеки.

Найчастішими і самими небезпечними (з погляду розміру збитку) є ненавмисні помилки користувачів, операторів, системних адміністраторів і інших осіб, обслуговуючих інформаційні системи. Іноді такі помилки приводять до прямого збитку (неправильно введені дані, помилка в програмі, що викликала зупинку або руйнування системи). Іноді вони створюють слабкі місця, якими можуть скористатися зловмисники (такі звичайно помилки адміністрування).

Згідно даним Національного Інституту Стандартів і Технологій США (NIST), 65% випадків порушення безпеки ІС - слідство ненавмисних помилок.

На другому місці за розмірами збитку розташовуються крадіжки і фальсифікації. В більшості розслідуваних випадків винуватцями виявлялися штатні співробітники організацій, відмінно знайомі з режимом роботи і захисними заходами.

Ключовим етапом для побудови надійної інформаційної системи є вироблення політики безпеки.

Під політикою безпеки розуміють сукупність документованих управлінських рішень, направлених на захист інформації і пов'язаних з нею ресурсів.

З практичної точки зору політику безпеки доцільно розділити на три рівні:

* Рішення, що зачіпають організацію в цілому. Вони носять вельми загальний характер і, як правило, виходять від керівництва організації.
* Питання, що стосуються окремих аспектів інформаційної безпеки, але важливі для різних систем, експлуатованих організацією.
* Конкретні сервіси інформаційної системи.

Третій рівень включає два аспекти - мета (політики безпеки) і правило їх досягнення.

**2. Методи забезпечення інформаційної безпеки.**

***Міжмережеве екранування***

Реалізації політики безпеки – вживання різних програмних і апаратно-технічних засобів в процесі побудови системи безпеки.

Використовування міжмережевого екрану.

Міжмережевий екран (firewall) - це засіб розмежування доступу клієнтів з однієї безлічі мережі до серверів з іншої безлічі мережі. Екран виконує свої функції, контролюючи всі інформаційні потоки між двома безліччю систем.

Вимоги до реальної системи, що здійснює міжмережеве екранування. В більшості випадків екрануюча система повинна:

* Забезпечувати безпеку внутрішньої (що захищається) мережі і повний контроль над зовнішніми підключеннями і сеансами зв'язку;
* Володіти могутніми і гнучкими засобами управління для повного і, наскільки можливо, простого втілення в життя політики безпеки організації;
* Працювати непомітно для користувачів локальної мережі і не утрудняти виконання ними легальних дій;
* Працювати достатньо ефективно і встигати обробляти весь вхідний і витікаючий трафік;
* Володіти властивостями самозахисту від будь-яких несанкціонованих дій, оскільки міжмережевий екран є ключем до конфіденційної інформації в організації;
* Якщо у організації є декілька зовнішніх підключень, у тому числі і у видалених філіалах, система управління екранами повинна мати нагоду централізований забезпечувати для них проведення єдиної політики безпеки;
* Мати засобу авторизації доступу користувачів через зовнішні підключення.

Екранування дозволяє підтримувати доступність сервісів усередині інформаційної системи, зменшуючи або взагалі ліквідовуючи навантаження, ініційоване зовнішньою активністю.

Екранування дає можливість контролювати інформаційні потоки, направлені в зовнішню область, забезпечуючи режим конфіденційності.

***Шифрування інформації***

TCP/IP володіє високою сумісністю як з різними по фізичній природі і швидкісним характеристикам каналами, так і з широким довкола апаратних платформ, сукупність цих характеристик робить протокол TCP/IP унікальним засобом для інтеграції великих розподілених гетерогенних інформаційних систем.

Технології інформаційної безпеки протоколу TCP/IP дозволяють з регульованим ступенем надійності захищати трафік всіх без виключення користувачів і прикладних систем при повній прозорості (невидимості для додатків) засобів захисту.

Такі засоби захисту включають:

Чим є ці засоби захисту?

Протокол, що управляє шифруванням трафіку SKIP (Simple Key management for Internet Protocol) і створений на його основі ряд продуктів захисту інформації (ряд програмних реалізацій протоколу SKIP для базових апаратно-програмних платформ, пристрій колективного захисту локальної мережі SKIPBridge, пристрій забезпечення регульованої політики безпеки SunScreen).

SKIP (Simple Key mamagement for Internet Protocol - Простий протокол управління криптоключами в інтермережі) розроблений компанією Sun Microsystems в 1994 році і запропонований як стандарт Internet.

У основі SKIP лежить криптографія відкритих ключів Діффі-Хеллмана.

SKIP має, в порівнянні з існуючими системами шифрування трафіку ряд унікальних особливостей:

* SKIP універсальний: він шифрує IP-пакеты, не знаючи нічого про додатки, користувачів або процеси, їх формуючих; він обробляє весь трафік, не накладаючи ніяких обмежень ні на вищерозміщене програмне забезпечення, ні на фізичні канали, на яких він використовується;
* SKIP сеансонезалежний: для організації захищеної взаємодії не вимагається додаткового інформаційного обміну;
* SKIP незалежний від системи шифрування - користувач може вибирати будь-який з пропонованих постачальником або використовувати свій алгоритм шифрування інформації.

Пристрій SKIPBridge забезпечує захист (шифрування) трафіку, спрямовуваного з внутрішньої мережі в зовнішню на основі протоколу SKIP, а також фільтрацію і дешифрування трафіку, що поступає із зовнішньої мережі у внутрішню.

IP-пакеты, що приймаються із зовнішньої мережі, обробляються протоколом SKIP. Пакети, що пройшли фільтрацію SKIP, за допомогою протоколу IP передаються програмному забезпеченню SKIPBridge, вирішальному задачі адміністративної безпеки (забезпечуючому пакетну фільтрацію), і потім - операційній системі.

SunScreen - це спеціалізована система захисту, розроблена компанією Sun Microsystems, вирішальна задачі фільтрації пакетів, аутентифікації і забезпечення конфіденційності трафіку. Пристрій SunScreen виконаний на основі апаратного модуля SPF-100. SPF-100 містить SPARC-процессор, що працює під управлінням ОС Solaris. SunScreen не має IP-адреса, тому він "невидимий" із зовнішньої мережі і несхильний до атаки.

Пристрій SunScreen, містить п'ять Ethernet-адаптеров, до яких можуть під'єднуватися чотири незалежні сегменти локальної мережі і комунікаційний провайдер. Для кожного сегменту забезпечується настройка індивідуальної політики безпеки шляхом завдання складного набору правил фільтрації пакетів.

**3. Інструментальні засоби аналізу захищеності інформаційних систем.**

Для перевірки захищеності інформаційних систем існують програмні продукти класу "сканер безпеки системи". Ці продукти на сьогоднішній день існують для більшості операційних систем. Найвідоміші: ASET (компонент ОС Solaris), KSA (для платформ NetWare і NT), SSS (System Security Scanner) (Unix-платформы).

***System Security Scanner***

Програма System Security Scanner призначена для проведення перевірки стану безпеки на окремих UNIX-компьютерах і пошуку уразливості ОС як зовні (по мережі з використанням Internet Scanner), так і зсередини (з самої ОС комп'ютера). При цьому проводиться перевірка прав доступу і прав власності файлів, конфігурацій мережних сервісів, установок ресурсів користувачів, програм аутентифікації і інших, пов'язаних з користувачами слабких місць (наприклад, паролів).

Пакет програм ***Internet Scanner SAFEsuite*** призначений для проведення комплексної оцінки ефективності політики безпеки на рівні мережних сервісів. Він надає можливості для ідентифікації і корекції більше 140 відомих слабких місць і постійного нагляду за станом безпеки для широкого діапазону мережних пристроїв - від web-узлов і міжмережевих екранів і до серверів і робочих станцій UNIX, Windows 95, Windows NT і всіх інших пристроїв працюючих з TCP/IP.

Складається з трьох програм: Web Security Scanner, Firewall Scanner, Intranet Scanner.

***Web Secure Scanner***

Призначений для пошуку слабких місць безпеки на web-серверах. Забезпечує аудит ОС, під управлінням якої працює web-сервер, програм-додатків, встановлених на web-сервере, і CSI scripts в web-приложениях. Проводить тестування конфігурації web-сервера, оцінює рівень безпеки основної файлової системи.

***Firewall Scanner***

Забезпечує пошук слабких місць в міжмережевих екранах, перш за все в їх конфігурації, і надає рекомендації по їх корекції. Проводить тестування реакції міжмережевих екранів на різні типи спроб порушення безпеки. Виконує сканування сервісів - ідентифікацію всіх мережних сервісів, доступ до яких здійснюється через міжмережевий екран.

***Intranet Scanner***

Призначений для автоматичного виявлення потенційних слабких місць усередині мереж з використанням різних тестів для перевірки реакції на несанкціоновані проникнення. Забезпечує перевірку різних мережних пристроїв, включаючи UNIX hosts, системи, що працюють під Microsoft NT/Windows 95, маршрутизатори, web-серверы і X-терминалы.

Сімейство продуктів SAFEsuite, розроблених американською компанією Internet Security Systems (ISS) - комплект засобів призначених для оцінки захищеності інформаційних систем.

Складається з системи аналізу захищеності на рівні мережі Internet Scanner, засобу аналізу захищеності на рівні хосту System Scanner і виявлення атак на рівні мережі RealSecure Network Engine, Database Scanner.

***Internet Scanner***

Система аналізу захищеності — Internet Scanner — призначена для проведення регулярних всесторонніх або вибіркових тестів мережних служб, операційних систем, прикладного, що використовується, ПО, маршрутизаторів, міжмережевих екранів, Web-серверов і т.п. Результатом тестування є звіти, що містять докладний опис кожної знайденої уразливості, її дислокації в корпоративній мережі, а також рекомендації по корекції або усуненню «слабкого місця».

Система аналізу захищеності — ***Database Scanner -*** призначена для виявлення проблем, пов'язаних з безпекою баз даних. В цьому ПО реалізовані перевірки підсистем аутентифікації, авторизації і контролю цілісності. Вбудована база знань, містить перелік коректуючих дій, що рекомендуються, для усунення знайдених уязвімостей.

Database Scanner підтримує СУБД Microsoft SQL Server, Sybase Adaptive Server, Oracle, Informix.

**5) Захист, доступ та аутентифікація**

**Основні завдання забезпечення безпеки**

Забезпечення безпеки комп'ютерних систем вимагає виконання комплексу завдань, найважливішими серед яких є виконання процедур аутентифікації, авторизації та аудиту, дотримання конфіденційності, доступності та цілісності даних.  
  
**Аутентифікація**  
  
*Аутентифікація*(authentication)— це процес, за допомогою якого одна сторона (система) засвідчує, що інша сторона (користувач) є тим, за кого себе видає. Під час аутентифікації потрібне свідчення (credentials), що найчастіше складається з інформації, відомої обом сторонам (наприклад, ним може бути пароль). Користувач, що пред'явив коректне свідчення, дістає позитивну відповідь на вимогу аутентифікації.

**Авторизація**  
  
Після того як аутентифікація відбулась успішно, користувач починає працювати із системою. Тепер йому може знадобитися доступ до різних ре­сур­сів.

*Авто­ри­за­ція*(authorization), або *керування доступом*(access control) — це процес, за допомогою якого перевіряють, чи має право користувач після успішної аутентифікації отримати доступ до запитаних ним ресурсів. Авторизацію здій­ню­ють порівнянням інформації про користувача з інформацією про права доступу, пов'я­заною із ресурсом. Зазвичай вона містить тип дії та відомості про кори­сту­ва­чів, яким дозволено цю дію виконувати. Якщо користувач має право на запитану дію­ із цим ресурсом, йому надають можливість її виконати.

**Аудит**  
  
 Під *аудитом*(auditing) розуміють збирання інформації про різні події у системі, важливі для її безпеки, і збереження цієї інформації у формі, придатній для подальшого аналізу. Подіями можуть бути успішні та безуспішні спроби аутентифікації у системі, спроби отримати доступ до об'єктів тощо. Інформацію звичайно зберігають у спеціальному системному журналі (system log). У деяких системах цей журнал має вигляд текстового файла, інші підтримують його спеціальний формат.

**Конфіденційність, цілісність і доступність даних**

Основним компонентом політики безпеки комп'ютерних систем є дотримання найважливіших характеристик даних.

*Конфіденційність*(data confidentiality) — можливість приховання даних від стороннього доступу. її зазвичай забезпечують криптографічним захистом даних за допомогою їхнього шифрування.

*Цілісність*(data integrity) — спроможність захистити дані від вилучення або зміни (випадкової чи навмисної). Технології підтримки цілісності даних також пов'язані із криптографічними методами, вони включають цифрові підписи і коди аутентифікації повідомлень.

*Доступність*(data availability) — гарантія того, що легітимний користувач після аутентифікації зможе отримати доступ до запитаного ресурсу, якщо він має на це право. Порушення доступності даних називають *відмовою від обслуговування*(denial of service), однієї із цілей політики безпеки є запобігання випадковому або навмисному доведенню системи до такої відмови.

Про ці завдання докладніше йтиметься далі.

**Принципи аутентифікації і керування доступом**

Цей розділ присвячено особливостям реалізації аутентифікації і контролю доступу в сучасних операційних системах.

**1. Основи аутентифікації**

Аутентифікація надає можливість розрізняти легітимні та нелегітимні спроби доступу до системи. Надійна аутентифікація дає змогу у багатьох випадках обмежити коло потенційних порушників легітимними користувачами системи, спрощуючи цим процедури забезпечення її безпеки.

Свідчення, які вимагаються від користувачів під час аутентифікації, найчастіше зводяться до знання секретної інформації, спільної для користувача і системи (наприклад, пароля). Саме про таку аутентифікацію і йтиметься в цьому розділі.

Розрізняють локальну і мережну аутентифікацію. У разі успішної локальної аутентифікації користувач доводить свою легітимність для використання ресурсів однієї комп'ютерної системи (свідчення користувача перевіряють локально), мережна аутентифікація дає змогу користувачу довести легітимність для використання всіх ресурсів мережі (свідчення користувача передають для перевірки на спеціальний сервер із будь-якого комп'ютера мережі).  
  
**Облікові записи**

Для того щоб аутентифікація користувача була можлива, у системі має зберігатись інформація про цього користувача. Таку інформацію називають *обліковим записом*(account). Із ним звичайно пов'язують такі дані:

- ім'я користувача, яке він вказує для входу у систему;

- ідентифікатор користувача, що зазвичай є чисельним значенням, унікальним у межах комп'ютера або групи комп'ютерів (цей ідентифікатор ОС використовує під

час аутентифікації і авторизації);

- інформація про пароль користувача;

- інформація про обмеження на вхід користувача у систему (термін легітимності облікового запису, періодичність зміни пароля, години і дні тижня, у які

користувач може отримувати доступ у систему тощо);

**-** інформація про групи, до яких належить цей користувач;

- місце знаходження домашнього каталогу користувача (у якому він може створювати свої файли);

**-**налаштування сесії користувача (шлях до його командного інтерпретатора тощо).  
 Інформацію про облікові записи зберігають у *базі даних облікових записів*(account database). Адміністратор системи може змінювати будь-яку інформацію в цій базі, для інших користувачів звичайно доступна лише зміна їхнього власного пароля.

**Групи користувачів**

У сучасних ОС для зручності адміністрування системи користувачі можуть об'єднуватись у групи. Користувач може одночасно належати до кількох груп. Під час авторизації доступу до об'єктів перевіряють не тільки права самого користувача, але й права груп, до яких він належить.

Інформацію про групи також зберігають у базі даних облікових записів. Звичайно ОС визначає кілька стандартних груп, які створюють під час її установки, зокрема, групу адміністраторів системи (які можуть виконувати в ній будь-які дії) і групу звичайних користувачів із обмеженим доступом.

**Аутентифікація з використанням односторонніх функцій**

Для перевірки пароля немає потреби знати цей пароль, досить уміти відрізняти правильний пароль від неправильного. Тому замість зберігання паролів доцільно зберігати односторонні функції цих паролів. Подивимося, як виглядатиме в дано­му випадку протокол аутентифікації.

1. Аліса посилає системі свої ім'я і пароль.
2. Система обчислює односторонню функцію від пароля.
3. Система порівнює результат обчислення односторонньої функції зі значен­ням, що зберігається у базі даних облікових записів.

У результаті зменшуються втрати, які може задати зловмисник, коли отримає доступ до списку паролів, оскільки навіть у цьому разі за односторонньою функ­цією відновити паролі неможливо. Проте цей підхід не позбавлений недоліків.

**Словникові атаки і сіль**

Якщо зловмисник володіє списком паролів, зашифрованих односторонньою функ­цією, можлива словникова атака. Зловмисник бере набір найпоширеніших паро­лів, застосовує до них односторонню функцію і зберігає всі зашифровані паролі. Потім він порівнює список зашифрованих паролів із цим файлом (словником) у пошуках збігів.

Один зі способів боротьби із такою атакою пов'язаний із використанням *солі*(salt). Сіль — це випадковий рядок *S,*який додають до пароля перед шифруван­ням. У список шифрованих паролів заноситься рядок *S + E(S + Р),*де *Р*— пароль, *Е*— функція шифрування, «+» — конкатенація рядків. Якщо кількість можливих значень солі достатньо велика, то це робить словникову атаку значно складні­шою, оскільки у словник потрібно вносити результати шифрування паролів із усіма можливими значеннями солі.

Солі потрібно досить багато. Наприклад, стандартний її обсяг, прийнятий в UNIX (12 біт, що дає 4096 можливих значень), є не зовсім достатнім (є словни­ки найуживаніших паролів, об'єднані з усіма значеннями солі).

**Аутентифікація за принципом «виклик-відповідь»**

Більш серйозна проблема, пов'язана із використанням описаного підходу, поля­гає в тому, що пароль передають мережею незашифрованим, і він може бути пере­хоплений зловмисником. Один зі способів вирішення цієї проблеми полягає в то­му, щоб передавати мережею не паролі, а їх односторонні хеші (дайджести). Цей підхід називають аутентифікацією за принципом «виклик-відповідь» (challenge-response authentication) або дайджест-аутентифікацією

Цей протокол був основним підходом до аутентифікації у системах лінії Win­dows ХР до появи Windows 2000 і дотепер підтримується у цих системах

Більш складним протоколом аутентифікації є *протокол Kerberos.*Це роз­поділена система аутентифікації користувачів із можливістю аутентифікації клієнта і сервера. Протокол Kerberos є основним протоколом мережної аутенти­фікації у системах лінії Windows ХР, починаючи із Windows 2000. Реалізація цього протоколу доступна і для UNIX-систем.

**Одноразові паролі**

Проблему пересилання пароля мережею можна також розв'язати, вико­рис­то­вую­­чи паролі, дійсні лише один раз під час сесії користувача. Перехоплення тако­го *одноразового пароля*(one-time password) нічого не дає зловмисникові.  
Та­кі паролі у сучасних системах можуть реалізовуватися за допомогою смарт-карт — електронних пристроїв, у які вбудований мікропроцесор із засобами гене­рації від­повідних одноразових паролів.

**2. Основи керування доступом**

Для реалізації керування доступом операційна система має можливість визнача­ти, що за дії і над якими об'єктами має право виконувати той чи інший користу­вач системи. Звичайний розподіл прав відображають у вигляді *матриці доступу,*у якій рядки відповідають суб'єктам авторизації (користувачам, групам користу­вачів тощо), стовпці — ресурсам (файлам, пристроям тощо), а на перетині рядка і стовпця зазначені права цього суб'єкта на виконання операцій над даним ресур­сом.  
 Зберігання повної матриці контролю доступу неефективне (вона займатиме багато місця), тому звичайно використовують два базові підходи для її компакт­ного відображення.

У разі реалізації ***списків****контролю доступу*(Access Control Lists, ACL) збері­гаються стовпці матриці. Для кожного ресурсу задано список суб'єктів, які мо­жуть використовувати цей ресурс.

У разі реалізації *можливостей*(capabilities) зберігаються рядки матриці. Для кожного суб'єкта задано список ресурсів, які йому дозволено використовувати.

**Списки контролю доступу**

Якщо реалізовано ACL, для кожного об'єкта задають список, що визначає, які ко­ристувачі можуть виконувати ті чи інші операції із цим об'єктом. Наприклад, для файлових систем такими об'єктами є файли або каталоги. У найзагальнішій формі елементи цього списку — це пари (користувач, набір цій), які називають*елементами контролю доступу*(access control elements, ACE).

Розглянемо деякі проблеми, які потрібно вирішити у разі реалізації списків контролю доступу.

* Розмір списку контролю доступу має бути не надто великим, щоб система могла ефективно ним керувати.
* Права мають бути досить гнучкими, але при цьому не дуже складними. Над­мірне ускладнення системи прав звичайно призводить до того, що користува­чі починають її «обходити», задаючи спрощені права; у результаті загальна безпека не підвищується, а ще більше знижується.

Вирішення цих проблем призвело до особливостей реалізації списків контро­лю доступу в різних ОС. Так, загальною концепцією у створенні списків є задання прав не лише для окремих користувачів, але й для груп користувачів, а також можливість визначити права доступу всіх користувачів системи. У деяких ОС обмежують кількість елементів у списку (наприклад, в UNIX список, як незабаром по­бачимо, обмежений трьома елементами). Водночас у системах лінії Windows ХР можна задавати списки контролю доступу, що складаються з необмеженої кілько­сті елементів (для окремих користувачів, груп, користувачів інших комп'ютерів тощо), і задавати різні комбінації прав — від узагальнених до детальних.  
  
**Можливості**  
  
 Під час визначення можливостей для кожного користувача задають, до яких фай­лів він може мати доступ і як саме. При цьому із користувачем пов'язують*список можливостей*(capability list), що складається із пар (об'єкт, набір дій).

Реалізація списків можливостей дає змогу забезпечити не тільки захист, але й задання імен. Можна зробити так, щоб кожний користувач бачив тільки ті фай­ли, до яких у нього є доступ. Якщо при цьому значенням за замовчуванням є від­сутність доступу, користувачі можуть починати роботу в «порожній» системі. За­галом можливості використовують у системах, де потрібно забезпечити більшу безпеку за рахунок деякого зниження зручності роботи.

Можливості можуть бути задані не тільки для користувачів, але й для окре­мих процесів. У результаті під час запуску кожного процесу можна визначити його права.

**Аутентифікація та керування доступом в UNIX**

У цьому розділі опишемо, як реалізувати аутентифікацію і керувати доступом в UNIX-системах на прикладі Linux.

**1. Облікові записи користувачів**

Перш ніж розглянути реалізацію аутентифікації в UNIX, зупинимося на концеп­ції користувача цієї системи.

**Користувачі та групи користувачів**

Кожному користувачу в UNIX ставлять у відповідність обліковий запис (account), що характеризується іменем користувача та ідентифікатором (uid). Як ім'я кори­стувача, так і його ідентифікатор мають бути унікальними в межах усієї системи. Крім цього, з обліковим записом користувача пов'язують його *домашній каталог*(home directory), у який він за замовчуванням може записувати дані. Після входу користувача у систему відбувається перехід у його домашній каталог.  
Користувачі об'єднуються в групи. Кожна група характеризується іменем та ідентифікатором (gid).

Загалом процес виконують із правами того користувача, який запустив відпо­відний виконуваний файл.

**Суперкористувач root**

Користувач із uid, що дорівнює нулю (звичайно його називають root) має в UNIX особливий статус — він може виконувати у системі будь-які дії без обмежень. Та­кого користувача називають також *суперкористувачем.*

Наявність єдиного суперкористувача (принцип «все або нічого») вважають головною слабкістю системи безпеки UNIX, оскільки компрометація єдиного па­роля root негайно призводить до того, що зловмисник отримує повний контроль над системою. Крім цього, процеси під час виконання не можуть бути обмежені якоюсь частиною прав суперкористувача. Фактично, процес, якому потрібна ли­ше невелика частина таких прав, змушений виконуватися під керуванням root із повним контролем над системою.

**2. Аутентифікація**

Для стандартної аутентифікації UNIX використовують підхід із використанням односторонньої функції від пароля і солі. Такою функ­цією традиційно був алгоритм DES, яким шифрувався рядок, що складався із ну­лів, при цьому в ролі ключа використовували значення пароля, об'єднане із сіл­лю. У сучасних версіях UNIX замість DES часто використовують односторонню хеш-функцію (звичайно MD5).

За вхід користувача у систему відповідають дві утиліти: getty — ініціалізує термінал, видає підказку «login:» і приймає ім'я користувача, і login, що видає підказку «password:», приймає значення пароля, робить аутентифікацію і починає сесію користувача (переходить у домашній каталог і запускає командний інтерпретатор).  
  
**Тіньові паролі**

У традиційних UNIX-системах до файла /etc/passwd мав доступ будь-який кори­стувач ОС. А тому зловмисникові достатньо було отримати непривілейований доступ до системи, щоб почати словникову атаку на цей файл.  
  
 Для вирішення даної проблеми потрібно заборонити доступ до цього файла для всіх користувачів, крім root. Проте таке рішення не є прийнятним, оскільки в цьому файлі, крім інформації про паролі, містяться імена та ідентифікатори ко­ристувачів, розташування їхніх домашніх каталогів та інші дані, необхідні біль­шості застосувань. У результаті всі програми, яким потрібна така інформація, до­велося б запускати із правами суперкористувача.

У сучасних UNIX-системах (зокрема в Linux) застосовують інший підхід — технологію *тіньових паролів*(shadow passwords). При цьому інформацію про па­ролі переносять із /etc/passwd в окремий тіньовий файл паролів (який зазвичай називають /etc/shadow). До нього може звертатися тільки суперкористувач. Іншу шформащю (імена та ідентифікатори користувачів тощо) зберігають у /etc/passwd, що залишається доступним для всіх користувачів. Тіньові паролі дають змогу значно підвищити надійність схеми аутентифікації системи.

**3. Керування доступом**

Реалізація керування доступом до файлів у UNIX збереглася, майже не змінив­шись від ранніх версій системи. Фактично вона є скороченою реалізацією списків контролю доступу.

**Основні принципи реалізації**

Наведемо принципи реалізації керування доступом в UNIX.

* Усі файли і каталоги в UNIX мають власника (owner), що належить до певної групи (group), і права доступу (permissions).
* Розрізняють три категорії прав доступу: для читання, записування і виконання. Для звичайних файлів назви прав відповідають їхньому змісту (зазначимо, що ядро UNIX намагатиметься завантажити у пам'ять і виконати будь-який файл, на який у поточного користувача є права на виконання).
* Для каталогів задають той самий набір прав, але вони відрізняються за змістом від прав для файлів:
* право читання для каталогу означає можливість отримання списку імен файлів, що містяться в ньому (тобто читання вмісту каталогу як файла);
* право записування в каталог означає можливість створення в каталозі но­вих файлів і вилучення наявних (тобто записування в каталог як у файл); зазначимо, що для вилучення файла прав на нього самого можна й не ма­ти — достатньо прав на каталог, де він зберігається;
* право виконання означає можливість пошуку в каталозі, тобто доступу до окремих файлів.

Із цього випливає, що якщо для каталогу задаються права «тільки для вико­нання», то доступ до окремих файлів у ньому можна отримати, коли знати їхні імена, список же всіх файлів отримати буде неможливо. Таке задання прав ви­користовують, аби сторонні особи не могли випадково виявити файли, які, од­нак, потребують спільного доступу. З іншого боку, якщо задати права «тільки для читання», можна переглядати список файлів каталогу, але доступ до окремих файлів стане неможливий.

4. Права кожної категорії задають окремо для власника файла, для користувачів його групи і для всіх інших користувачів усього дев'ять базових комбінацій прав; можна сказати, що із кожним файлом пов'язаний список контролю доступу із трьох елементів.

**Недоліки схеми керування доступом UNIX**

Описана схема керування доступом проста для розуміння, але багато в чому об­межена. Основне обмеження пов'язане із довжиною списку контролю доступу (З елементи). Звідси виникають такі проблеми, як неможливість надання конкретному користувачу прав доступу до файла без створення для нього окремої групи (що не можливо зробити без наявності прав адміністратора).  
Останнім часом в UNIX-системах усе ширше використовують списки контро­лю доступу без обмеження кількості елементів (у Linux їхня реалізація стала доступна у ядрі 2.6).

**Аутентифікація і керування доступом у Windows ХР**

**1. Загальна архітектура безпеки**

Архітектури безпеки Windows ХР містять такі основні компоненти.  
*Процес реєстрації користувачів*(logon process, winlogon) обробляє запити ко­ристувачів на реєстрацію у системі та приймає дані від них.  
 *Менеджер аутентифікації*(Local Security Authority Subsystem, LSASS) безпо­середньо проводить аутентифікацію користувача. Цей компонент — централь­ний у підсистемі безпеки. Крім аутентифікації, він контролює політику ауди­ту.

*Менеджер облікових записів*(Security Accounts Manager, SAM) підтримує базу даних облікових записів (базу даних SAM), що містить імена локальних кори­стувачів і груп, а також паролі. Під час перевірки прав користувача SAM взає­модіє із менеджером аутентифікації.

*Довідковий монітор захисту*(Security Reference Monitor, SRM) перевіряє пра­ва користувача на доступ до об'єкта і виконує необхідну дію з об'єктом за на­явності цих прав. Це єдиний компонент, що виконується в режимі ядра, він реалізує політику контролю доступу, визначену менеджером аутентифікації. SRM гарантує, що будь-який користувач або процес, що дістав доступ до об'єкта, має всі права на нього.

Ця архітектура реалізована у системах, що не використовують мережної аутентифікації. Для неї інформація про облікові записи має зберігатися не у базі даних SAM, а у спеціальному централізованому сховищі даних — *активному ка­талозі*(Active Directory). Під час мережної аутентифікації менеджер аутентифі­кації звертається до служби активного каталогу віддаленого комп'ютера, на якому розташований цей каталог. База даних SAM, однак, є у будь-якій установці ОС лінії Windows ХР — у ній зберігають облікові записи для локальної аутентифікації. Подальший виклад торкатиметься локальної аутентифікації.

**2. Аутентифікація**

Windows ХР вимагає, щоб кожному користувачу відповідав обліковий запис. Він пов'язаний із *профілем захисту,*який є набором інформації щодо контролю досту­пу (ім'я користувача, список його груп, пароль тощо). Профілі захисту зберігають у базі даних SAM і використовують для аутентифікації.  
  
 Розглянемо послідовність кроків реєстрації користувача у системі. Процес winlogon очікує введення від користувача. Потік цього процесу виявляє спробу користувача ввійти у систему (натискання комбінації клавіш Ctrl+Alt+Del) і про­понує йому ввести ім'я облікового запису та пароль. При цьому для реалізації такого введення winlogon звертається до спеціальної DLL графічної ідентифіка­ції та аутентифікації (GINA). Стандартне вікно введення даних користувача реа­лізоване у msgina.dll, програміст може встановити свою версію цієї динамічної біб­ліотеки, що реалізує альтернативний метод аутентифікації (наприклад, на основі смарт-карт або біометричних даних).

Дані від користувача передаються процесу winlogon, і аутентифікація із вико­ристанням бази даних SAM (за яку відповідає LSASS) відбувається відповідно до протоколу «виклик-відповідь». Можна використати і протокол Керберос (цей підхід тут не розглядатиметься).

Якщо аутентифікація пройшла успішно, створюють об'єкт, що унікальним чи­ном визначає цього користувача в усіх його подальших діях. Цей об'єкт, який на­зивають *маркером доступу*(access token), відіграє ключову роль у підсистемі за­хисту: він визначає, до яких системних ресурсів мають доступ потоки, створені цим користувачем.

Після успішної аутентифікації користувача LSASS створює процес і приєднує до нього маркер доступу користувача. Цей процес передають підсистемі Win32, що запускає в його адресному просторі застосування, визначене у реєстрі як оболонка системи (за замовчуванням ним є стандартна оболонка explorer.exe). Застосуван­ня формує візуальне відображення параметрів робочого столу для користувача.

**Ідентифікатори безпеки**

Із кожним користувачем і групою у Windows ХР пов'язують унікальний *іденти­фікатор безпеки*(Security Identifier, SID). Це цілочислове значення, що склада­ється із заголовка і випадкової частини. Система безпеки звертається до користу­вачів і груп тільки за їхнім SID.

**3. Керування доступом**

Під час створення будь-якого об'єкта Windows ХР, який може бути використаний більш як одним процесом (включаючи файли, поіменовані канали, синхроніза­ційні об'єкти тощо), йому присвоюють *дескриптор захисту*(security descriptor).

До найважливіших елементів дескриптора захисту належать:

- SID власника об'єкта (власник завжди може змінювати атрибути безпеки об'єкта, навіть якщо в нього немає прав на доступ до його даних);   
 - список контролю доступу (ACL), що визначає права доступу до об'єкта.  
Кожний елемент списку контролю доступу (АСЕ) містить такі елементи:   
-тип АСЕ (виділяють, зокрема, дозволяючі і забороняючі АСЕ);   
- ідентифікатор безпеки (SID);

-набір прав доступу (читання, записування, повний контроль тощо).  
Сума прав доступу, наданих окремими АСЕ, формує загальний набір прав доступу, наданих ACL.

**6) Моделі захисту. Захист пам'яті**

*1. Фактори загроз збереження інформації в інформаційних системах.*

Умисні чинники збереження інформації в СОД зарубіжні [спеціалісти](http://ua-referat.com/%D0%A1%D0%BF%D0%B5%D1%86%D1%96%D0%B0%D0%BB%D1%96%D1%81%D1%82) поділяють на погрози з боку користувачів ЕОМ та осіб, які не є користувачами. Несанкціонований доступ до інформації може включити неавторизоване користування інформацією системи та активну інфільтрацію. Неавторизоване користування інформацією ототожнюється з [ситуацією](http://ua-referat.com/%D0%A1%D0%B8%D1%82%D1%83%D0%B0%D1%86%D1%96%D1%8F), коли неавторизований користувач отримує можливість ознайомитися з інформацією, що зберігається в системі, і використовувати її в своїх цілях (прослуховування ліній зв'язку користувачів з ЕОМ, аналіз інформаційних потоків, використання програм, які є чужою власністю).

Під активною інфільтрацією інформації розуміються такі дії, як перегляд чужих фай­лів через віддалені термінали, [маскування](http://ua-referat.com/%D0%9C%D0%B0%D1%81%D0%BA%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F) під конкретного користувача, фізичний збір і ана­ліз файлів на картах, магнітних стрічках і дисках і т.д.

На­в­ми­сні спроби проникнення в СОД можуть бути класифіковані як пасивні і активні.   
 Пасивне проникнення - це підключення до ліній зв'язку або збір електромагнітних випромінювань цих ліній в будь-якій точці системи особою, яка не є користувачем ЕОМ.   
Акти­вне проникнення в систему являє собою пряме використання інформації з файлів, що збе­рігаються в СОД. Таке проникнення реалізується звичайними процедурами доступу: ви­ко­ристанням відомого способу доступу до системи або її частини з метою завдання за­бо­ро­не­них питань, звернення до файлів, що містить інформацію, що цікавить; [маскуванням](http://ua-referat.com/%D0%9C%D0%B0%D1%81%D0%BA%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F) під істи­нного користувача після отримання характеристик (ідентифікаторів) доступу; ви­ко­рис­тан­ням службового становища, тобто незапланованого перегляду (ревізії) інформації файлів спів­робітниками обчислювальної установки. Акти­вне проникнення в СОД може здій­сню­ватися таємно, тобто в ужиток [контрольних](http://ua-referat.com/%D0%9A%D0%BE%D0%BD%D1%82%D1%80%D0%BE%D0%BB%D1%8C) програм забезпечення схоронності інформації.   
 Найбільш [характерні](http://ua-referat.com/%D0%A5%D0%B0%D1%80%D0%B0%D0%BA%D1%82%D0%B5%D1%80) прийоми проникнення: використання точок входу, вста­нов­ле­них в системі програмістами, обслуговуючим персоналом, або точок, виявлених при пере­вір­ці ланцюгів системного контролю; підключення до мережі зв'язку спеціального терміналу, що­ забезпечує вхід в систему шляхом перетину лінії зв'язку законного користувача з ЕОМ з по­дальшим відновленням зв'язку за типом помилкового повідомлення, а також у момент, ко­ли законний користувач не виявляє активності, але продовжує займати канал зв'язку; ану­лю­ван­ня [сигналу](http://ua-referat.com/%D0%A1%D0%B8%D0%B3%D0%BD%D0%B0%D0%BB) користувача про завершення роботи з системою і подальше продовження ро­бо­ти від його імені.

За допомогою цих [прийомів](http://ua-referat.com/%D0%9F%D1%80%D0%B8%D0%B9%D0%BE%D0%BC%D1%83) порушник, підміняючи на час його законного користувача, може використовувати лише доступні цьому користувачеві файли; неавторизована модифікація - неавторизований користувач вносить зміни до інформації, що зберігається в системі. в результаті користувач, якій ця [інформація](http://ua-referat.com/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%8F)належить, не може отримати до неї доступ.

[Поняття](http://ua-referat.com/%D0%9F%D0%BE%D0%BD%D1%8F%D1%82%D1%82%D1%8F) "неавторизований" означає, що перераховані дії виконуються всупереч вказівкам користувача, відповідального за [зберігання інформації](http://ua-referat.com/%D0%97%D0%B1%D0%B5%D1%80%D1%96%D0%B3%D0%B0%D0%BD%D0%BD%D1%8F_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97), або навіть в обхід обмежень, що накладаються на режим доступу в цій системі. Подібні спроби проникнення можуть бути викликані не тільки простим задоволенням цікавості грамотного програміста (користувача), але і навмисним отриманням інформації обмеженого використання.   
Можливі й інші види порушень, що призводять до втрати або витоку інформації. Так, електромагнітні [випромінювання](http://ua-referat.com/%D0%92%D0%B8%D0%BF%D1%80%D0%BE%D0%BC%D1%96%D0%BD%D1%8E%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F) при роботі ЕОМ та інших технічних засобів СОД можуть бути перехоплені, декодовані і представлені у вигляді бітів, складових потік інформації.

*2. Вимоги до захисту інформаційних систем.*

Одне з істотних вимог до системи забезпечення схоронності інформації - окрема ідентифікація індивідуальних користувачів, терміналів, індивідуальних програм (завдань) на ім'я та [функції](http://ua-referat.com/%D0%A4%D1%83%D0%BD%D0%BA%D1%86%D1%96%D1%97), а також даних при необхідності до рівня запису або елемента. Обмежити доступ до інформації дозволяє сукупність наступних способів: - ієрархічна класифікація доступу; - класифікація інформації за важливістю і місцем її виникнення; - вказівка ​​специфічних обмежень і додаток їх до специфічних об'єктів, наприклад користувач може здійснювати тільки [читання](http://ua-referat.com/%D0%A7%D0%B8%D1%82%D0%B0%D0%BD%D0%BD%D1%8F) файлу без права на запис до нього; - зміст даних або окремих груп даних (не можна читати інформацію по окремих об'єктах); - процедури, представлені тільки конкретним користувачам. Користувачі програм повинні обмежуватися лише однієї або всіма привілеями: [читанням](http://ua-referat.com/%D0%A7%D0%B8%D1%82%D0%B0%D0%BD%D0%BD%D1%8F), записом, видаленням інформації.

При реалізації запису передбачається її модифікація (збільшення, зменшення, зміна), нарощування (елементу, записи, файлу) і введення (елементу, записи, файлу). Система забезпечення схоронності інформації повинна гарантувати, що будь-який рух даних ідентифікується, авторизується, виявляється і документується.

[Організаційні](http://ua-referat.com/%D0%9E%D1%80%D0%B3%D0%B0%D0%BD%D1%96%D0%B7%D0%B0%D1%86%D1%96%D1%8F) вимоги до системи захисту реалізуються сукупністю адміністративних та процедурних заходів. Вимоги щодо забезпечення збереження повинні виконуватися перш за все на адміністративному рівні. З цією метою: - обмежується несупроводжуваний доступ до обчислювальної системи (реєстрація та супровід відвідувачів); - здійснюється [контроль](http://ua-referat.com/%D0%9A%D0%BE%D0%BD%D1%82%D1%80%D0%BE%D0%BB%D1%8C) за зміною в системі програмного забезпечення; - виконується [тестування](http://ua-referat.com/%D0%A2%D0%B5%D1%81%D1%82%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F) і верифікація зміни в системі програмного забезпечення і програмах захисту; - організується і підтримується взаємний [контроль](http://ua-referat.com/%D0%9A%D0%BE%D0%BD%D1%82%D1%80%D0%BE%D0%BB%D1%8C) за виконанням правил забезпечення збереження даних; - обмежуються привілеї персоналу, обслуговуючого СОД; - здійснюється запис [протоколу](http://ua-referat.com/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB) про доступ до системи; - гарантується компетентність обслуговуючого персоналу.

[Організаційні](http://ua-referat.com/%D0%9E%D1%80%D0%B3%D0%B0%D0%BD%D1%96%D0%B7%D0%B0%D1%86%D1%96%D1%8F) заходи, що проводяться з метою підвищення ефективності забезпечення схоронності інформації, можуть включати такі процедури: - розробку послідовного підходу до забезпечення схоронності інформації для всієї організації; - організацію чіткої роботи служби стрічкової і дискової бібліотек; - комплектування основного персоналу на базі інтегральних оцінок і твердих знань ; - організацію системи [навчання](http://ua-referat.com/%D0%9D%D0%B0%D0%B2%D1%87%D0%B0%D0%BD%D0%BD%D1%8F) та [підвищення кваліфікації](http://ua-referat.com/%D0%9F%D1%96%D0%B4%D0%B2%D0%B8%D1%89%D0%B5%D0%BD%D0%BD%D1%8F_%D0%BA%D0%B2%D0%B0%D0%BB%D1%96%D1%84%D1%96%D0%BA%D0%B0%D1%86%D1%96%D1%97) обслуговуючого персоналу.

З точки зору забезпечення доступу до СОД необхідно виконувати наступні процедурні заходи: - розробити та затвердити письмові інструкції на запуск і зупинка системи: - контролювати використання магнітних стрічок, дисків, карт, лістингів, порядок зміни програмного забезпечення і доведення цих змін до користувача. - Розробити процедуру відновлення системи при збійних [ситуаціях](http://ua-referat.com/%D0%A1%D0%B8%D1%82%D1%83%D0%B0%D1%86%D1%96%D1%8F); - [встановити](http://ua-referat.com/%D0%92%D1%81%D1%82%D0%B0%D0%BD%D0%BE%D0%B2%D0%B8) політику обмежень при дозволених візити в обчислювальний центр і визначити обсяг видаваної інформації; - розробити систему протоколювання використання ЕОМ, введення даних і виведення результатів; - забезпечити проведення періодичної чистки архівів та сховищ стрічок, дисків, карт для виключення та ліквідації невикористовуваних; - підтримувати документацію обчислювального центру відповідно до встановлених [стандартів](http://ua-referat.com/%D0%A1%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82).

*3. Класифікація схем захисту інформаційних систем.*

Збереження інформації може бути порушена у двох основних випадках: при отриманні несанкціонованого доступу до інформації та порушенні функціонування ЕОМ. система захисту від цих загроз включає такі основні елементи: захист СОД і її апаратури, [організаційні](http://ua-referat.com/%D0%9E%D1%80%D0%B3%D0%B0%D0%BD%D1%96%D0%B7%D0%B0%D1%86%D1%96%D1%8F) заходи щодо забезпечення збереження інформації, захист операційної системи, файлів, терміналів і каналів зв'язку.

Слід [мати](http://ua-referat.com/%D0%9C%D0%B0%D1%82%D0%B8) на увазі, що всі типи захисту взаємопов'язані і при виконанні своїх функцій хоча б однієї з них зводить нанівець зусилля інших. Пропоновані і реалізовані схеми захисту інформації в СОД дуже різноманітні, що спричинене в основному вибором найбільш зручного і легко [здійсненного](http://ua-referat.com/%D0%97%D0%B4%D1%96%D0%B9%D1%81%D0%BD%D0%B5%D0%BD%D0%BD%D1%8F) методу контролю доступу, тобто змі­ною­ [фун­кці­ональ­них](http://ua-referat.com/%D0%A4%D1%83%D0%BD%D0%BA%D1%86%D1%96%D0%BE%D0%BD%D0%B0%D0%BB%D1%96%D0%B7%D0%BC)­ влас­ти­востей системи.

В якості класифікаційної ознаки для схем захисту можна вибрати їх функціональні властивості. На основі цієї ознаки виділяються системи: без схем захисту, з повним захистом, з єдиною схемою захисту, з програмованою схемою захисту і системи з засекречуванням. У деяких системах відсутній механізм, що перешкоджає користувачеві в доступі до будь-якої інформації, що зберігається в системі. [Характерно](http://ua-referat.com/%D0%A5%D0%B0%D1%80%D0%B0%D0%BA%D1%82%D0%B5%D1%80), що більшість найбільш поширених і широко застосовуються за кордоном СОД з пакетною обробкою не мають механізму захисту. Проте такі системи містять зазвичай розвинений апарат виявлення і запобігання помилок, що гарантує виключення руйнувань режиму функціонування.   
 У системах з повним захистом забезпечується взаємна ізоляція користувачів, що порушується тільки для інформації загального користування (наприклад, бібліотеки загального користування). В окремих системах кошти роботи з бібліотеками загального користування дозволяють включити в них інформацію користувачів, яка теж стає загальним надбанням.   
 У системах з єдиною схемою захисту для кожного файлу створюється список авторизованих користувачів. Крім [того](http://ua-referat.com/%D0%A2%D0%BE%D0%B3%D0%BE), стосовно кожного файлу вказуються вирішуються режими його використання: читання, запис або виконання, якщо цей [файл](http://ua-referat.com/%D0%A4%D0%B0%D0%B9%D0%BB) є програмою. Основні концепції захисту тут досить прості, однак їх реалізація досить складна.   
У системах з програмованою схемою захисту передбачається механізм захисту даних з урахуванням специфічних вимог користувача, наприклад, обмеження[календарного](http://ua-referat.com/%D0%9A%D0%B0%D0%BB%D0%B5%D0%BD%D0%B4%D0%B0%D1%80) часу роботи системи, доступ тільки до середніх значень файлу даних, локальна захист окремих елементів масиву даних і т.д.

У таких системах користувач повинен мати можливість виділити захищені об'єкти і підсистеми. Захищається підсистема являє собою cовокупность програм і даних, правом доступу до яких наділені лише вхідні в підсистему программи.Обращеніе до цих програм можливо, у свою чергу, тільки в заздалегідь обмежених точках. Таким чином, програми підсистеми контролюють доступ до захищених об'єктів. Подібний механізм захисту з різ­ни­ми­ модифікаціями реалізований тільки в найбільш досконалих СОД.

У системах з засекречуванням вирішуються не питання обмеження доступу програм до інформації, а здійснюється контроль над подальшим використанням отриманої інформації. Наприклад, в системі використання грифів секретності на документах гриф служить повідомленням про міру контролю. У СОД ця схема захисту використовується рідко. Відмітна особливість розглянутих схем захисту - їх динамічність, тобто можливість введення і зміни правил доступу до даних в процесі роботи системи. Однак, забезпечення динамічності схем захисту значно ускладнює їх реалізацію.

Питання організації захисту інформації повинні вирішуватися вже на передпроектній стадії розробки СОД. Слід враховувати, що інфільтрація у систему буде зростати із зростанням значення доступу до інформації обмеженого доступу. [Саме](http://ua-referat.com/%D0%A1%D0%B0%D0%BC%D0%B5) на цій стадії необхідно чітко уявляти можливості потенційного порушника з тим, щоб надмірно не "утяжелить" систему. Досвід проектування систем захисту ще недостатній.   
Однак уже можна зробити деякі узагальнення. Похибки захисту можуть бути значною мірою знижені, якщо при проектуванні враховувати такі основні принципи побудови системи захисту.   
 1. Простота механізму захисту. Цей принцип загальновідомий, але не завжди глибоко усвідомлюється. Дійсно, деякі помилки, не виявлені в ході проектування і реалізації, дозволяють знайти невраховані шляхи доступу. Тому необхідно ретельне тестування програмного або схемного апарата захисту, але на практиці така перевірка можлива тільки для простих і компактних схем.

2. У [механізмі](http://ua-referat.com/%D0%9C%D0%B5%D1%85%D0%B0%D0%BD%D1%96%D0%B7%D0%BC%D1%96) захисту дозволу повинні переважати над заборонами. А це означає, що в нормальних умовах доступ повинен бути відсутніми і для роботи схеми захисту необхідні умови, при яких доступ стає можливим. Крім того вважається, що заборона доступу при відсутності особливих вказівок забезпечує високу ступінь надійності механізму захисту. Помилка в схемі захисту, заснованої на використанні дозволів, призводить до розширення сфери дії заборон. Цю помилку легше виявити, і вона не порушить загального статусу захисту.

3. Контроль повинен бути всеосяжним. Цей принцип передбачає необхідність перевірки повноваження будь-якого звернення до будь-якого об'єкту і є основою системи захисту. Завдання управління доступом з урахуванням цього принципу повинна вирішуватися на загальносистемному рівні і для таких режимів роботи, як запуск, відновлення після збою, виключення і профілактичне обслуговування. При цьому необхідно забезпечити надійне визначення джерела будь-якого звернення до даних.   
 4. Механізм захисту може не засекречуватися, тобто не має сенсу засекречувати деталі реалізації системи захисту, призначеної для широкого використання. Ефективність захисту не повинна залежати від того, наскільки досвідчені потенційні порушники, тому що набагато [простіше](http://ua-referat.com/%D0%9F%D1%80%D0%BE%D1%81%D1%82%D1%96%D1%80) забезпечити захист списку паролів (ключів). Відсутність же зв'язку між [механізмом](http://ua-referat.com/%D0%9C%D0%B5%D1%85%D0%B0%D0%BD%D1%96%D0%B7%D0%BC%D1%96) захисту і паролями дозволяє зробити за необхідності схеми захисту предметом широкого обговорення серед фахівців, не зачіпаючи при цьому інтереси користувачів.   
 5. Поділ повноважень, тобто застосування кількох ключів захисту. У СОД наявність кількох ключів захисту зручно в тих випадках, коли [право](http://ua-referat.com/%D0%9F%D1%80%D0%B0%D0%B2%D0%BE) на доступ визначається вико­нан­ням­ низки умов.

6. Мінімальні повноваження. Для будь-якої програми і будь-якого користувача повинен бути визначений мінімальний коло повноважень, необхідних для виконання дорученої роботи. Завдяки цим діям значною мірою зменшується шкоду, яку завдають при збоях і випадкових порушення. Крім того, скорочення числа обмінів даними між привілейованими програмами до необхідного мінімуму зменшує ймовірність ненавмисного, небажаного або помилкового застосування повноважень. Таким чином, якщо схема захисту дозволяє розставити "бар'єри" у системі, то принцип мінімальних повноважень забезпечує

найбільш раціональне розташування цих "бар'єрів".

7. Максимальна відособленість механізму захисту. З метою виключення обмінів інформацією між користувачами при проектуванні схеми захисту рекомендується зводити до мінімуму число загальних для декількох користувачів параметрів і характеристик механізму захисту. Незважаючи на те, що [функції](http://ua-referat.com/%D0%A4%D1%83%D0%BD%D0%BA%D1%86%D1%96%D1%97)операційної системи дозволу доступу пере­кри­ваю­ть­ся, система дозволу доступу повинна [конструюватися](http://ua-referat.com/%D0%9A%D0%BE%D0%BD%D1%81%D1%82%D1%80%D1%83%D1%8E%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F) як ізольований програмний модуль, тоб­то захист повинен бути відділена від функцій управління даними. Виконання цього прин­ци­пу дозволяє програмувати систему дозволу доступу як автономний пакет програм з по­даль­шою незалежної налагодженням та перевіркою. Пакет програм повинен розміщуватися для роботи в захищеному поле пам'яті, щоб забезпечити системну локалізацію спроб про­ник­нен­ня ззовні. Навіть спроба проникнення з боку програм операційної системи пови­н­на [автоматично](http://ua-referat.com/%D0%90%D0%B2%D1%82%D0%BE%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0)фіксуватися, [документуватися](http://ua-referat.com/%D0%94%D0%BE%D0%BA%D1%83%D0%BC%D0%B5%D0%BD%D1%82%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F) і відхилятися, якщо виклик виконаний не­ко­рек­тно. [Природно](http://ua-referat.com/%D0%9F%D1%80%D0%B8%D1%80%D0%BE%D0%B4%D0%B0), що в результаті реалізації відокремленого механізму захисту можуть зрости обсяги програми і [терміни](http://ua-referat.com/%D0%A2%D0%B5%D1%80%D0%BC%D1%96%D0%BD%D0%B8) на її розробку, виникнути дублювання керуючих і допоміжних програм, а також необхідність у розробці самостійних викликаються функцій.   
 8. Психологічна привабливість. Схема захисту повинна бути в реалізації простої. [Природно](http://ua-referat.com/%D0%9F%D1%80%D0%B8%D1%80%D0%BE%D0%B4%D0%B0), чим точніше збігається уявлення користувача про схему захисту з її фактичними можливостями, тим менше помилок виникає в процесі застосування. Використання деяких штучних мов при зверненні до схеми захисту зазвичай служить дже­ре­лом­ додаткових помилок.

*4. Аналіз збереження інформаційних систем.*

Аналіз збереження інформаційних систем грунтується на постійному вив­чен­ні [протоколів](http://ua-referat.com/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB) (як машинних, так і ручних), перевірці аварійних сигналізаторів та інших пристроїв. Важливим фактором є також і те, що [такий](http://ua-referat.com/%D0%A2%D0%B0%D0%BA%D0%B8%D0%B9) огляд підтримує інтерес до питань забезпечення схоронності.

За проведення аналізу [відповідає](http://ua-referat.com/%D0%92%D1%96%D0%B4%D0%BF%D0%BE%D0%B2%D1%96%D0%B4%D1%8C) співробітник, що займається питаннями забезпечення схоронності. Прилади аварійної сигналізації повинні перевірятися досить часто, але у випадкові моменти часу. До їх числа відносяться детектори вогню і диму, [датчики](http://ua-referat.com/%D0%94%D0%B0%D1%82%D1%87%D0%B8%D0%BA%D0%B8) вологості і температури, апаратура сигналізації при спробах проникнення в приміщення, пристрої фізичного контролю доступу, дверна сигналізація та інші аналогічні прилади. проводиться також перевірка [стану](http://ua-referat.com/%D0%A1%D1%82%D0%B0%D0%BD%D1%83)протипожежного обладнання, доступу до аварійних виходів і системам відключення електро-, водо-і теплопостачання. Щотижня перевіряється справність пристроїв та ліній зв'язку. Оглядається також [простір](http://ua-referat.com/%D0%9F%D1%80%D0%BE%D1%81%D1%82%D1%96%D1%80) під технологічним [підлогою](http://ua-referat.com/%D0%9F%D1%96%D0%B4%D0%BB%D0%BE%D0%B3%D1%96) та інші порожнини, в яких можуть накопичуватися відходи, що створюють небезпеку самозаймання, або [вода](http://ua-referat.com/%D0%92%D0%BE%D0%B4%D0%B0) при її витоках. З проведених робіт ведеться [протокол](http://ua-referat.com/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB) перевірки, кожен запис якого супроводжується зауваженнями про відхилення. Зарубіжні фахівці вважають, що цій роботі має приділятися близько однієї го­ди­ни­ на тиждень.

Інша важлива і регулярна [робота](http://ua-referat.com/%D1%80%D0%BE%D0%B1%D0%BE%D1%82%D0%B0) пов'язана з вивченням ручних і машин­них [протокольних](http://ua-referat.com/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB) записів. результати регулярних перевірок протоколів мають оформлятися за­ певним зразком з тим, щоб не пропустити будь-який вид перевірки. Рекомендується ре­тель­но досліджувати будь-які підозрілі [тенденції](http://ua-referat.com/%D0%A2%D0%B5%D0%BD%D0%B4%D0%B5%D0%BD%D1%86%D1%96%D1%97) і відхилення від прийнятих стандартів у ро­бо­ті.

Більш того, описані операції самі по собі є об'єктом, збереження якого необхідно забезпечити, тому має бути виділено спеціальне приміщення з терміналом, на якому виконуються тільки роботи щодо забезпечення схоронності. Побічним продуктом аналізу схоронності може виявитися [статистична](http://ua-referat.com/%D0%A1%D1%82%D0%B0%D1%82%D0%B8%D1%81%D1%82%D0%B8%D0%BA%D0%B0) [оцінка](http://ua-referat.com/%D0%9E%D1%86%D1%96%D0%BD%D0%BA%D0%B0) ефективності використання устаткування організації та оцінка ефективності роботи користувачів. На основі результатів перевірки проводяться щотижневі наради [керівників](http://ua-referat.com/%D0%9A%D0%B5%D1%80%D1%96%D0%B2%D0%BD%D0%B8%D0%BA) організації, на якому заслуховується повідомлення співробітника, відповідального за забезпечення схоронності. Такі наради дозволяють оцінити зусилля по захисту і виробити додаткові рекомендації щодо вдосконалення прийнятих методів забезпечення схоронності.

Слід аналізувати всі можливості порушення збереження і відшукувати засоби боротьби з ними. Якщо [стандартні](http://ua-referat.com/%D0%A1%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82) процедури не виконуються, то повторюють інструктаж з метою виконання цих процедур. Крім звичайних регулярних перевірок, описаних вище, співробітник, відповідальний за забезпечення схоронності, зобов'язаний виконувати тестовий контроль перевірки апаратури і програмного забезпечення. Результати тестування фіксуються в спеціальному журналі. Це вимагає деяких витрат ручної праці та машинного часу. У СОД, в яких рівень забезпечення схоронності високий, тестування повинно проводитись більш часто і по можливості автоматично. Результати тестування також ана­лізують­ся співробітником, відповідальним за забезпечення схоронності.

*5. Комплексний*[*захист інформації*](http://ua-referat.com/%D0%97%D0%B0%D1%85%D0%B8%D1%81%D1%82_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97)*в персональних ЕОМ.*

За [статистикою](http://ua-referat.com/%D0%A1%D1%82%D0%B0%D1%82%D0%B8%D1%81%D1%82%D0%B8%D0%BA%D0%B0) більше 80% компаній і агентств несуть фінансові [збитки](http://ua-referat.com/%D0%97%D0%B1%D0%B8%D1%82%D0%BA%D0%B8) через порушення безпеки даних.  Багато фірм зараз займаються розробкою різних антивірусних програм, систем розмежування доступу до даних, захисту від копіювання і т.д. Пояснюється це порівняльної простотою розробки подібних методів і в той же час досить високою їх ефективністю.   
 Розглянемо основні механізми реалізації конкретних програмних засобів захисту інформації.   
 Програми-ідентифікатори служать для контролю входу в ЕОМ, аутентифікації користувача з введення пароля та розмежування доступу до ресурсів ЕОМ. Під ідентифікацією користувача розуміється процес розпізнавання конкретного суб'єкта системи, зазвичай за допомогою заздалегідь визначеного ідентифікатора; кожен суб'єкт системи повинен бути однозначно ідентифікуємо. А під аутентифікацією розуміється перевірка ідентифікації користувача, а також перевірка цілісності даних при їх зберіганні або передачі для запобігання несанкціонованої модифікації.

При завантаженні з накопичувача на жорсткому магнітному диску систе­мА­ [BIOS](http://ua-referat.com/Bios) виконує зчитування 1го сектору 0-го циліндра 0-ой доріжки. Цей сектор називається "Голо­вний завантажувальний запис" - Master boot record / МВR /. Зазвичай програма, за­пи­са­на в МВR, завантажує запис BOOT RECORD / BR / активного розділу. Однак можна ви­ко­рис­товувати МВR для організації контролю входу в [ПЕОМ](http://ua-referat.com/%D0%9F%D0%95%D0%9E%D0%9C). Так як розмір програми МВК неве­ликий, то на неї можна покласти дуже обмежені функції. Наприклад, можна спробувати "укла­сти" в неї разом з основною [функцією](http://ua-referat.com/%D0%A4%D1%83%D0%BD%D0%BA%D1%86%D1%96%D1%97) і програму перевірки пароля.

Про­те ефективніше використовувати МВR для завантаження іншої, більшої за обсягом прог­ра­ми. При застосуванні [стандартної](http://ua-referat.com/%D0%A1%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82) розбивки НЖМД на розділи за допомогою програми FDISK сектору з номером, більше або рівним 3, 0-ой доріжки 0-го циліндра не ви­ко­рис­то­вую­ться, тому їх можна застосувати для зберігання більшої за обсягом програми, що виконує фун­кції контролю. Крім цього в запису МВR зберігається первинна таблиця описувачів логі­ч­них дисків. Зміна цієї [таблиці](http://ua-referat.com/%D0%A2%D0%B0%D0%B1%D0%BB%D0%B8%D1%86%D1%96) дозволяє запобігти доступ до логічного диска (розділу) на рів­ні системи DOS при завантаженні з дискети. Перший сектор активного розділу містить за­ван­тажувальну запис ВК, що здійснює завантаження операційної системи. На початку цього запи­су міститься таблиця параметрів логічного диска. BR може використовуватися для зава­н­та­ження не операційної системи, а деякої іншої програми, що [реалізує](http://ua-referat.com/%D0%A0%D0%B5%D0%B0%D0%BB%D1%96%D0%B7%D0%BC) розмежування дос­ту­пу. Ця програма в свою чергу повинна в кінці своєї роботи завантажити [операційну](http://ua-referat.com/%D0%9E%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D1%96%D1%8F) систему. Обсяг ВR достатній для розміщення програми, що реалізує завантаження довільного файлу з кореневого каталогу логічного диска. Модифікація таблиці параметрів деякого логічного диска може використовуватися і для запобігання доступу до цього логічного диска при завантаженні ЕОБ з дискети.

Прикладом програм такого роду є система SHIELD, яка складається з 2-х файлів: sset.com і sswith.com При першій установці системи файл sset.com копіює оригінальний МВR в 2-ій сектор 0-ой доріжки нульового циліндра, а в першому секторі залишає модифікований варіант МВR, який перед завантаженням DOS запитує пароль. Якщо пароль невірний, то жорсткий диск виявляється недоступний. Для зняття захисту використовується файл sswitch.com, який повертає на місце оригінальний сектор з МВR. Програми такого роду доцільно використовувати для захисту комп'ютера без НГМД, так як при завантаженні з дискети можна безперешкодно читати і копіювати дані з НЖМД.

Крім того, для професіонала подібний захист не представляє серйозних труднощів. У [стандартному](http://ua-referat.com/%D0%A1%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82) середовищі DOS в якості командного [процесора](http://ua-referat.com/%D0%9F%D1%80%D0%BE%D1%86%D0%B5%D1%81%D0%BE%D1%80)використовується COMMAND.СОМ. Однак система допускає установку іншого командного процесора по команді SHELL у файлі СОМГ10.БУБ. За допомогою нового командного процесора можна дозволити запуск лише певних програм і заборонити запуск інших.

Написання нового командного процесора - завдання досить складна і не завжди виправдана, тому що можливе рішення тих же самих завдань більш простими способами (написання драйвера або програми, що запускається з файлу AUTOEXEC. ВАТ). Приклад командного процесора - файл PWLOAD.СОМ, розроблений 2В Рrogrammers Groups. Ця програма запитує пароль і, якщо він набраний неправильно, то робота ЕОМ блокується.   
[Функції](http://ua-referat.com/%D0%A4%D1%83%D0%BD%D0%BA%D1%86%D1%96%D1%97) розмежування доступу також можна реалізувати за допомогою драйвера пристрою, що визначається у файлі CONFIG.SYS. Цей драйвер може контролювати доступ до файлів, каталогів та нестандартно певним логічним дискам. Для цієї мети зазвичай здійснюється перехоплення переривання DOS INT 2lh та інших переривань операційної системи, організується посекторного захист від читання / запису, захист від перейменування і переміщення.   
 Це пов'язано з певними труднощами, так як необхідно зберігати таблиці великого обсягу, що описують повноваження з доступу до кожного сектору, і тіньові таблиці FАТ і DIR для перевірки коректності при їх перезапису. У загальному випадку ця проблема видається важкою з-за великого обсягу даних, що підлягають зберіганню та обробці в системі розмежування доступу. На драйвер можна також покласти запит пароля на вхід в систему.   
 Існують драйвери для організації режиму прозорого шифрування даних на дисках. [Такий](http://ua-referat.com/%D0%A2%D0%B0%D0%BA%D0%B8%D0%B9) драйвер здійснює перехоплення [переривання BIOS](http://ua-referat.com/%D0%9F%D0%B5%D1%80%D0%B5%D1%80%D0%B8%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F_BIOS) INT 13h, контролюючи таким чином всі операції з диском (читання, запис і т.д.) При цьому дані на захищеному диску (або його розділі) знаходяться в зашифрованому вигляді, а ключі можуть зберігатися на нестандартно відформатованої ключовою дискеті для більшої безпеки даних. Така міра захисту зручна для запобігання читання даних з НЖМД при завантаженні з дискети.   
Але і тут є ряд істотних недоліків. По-перше, ключі шифрування зберігаються в оперативній пам'яті, а тому можуть бути лічені зловмисниками. По-друге, завжди можна отримати відкрите вміст файлу, переписавши його в деякий файл, розташований не в групі файлів прозорого шифрування.

Приклад драйвера - система DISKREET з пакету NORTON UTILITES: включає в себе файли DISKREET.SYS і DISKREET.ЕХЕ. DISKREET.SYS драйвер, що завантажується з CONFIG.SYS і що дозволяє створювати нестандартно певні логічні диски, захищені паролем, які до того ж зашифровані за оригінальним алгоритмом.

Програма DISKREET.ЕХЕ дозволяє зашифровувати і розшифровувати будь-які файли і каталоги на дисках. Програми, резидентні в пам'яті, можуть виконувати ті ж функції, що і драйвери. Існує різниця лише при завантаженні: драйвер завантажується з CONFIG.SYS командою DEVICE, а резидентні програми з файлу AUTOEXEC.ВАТ.

Крім цього такі програми часто використовуються для контролю та запобігання зараження комп'ютера вірусами. Прикладом такої програми може служити ревізор-V.СОМ з антивірусного пакету Є. Касперського. Програми-шифрувальники виконують тільки одну функцію - шифрування даних: файлів, каталогів і дисків по ключу, що вводиться користувачем. Застосовуються найрізноманітніші алгоритми шифрування: від криптографічно стійких DES і FEAL до тривіальних алгоритмів побітового складання з ключем. Прикладів таких програм досить багато. До переваг програмних засобів захисту можна віднести їх невисоку вартість, простоту розробки. Недоліком таких систем є невисокий ступінь захищеності інформації. Для посилення захисту можна запропонувати використання декількох програмних засобів одночасно.

Наприклад, використовувати пароль при вході, систему розмежування доступу і режим прозорого шифрування. При цьому виникнуть певні незручності в роботі, але разом з тим зросте надійність.

Розглянемо далі основні види програмно - апаратних засобів захисту інформації. Вони характеризуються більш високою стійкістю і, як наслідок, більш високою вартістю. Але при застосуванні апаратно-програмних комплексів на підприємствах з підвищеним ризиком появи загроз (наприклад, на військових об'єктах або в комерційних банках) [витрати](http://ua-referat.com/%D0%92%D0%B8%D1%82%D1%80%D0%B0%D1%82%D0%B8) на установку такого захисту окупаються повністю. Багато фірм - виробники комп'ютерів передбачають захист їх від несанкціонованого доступу на рівні мікросхеми ПЗУ з BIOS. Так, при завантаженні комп'ютера при включенні живлення ще під час процедури POST потрібно вказати правильний пароль, щоб машина продовжувала роботу. Іноді можливість установки пароля реалізована в BIOS, але не описана в документації. Деякі[віруси](http://ua-referat.com/%D0%92%D1%96%D1%80%D1%83%D1%81%D0%B8) можуть записувати в полі пароля випадкову інформацію, і одного разу користувач виявляє, що його машина непогано захищена від нього. Сам пароль зберігається в області CMOS і при великому бажанні може бути стертий. [Фірма](http://ua-referat.com/%D0%A4%D1%96%D1%80%D0%BC%D0%B0) Сompaq пішла далі і включила в BIOS програми, що підтримують наступні області поділу доступу: можливість швидкому замикання комп'ютера, захист жорсткого диска, гнучкого диска, послідовного й паралельного портів. Запуск захисних програм з BIOS регулюється перемикачами на платі комп'ютера.

Слід зазначити, що ефективність такого захисту досягається тільки в поєднанні з організаційними заходами захисту, так як при наявності вільного доступу до "нутрощів" комп'ютера [зловмисникові](http://ua-referat.com/%D0%97%D0%BB%D0%BE%D0%B2%D0%BC%D0%B8%D1%81%D0%BD%D0%B8%D0%BA%D0%B8) не складе великих труднощів замінити мікросхему з BIOS або розрядити батарею живлення, нейтралізувавши таким чином перераховані вище захисні заходи. Шифруюча плата вставляється в слот розширення на материнській платі комп'ютера і виконує функцію шифрування. Режим шифрування може бути прозорим або попереднім. Можуть шифруватися як окремі файли, так і каталоги або цілі диски. На платі знаходиться датчик псевдовипадкових чисел для генерації ключів та вузли шифрування, апаратно реалізовані в спеціалізованих однокристальних мікроЕОМ. Ключі шифрування зберігаються на спеціально створеній для цього дискеті. Програмна частина комплексу містить драйвер плати для взаємодії програм користувача з платою шифрування.

В якості прикладу розглянемо продукт [фірми](http://ua-referat.com/%D0%A4%D1%96%D1%80%D0%BC%D0%B8) "АНКАД" - програмно-апаратний комплекс "Криптон" (версії 1,2,3,4). Цей пристрій забезпечує високу криптографічну [стійкість](http://ua-referat.com/%D0%A1%D1%82%D1%96%D0%B9%D0%BA%D1%96%D1%81%D1%82%D1%8C), шифрування проводиться за алгоритмом ГОСТ 28174 - 89. Відкритий інтерфейс дозволяє розробляти додаткове [програмне забезпечення](http://ua-referat.com/%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BD%D0%B5_%D0%B7%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%BD%D1%8F) спеціального призначення. Довжина ключа - 256 біт. Швидкість шифрування - до 200 Кбайт / сек. Апаратні вимоги: IBM PC ХТ / АТ, [MS-DOS](http://ua-referat.com/MS-DOS) 3,0 і вище. Програмна підтримка дозволяє здійснювати: шифрування файлів, розділів, дисків; розмежування і контроль доступу до комп'ютера; електронний підпис юридичних і фінансових документів; прозоре шифрування жорстких і гнучких дисків. Шифрувальні плати мають високу гарантією захисту інформації, але їх застосування вносить певні незручності в роботу ПЕОМ, перш за все - це значне зниження швидкості обробки даних, а також необхідність ініціалізувати плату при кожному включенні комп'ютера.

Останнім часом широкого поширення набули електронні ключі. Це пристрій підключається до комп'ютера через порт LPT (є моделі, які використовують СОМ порт). При цьому електронний ключ не заважає нормальній роботі паралельного порту і повністю "прозорий" для принтера та інших пристроїв. Ключі можуть з'єднуватися каскадно, як правило, до 8 штук підряд. При цьому в ланцюжку можуть працювати абсолютно різнотипні ключі, випущені різними фірмами.

[Електронні ключі](http://ua-referat.com/%D0%95%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D1%96_%D0%BA%D0%BB%D1%8E%D1%87%D1%96) можуть виконувати різні функції. Наприклад, захист програм від несанкціонованому копіювання, при цьому у виконуваний модуль-СОМ або-ЕХЕ файл вбудовуються фрагменти коду для обміну з електронним ключем і управління ним (розмір коду зазвичай не перевищує 2 Кбайт).[Електронні](http://ua-referat.com/%D0%95%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%B2%D0%BE%D0%B7%D0%B8) ключі дозволяють захищати не тільки-СОМ і-ЕХЕ програми, але і працювати з не виконує, додатками, наприклад: AUTOCAD LISP, макросами електронних таблиць типу LOTUS, RUNTIME - модулями, інтерпретаторами, базами даних, кодованими графічними файлами і т.п. Крім основних захисних функцій ключі багатьох фірм здатні виявляти факт зараження захищеної програми різними видами файлових вірусів. Дуже ефективним є застосування електронних ключів для зберігання і передачі шифрувальної ключа при застосуванні різних методів шифрування (DES, DSS, RSA, ГОСТ тощо), оскільки зберігання та передача ключів - найслабше місце у більшості існуючих алгоритмів. А при використанні електронних ключів для генерації шифрувальних ключів відпадає необхідність їх запам'ятовувати або записувати, а потім вводити з клавіатури. Ключ не має вбудованих джерел живлення і зберігає записану в нього інформацію при відключенні від комп'ютера. У нашій країні найбільш поширені ключі [американської](http://ua-referat.com/%D0%90%D0%BC%D0%B5%D1%80%D0%B8%D0%BA%D0%B0%D0%BD%D1%81%D0%BA%D0%B8%D0%B9) фірми "Software Security Inc". Ця [фірма](http://ua-referat.com/%D0%A4%D1%96%D1%80%D0%BC%D0%B0) випускає ключі для DOS, [WINDOWS](http://ua-referat.com/Windows), UNIX, OS / 2, Macintosh. Ключі можуть бути як з одноразовою записом, так і перепрограмувальні; можуть містити енергонезалежну пам'ять або не утримувати.[Електронні](http://ua-referat.com/%D0%95%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BB%D1%96%D0%B7) ключі являють собою одне з найбільш ефективних і зручних засобів захисту від копіювання.

Пластикові ідентифікаційні картки (ІК) впроваджуються в багато сфер нашого життя. Маленькі розміри карти, зручність зберігання, досить високий обсяг пам'яті роблять ІК незамінними в багатьох галузях людської діяльності.

Є безліч прикладів використання ІК в СЗІ, наприклад, для реалізації захисту ПЕОМ від несанкціонованого доступу. [Такий](http://ua-referat.com/%D0%A2%D0%B0%D0%BA%D0%B8%D0%B9) апаратно - програмний комплекс складається з апаратної частини: спеціальної плати, яка вставляється в слот розширення ПК, пристрої зчитування інформації з ІК і самих ІК; також є програмна частина: драйвер для управління платою і пристроєм зчитування з ІК.

У програмну частину комплексу може входити також програмне забезпечення для організації розмежування доступу до частин і розділів жорсткого диска. Крім того система захисту запитує пароль. Таким чином виключається вхід в систему по вкраденої картці.   
Приклад апаратно - програмного комплексу захисту - розробка фірми Datamedia. Серія її комп'ютерів Netmate обладнана спеціальним пристроєм Securecard reader - зчитувач карт безпеки. Карти безпеки у виконанні - варіант кредитних карт; на їх магнітному носії за допомогою спеціальної апаратури, яка є тільки у розпорядженні адміністратора, робиться запис про користувача: його ім'я, пароль і описуються всі повноваження, які він отримує при вході в систему. Зокрема, на карті записано, скільки разів користувач може намагатися ввести пароль при вході. Таким чином, випадкова втрата карти безпеки або її [крадіжка](http://ua-referat.com/%D0%9A%D1%80%D0%B0%D0%B4%D1%96%D0%B6%D0%BA%D0%B0) не дозволяє зловмисникові одержати доступ до комп'ютера: якщо ім'я користувача ще можна дізнатися, не привертаючи уваги, то пароль йому невідомий. Тільки свідома передача карти безпеки кому-то одночасно з розголошенням пароля може відкрити доступ до комп'ютера [сторонній](http://ua-referat.com/%D0%A1%D1%82%D0%BE%D1%80%D0%BE%D0%BD%D0%BD%D1%96%D0%B9) особі.   
 Адміністратор системи створює карту безпеки для легальних користувачів. На цій карті крім вже перерахованої інформації описується профіль користувача. У ньому включаються, наприклад: можливість доступу до програми SETUP, тобто фіксуються такі характеристики комп'ютера, як екран, кількість і типи дисків; також визначається, які з локальних пристроїв (гнучкі диски, [жорсткі диски](http://ua-referat.com/%D0%96%D0%BE%D1%80%D1%81%D1%82%D0%BA%D1%96_%D0%B4%D0%B8%D1%81%D0%BA%D0%B8), послідовні і паралельні порти) доступні цьому користувачеві, з яких локальних або мережевих пристроїв він може завантажуватися. Передбачена трансляція паролів: той пароль, який призначається користувачеві, як правило, легко запам'ятовується, але зовсім не той, з яким [працює](http://ua-referat.com/%D0%9F%D1%80%D0%B0%D1%86%D1%8E%D1%94) система. При спробі просто висмикнути карту безпеки з зчитувача - доступ до комп'ютера намертво блокується, поки в зчитувач не буде вставлена ​​та ж карта безпеки. При неправильному паролях (якщо перевищено кількість спроб, дозволене для даного користувача) - машина блокується, і лише адміністратор зможе "оживити" її, тобто стимулюється необхідність довести до відома адміністрації всі випадки порушення режиму секретності.

З точки зору захисту від вірусів перераховані системи, теж важливі, оскільки вони, крім ідентифікації користувача певним чином організують його роботу на комп'ютері, забороняючи окремі небезпечні дії типу запуску програм з дискети, завантаження з дискети. Обмеження на використання певних ресурсів системи типу мережевих карт, послідовних портів також корисні з точки зору захисту від вірусів, оскільки обмежують можливість або навіть відсікають деякі шляхи розповсюдження або отримання зарази, Нарешті, підвищений рівень тривоги, [характерний](http://ua-referat.com/%D0%A5%D0%B0%D1%80%D0%B0%D0%BA%D1%82%D0%B5%D1%80) для цієї системи дуже корисний і з антивірусною точки зору: будь-які неполадки і дива в роботі комп'ютерів негайно повинні ставати надбанням адміністрації і також негайно доводитись до відома фахівців, що різко зменшує розміри збитків від проникнення вірусів.

ІК можуть використовуватися і для зберігання ключів шифрування в системах криптографічного захисту.

Недоліком такої системи є низька захищеність ІК з магнітною смугою. Як показує досвід, інформація з них може бути безперешкодно лічена. А застосування ІК з вбудованим чіпом через високу вартість таких ІК веде до значного збільшення витрат на встановлення системи захисту, Крім того, дорого обходиться і обладнання для зчитування інформації з ІК. Але, незважаючи на високу вартість, системи захисту на базі ІК знаходять широке застосування там, де необхідна висока надійність, наприклад, у комерційних структурах.   
В даний час велику популярність здобуло сімейство приладів Touch memory (ТМ), вироблене фірмою Dallas Semiconductods.

Даний [вибір](http://ua-referat.com/%D0%92%D0%B8%D0%B1%D1%96%D1%80) був визначений насамперед високою надійністю, оскільки вивести touch-memory з ладу досить важко. Одним з основних відмінностей приладів Touch Memory від інших компактних носіїв інформації є конструкція корпусу. Крім захисту сталевий корпус виконує також роль електричних контактів. Прийнятні і масо-габаритні характеристики - таблетка діаметром з двокопієчну монету і товщиною 5 мм дуже підходить для таких застосувань. Кожен прилад сімейства є унікальним, тому що має свій власний серійний номер, який записується в прилад за допомогою лазерної установки під час його виготовлення і не може бути змінений протягом усього терміну служби приладу. У процесі запису та тестування на заводі гарантується, що ні буде виготовлено двох приладів з однаковими серійними номерами.

Таким чином, виключається можливість підробки приладів. Цілком прийнятною при використанні Touch-memory є і ціна: вона більш ніж в 4 рази нижче, ніж при використанні пластикових карток. Прилади Toich Memory представляють собою енергонезалежну статичну пам'ять з багаторазовою записом / читанням, що розміщується всередині металевого корпусу. На відміну від звичайної пам'яті з паралельним портом адреси / даних, пам'ять приладів Toich Mempry має послідовний інтерфейс. Дані записуються / читаються в пам'ять по одній двобічної сигнальної лінії. З цієї лінії в прилад передаються команди і дані, зчитуються дані. При цьому використовується широтно-імпульсний метод кодування. Логічні [сигнали](http://ua-referat.com/%D0%A1%D0%B8%D0%B3%D0%BD%D0%B0%D0%BB) "1" і "0" з рівнем від +5 В до ВВ передаються імпульсами різної тривалості. Такий цифровий інтерфейс дозволяє підключати прилади Touch Memory безпосередньо до персональних ЕОМ або через [мікропроцесорний](http://ua-referat.com/%D0%9C%D1%96%D0%BA%D1%80%D0%BE%D0%BF%D1%80%D0%BE%D1%86%D0%B5%D1%81%D0%BE%D1%80%D0%B8)контролер.

Важливою особливістю приладів є низька споживана потужність, що дозволяє використовувати вбудовану в корпусі приладу мініатюрну літієвий акумулятор для збереження інформації в пам'яті протягом 10 років.

Існують конкретні розробки апаратно - програмних комплексів захисту інформації на базі ТМ. В якості прикладу розглянемо систему QPDOS, розроблену фахівцями з АТ "РНТ". QPDOS є [функціональним](http://ua-referat.com/%D0%A4%D1%83%D0%BD%D0%BA%D1%86%D1%96%D0%BE%D0%BD%D0%B0%D0%BB%D1%96%D0%B7%D0%BC) розширенням MS-DOS і призначена для використання у складі ПК на базі IBM РС / АТ. QPDOS повністю [контролює](http://ua-referat.com/%D0%9A%D0%BE%D0%BD%D1%82%D1%80%D0%BE%D0%BB%D1%8C) і управляє доступом всіх користувачів до ресурсів і даних ПК. Як функціональних частин ЗЗІ QPDOS можуть бути включені наступні підсистеми: реєстрації та обліку, призначену для протоколювання подій, що відбуваються в системі, контролю за можливими спробами НСД, обліку сеансів користувачів і генерації звітів; оперативного контролю, що дозволяє оперативно спостерігати з ПК адміністратора системи за подіями і діями користувачів, які відбуваються на будь-якому ПК в складі мережі; контролю цілісності та захисту від копіювання програмного забезпечення; заборони початковій завантаження з ГМД, що запобігає можливість обходу системи захисту порушником за допомогою завантаження ПК зі своєю системної дискети; криптографічну, яка представляє собою драйвер MS -DOS, здійснює зашифрування і розшифрування інформації на окремих логічних дисках ПК в прозорому для прикладних програм режимі.   
Крім цього підсистема включає засоби для генерації ключів шифрування і перешіфрованія інформації на новому ключі, і введення ключів шифрування в систему з електронних ключів Touch Memory. Система криптографічного захисту може використовуватися як в чисто програмному варіанті, так і з апаратною підтримкою у вигляді кріптоплати "Криптон - 3", що підвищує [продуктивність](http://ua-referat.com/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82%D0%B8%D0%B2%D0%BD%D1%96%D1%81%D1%82%D1%8C) системи.   
 Слід зазначити, що заходи комп'ютерної безпеки не обмежуються лише засобами захисту, розташованими в самому комп'ютері - всередині комп'ютера, або у вигляді зовнішніх пристроїв. Всі перераховані вище програмні та апаратно-програмні [засоби захисту інформації](http://ua-referat.com/%D0%97%D0%B0%D1%81%D0%BE%D0%B1%D0%B8_%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82%D1%83_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97) стають ефективними лише при [суворому](http://ua-referat.com/%D0%A1%D1%83%D0%B2%D0%BE%D1%80%D0%BE%D0%B2)дотриманні цілого ряду адміністративних та [організаційних](http://ua-referat.com/%D0%9E%D1%80%D0%B3%D0%B0%D0%BD%D1%96%D0%B7%D0%B0%D1%86%D1%96%D1%8F) заходів. Перш ніж будувати систему захисту, необхідно оцінити витрати на її створення та можливі витрати на ліквідацію наслідків у разі втрати захищаються даних. Захист буде [економічно](http://ua-referat.com/%D0%95%D0%BA%D0%BE%D0%BD%D0%BE%D0%BC%D1%96%D0%BA%D0%B0) доцільна лише в тому випадку, якщо витрати на її створення будуть менше можливих втрат.

**Математичні моделі безпеки**

Формальне визначення політики безпеки називають математичною моделлю безпеки. Згідно з вимогами нормативних документів у сфері захисту інформації в інформаційних системах системи захисту інформації будують на основі математичних моделей захисту інформації. Використання цих моделей дає змогу теоретично обґрунтувати відповідність системи захисту інформації вимогам заданої політики безпеки.

Основні види математичних моделей безпеки наведено на рис 1.

Математичні

моделі

безпеки

Суб'єктно

орієнтована

модель

ізольованого

програмного

середовища

Безпека

інформаційних

потоків

Дискреційне

розмежування

доступу

Ролеве

розмежування

доступу

Мандатне

розмежування

доступу

Програмна

модель

Автоматна

модель

Імовірнісна

модель

Модель

Харрісона-

Руззо-

Ульмана

Класична

модель

Take-Grant

Модель

типізованих

матриць

доступу

Розширена

модель

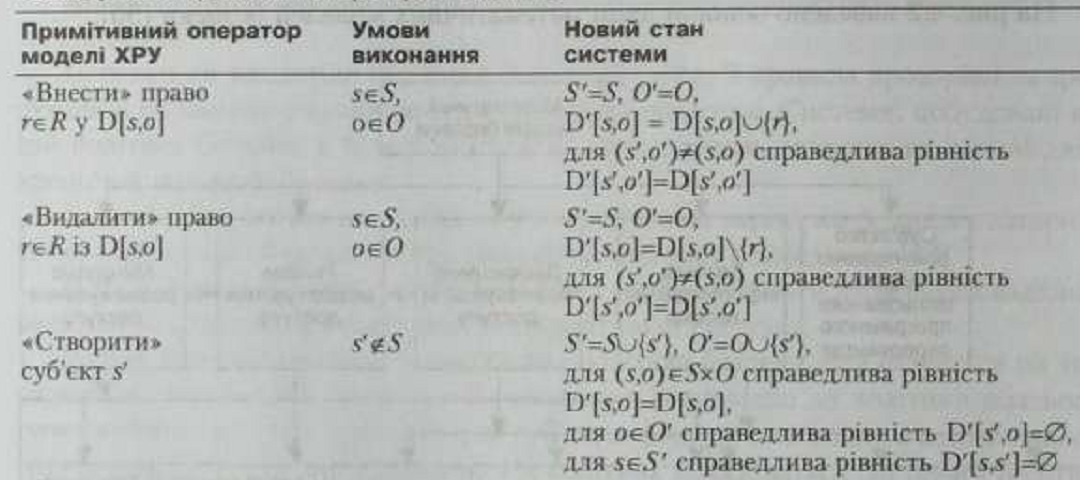
Take-Grant

Рис. 1. Математичні моделі безпеки

Модель Харрісона-Руззо-Ульмана (ХРУ) реалізує дискреційну політику.

Основні елементи цієї моделі наступні. Нехай О – множина об’єктів системи, S – множина суб’єктів системи, причому S ⊆O, матриця D розміром |S|x|O| - матриця доступу, рядки якої відповідають суб'єктам s, а стовпці - об'єктам о. Кожний елемент матриці доступу D[s,o]⊆R визначає права доступу суб’єкта s до об’єкта o, де R - множина прав доступу – read, write та інші.

Функціонування системи, побудованої на основі моделі ХРУ, здійснюється шляхом змін у матриці доступів D[s,o] із використанням примітивних операторів (рис. 2.).



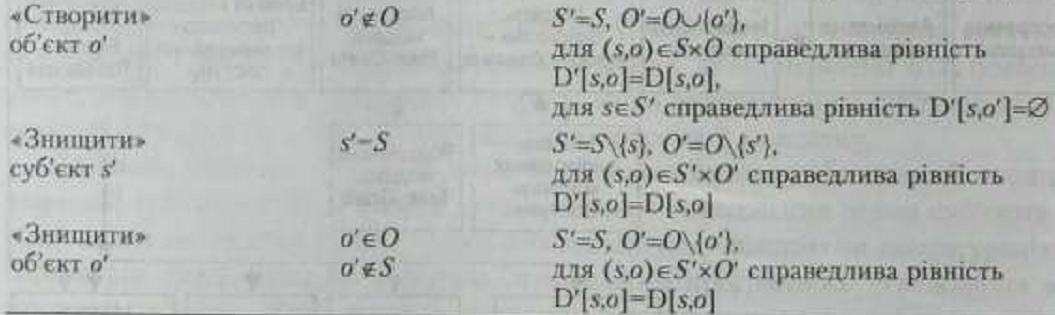


Рис. 2. Примітивні оператори моделі ХРУ

За допомогою примітивних операторів складають команди, якими описують перехід системи із стану q=(SOD) в результуючий стан q′=(S′O′D′)

Модель Take-Grant допускає наявність прав доступу не лише у суб’єктів до об'єктів, але й в об'єктів до об'єктів. Ця модель призначена для аналізу шляхів розповсюдження прав доступу за вихідним графом прав доступу в систе­мах дискреційного розмежування доступу.

Найпоширеніші моделі аналізу систем захисту, які реалізують мандату політику - це модель мандатної політики конфіден­ційності Белла — ЛаПадула та модель мандатної політики цілісності Біба, яка базується на моделі Белла – ЛаПадула.

Модель конфіденційності Белла — ЛаПадула є базовою моделлю мандатної політики безпеки. Зви­чайно цю модель застосовують для аналізу систем захисту інформації на імовір­ність наявності умов виникнення інформаційних потоків від об'єктів, що мають більший рівень конфіденційності до об'єктів із меншим рівнем конфіденційності.

Виконання умов цієї політики гарантує, що суб’єкт зможе отримати доступ до інформації лише за умови, що матиме на це достатні повноваження і будь-який суб'єкт (крім адміністратора, якому надано повноваження встановлювані рівні конфіденційності об'єктів) жодним чином не зможе здійснити перенесення даних із об’єкта з вищим рівнем конфіденційності в об'єкт, що має нижчий рівень конфіденційності (рис. 3.).

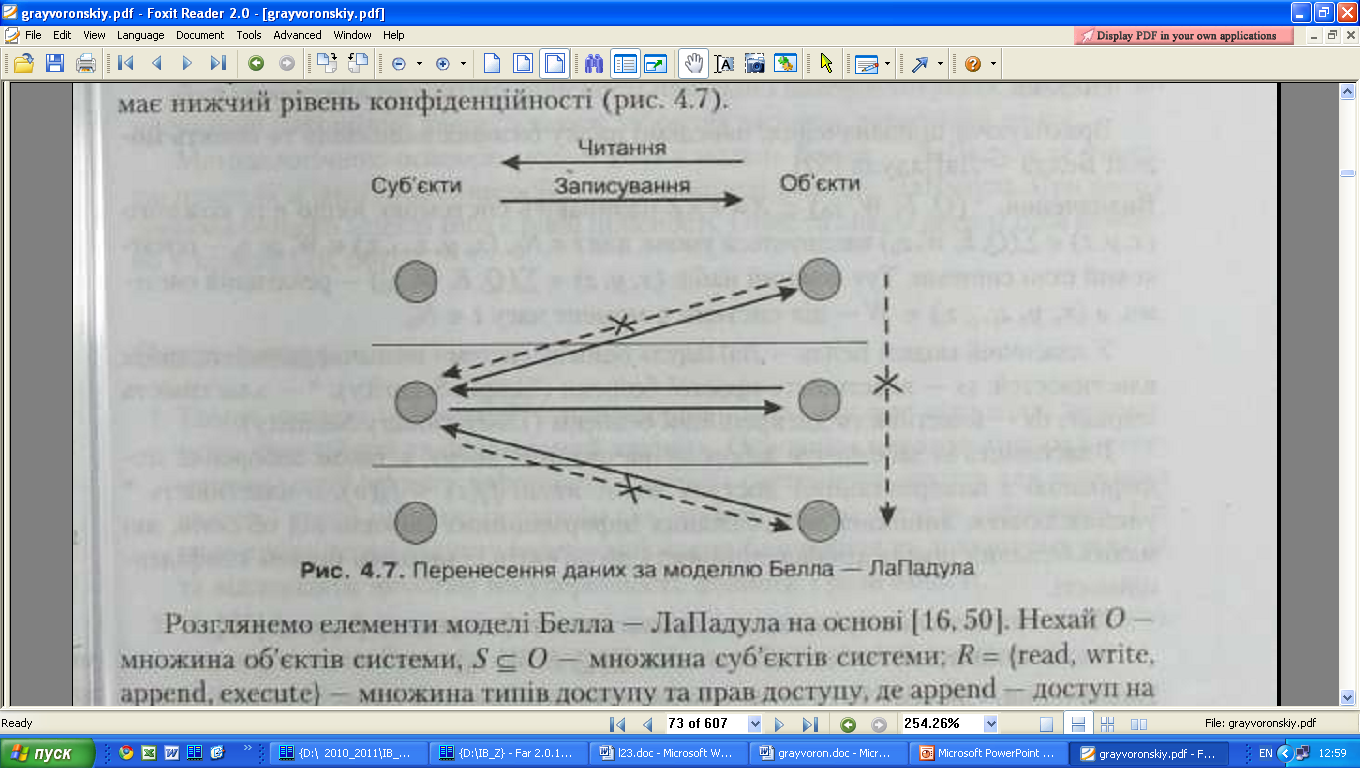


Рис. 3. Перенесення даних за моделлю мандатної політики конфіден­ційності Белла-ЛаПадула

*Модель цілісності Біба.*

На підміну від моделі конфіденційності Белла-ЛаПадула, модель безпеки Біба застосовують для забезпечення мандатної політики цілісності. Контроль цілісності інформації - важливе завдання системи захисту інформації. Найва­гомішу загрозу цілісності інформації (імовірність модифікації або знищення) мо­же становити записування інформації вверх суб'єктом із нижчого рівня безпеки інформації. Інколи читання інформації суб'єктом із низьким рівнем безпеки з об'єкта, що має більш високий рівень, також може нести загрозу іі цілісності.

Для уникнення цих загроз цілісності природно використовувати заборону за­писування інформації вверх, а також заборону читання інформації знизу.

Методологічною основою моделі Біба с модель Белла-ЛаПадула за умови, що правила моделі Біба є інверсією правил моделі Белла-ЛаПадула.

*Проблема захисту даних в хмарних обчисленнях*

**Управління проблемами безпеки за допомогою віртуальної пам'яті (ВП)**

І для IBM Blue Cloud, і Microsoft Windows Azure, технології віртуальних мА-шин розглядаються як платформа основних компонентів хмарних обчислень, а різ-ни­ця між Cloud Blue і Windows Azure полягає в тому, що віртуальна машина пра­цює на операційній системі [Linux](http://uk.wikipedia.org/wiki/Linux) або [Microsoft Windows](http://uk.wikipedia.org/wiki/Microsoft_Windows). Технологія віртуальних ма­шин демонструє очевидні переваги, вона сприяє роботі сервера, який залежить не від фізичного пристрою, а від віртуальних серверів. У віртуальних машинах, змі­на фізичних параметрів або їх переміщення не впливає на надані пос­та­чаль­ни­ком послуги. Якщо користувачеві необхідно більше послуг, постачальник може задо­вольнити потреби користувачів без втручань в устаткування.

Проте, віртуальний сервер з групи логічних серверів приносить багато проб­лем, пов'язаних з безпекою. Традиційний центр обробки та забезпечення безпеки да­них співвідноситься з межами апаратної платформи, тоді як хмарні обчислення мо­жуть належати серверу з числа віртуальних серверів, віртуальний сервер може ста­витися до різних груп логічних серверів, тому існує можливість взаємної атаки, що веде до загрози захисту віртуальних серверів.

Віртуальна машина, яка виходить за межі хмар, призводить до зникнення кордонів мережі, таким чином, це негативно позначається практично на всіх аспектах безпеки, а традиційна фізична ізоляція і апаратна інфраструктура безпеки не можуть захистити хмарний простір комп'ютера від взаємних атак віртуальних машин.

**Існування супер-користувача**

Для підприємств, які надають послуги, пов'язані з хмарними обчисленнями, і можуть здійснювати управління і технічне обслуговування даних, присутність супер-користувача значно спрощує функції управління даними, але з іншого боку створює серйозну загрозу для секретності користувачів.

Надсила - це двосторонній клинок, з одного боку він супроводжує зручностям користувачів, але в той же час являє собою загрозу для них. В епоху недоторканності приватного життя, особисті дані повинні бути по-справжньому захищені, і суть полягає в тому, що платформа хмарних обчислень, яка надає послуги захисту конфіденційності особистого життя, повинна бути перевірена на наявність дефектів. Не тільки окремі користувачі, а й організації мають аналогічні потенційні загрози, наприклад, секрети корпоративних користувачів і торгових підприємств, які зберігаються на платформі, можуть бути вкрадені. Тому використання прав супер-користувачів повинні контролюватися в хмарі.

**Сумісність Даних**

Середовище ОК - це динамічний простір, в якому дані користувача пере­да­ють­ся з центру обробки даних до клієнта користувача. Для системи, дані кори­с­ту­ва­ча змінюються постійно.

Можливість читання та запису даних залежить від ідентичності ауте­нти­фі­кації користувачів та параметрів доступу. У віртуальній машині, можуть зна­хо­ди­ти­ся різні дані користувача, які повинні підлягати чіткому контролю.

Традиційна модель управління доступом побудована на контурах ком­п'ю­те­ра, тому це призводить до слабкого контролю за читанням і зміною даних в роз­по­ді­лених обчислювальних системах. Ясно те, що традиційний контроль доступу не під­ходить для середовища хмарних обчислень. У середовищі хмарних обчислень тра­диційний механізм контролю за доступом володіє серйозними дефектами.

**Нова технологія**

Концепція хмарних обчислень побудована на новій конфігурації. Нова кон­фі­гурація складається з розмаїття нових технологій, таких як Hadoop, Hbase, що під­вищує продуктивність системи хмарних обчислень, але в той же час може при­зве­сти до ризику. У середовищі хмарних обчислень користувачі створюють багато ди­намічних віртуальних організацій, які в першу чергу ґрунтуються на довірі між орга­нізаціями більше, ніж на рівні індивідуалів. Тому з тими користувачами, які ґру­нтуються на вираженні обмежень на базі стратегії підтверджень, працювати набагато важче, це часто зустрічається на багатьох інтерактивних вузлах між віртуальними машинами, і є динамічним, непередбачуваним. Середовище хмарних обчислень дає користувачеві можливість "купити" повний доступ до ресурсів, які також збільшили ризик загрози безпеки.

**Вимоги до безпеки**

Після аналізу широко використовуваної технології хмарних обчислень - HDFS (HadoopDistributed File System), ми отримаємо вимоги до безпеки даних для хмарних обчислень. HDFS використовується в великомасштабних хмарних обчисленнях в типовій конфігурації розподіленої файлової системи, її основна мета полягає в управлінні комерційних апаратних засобів, у зв'язку з підтримкою Google, і перевагами відкритого вихідного коду, вона була застосована на основі можливостей хмарних обчислень. HDFS дуже схожа на існуючу розподілену файлову систему, таку як GFS (Google File System); вони мають ідентичні цілі, продуктивність, доступність і стабільність. HDFS спочатку використовувалися в мережевий пошуковій системі [Apache Nutch](http://uk.wikipedia.org/wiki/Apache_Nutch) і стала основою проекту [Apache Hadoop](http://uk.wikipedia.org/wiki/Apache_Hadoop).  
 HDFS використовувала провідний резервний режим. Як показано на рис.1 провідним називається Вузол імені (NameNode), який управляє простором імені файлів і контролює доступ до клієнта. Інший керуючий вузол Вузол даних (DataNode) контролює доступ до свого клієнта. У цій накопичувальній системі, файл поділяється на невеликі складові, Вузол імені відображає файлові блоки Вузлу даних зверху. У той час як HDFS не володіє сумісністю [POSIX](http://uk.wikipedia.org/wiki/POSIX), файлова система все одно підтримує створення, усунення, відкриття, закриття, читання, змінення або інші операції з файлами.

Аналізуючи HDFS, вимоги безпеки даних до хмарних обчислень можна розділити на наступні групи:

* Перевірка достовірності Логіна клієнта: Переважна більшість хмарних обчислень перевіряють браузер клієнта, такі як ІЕ, і проводять ідентифікацію користувача згідно із запитом програм хмарних обчислень для первинної потреби.
* Присутність одиничної помилки з Вузлом імені: якщо Вузол імені атакують або зламують, це може привести до катастрофічних наслідків в системі. Тому ефективність Вузла імені в хмарних обчисленнях і його дієвість це ключ до успіху в інформаційній безпеці, тому посилення захисту Вузла імені дуже важливо.
* Швидке відновлення блоків даних і контроль за правом читання / запис: Вузол даних (DataNode) - це вузол накопичення даних, де можливі невдачі і труднощі з доступом до даних. В даний час кожен блок накопичення даних в HDFS має, по крайній мірі, 3 репліки, які представляють резервну стратегію HDFS. Якщо необхідно забезпечити безпеку читання і запису даних, і HDFS не дала жодних докладних пояснень, необхідно забезпечити швидке відновлення і повністю контролювати операцію читання і запису даних, що не можна ігнорувати.

В доповнення до трьох вищезазначених вимог, необхідно також враховувати і інші можливості, такі як контроль доступу, шифрування файлів, таких як попит на хмарні обчислення моделі з питань безпеки даних.

**Модель захисту даних**

**Принцип захисту даних**

Вся процедура захисту даних побудована на конфіденційності, цілісності та доступності цих трьох основних принципів. Конфіденційність відноситься до так званої прихованої функції фактичних даних або інформації, особливо у військових та інших стратегічних сферах, конфіденційність даних одна з найжорсткіших вимог. У випадку хмарних обчислень, дані накопичуються в центрах обробки даних, де безпека та конфіденційність даних ще важливіші. Так звана цілісність даних в будь-якому вигляді не грає значної ролі для гарантії несанкціонованого видалення, зміни або пошкодження. Доступність даних означає, що користувачі можуть використовувати дані за рахунок використання потенціалу.

**Модель захисту даних**

Модель даних у хмарних обчисленнях можна описати за допомогою математичних формул наступним чином:

*Df* = (NameNode); (1)

*Kf* = *f* \* *Df*; (2)

С(.): огляд вузлів;

*Df* : розподілена матриця файлу *f*;

*Kf* : режим розподілу даних у вузлі даних;

*f* - файл, *f* можно описати як

*f* = {F (1), F (2), ... .. F (N)} що означає, що *f* - це множина n блоків файлів, де F(i)∩F(j)=∅,i≠j;I,j ∈1,2,3,…n;

*Df* являється нульовою матрицею,- це L \* L, де L - кількість вузлів даних.

Для підвищення безпеки даних хмарних обчислень, представляється Режим захисту даних для хмарних обчислень, який називається C2DSM. Його можна описати таким чином:

*D*'*f* = *CA* (Вузол імені) (3)

*Вf* = M.*D*'*f* (4)

*Kf* = E(*f*)*Df* (5)

*CA*(.): аутентифікація доступу до Вузлу імені;

*Df* : модель захисту конфіденційності матриці розподілу файлів;

M - рішення окремих матриць;

E(*f*) - зашифрований файл *f* блок за блоком, отримання зашифрованого файлового вектора.

У моделі використовувалася тришарова захисна структура системи, кожен шар якої виконує свої власні завдання для забезпечення захисту даних на всіх рівнях хмари.

* Перший шар відповідає за аутентифікацію користувачів, користувачів цифрових сертифікатів, виданих відповідними органами; управляє кодами доступу користувачів.
* Другий шар: відповідальний за шифрування даних користувача, а також захист конфіденційності користувачів певним способом.
* Третій шар: використання даних користувача для швидкого відновлення.

Захист всієї системи - це останній рівень даних користувача. За допомогою три­рі­в­невої структури аутентифікація користувача використовується для за­без­пе­чен­ня цілісності даних. Аутентифікація користувача може керувати даними за до­по­мо­гою таких операцій: додати, редагувати, видалити та ін. Якщо в системі ауте­нти­фікації користувача відбулося нелегальне втручання і небезпечний користувач вхо­дить в систему, шифрування файлів і захист конфіденційності можуть забе­з­пе­чи­ти цей рівень захисту.

На цьому рівні дані користувача шифруються у випадку, якщо ключ доступу був введений нелегально, через функцію захисту конфіденційності, небезпечний кори­стувач не зможе отримати повного доступу до інформації, що дуже важливо для захисту комерційних таємниць ділових користувачів в середовищі хмарних обчи­слень. Нарешті, швидке відновлення шару файлів за допомогою алгоритму від­новлення дає даними користувача можливість швидко відновлюватися навіть при великих пошкодженнях.

У даній моделі виділяють наступні теореми.

* Теорема 1.

Якщо дані не в повному порядку тоді користувач, втрачає їх.

Перевірка:

*Df*, якщо матриця розподілу файлів, то з формули (5), *Kf* є довжиною вектора L.

Якщо *Df*, не в повному порядку, *Df* можна перетворити в

*D*\**f*,*D*\**f* , що є (L-i) \* (L-i) матрицею, i≥1;

*Kf* стає L-I вектором довжини, які приводять до скорочення у визначеній моделі.

* Теорема 2.

Якщо \sum_{i=1}^n*Kf* (i) <n, то дані користувача будуть пошкоджені. *Kf* (i) позначає значення точки i файлового вектора *Kf*.

Перевіримо:

\sum_{i=1}^n*Kf* (i) означає кількість даних, які зберігаються у вузлі даних, з визначенням

*f* = {F (1), F (2), ... .. F (N)}, якщо F (i) не існують, і = 1,2 .... n, то приводить до помилки файлової пам’яті.

Якщо \sum_{i=1}^n*Kf* (i) <n, то буде і = 1,2 .... n, нехай *Kf* (i) = 0, F(i) не існує в *f*, файл пошкоджено.

* Теорема 3.

Якщо існує матриця J, J≠M, але *Df* = J.*Df* , відбувається витік даних користувача.

Перевіримо:

М – матриця конфіденційності користувача. За допомогою матриці M ми можемо отримати *Df*.

Якби існувала J, то незаконний користувач міг би отримати *Df* за допомогою J. Тоді б стався витік особистих даних.

**7) Шифрування даних**

Шифрува́ння — оборотне перетворення даних, з метою приховання інформації. Шифрування з'явилось близько 4 тис. років назад. Першим відомим зразком шифру вважається єгипетський текст, створений приблизно в 1900 р. до н. е., в якому замість звичних для єгиптян ієрогліфів використовувались інші символи.

Методи шифрування: симетричний та асиметричний.

Симетричне шифрування

В симетричному шифруванні один і той самий ключ (що зберігається в секреті) використовується як для шифрування, так і для розшифрування. Розроблено ефективні (швидкі й надійні) методи шифрування.

Переваги

Шифри із симетричним ключем спроектовані так, щоб мати велику пропускну здатність. Ключі для шифрів із симетричним ключем відносно короткі

Шифри із симетричним ключем можна використати як примітиви для побудови різних криптографічних механізмів включно з псевдовипадковими генераторами чисел, геш-функціями, обчислювально ефективних схем підпису та ін.

Шифри із симетричним ключем можна комбінувати для отримання сильніших шифрів

Недоліки

При зв'язку між двома особами, ключ потрібно тримати в секреті на обох кінцях. У великій мережі потрібно опікуватись багатьма ключами. У зв'язку між двома особами криптографічна практика вимагає частої зміни ключів

Асиметричне шифрування

Проблемою симетричного шифрування є необхідність передачі ключа, для розшифрування інформації, таким чином ключ може бути перехоплений кимось іншим.

Будь хто, знаючи секретний ключ, може розшифрувати інформацію. Тоді як в асиметричному шифруванні є два пов'язаних ключа — пара ключів. Відкритий ключ (англ. public key) — публічний, до нього повинні мати доступ всі ті, хто матиме потребу зашифрувати інформацію. Тоді як закритий ключ — приватний ключ (англ. private key), повинен бути доступним лише тому хто має право розшифрувати інформацію, за своїм розміром він значно більший від секретного ключа симетричного шифрування[1].

Будь-яку інформацію, зашифровану за допомогою відкритого ключа можна розшифрувати лише застосовуючи той самий алгоритм, але з використанням відповідного приватного ключа. Також всю інформацію, зашифровану за допомогою приватного ключа, можна розшифрувати лише за допомогою відповідного відкритого ключа. Це означає, що немає необхідності хвилюватись за передачу ключа, відкритий ключ повинен бути публічним. Але асиметричне шифрування є значно повільнішим від симетричного. Також потребує значно більше обчислювальної потужності як для шифрування, так і для розшифрування інформації.

Через вади в швидкодії асиметричного методу цей метод доводиться використовувати разом з симетричним (асиметричні методи на 3 - 4 порядки повільніші). Так, для розв'язання задачі ефективного шифрування з передаванням секретного ключа, використаного відправником, інформація спочатку симетрично зашифровується випадковим ключем, потім цей ключ зашифровують відкритим асиметричним ключем одержувача, після чого повідомлення і ключ відправляються по мережі.

***Шифрування даних на рівні файлових систем***.

Підтримка шифрувальних файлових систем у Linux

У Linux є кілька реалізацій файлових систем із підтримкою шифрування да­них. Найвідоміші з них CFS і TCFS. Підтримка файлової системи CFS реалізована в­ режимі користувача і дає змогу шифрувати дані на будь якій наявній файловій сис­темі ціною певної втрати продуктивності. Як алгоритм шифрування ви­ко­рис­то­вують потрійний DES . Шифрування може бути застосоване для окремих каталогів фай­лів. Підтримка системи TCFS реалізована в режимі ядра , що дає змогу досягти ви­щої продуктивності і ступеня захисту. Встановлення підтримки цієї файлової сис­теми , однак , складніше (потрібні внесення змін в код ядра Linux і його пе­ре­ком­піляції) . Ця файлова система реалізує концепцію динамічних модулів шиф­ру­ван­ня , надаючи користувачу можливість вибору алгоритму і режиму шифрування, які будуть використовані для конкретної файлової системи окремого каталогу або фай­ла.

Шифрувальна файлова система Windows XP

Засобом підтримки шифрування файлів ОС лінії Windows XP описані під загальною назвою шифрувальної файлової системи . Для цього використовують драйвер файлової системи розташований над драйвером NTFS.

Принципи роботи EFS

Реалізація EFS – це гібридна криптосистема із кількома рівнями шифрування.

1. Безпосередньо для шифрування даних файла використовують симетричний алго­ритм (посилений аналог DES , можливе використання інших алгоритмів ). Ключ для нього генерують випадково під час кожної спроби зашифрувати файл.

2. Для шифрування FEK використовують алгоритм із відкритим ключем (RSA). Для кожного користувача генерують пару RSA – ключів, при цьому FEK шиф­рують відкритим ключем цієї пари. Результат шифрування FEK зберігають у за­го­лов­ку файла . Крім того передбачено можливість дешифрування файла довіреною осо­бою у разі втрати ключа користувача. Для цього результат шифрування FEK від­критими ключами довірених агентів також зберігають у заголовку файлів.

3. Відкритий ключ користувача зберігають у вигляді сертифіката у сховищі сер­ти­фі­катів, розташованому в домашньому каталозі користувача на локальному ком­п’ю­тері. Крім того у цьому сховищі містяться сертифікати всіх агентів від­нов.­лен­ня.

4. Для шифрування закритого ключа користувача використовують симетричний алго­ритм RC 4 із ключем , який система генерує випадково і періодично обновлює. Цей ключ називають майстер – ключем. Результат шифрування закритого ключа май­стер – ключем зберігають на файловій системі в домашньому каталозі кори­сту­ва­ча.

5. Для шифрування майстер - ключа теж використовують симетричний алгоритм RC4, але із більшою довжиною ключа. Його генерують на застосуванні одно­сто­рон­ньої хеш – функції SHA-1 до даних облікового запису користувача. Результат шиф­рування майстер – ключа цим ключем також зберігають на файловій системі.

Програмний інтерфейс EFS

Для шифрування файла або каталогу використовують EncryptFile , а для де­шиф­рування - DecryptFile.

EncryptFile (“myfile.txt”):

DecryptFile(“myfile.txt”. 0):

Для перевірки того , чи файл зашифрований , використовують функцію File-EncryptionStatus():

BOOL FileEncryptionStatus(LPCTSTR fname. LPDWORD status):

де: fname – імя файла або каталогу ;

status – покажчик на змінну, у яку заноситься інформація про підтримку шиф­ру­ван­ня для файла (FILE\_ENSCRYPTED файл може бути зашифрований, FILE\_IS\_ENSCRYPTED – файл зашифрований ; інші значення показують , що шиф­рування не підтримується).

Ця функція повертає FALSE , якщо під час перевірки виникла помилка. DWORD stutus:

If { FileEncryptionStatus ((“myfile.txt”.&status}} {

If ( status == FILE\_IS\_ENSCRYPTED ) print ( “ Файл зашифрований\n”):

}

Для деяких каталогів має сенс заборонити шифрування. Для цього необхідно помістити в такий каталог файл desktop.ini з інформацією:

[Encryption]

Disable=1

Механізм EFS

EFS використовує засоби підтримки шифрування, введені Microsoft ще в Windows NT 4. При першому шифрування файлу EFS призначає профілю ко­рис­ту­ва­ча, шифрувального цей файл, криптографічну пару - закритий і відк­ри­тий ключі.

Користувачі можуть шифрувати файли за допомогою Windows Explorer; для цього потрібно відкрити діалогове вікно Властивості стосовно потрібного файлу, натиснути кнопку Інші та встановити прапорець Шифрувати вміст для захисту да­них. Користувачі також можуть шифрувати файли здопомогою утиліти коман­дно­го рядка cipber.Windows 2000 автоматично шифру єфайли в каталогах, позначених за­шиф­рованими. При шифрування файлу EFS генерує випадкове число, зване шиф­рувальним ключем файлу (fileencryption key, FEK8). EFS використовує FEK для шифрування вмісту файлуза більш стійкого варіанту DES3 (Data Encryption Standard) - DESX4. EFSзберігає FEK разом з самим файлом, але FEK шифрується за алгоритмом RSA -шифрування на основі відкритого ключа.

Після виконання EFS цих дійфайл захищений: інші користувачі не зможуть роз­ши­фрувати дані безрозшифроване FEK файлу, а FEK вони не зможуть роз­шиф­ру­вати без закритогоключа користувача - власника файлу. Для шифрування FEK ви­користовується алгоритм криптографічного пари, а дляшифрування файлових да­них - DESX, алгоритм симетричного шифрування (у ньомузастосовується один і той же ключ для шифрування і дешифрування). Як правило,алгоритми си­мет­рич­но­го шифрування працюють дуже швидко, що робить їхвідповідними для шиф­ру­ван­ня великих об'ємів даних, зокрема файлових. Однак у алгоритмів симетричного шиф­рування є одна слабка сторона:зашифрований ними файл можна розкрити, отри­мавши ключ. Якщо кілька чоловікзбирається користуватися одним файлом, за­хищеним тільки DESX, кожному зних знадобиться доступ до FEK файлу. Оче­вид­но, що незашифрований FEK --серйозна загроза безпеці. Але шифрування FEK все одно не вирішує проблему, оскільки в цьому випадку кільком людям до­во­диться користуватисяодним і тим же ключем розшифровки FEK.

Захист FEK склад­на проблема, для розв'язання якої EFS використовує ту час­тину своєї крип­тог­рафічного архітектури, яка спирається на техно­логії шиф­ру­ван­ня з відкритим клю­чем. Шифрування FEK на індивідуальній основі дозволяє кіль­ком особам спі­ль­но використовувати зашифрований файл. EFS може заши­фру­ва­ти FEK файлу за до­помогою відкритого ключа кожного користувачаі зберігати їх FEK разом з фай­лом. Кожен може отримати доступ до відкритого ключа ко­рис­ту­вача, але ніхто не змо­же розшифрувати з його допомогою дані, зашифровані з цьо­го ключа. Єдиний спосіб розшифровки файлаполягає у використанні опе­ра­цій­ною системою закритого ключа, якийвона.

Як правило, зберігає в безпечному міс­ці. Закритий ключ допо­магає ­роз­шиф­ру­вати потрібний FEK файлу. Windows 2000 збе­рігає закриті ключі нажорсткому дис­ку, що не дуже безпечно, але в наступних ви­пусках операційної системи кори­с­ту­вачі зможуть зберігати закриті ключі на ком­пактних носіях на зразок смарт-карт. Алго­ритми на основі відкритого ключа звичайно досить повільні. Тому вони ви­ко­рис­товується EFS тільки для шифрування FEK. Поділ ключів на відкритий і зак­ри­тий трохи спрощує управління ключами в порівнянні з таким в алгоритмах си­мет­ри­чног ошифрування і вирішує дилему, пов'язану із захистом FEK. EFS реа­лі­зо­ва­на у вигляді драйвера пристрою, що працює в режимі ядра ітісно пов'язаного з драй­вером файлової системи NTFS. Кожного разу, коли NTFS зустрічає заши­фро­ва­ний файл, вона викликає функції з драйвера EFS,зареєстровані їм в NTFS при іні­ціалізації EFS. Опції EFSздійснюють шифрування і розшифровку файлових да­них по мірі зверненнядодатків до шифрованих файлів. Хоча EFS зберігає FEK ра­зом з даними файлу, FEK шифрується за допомогою відкритого ключа інди­ві­дуаль­ного користувача. Для шифрування або розшифрування файлових даних EFS пови­нна розшифрувати FEK файлу, звертаючись до криптографічних сервісів ре­жи­му користувача.

**СТАНДАРТ ШИФРУВАННЯ**

Стандарт шифрування даних (DES) — блоковий шифр із симетричними ключами, розроблений Національним Інститутом Стандартів і Технології (NIST – National Institute of Standards and Technology).

У l973 року NIST видав запит для розробки пропозиції національної криптографічної системи із симетричними ключами.

Запропонована IBM модифікація проекту, названа Lucifer, була прийнята як DES. DES були видані в ескізному виді у Федеральному Регістрі в березні 1975 року якФедеральний Стандарт Обробки Інформації (FIPS – Federal Information Processing Standard).

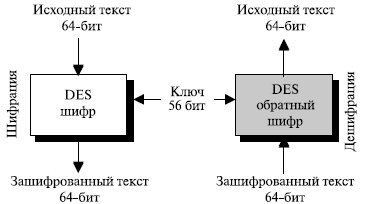
Після публікації ескіз строго критикувався із двох причин. Перша: критикувалася сумнівно маленька довжина ключа (тільки 56 бітів), що могло зробити шифр уразливим до атаки "грубої силою". Друга причина: критики були стурбовані деякою схованою побудовою внутрішньої структури DES.

Вони підозрювали, що деяка частина структури ( S-Блоки) може мати сховану лазівку, яка дозволить розшифровувати повідомлення без ключа. Згодом проектувальники IBM повідомили, що внутрішня структура була дороблена, щоб запобігти криптоаналіз.

DES був нарешті виданий як FIPS 46 у Федеральному Регістрі в січні 1977 року. Однак FIPS оголосив DES як стандарт для використання в неофіційних додатках. DES був найбільше широко використовуваним блоковим шифром із симетричними ключами, починаючи з його публікації. Пізніше NIST запропонував новий стандарт (FIPS 46-3), який рекомендує використання потрійного DES (трикратно повторений шифр DES) для майбутніх додатків. Як ми побачимо далі, у лекціях 9-10, передбачається, що більш новий стандарт AES замінить DES.

**1. Основні положення**

Як показано на рис. 1. , DES — блоковий шифр.

  
Рис. 1. Шифрування й дешифрування в DES

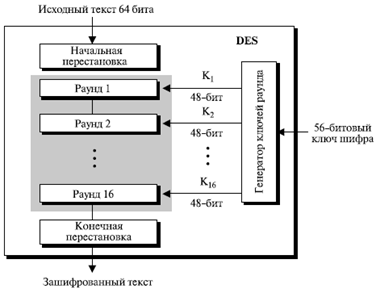
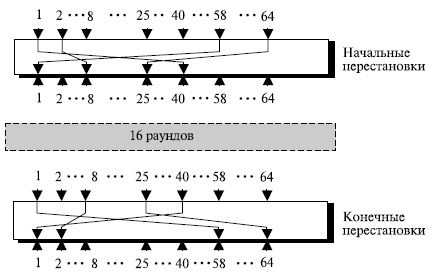
На стороні шифрування DES ухвалює 64-бітовий вихідний текст і породжує 64-бітовий зашифрований текст; на стороні дешифрування DES ухвалює 64-бітовий зашифрований текст і породжує 64-бітовий вихідний текст. На обох сторонах для шифрування й дешифрування застосовується той самий 56-бітовий ключ.

**2. Структура DES**

Розглянемо спочатку шифрування, а потім дешифрування. Процес шифрування складається із двох перестановок ( P-Блоки) — вони називаються початкові й кінцеві перестановки, — і шістнадцяти раундів Файстеля.

**Початкові й кінцеві перестановки**

Кожна з перестановок ухвалює 64-бітовий вхід і переставляє його елементи за заданим правилом. Ці перестановки — прямі перестановки без ключів, які інверсні один одному. Наприклад, у початковій перестановці 58-й біт на вході переходить у перший біт на виході. Аналогічно, у кінцевій перестановці перший вхідний біт переходить в 58-й біт на виході. Інакше кажучи, якщо між цими двома перестановками не існує раунду, 58-й біт, що зробив на вхід обладнання початкової перестановки, буде доставлений на 58-й вихід фінальною перестановкою.

  
  
Рис. 2. Структура DES

Правила перестановки для цього P-Блоку показано в таблице 1. Таблицю можна представити як 64-елементний масив. Помітимо, що значення кожного елемента визначає номер вхідного порту, а порядковий номер (індекс) елемента визначає номер вихідного порту.

**Таблиця 1.** **Таблиця початкових і кінцевих перестановок**

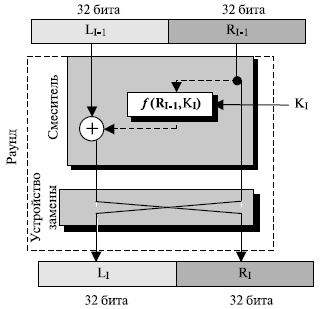
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Початкові перестановки** | | | | | | | | **Кінцеві перестановки** | | | | | | | |
| 58 | 50 | 42 | 34 | 26 | 18 | 10 | 02 | 40 | 08 | 48 | 16 | 56 | 24 | 64 | 32 |
| 60 | 52 | 44 | 36 | 28 | 20 | 12 | 04 | 39 | 07 | 47 | 15 | 55 | 23 | 63 | 31 |
| 62 | 54 | 46 | 38 | 30 | 22 | 14 | 06 | 38 | 06 | 46 | 14 | 54 | 22 | 62 | 30 |
| 64 | 56 | 48 | 40 | 32 | 24 | 16 | 08 | 37 | 05 | 45 | 13 | 53 | 21 | 61 | 29 |
| 57 | 49 | 41 | 33 | 25 | 17 | 09 | 01 | 36 | 04 | 44 | 12 | 52 | 20 | 60 | 28 |
| 59 | 51 | 43 | 35 | 27 | 19 | 11 | 03 | 35 | 03 | 43 | 11 | 51 | 19 | 59 | 27 |
| 61 | 53 | 45 | 37 | 29 | 21 | 13 | 05 | 34 | 02 | 42 | 10 | 50 | 18 | 58 | 26 |
| 63 | 55 | 47 | 39 | 31 | 23 | 15 | 07 | 33 | 01 | 41 | 09 | 49 | 17 | 57 | 25 |

Ці дві перестановки не мають ніякого значення для криптографії в DES. Обидві перестановки – без ключів і обумовлені. Причина, чому вони включені в DES, не ясна й не була зазначена проектувальниками DES. Можна припустити, що DES був проектом, який передбачалося реалізувати в апаратних засобах (на чипах), і що ці дві складні перестановки повинні були утруднити програмне моделювання механізму шифрування.

**Початкові й кінцеві перестановки – це прямі P-**Блоки**, які інверсні один одному. Вони не мають значення для криптографії DES.**

**Раунди**

DES використовує 16 раундів. Кожний раунд DES застосовує шифр Файстеля, як це показане на рис. 2.

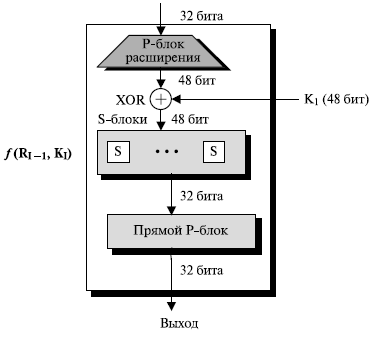
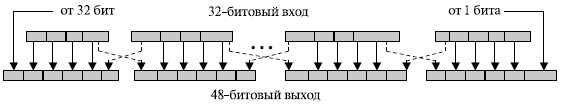
  
Рис. 3. Раунд в DES (сторона шифрування)

Раунд ухвалює LI-1 RI-1 від попереднього раунду (або початкового блоку перестановки) і створює для наступного раунду LI І RI, які надходять на наступний раунд (або кінцевий блок перестановки). Можна прийняти, що кожний раунд має два елементи шифру (змішувач і обладнання заміни). Кожний із цих елементів є оборотним. Обладнання заміни — очевидно оборотне, воно міняє місцями ліву половину тексту із правою половиною. Змішувач є оборотним, тому що операція, ЩО ВИКЛЮЧАЄ АБО оборотна. Усі необоротні елементи зосереджені у функції f (RI-1,KI).

**Функція DES**

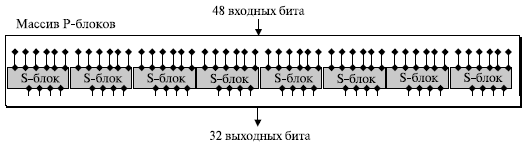
Основний блок DES — функція DES. Функція DES за допомогою 48-бітового ключа зашифровує 32 самих правих біт RI-1, щоб одержати на виході 32-бітове слово. Ця функція містить, як це показане на рис. 4, чотири секції: відбілювач (whitener), P-Блок розширення, групу S-Блоків і прямій P-Блок.

**P-Блок розширення.**Тому що вхід RI-1 має довжину 32 біта, а ключ KI — довжину 48 бітів, ми спочатку повинні розширити RI-1 до 48 біт. RI-1 розділяється на 9 секцій по 4 біта. Кожна секція на 4 біта розширюється до 6 біт. Ця перестановка розширення випливає по заздалегідь певних правилах. Для секції значення вхідних біт 1, 2, 3 і 4 привласнюються биткам 2, 3, 4 і 5 відповідно на виході. Вихідний біт 1 формується на основі вхідного біта 4 з попередньої секції; біт виходу 6 формується з біта 1 у наступній секції. Якщо секції 1 і 8 розглядати як сусідні секції, то ті ж самі правила застосовуються до биток 1 і 32. Рисунок 4 показує входи й виходи в перестановці розширення.

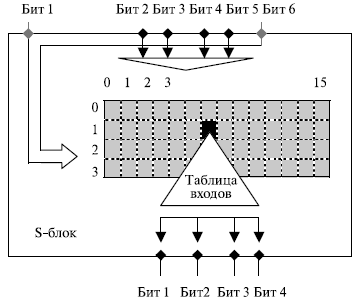
  
  
Рис. 4. Функція DES

**Відбілювач (whitener).**Після розширення DES використовує операцію XOR (, ЩО ВИКЛЮЧАЄ АБО) над розширеною частиною правої секції й ключем раунду. Помітимо, що права секція й ключ мають довжину 48 біт. Також помітимо, що ключ раунду використовує тільки цю операцію.

**S-Блоки.**S-Блоки змішують інформацію (операція перемішування). DES використовує S-Блоки, кожний з 6-ю вхідними бітами й 4-мя вихідними.

  
Рис. 5. S-Блок

Дані з 48 бітів від другої операції DES розділені на вісім шматків по 6 бітів, і кожний шматок надходить у блок. Результат кожного блоку — шматок на 4 біта; коли вони об'єднані, результат виражається в 32-бітовому тексті. Підстановка в кожному блоці випливає по заздалегідь певних правилах, заснованих на таблиці з 4-х рядків і 16-ти стовпців. Комбінація бітів 1 і 6 на вході визначає одну із чотирьох рядків; комбінація бітів від 2-го до 5-го визначає один із шістнадцяти стовпців, як показано на рис. . Далі ми пояснимо це прикладами.

  
Рис. 6. Схема S-Блоку

Оскільки для кожного S-Блоку є власна таблиця, необхідно мати вісім таблиць, наприклад таких, як це показано в таблицях 8.3-8.10. Значення входу (номер рядка й номер стовпця) і значення виходу даються як десяткові номери, щоб заощадити місце на сторінці. У реальності вони можуть бути замінені двійковими числами.

**Таблиця 2. S-Блок 1**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** |
| **0** | 14 | 04 | 13 | 01 | 02 | 15 | 11 | 08 | 03 | 10 | 06 | 12 | 05 | 09 | 00 | 07 |
| **1** | 00 | 15 | 07 | 04 | 14 | 02 | 13 | 10 | 03 | 06 | 12 | 11 | 09 | 05 | 03 | 08 |
| **2** | 04 | 01 | 14 | 07 | 13 | 06 | 02 | 11 | 15 | 12 | 09 | 07 | 03 | 10 | 05 | 00 |
| **3** | 15 | 12 | 08 | 02 | 04 | 09 | 01 | 07 | 05 | 11 | 03 | 14 | 10 | 00 | 06 | 13 |

**Пряма перестановка** — остання операція у функції DES — пряма перестановка з 32 бітами на вході й 32 бітами на виході. Відносини " вхід-вихід" для цієї операції показано в таблиці 3. Вони випливають тим же самим загальним правилам перестановки, що як і попередні таблиці. Наприклад, сьомий біт входу стає другим бітом виходу.

**Таблиця 3. Таблиця прямої перестановки**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 16 | 07 | 20 | 21 | 29 | 12 | 28 | 17 |
| 01 | 15 | 23 | 26 | 05 | 18 | 31 | 10 |
| 02 | 08 | 24 | 14 | 32 | 27 | 03 | 09 |
| 19 | 13 | 30 | 06 | 22 | 11 | 04 | 25 |

**Шифр і зворотний шифр**

Використовуючи змішувач і обладнання заміни, ми можемо створити шифр і зворотний шифр для кожного з 16-ти раундів. Шифр використовується на стороні шифрування; зворотний шифр — на стороні дешифрування. Алгоритми створення шифру й зворотного шифру аналогічні.

**Перший спосіб**

Один з методів, щоб досягти поставленої мети (шифрування й зворотне шифрування), полягає в тому, щоб зробити останній раунд одмінним від інших; він буде містити тільки змішувач і не буде містити обладнання заміни.

**У першому методі останній раунд не має заміни.**

**Альтернативний спосіб**

При першому способі раунд 16 відрізняється від інших раундів тим, що там не застосовується обладнання заміни. Це необхідно, щоб зробити останній і перший змішувачі в шифрі однаковими. Ми можемо робити всі 16 раундів однаковими, додаючи до 16-му раунду додаткове обладнання заміни (два обладнання заміни дозволяють нейтралізувати один одного).

**Генерація ключів**

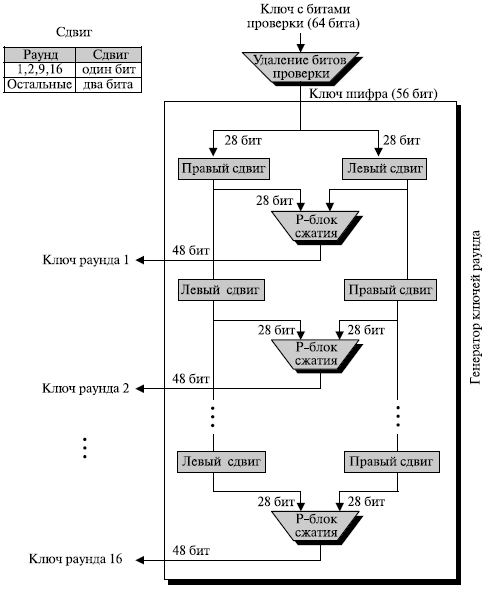
**Генератор ключів** створює шістнадцять ключів по 48 бітів із ключа шифру на 56 бітів. Однак ключ шифру звичайно дається як ключ із 64-х бітів, у якім 8 додаткових бітів є бітами перевірки. Вони відкидаються перед фактичним процесом генерації ключів.

**Видалення бітів перевірки**

Попередній процес перед розширенням ключів — перестановка стиску, яку ми називаємо **видаленням бітів перевірки.**Він видаляє біти парності (біти 8, 16, 24, 32..., 64) з 64-бітового ключа й переставляє іншу частину бітів згідно з таблице 4. значення, що залишається, на 56 бітів — фактичний ключ шифру, який використовується, щоб генерувати ключі раунду. Біти віддаляються за допомогою перестановки ( P-Блоку стиску), як це показано в таблице 4.

**Таблиця 4. Таблиця видалення перевірочних бітів**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 57 | 49 | 41 | 33 | 25 | 17 | 09 | 01 |
| 58 | 50 | 42 | 34 | 26 | 18 | 10 | 02 |
| 59 | 51 | 43 | 35 | 27 | 19 | 11 | 03 |
| 60 | 52 | 44 | 36 | 63 | 55 | 47 | 39 |
| 31 | 23 | 15 | 07 | 62 | 54 | 46 | 37 |
| 30 | 22 | 14 | 06 | 61 | 53 | 45 | 37 |
| 29 | 21 | 13 | 05 | 28 | 20 | 12 | 04 |

  
Рис. 7. Генерація ключів

**Зрушення вліво**

Після прямої перестановки ключ розділений на дві частини по 28 бітів. Кожна частина зрушується вліво (циклічне зрушення) на один або два біти. У раундах 1, 2, 9 і 16 зсув – на один біт, в інших раундах — на два біти. Потім ці дві частини поєднуються, щоб створити частина в 56 біт. Таблиця 5 показує число зрушень маніпуляцій для кожного раунду.

**Таблиця 5. Число, що зрушуються біт**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Раунд | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| Число біт | 1 | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 1 |

**Перестановка стиску**

Перестановка стиску ( P-Блок) змінює 56 бітів на 48 бітів, які використовуються для формування ключа раунду. Перестановка стиску показано в таблице 6.

**Таблиця 6. Таблиця стиску ключа**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 14 | 17 | 11 | 24 | 01 | 05 | 03 | 28 |
| 15 | 06 | 21 | 10 | 23 | 19 | 12 | 04 |
| 26 | 08 | 16 | 07 | 27 | 20 | 13 | 02 |
| 41 | 52 | 31 | 37 | 47 | 55 | 30 | 40 |
| 51 | 45 | 33 | 48 | 44 | 49 | 39 | 56 |
| 34 | 53 | 46 | 42 | 50 | 36 | 29 | 32 |

**Аналіз DES**

DES був підданий ретельному аналізу. Були проведені випробування, щоб виміряти інтенсивність деяких бажаних властивостей у блоковому шифрі. Елементи DES пройшли дослідження на відповідність деяким критеріям. Нижче ми обговоримо деякі з них.

**Властивості**

Дві бажані властивості блокового шифру — ефект лавини й закінченість.

**Лавинний ефект**

**Лавинний ефект** означає, що невеликі зміни у вихідному тексті (або ключі) можуть викликати значні зміни в зашифрованому тексті. Було доведено, що DES має всі ознаки цієї властивості.

**Ефект повноти**

Ефект повноти полягає в тому, що кожний біт зашифрованого тексту повинен залежати від багатьох бітів вихідного тексту. Розсіювання й перемішування, зроблене P-Блоками й S-Блоками в DES, указує на дуже сильний ефект повноти.

**Число раундів**

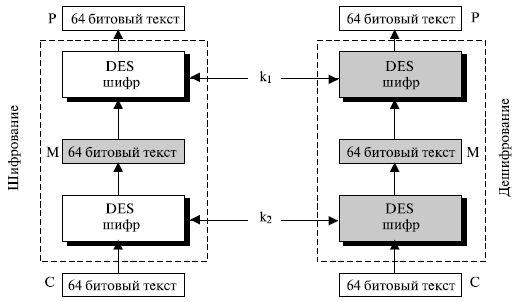
DES використовують шістнадцять раундів шифру Файстеля. Доведене, що після того як кожний текст зашифровано вісім раундів, кожний біт зашифрованого тексту — функція кожного біта вихідного тексту й кожного ключового біта. Зашифрований текст — повністю випадкова функція вихідного тексту й зашифрованого тексту. Звідси начебто б випливає, що восьми раундів повинне бути досить для гарного шифрування. Однак експерименти показують, що деякі версії DES з менш чим шістнадцятьома раундами більш уразливі до атак знання вихідного тексту, чому до атаки грубої сили, яка вимагає використання шістнадцяти раундів DES.

**3. Багаторазове використання DES**

**Дворазовий DES**

Перший підхід полягає в тому, щоб використовувати **дворазовий DES (2DES).** При цьому підході ми застосовуємо два типи шифрів DES для шифрування й два типи зворотних шифрів для дешифрування. Кожний тип використовує різний ключ, що означає, що розмір ключа тепер подвоївся (112 бітів). Однак дворазовий DES уразливий до атаки знання відкритого тексту, як це обговорюється в наступному розділі.

На перший погляд дворазові DES збільшують число випробувань при пошуку ключа від 256 (в однократному DES) до 2112 (у дворазовому DES). Однак при використанні атаки знання вихідного тексту, називаною **атакою відомості до середини,**можна довести, що дворазовий DES поліпшує цю стійкість ( до 257 по випробуваннях), але не надзвичайно (до 2112). Рисунок 8 показує діаграму для дворазового DES. Аліса використовує два ключі, k1 і k2, щоб зашифровувати вихідний текст P у зашифрований текст C; Боб використовує зашифрований текст C і два ключі, k2 і k1, для відновлення P.

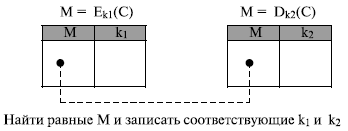
  
Рис. 8. Атака відомості до середини у дворазовому DES

У середній крапці М — текст, створений першим шифруванням або першим дешифруванням. Для забезпечення правильної роботи він повинен бути однаковим для шифрування й дешифрування. Інакше кажучи, ми маємо два відносини:

M = EK1(P) і M = EK2(C)

Припустимо, що Єва перехопила попередню пару P і C (атака знання вихідного тексту). Базуючись на першім відношенні зі згаданих вище, Єва зашифровує P, використовуючи всі можливі значення(256) k1, і записує всі значення, отримані для М. Базуючись на других відносинах, згаданих вище, Єва розшифровує C, використовуючи всі можливі значення (256) k2. Вона записує всі значення, отримані для М. Далі Єва створює дві таблиці, відсортовані згідно зі значеннями M. Вона порівнює значення для М, поки не знаходить ті пари k1 і k2, для яких значення М є тим самим в обох таблицях ( як показано на рис. 9). Зверніть увагу, що повинна бути принаймні одна пара, тому що вона робить вичерпний пошук комбінації двох ключів.

1. Якщо є тільки одна відповідність. Єва знайшла два ключі (k1 і k2). Якщо є більше чому один кандидат, Єва переміщається в наступний крок.
2. Вона бере іншу перехоплену пару зашифрованого тексту й вихідного тексту й використовує кожного кандидата для одержання пари ключів, щоб установити, чи може вона одержати зашифрований текст із вихідного тексту. Якщо вона знаходить більше чому одного кандидата у вигляді пари ключів, вона повторює крок 2, поки, нарешті, не знаходить унікальну пару.

  
Рис. 9. Таблиці для атаки "відомості до середини"

Було доведено, що після застосування другого кроку до декільком перехопленим парам "зашифрований текст — вихідний текст" ключі були знайдені. Це означає, що замість того щоб використовувати пошук ключів за допомогою 2112 випробувань, Єва використовує 256 випробувань пошуку ключа й перевіряє два рази (трохи більше випробувань потрібно, якщо знайдений на першому кроці єдиний кандидат). Інакше кажучи, рухаючись від однократного DES до дворазового DES, ми збільшили об'єм випробувань від 256 до 257 (а не до 2112, як це видасться при поверхневому підході).

**Трикратний DES**

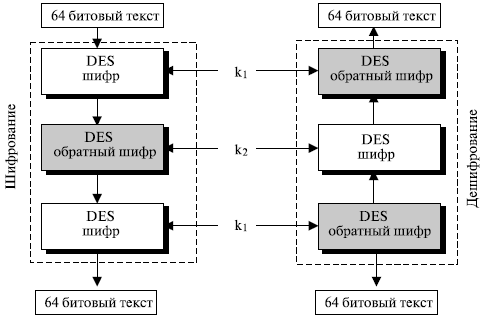
Для того щоб поліпшити безпеку DES, був запропонований **трикратний DES (3DES).**Він використовує три каскади DES для шифрування й дешифрування. Сьогодні використовуються дві версії трикратних DES: трикратний DES із двома ключами й трикратний DES із трьома ключами.

**Трикратний DES із двома ключами**

**У трикратному DES із двома ключами**є тільки два ключі: k1 і k2. Перший і третій каскади використовують k1; другий каскад використовує k2. Щоб зробити трикратний DES сумісним з DES, середній каскад застосовує дешифрування (зворотний шифр) на стороні шифрування й шифрування (шифр) на стороні дешифрування. Таким способом повідомлення, зашифроване Des-Ключем k, може бути розшифроване трикратним DES, якщо k1 = k2 = k. Хоча трикратний DES із двома ключами також уразливий при атаці "знання вихідного тексту", він набагато стійкіше, чим дворазовий DES. Він був прийнятий для банків. Рисунок 10 показує трикратний DES із двома ключами.

**Трикратний DES із трьома ключами**

Можливість атак "знання вихідного тексту" при трикратному DES із двома ключами "спокусила" деякі додатки використовувати **трикратний DES із трьома клю­ча­ми.**Алгоритм може застосовувати три каскади шифру DES на стороні шифрування й три кас­кади зворотних шифрів на стороні дешифрування. Для сумісності з однократним DES сто­рона шифрування використовує EDE, а сторона дешифрування — DED. E (encryption) — кас­кад шифрування, D (decryption) — каскад дешифрування. Сумісність із однократним DES забезпечується при k1 = k і установкою k2 і k3 до тому самому довільному ключу, обраному приймачем. Трикратний DES із трьома ключами використовується багатьма додатками, такими як PGP (Pretty Good Privacy), оскільки гарантує дуже гарну конфіденційність.

  
Рис. 10. Трикратний DES із двома ключами

**4. Безпека DES**

DES, як перший блоковий шифр, що має важливе значення, пройшов через багато випробувань на безпеку. Серед початих атак лише три становлять інтерес: груба сила, диференціальний криптоаналіз і лінійний криптоаналіз.

**Атака грубої сили**

Ми вже обговорювали слабість шифру з коротким ключем. Слабість ключа разом з іншими розглянутими недоліками, робить очевидним, що DES може бути зламаний із числом випробувань 255. Однак сьогодні більшість додатків використовує або 3DES із двома ключами (розмір ключа 2112), або 3DES із трьома ключами (розмір ключа 2168). Ці дві багаторазові версії DES дозволяють йому показувати істотну стійкість до атак грубої сили.

**Диференціальний криптоаналіз**

Ми уже обговорювали методику диференціального криптоаналізу для сучасних блокових шифрів. DES не є стійким до такого виду атаки. Однак багато чого вказує, що розроблювачі DES уже знали про цей тип атаки й проектували S-Блоки й спеціально вибрали число раундів, щоб зробити DES стійким до цього типу атаки. Сьогодні показане, що DES може бути зламаний, використовуючи диференціальний криптоаналіз, якщо ми маємо 247 вибірок вихідного тексту або 255 відомих вихідних текстів. Хоча це виглядає більш ефективно, ніж в атаці грубої сили, припустити, що хтось знає 247 вибірок вихідного тексту або 255 вибірок вихідного тексту, практично неможливо. Тому ми можемо сказати, що DES є стійким до диференціального криптоаналізу. Також показане, що збільшення числа раундів до 20 збільшує число необхідних вибірок вихідного тексту для атаки більш ніж до 264. Таке збільшення неможливе, тому що число блоків вихідного тексту в DES тільки 264.

**Лінійний крипто аналіз**

Лінійний криптоаналіз — більш нова методика, чому диференціальний криптоаналіз. DES більш уразливий до застосування лінійного криптоаналізу, чому до диференціального криптоаналізу — імовірно тому, що цей тип атак не був відомий проектувальникам DES і S-Блоки не є дуже стійкими до лінійного криптоаналізу. Показане, що DES може бути зламано з використанням 243 пари відомих вихідних текстів. Однак із практичної точки зору перехоплення такої кількості пара дуже малоймовірна.

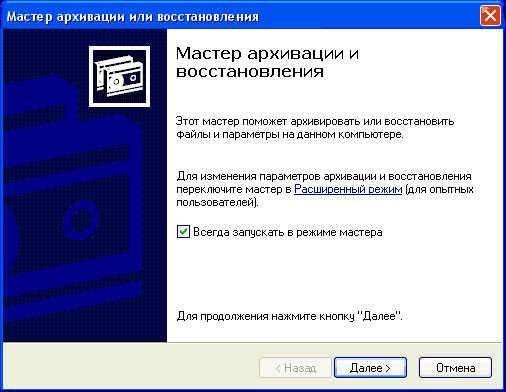
**8) Управління відновленням**

**Архівування й відновлення даних**

Ефективне відновлення загублених даних — мета будь-якого завдання архівування. Завдання архівування (Задача архивации або backup job) — це окремий процес резервного копіювання даних. Регулярне [архівування даних](http://schoolnet.elitno.net/Administrator/course/09A35B2FF568627FC2256E47003D957A.html#%D0%90%D0%A0%D0%A5%D0%86%D0%92%D0%A3%D0%92%D0%90%D0%9D%D0%9D%D0%AF [archivat) на[жорстких дисках](http://schoolnet.elitno.net/Administrator/course/09A35B2FF568627FC2256E47003D957A.html#%D0%92%D0%86%D0%9D%D0%A7%D0%95%D0%A1%D0%A2%D0%95%D0%A0%D0%A1%D0%AC%D0%9A%D0%98%D0%99 %D0%94%D0%98) серверів і клієнтських комп'ютерів дозволяє запобігти втраті даних через несправність жорстких дисків, несподіване вимикання електроживлення, інфікування комп'ютерним вірусом й іншими аналогічними причинами. Якщо регулярно проводити резервне копіювання даних, то втрата даних вам не загрожує: ви зможете відновити дані - окремі файли або вміст усього диску.

**Загальні відомості про утиліти резервного копіювання**

В [Windows](http://schoolnet.elitno.net/Administrator/course/09A35B2FF568627FC2256E47003D957A.html#%D0%9E%D0%9F%D0%95%D0%A0%D0%90%D0%A6%D0%86%D0%99%D0%9D%D0%90 %D0%A1%D0%98%D0%A1%D0%A2%D0%95%D0%9C_0)ХР Professional передбачений **Майстер архівування або відновлення** (Мастер архивации иливосстановления абоBackup or Restore Wizard) (рис. 6.6), який забезпечує просте резервне копіювання даних.



**Рис. 6.6.** Перша сторінка **Майстра архівування** **або відновлення**    
(Мастер архивации иливосстановления абоWelcome To The Backup Or Restore Wizard)

|  |  |  |
| --- | --- | --- |
| |  |  | | --- | --- | | [http://schoolnet.elitno.net/Administrator/course/images/B566B34838BCE936C2256E77003016B2_2.gif](http://schoolnet.elitno.net/Administrator/course/105BC7FA416EE93CC2256E7700346A1F.html) | відео-ролик відображує процес доступу до функцій [дефрагментації](http://schoolnet.elitno.net/Administrator/course/09A35B2FF568627FC2256E47003D957A.html#%D0%94%D0%95%D0%A4%D0%A0%D0%90%D0%93%D0%9C%D0%95%D0%9D%D0%A2%D0%90%D0%A6%D0%86%D0%AF [def), перевірки жорстких дисків та архівування | |

Для звернення до **Майстра архівування або відновлення** (Мастер архивации иливосстановления абоBackup or Restore Wizard) меню **Пуск**(Start) підведіть покажчик до пунктів **Всі програми** (Все программы абоАll Programs),**Стандартні** (Стандартные або Accessories), **Службові** (Служебные або Syster Tools) і натисніть **Архівування** (Архивация абоBackup). Якщо цей спосіб вам не сподобався, в меню **Пуск** (Start) натисніть команду **Виконати** (Выполнить абоRun) введіть **ntbackup**, а потім натисніть **ОК**. Майстер архівування або відновлення (Мастер архивации иливосстановления абоBackup or Restore Wizard) призначений для ручного архівування даних або для створення автоматичного процесу резервного копіювання, що регулярно виконується. Передбачено архівування даних у файл або на магнітну стрічку. Файли можна зберігати на жорсткому диску, змінних носіях (таких, як Iomega Zip й Jaz), перезаписуваних компакт-дисках й оптичних дисках.

На першій сторінці **Майстра архівування або відновлення** (Мастер архивации или восстановления абоWelcome To The Backup Or Restore Wizard) натисніть кнопку **Далі** (Далее абоNext). Сторінка **Архівування або відновлення**(Архивация или восстановление абоBackup Or Restore) дозволяє вказати, чи варто виконувати архівування файлів і параметрів або їхнє відновлення.

Для успішного архівування й відновлення даних на комп'ютері під управлінням Windows XP Professional ви повинні мати відповідні дозволи й права користувача, вони перераховані далі.

Всім користувачам надане право архівувати власні файли й [папки](http://schoolnet.elitno.net/Administrator/course/09A35B2FF568627FC2256E47003D957A.html#%D0%9A%D0%90%D0%A2%D0%90%D0%9B%D0%9E%D0%93, %D0%B4%D0%B8%D1%80%D0%B5%D0%BA%D1%82%D0%BE%D1%80), а також ті файли, для яких мають дозвіл **Читання** (Чтение або Read), **Читання й виконання** (Чтение и выполнение або Read and Execute), **Змінити** (Изменить або Modify) або **Повний доступ** (Полный доступ або Full Control).

Всі користувачі мають право відновлювати файли, для яких їм надані дозволи **Запис** (Запись або Write), **Змінити**(Изменить або Modify) або **Повний доступ** (Полный доступ абоFull Control).

Члени груп **Адміністратори** (Администраторы абоAdministrators) і­ **Опе­ра­то­ри­**[**архі­ву**](http://schoolnet.elitno.net/Administrator/course/09A35B2FF568627FC2256E47003D957A.html#%D0%90%D0%A0%D0%A5%D0%86%D0%92 [archive]. %D0%A1%D1%83%D0%BA%D1%83%D0%BF)**­** (Операторы архи-ва абоBackup Operators) можуть архівувати й відновлювати будь-які фай­ли (незалежно від призначених дозволів). За замовчуванням члени цих груп мають пра­ва **Архівування файлів** **і**[**каталогів**](http://schoolnet.elitno.net/Administrator/course/09A35B2FF568627FC2256E47003D957A.html#%D0%9A%D0%90%D0%A2%D0%90%D0%9B%D0%9E%D0%93, %D0%B4%D0%B8%D1%80%D0%B5%D0%BA%D1%82%D0%BE%D1%80)(Архивирование файлов и каталогов абоBackup Files and Directories) і **Відновлення файлів і каталогів** (Восстановление файлов и каталогов або Restore Files and Directories)

**Планування архівування**

Рекомендується планувати завдання архівування, щоб вони відповідали вашим потребам. Головна мета архівування - швидке відновлення даних, якщо буде потреба, саме її й повинен забезпечувати план архівування. Існує кілька можливих планів архівування для мережі.

Як створювати план архівування, дивіться нижче.

Визначте файли й папки, які варто архівувати.

Завжди архівуйте критично важливі для вашої роботи файли й папки, такі як фінансові звіти, [реєстр](http://schoolnet.elitno.net/Administrator/course/09A35B2FF568627FC2256E47003D957A.html#%D0%A0%D0%95%D0%84%D0%A1%D0%A2%D0%A0, %D1%80%D0%B5%D1%94%D1%81%D1%82%D1%80 Window) для кожного сервера та, якщо ваш комп'ютер входить у [домен](http://schoolnet.elitno.net/Administrator/course/09A35B2FF568627FC2256E47003D957A.html#%D0%94%D0%9E%D0%9C%D0%95%D0%9D [domain]. 1. %D0%A3 %D1%81%D0%B8%D1%81), файли служби каталогів, заснованої на службі Microsoft Active Directory service.

**Визначіть частоту виконання архівування**

Якщо дані критично важливі для діяльності компанії, архівуйте їх щодня. Якщо користувач створює або модифікує звіт раз у тиждень, досить щотижневого копіювання. У загальному випадку необхідно архівувати дані так часто, як часто вони змінюються. Так, не обов'язково щодня копіювати рідко змінювані файли, наприклад щомісячні звіти або файли [операційної системи](http://schoolnet.elitno.net/Administrator/course/09A35B2FF568627FC2256E47003D957A.html#%D0%9E%D0%9F%D0%95%D0%A0%D0%90%D0%A6%D0%86%D0%99%D0%9D%D0%90 %D0%A1%D0%98%D0%A1%D0%A2%D0%95%D0%9C) Windows XP Professional.

**Визначте пристрій для зберігання архівних файлів**

[Утиліти](http://schoolnet.elitno.net/Administrator/course/09A35B2FF568627FC2256E47003D957A.html#%D0%9E%D0%91%D0%A1%D0%9B%D0%A3%D0%93%D0%9E%D0%92%D0%A3%D0%AE%D0%A7%D0%90 %D0%9F%D0%A0%D0%9E%D0%93)архівування дозволяють використати для зберігання архівів різні змінні носії

**Файли**. Ви можете зберігати файли на змінних носіях, таких, як диски Iomega Zip, або в мережі, наприклад на [файловому сервері.](http://schoolnet.elitno.net/Administrator/course/09A35B2FF568627FC2256E47003D957A.html#%D0%A4%D0%90%D0%99%D0%9B%D0%9E%D0%92%D0%98%D0%99 %D0%A1%D0%95%D0%A0%D0%92%D0%95%D0%A0, %D1%84) Створювані файли мають розширення bkf і містять файли й папки, обрані вами для архівування. Користувач може архівувати особисті дані на мережному сервері. Використайте цей спосіб тільки для тимчасових завдань архівування.

**Стрічка**. Менш дорогі в порівнянні з іншими змінними носіями, стрічки частіше використовуються для більших завдань архівування, оскільки дозволяють зберігати більший обсяг інформації. Однак стрічки мають менший строк зберігання й можуть псуватися. Варто додержуватися рекомендацій щодо використання, що надані виробником.

|  |  |  |
| --- | --- | --- |
| |  |  | | --- | --- | | http://schoolnet.elitno.net/Administrator/course/images/B566B34838BCE936C2256E77003016B2_4.gif | **Примітка.**  Якщо для архівування й відновлення ви використовуєте змінні носії, переконайтеся що ці пристрої підтримуються Windows XP Professional і зазначені в списку сумісного обладнання (Hardware Compatibility List, HCL). | |

**Виберіть мережне або локальне архівування**

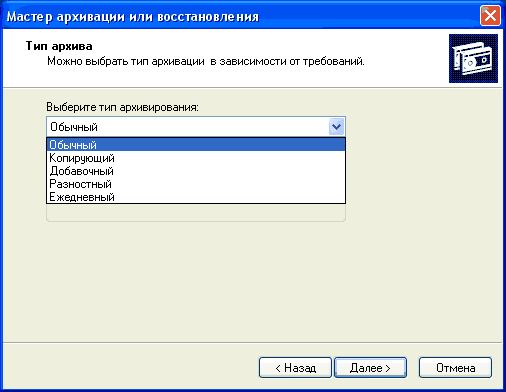
При мережному архівуванні збираються дані декількох комп'ютерів у мережі. Це дозволяє спільно архівувати дані з декількох комп'ютерів на один змінний носій, причому все архівування в мережі може виконувати один адміністратор. Вибір мережного або локального архівування залежить від того, які дані необхідно архівувати. Наприклад, ви можете архівувати тільки реєстр і файли Active Directory на комп'ютері, на якому виконується архівування.

Локальне архівування необхідно виконувати на кожному комп'ютері, включаючи сервери й клієнтські комп'ютери. Тому вам доведеться обходити всі комп'ютери для виконання архівування на кожному з них або зобов'язати користувачів виконувати архівування на їхніх особистих комп'ютерах. Однак останнє важко виконати: більшість користувачів забувають регулярно виконувати архівування, крім того, варто взяти до уваги необхідну кількість змінних пристроїв зберігання даних. Якщо ви використаєте, наприклад, стримери, вам буде потрібно по одному пристрою для кожного комп'ютера або доведеться переносити стример від комп'ютера до комп'ютера для виконання локального архівування на кожному з них.

Можлива комбінація мережного й локального архівування. Цьому способу варто віддати перевагу, коли критично важливі дані розташовані на серверах і на клієнтських комп'ютерах і у вас немає змінних пристроїв зберігання даних для кожного комп'ютера. Користувачі локально архівують дані й зберігають [архівні файли](http://schoolnet.elitno.net/Administrator/course/09A35B2FF568627FC2256E47003D957A.html#%D0%90%D0%A0%D0%A5%D0%86%D0%92%D0%9D%D0%98%D0%99 %D0%A4%D0%90%D0%99%D0%9B [archiv) на сервері, після цього ви виконуєте архівування на сервері.

**Вибір типу архів архівування**

Утиліти архівування забезпечують п'ять типів операцій архівування, що визначають, які дані необхідно архівувати, наприклад тільки ті файли, які були змінені після останнього архівування (рис. 6.7).



**Рис. 6.7**. Доступні типи архівування

Деякі типи архівування використовують [маркери](http://schoolnet.elitno.net/Administrator/course/09A35B2FF568627FC2256E47003D957A.html#%D0%9C%D0%90%D0%A0%D0%9A%D0%95%D0%A0 [mark, marker] 1 %D0%A2)архівування, також названі атрибутами архівування; цими маркерами відзначаються змінені файли. Коли файл змінюється, [атрибут](http://schoolnet.elitno.net/Administrator/course/09A35B2FF568627FC2256E47003D957A.html#%D0%90%D0%A2%D0%A0%D0%98%D0%91%D0%A3%D0%A2 [attribute]. 1. %D0%9E)файлу встановлюється, що свідчить про те, що файл був змінений після останнього архівування. Коли ви архівуєте файли, атрибути скидаються.

**Звичайне архівування**

У цьому випадку архівуються всі обрані файли й папки. При звичайному архівуванні не використовуються маркери, щоб визначити, які файли варто архівувати. Всі маркери скидаються, і кожен файл відзначається як архівований. При цьому типі архівування прискорюється процес відновлення, оскільки в архіві завжди перебувають поточні версії файлів і не треба виконувати кілька завдань відновлення.

**Копіювальне архівування**

У процесі копіювального архівування архівуються всі обрані файли й папки. На маркери ця операція ніякого впливу не має. Якщо ви не хочете знімати маркери й впливати на інші завдання архівування, використайте копіювальне архівування. Наприклад, застосовуйте його між звичайним й додатковим архівуванням для створення архівної копії мережних даних.

**Додаткове архівування**

При цьому архівуються тільки ті з обраних файлів і папок, які відзначені маркером. У процесі архівування маркер скидається. Тому, якщо ви виконали два послідовних додаткових архівування й не змінювали файл між виконанням архівування, іншим разом файл архівуватися не буде.

**Різницеве (разностное) архівування**

У цьому випадку архівуються тільки ті з обраних файлів і папок, які відзначені маркером. У процесі архівування маркер залишається незмінним. Тому, якщо ви виконаєте два послідовних різницевих (разностных) архівувань й не будете змінювати файл між виконанням архівування, файл буде поміщений в архів обидва рази.

**Щоденне архівування**

При цьому архівуються тільки ті з обраних файлів і папок, які були створені або змінені в день архівування незалежно від стану маркера. Використайте щоденне архівування, якщо необхідно - резервну копію файлів і папок, змінених протягом дня.

**Комбінування типів архівування**

Найбільш ефективна комбінація різних типів архівування. Одні типи архівування виконуються довше, але вимагають менше часу на відновлення. Інші типи виконуються швидше, але вимагають більше часу на відновлення. Якщо ви комбінуєте різні типи архівування, важливо пам'ятати про стан маркерів. Додаткове й різницеве архівування перевіряють стан маркерів.

Нижче показано кілька прикладів комбінування різних типів архівування.

**Звичайне й різницеве (разностное)** **архівування**. У понеділок виконується звичайне архівування, а з вівторка по п'ятницю – різницеве (разностное). При різницевому (разностном) архівуванні маркери не очищаються, так що при кожному архівуванні зберігаються всі зміни, зроблені з понеділка. Якщо в п'ятницю дані будуть ушкоджені, вам належить відновити дані звичайного архівування, виконаного в понеділок, і дані різницевого (разностного) архівування, виконаного в четвер. Така комбінація вимагає багато часу на проведення архівування, але забезпечує швидке відновлення даних.

**Звичайне й додаткове архівування**. У понеділок виконується звичайне архівування, а з вівторка по п'ятницю - додаткове. При додатковому архівуванні маркери очищаються, так що при кожному архівуванні зберігаються зміни, зроблені з моменту останнього архівування. Якщо в п'ятницю дані будуть ушкоджений варто відновити дані звичайного архівування, виконаного в понеділок, і дані всіх додаткових архівувань, виконаних з вівторка по п'ятницю. Ця комбінація вимагає менше часу на виконання архівування за рахунок збільшення часу відновлення.

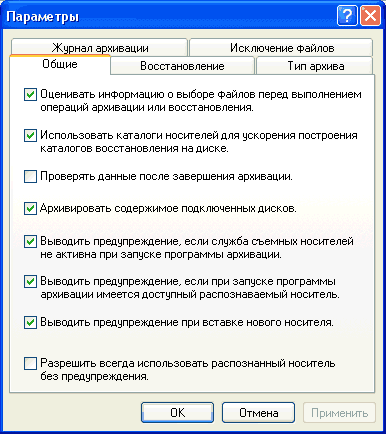
**Звичайне, різницеве (разностное)** і**копіювальне архівування**. Ця комбінація аналогічна першому прикладу з використанням звичайного й різницевого (разностного) архівування. Відмінність — проведення в середовищі копіювального архівування. Йому піддаються всі обрані файли, причому копіювальне архівування не впливає на маркери й не заважає подальшому виконанню операцій резервного копіювання. Таким чином, кожному різницевому (разностному) архівуванню піддаються всі файли, змінені після архівування в понеділок. Копіювальне архівування не використовується при відновленні. Його застосовують, якщо вам необхідно створити образ ваших даних.

**Зміна заданих за замовчуванням параметрів архівування**

Утиліти архівування дозволяють змінити задані за замовчуванням параметри для всіх операцій архівування й відновлення. Ці параметри розташовані на вкладках діалогового вікна **Параметри** (Параметры або Options). Для доступу до діалогового вікна **Параметри** (Параметры або Options) на першій сторінці **Майстра архівування й відновлення** (Мастера архивации и восстановления абоWelcome To The Backup Or Restore Wizard) натисніть посилання**Розширений режим** (Расширенный режим або Advanced Mode), а потім у меню **Сервіс**(Сервис абоTools) натисніть пункт **Параметри** (Параметры абоOptions).

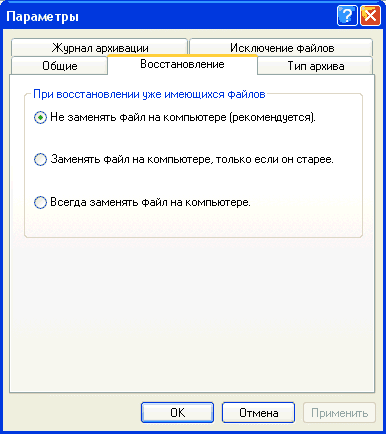
Далі коротко описані параметри утиліти архівування.

Вкладка **Загальні** (Общие абоGeneral). Її параметри налаштовують перевірку даних, інформацію про стан завдань архівування й відновлення, виведені повідомлення й предмет архівування. На рис. 6.8 показані параметри, встановлені за замовчуванням на вкладці **Загальні** (Общие абоGeneral). Варто встановити прапорець **Перевіряти дані після завершення архівування** (Проверять данные после завершения архивации абоVerify Data After The Backup Completes), якщо ви не хочете, щоб дані в архіві виявилися ушкодженими.



**Рис. 6.8**. Вкладка **Загальні** (Общие або General) діалогового вікна **Параметри**    
(Параметры абоOptions) програми архівування

Вкладка **Відновлення** (Восстановление абоRestore). Її параметри визначають, чи будуть відновлюватися файли, ідентичні вже існуючим на комп'ютері. На рис. 6.9 показані доступні параметри, установлені за замовчуванням.



**Рис. 6.9.** Вкладка **Відновлення** (Восстановление абоRestore) діалогового вікна **Параметри**    
(Параметры абоOptions) програми архівування

Вкладка **Тип архіву** (Тип Архива абоBackup Type). Її параметри впливають на тип архівування, який обирається за замовчуванням при виконанні завдань архівування. Обраний параметр залежить від того, як часто ви проводите архівування, наскільки швидке відновлення потрібно і як багато місця доступно на пристрої зберігання даних. Доступні наступні типи архіву: **Звичайний** (Обычный абоNormal) (обраний за замовчуванням), **Копіювальний** (Копирующий абоСopy), **Різницевий** (Разностный абоDifferential), **Додатковий** (Добавочный або Incremental) і **Щоденний** (Ежедневный абоDaily).

Вкладка **Журнал архівування** (Журнал архивации або Backup Log). Її параметри впливають на тип інформації, що заноситься в журнал архівування. За замовчуванням встановлений перемикач **Коротке зведення** (Краткая сводка абоSummary), що забезпечує запис у журналі тільки основних операцій, таких, як [завантаження](http://schoolnet.elitno.net/Administrator/course/09A35B2FF568627FC2256E47003D957A.html#%D0%97%D0%90%D0%92%D0%90%D0%9D%D0%A2%D0%90%D0%96%D0%95%D0%9D%D0%9D%D0%AF [loading)стрічки, початок архівування або помилка відкриття файлів. Доступні ще два перемикачі: **Докладна** (Подробная абоDetailed), при виборі якого в журнал записується вся інформація, включаючи імена файлів і папок, і **Ніякої** (Никакой абоNone), вибір якого забороняє ведення журналу.

Вкладка **Виключення файлів** (Исключение файлов абоExclude Files). Її параметри визначають, які файли будуть виключені при виконанні завдань архівування.

Ви можете змінити деякі задані за замовчуванням параметри в**Майстру архівування або відновлення** (Мастер архивации или восстановления абоBackup or Restore Wizard) для окремих завдань архівування. Наприклад, за замовчуванням виконується звичайне архівування, але ви можете змінити тип архівування в **Майстрі архівування або відновлення** (Мастер архивации или восстановления або Backup or Restore Wizard). Незважаючи на це, коли ви наступного разу запустите Майстер архівування або відновлення, у ньому знову буде обраний заданий за замовчуванням тип архівування (звичайний).

**9) Основні напрямки розвитку сучасної криптографії**

**Історія криптографії**

*План:*

[*Введення*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link0)

* [*1*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link1)[*Криптографія в Стародавньому світі*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link1)
  + [*1.1*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link2)[*Стародавній Єгипет*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link2)
  + [*1.2*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link3)[*Атбаш*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link3)
  + [*1.3*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link4)[*Скитала*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link4)
  + [*1.4*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link5)[*Диск Енея, лінійка Енея, книжковий шифр*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link5)
  + [*1.5*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link6)[*Квадрат Полібія*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link6)
  + [*1.6*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link7)[*Шифр Цезаря*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link7)
* [*2*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link8)[*Тайнопису*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link8)
* [*3*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link9)[*Криптографія від Середніх століть до Нового часу*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link9)
  + [*3.1*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link10)[*Розвиток криптографії в арабських країнах*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link10)
  + [*3.2*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link11)[*Криптографія епохи Відродження*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link11)
  + [*3.3*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link12)[*Іспанська імперія і колонії в Америці.*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link12)[*"Індіанська криптографія"*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link12)
  + [*3.4*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link13)[*Чорні кабінети*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link13)
  + [*3.5*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link14)[*Криптографія в британських колоніях і США*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link14)
  + [*3.6*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link15)[*На шляху до математичної криптографії*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link15)
* [*4*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link16)[*Криптографія в літературі*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link16)
* [*5*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link17)[*Криптографія Першої світової війни*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link17)
  + [*5.1*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link18)[*Росія*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link18)
  + [*5.2*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link19)[*Англія*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link19)
  + [*5.3*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link20)[*Франція*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link20)
  + [*5.4*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link21)[*Німеччина*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link21)
* [*6*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link22)[*Криптографія Другої світової війни*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link22)
  + [*6.1*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link23)[*Німеччина: "Енігма", "Fish"*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link23)
  + [*6.2*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link24)[*Японія*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link24)
  + [*6.3*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link25)[*СРСР*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link25)
  + [*6.4*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link26)[*США*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link26)
* [*7*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link27)[*Математична криптографія*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link27)
* [*8*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link28)[*Відкрита криптографія і держава*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link28)
* [*9*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link29)[*Сучасна криптографія*](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link29)

**Введення**

**Історія криптографії** налічує близько 4 тисяч років. В якості основного критерію періодизації криптографії можливо використовувати технологічні характеристики використовуваних методів шифрування.

Перший період (приблизно з 3-го тисячоліття до н. Е..) Характеризується пануванням моноалфавитной шифрів (основний принцип - заміна алфавіту вихідного тексту іншим алфавітом через заміну букв іншими буквами або символами). Другий період (хронологічні рамки - з [IX століття](http://znaimo.com.ua/IX_%D1%81%D1%82%D0%BE%D0%BB%D1%96%D1%82%D1%82%D1%8F) на Близькому Сході ( [Ал-Кінді](http://znaimo.com.ua/%D0%90%D0%BB-%D0%9A%D1%96%D0%BD%D0%B4%D1%96)) і з[XV століття](http://znaimo.com.ua/XV_%D1%81%D1%82%D0%BE%D0%BB%D1%96%D1%82%D1%82%D1%8F) в Європі ( [Леон Баттіста Альберті](http://znaimo.com.ua/%D0%90%D0%BB%D1%8C%D0%B1%D0%B5%D1%80%D1%82%D1%96_%D0%9B%D0%B5%D0%BE%D0%BD_%D0%91%D0%B0%D1%82%D1%82%D1%96%D1%81%D1%82%D0%B0)) - до початку [XX століття](http://znaimo.com.ua/XX_%D1%81%D1%82%D0%BE%D0%BB%D1%96%D1%82%D1%82%D1%8F)) ознаменувався введенням в обіг поліалфавітних шифрів. Третій період (з початку і до середини XX століття) характеризується впровадженням електромеханічних пристроїв в роботу шифрувальників. При цьому продовжувалося використання поліалфавітних шифрів.

Четвертий період - з середини до 70-х років XX століття - період переходу до математичної криптографії. У роботі [Шеннона](http://znaimo.com.ua/%D0%A8%D0%B5%D0%BD%D0%BD%D0%BE%D0%BD_%D0%9A%D0%BB%D0%BE%D0%B4_%D0%95%D0%BB%D0%B2%D1%83%D0%B4) з'являються суворі математичні визначення [кількості інформації](http://znaimo.com.ua/%D0%92%D0%BB%D0%B0%D1%81%D0%BD%D0%B0_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%8F), передачі даних, [ентропії](http://znaimo.com.ua/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D0%B5%D0%BD%D1%82%D1%80%D0%BE%D0%BF%D1%96%D1%8F), функцій шифрування. Обов'язковим етапом створення шифру вважається вивчення його вразливості до різних відомим атакам - [лінійному](http://znaimo.com.ua/%D0%9B%D1%96%D0%BD%D1%96%D0%B9%D0%BD%D0%B8%D0%B9_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B0%D0%BD%D0%B0%D0%BB%D1%96%D0%B7) і [диференціальному](http://znaimo.com.ua/%D0%94%D0%B8%D1%84%D0%B5%D1%80%D0%B5%D0%BD%D1%86%D1%96%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D0%B9_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B0%D0%BD%D0%B0%D0%BB%D1%96%D0%B7) криптоанализу. Проте до [1975](http://znaimo.com.ua/1975) криптографія залишалася "класичної", або ж, більш коректно, криптографією з секретним ключем.

Сучасний період розвитку криптографії (з кінця 1970-х років по теперішній час) відрізняється зародженням та розвитком нового напрямку - [криптографія з відкритим ключем](http://znaimo.com.ua/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%8F_%D0%B7_%D0%B2%D1%96%D0%B4%D0%BA%D1%80%D0%B8%D1%82%D0%B8%D0%BC_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%BC). Її поява знаменується не тільки новими технічними можливостями, але і порівняно широким поширенням криптографії для використання приватними особами. Правове регулювання використання криптографії приватними особами в різних країнах сильно розрізняється - від дозволу до повної заборони.

Сучасна криптографія утворює окремий науковий напрям на сти­ку­ [ма­те­ма­ти­ки](http://znaimo.com.ua/%D0%9C%D0%B0%D1%82%D0%B5%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0)­ і­ [інфо­р­матики](http://znaimo.com.ua/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0) - роботи в цій галузі публікуються в наукових журналах, організовуються регулярні кон­ференції. Практичне застосування криптографії стало невід'ємною частиною життя суча­с­но­го суспільства - її використовують в таких галузях як електронна комерція, електронний до­кументообіг (включаючи [цифрові підписи](http://znaimo.com.ua/%D0%95%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B8%D0%B9_%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B8%D0%B9_%D0%BF%D1%96%D0%B4%D0%BF%D0%B8%D1%81)), телекомунікації та інших.

**1. Криптографія в**[**Стародавньому світі**](http://znaimo.com.ua/%D0%A1%D1%82%D0%B0%D1%80%D0%BE%D0%B4%D0%B0%D0%B2%D0%BD%D1%96%D0%B9_%D1%81%D0%B2%D1%96%D1%82)

Є свідчення, що криптографія як техніка захисту тексту виникла разом з писемністю, і способи таємного листа були відомі вже древнім цивілізаціям [Індії](http://znaimo.com.ua/%D0%94%D0%B0%D0%B2%D0%BD%D1%8F_%D0%86%D0%BD%D0%B4%D1%96%D1%8F), [Єгипту](http://znaimo.com.ua/%D0%A1%D1%82%D0%B0%D1%80%D0%BE%D0%B4%D0%B0%D0%B2%D0%BD%D1%96%D0%B9_%D0%84%D0%B3%D0%B8%D0%BF%D0%B5%D1%82)і [Месопотамії](http://znaimo.com.ua/%D0%9C%D0%B5%D1%81%D0%BE%D0%BF%D0%BE%D1%82%D0%B0%D0%BC%D1%96%D1%8F). В [давньоіндійських текстах](http://znaimo.com.ua/%D0%9A%D0%B0%D0%BC%D0%B0%D1%81%D1%83%D1%82%D1%80%D0%B0) серед 64-х мистецтв названі способи зміни тексту, деякі з них мож­на віднести до криптографічних. Автор таблички з рецептом для вигото­влен­ня [глазурі](http://znaimo.com.ua/%D0%93%D0%BB%D0%B0%D0%B7%D1%83%D1%80) для гончарних виробів з Месопотамії використовував рідкісні позначення, про­пус­кав букви, а імена заміняв на цифри, щоб сховати написане. Надалі зустрічаються різні згад­ки про використання криптографії, велика частина відноситься до використання у військовій спра­ві.

**1.1. Стародавній Єгипет**

Першим відомим застосуванням криптографії прийнято вважати використання спе­ціаль­них ієрогліфів близько 4000 років тому в [Стародавньому Єгипті](http://znaimo.com.ua/%D0%A1%D1%82%D0%B0%D1%80%D0%BE%D0%B4%D0%B0%D0%B2%D0%BD%D1%96%D0%B9_%D0%84%D0%B3%D0%B8%D0%BF%D0%B5%D1%82). Елементи криптографії вияв­лені вже в написах [Старого](http://znaimo.com.ua/%D0%94%D0%B0%D0%B2%D0%BD%D1%94_%D1%86%D0%B0%D1%80%D1%81%D1%82%D0%B2%D0%BE) і [Середнього царств](http://znaimo.com.ua/%D0%A1%D0%B5%D1%80%D0%B5%D0%B4%D0%BD%D1%94_%D1%86%D0%B0%D1%80%D1%81%D1%82%D0%B2%D0%BE_(%D0%A1%D1%82%D0%B0%D1%80%D0%BE%D0%B4%D0%B0%D0%B2%D0%BD%D1%96%D0%B9_%D0%84%D0%B3%D0%B8%D0%BF%D0%B5%D1%82)), повністю криптографічні тексти відомі з періоду [XVIII династії](http://znaimo.com.ua/XVIII_%D0%B4%D0%B8%D0%BD%D0%B0%D1%81%D1%82%D1%96%D1%8F). [Ієрогліфічне письмо](http://znaimo.com.ua/%D0%84%D0%B3%D0%B8%D0%BF%D0%B5%D1%82%D1%81%D1%8C%D0%BA%D1%96_%D1%96%D1%94%D1%80%D0%BE%D0%B3%D0%BB%D1%96%D1%84%D0%B8), що відбулося від [піктографії](http://znaimo.com.ua/%D0%9F%D1%96%D0%BA%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%B8), буя­ло­ [іде­ог­ра­ма­ми](http://znaimo.com.ua/%D0%86%D0%B4%D0%B5%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%B0) і, в результаті відсутності [огласовки](http://znaimo.com.ua/%D0%9E%D0%B3%D0%BB%D0%B0%D1%81%D0%BE%D0%B2%D0%BA%D0%B0), дало можливість створювати [фонограми](http://znaimo.com.ua/%D0%A4%D0%BE%D0%BD%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%B0_(%D0%BB%D1%96%D0%BD%D0%B3%D0%B2%D1%96%D1%81%D1%82%D0%B8%D0%BA%D0%B0)) за принци­пом ребусів. Криптографія єгиптян використовувалася не з метою утруднити читання, а найімо­вірніше, з прагненням [переписувачів](http://znaimo.com.ua/%D0%9F%D0%B5%D1%80%D0%B5%D0%BF%D0%B8%D1%81%D1%83%D0%B2%D0%B0%D1%87) перевершити один одного в дотепності та вина­хід­ливості, а також, за допомогою незвичайності та загадковості, привернути увагу до своїх тек­стів . Одним з показових прикладів є тексти прославлення вельможі Хнумхотепа II *(нім.­*[Chnumhotep II](http://ru.wikipedia.org/de.wikipedia.org/wiki/Chnumhotep_II.), XIX ст. до н. е..) знайдені в добре збереглася гробниці № BH 3 в місцевості Бені-Хасан *(англ.* [Beni Hasan](http://ru.wikipedia.org/en.wikipedia.org/wiki/Beni_Hasan)) [[5]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link38) [[6]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link39).

**1.2. Атбаш**

Приклади використання криптографії можна зустріти в священних іудейських книгах, у тому числі в [книзі пророка Єремії](http://znaimo.com.ua/%D0%9A%D0%BD%D0%B8%D0%B3%D0%B0_%D0%BF%D1%80%D0%BE%D1%80%D0%BE%D0%BA%D0%B0_%D0%84%D1%80%D0%B5%D0%BC%D1%96%D1%97) ( [VI століття до н.е..](http://znaimo.com.ua/VI_%D1%81%D1%82%D0%BE%D0%BB%D1%96%D1%82%D1%82%D1%8F_%D0%B4%D0%BE_%D0%BD_%D0%B5)), де використовувався простий метод шифрування під назвою [атбаш](http://znaimo.com.ua/%D0%90%D1%82%D0%B1%D0%B0%D1%88). [[7]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link40)

**1.3. Скитала**

[](http://ru.wikipedia.org/w/index.php?title=%D0%A4%D0%B0%D0%B9%D0%BB:Skytale.png&filetimestamp=20070220183311)

Скитала

Скитала, також відома як "шифр [древньої Спарти](http://znaimo.com.ua/%D0%A1%D0%BF%D0%B0%D1%80%D1%82%D0%B0) ", також є одним з найдавніших відомих криптографічних пристроїв.

Безперечно відомо, що скитала використовувалася у війні Спарти проти Афін в кінці [V століття до н.е..](http://znaimo.com.ua/V_%D1%81%D1%82%D0%BE%D0%BB%D1%96%D1%82%D1%82%D1%8F_%D0%B4%D0%BE_%D0%BD_%D0%B5) [[8]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link41) [[9]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link42) Можливо також, що її згадують поети [Архілох](http://znaimo.com.ua/%D0%90%D1%80%D1%85%D1%96%D0%BB%D0%BE%D1%85) [[10]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link43) ([VII століття до н.е..](http://znaimo.com.ua/VII_%D1%81%D1%82%D0%BE%D0%BB%D1%96%D1%82%D1%82%D1%8F_%D0%B4%D0%BE_%D0%BD_%D0%B5)) і [Піндар](http://znaimo.com.ua/%D0%9F%D1%96%D0%BD%D0%B4%D0%B0%D1%80) [[11]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link44), хоча найімовірніше, що в їхніх віршах слово "скитала" використано у своєму первинному значенні "посох".

Принцип її дії виклали [Аполлоній Родоський](http://znaimo.com.ua/%D0%90%D0%BF%D0%BE%D0%BB%D0%BB%D0%BE%D0%BD%D1%96%D0%B9_%D0%A0%D0%BE%D0%B4%D0%BE%D1%81%D1%8C%D0%BA%D0%B8%D0%B9) [[12]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link45) (середина [III століття до н.е..](http://znaimo.com.ua/III_%D1%81%D1%82%D0%BE%D0%BB%D1%96%D1%82%D1%82%D1%8F_%D0%B4%D0%BE_%D0%BD_%D0%B5)) і [Плутарх](http://znaimo.com.ua/%D0%9F%D0%BB%D1%83%D1%82%D0%B0%D1%80%D1%85) (близько 45-125 н. е..), але збереглося лише опис останнього. [[13]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link46)

Скитала представляла собою довгий стрижень, на який намотувалася стрічка з пергаменту. На стрічку наносився текст вздовж осі скіталу, так, що після розмотування текст ставав нечитабельним. Для його відновлення потрібна скитала такого ж діаметру.

Вважається, що автором способу злому шифру скіталу є [Аристотель](http://znaimo.com.ua/%D0%90%D1%80%D0%B8%D1%81%D1%82%D0%BE%D1%82%D0%B5%D0%BB%D1%8C), який намотував стрічку на [конусоподібну](http://znaimo.com.ua/%D0%9A%D0%BE%D0%BD%D1%83%D1%81) палицю до тих пір, поки не з'являлися читаються уривки тексту.

**1.4. Диск Енея, лінійка Енея, книжковий шифр**

З ім'ям [Енея Тактика](http://znaimo.com.ua/%D0%95%D0%BD%D0%B5%D0%B9_%D0%A2%D0%B0%D0%BA%D1%82%D0%B8%D0%BA), полководця [IV століття до н.е..](http://znaimo.com.ua/IV_%D1%81%D1%82%D0%BE%D0%BB%D1%96%D1%82%D1%82%D1%8F_%D0%B4%D0%BE_%D0%BD_%D0%B5), пов'язують декілька технік шифрування і тайнопису.

[Диск Енея](http://znaimo.com.ua/%D0%94%D0%B8%D1%81%D0%BA_%D0%95%D0%BD%D0%B5%D1%8F) представляв собою диск діаметром 10-15 см з отворами по числу букв алфавіту. Щоб створити нитка простягалася через отвори в диску, відповідним буквам повідомлення. При читанні одержувач витягав нитку, і отримував літери, правда, в зворотному порядку. Хоча недоброзичливець міг прочитати повідомлення, якщо перехопить диск, Еней передбачив спосіб швидкого знищення повідомлення - для цього було достатньо висмикнути нитку, закріплену на котушці в центрі диска.

Першим дійсно криптографічним інструментом можна назвати [лінійку Енея](http://znaimo.com.ua/%D0%9B%D1%96%D0%BD%D1%96%D0%B9%D0%BA%D0%B0_%D0%95%D0%BD%D0%B5%D1%8F), що реалізує шифр заміни. Замість диска використовувалася лінійка з отворами по числу букв алфавіту, котушкою і прорізом. Для шифрування нитка простягалася через проріз і отвір, після чого на нитки зав'язувався черговий вузол. Для дешифрування необхідно було мати саму нитку і лінійку з аналогічним розташуванням отворів. Таким чином, навіть знаючи алгоритм шифрування, але не маючи ключа (лінійки), прочитати повідомлення було неможливо. [[15]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link49)

У своєму творі "Про перенесення облоги" Еней описує ще одну техніку тайнопису, пізніше названу " [книжковий шифр](http://znaimo.com.ua/%D0%9A%D0%BD%D0%B8%D0%B6%D0%BA%D0%BE%D0%B2%D0%B8%D0%B9_%D1%88%D0%B8%D1%84%D1%80_%D0%95%D0%BD%D0%B5%D1%8F) ". Він запропонував робити малопомітні дірки поряд з лі­те­­рами в книзі або іншому документі . Значно пізніше, аналогічний шифр вико­ристо­ву­ва­ли [німецькі](http://znaimo.com.ua/%D0%9D%D1%96%D0%BC%D0%B5%D1%87%D1%87%D0%B8%D0%BD%D0%B0) шпигуни в [Першій світовій війні](http://znaimo.com.ua/%D0%9F%D0%B5%D1%80%D1%88%D0%B0_%D1%81%D0%B2%D1%96%D1%82%D0%BE%D0%B2%D0%B0_%D0%B2%D1%96%D0%B9%D0%BD%D0%B0).

**1.5. Квадрат Полібія**

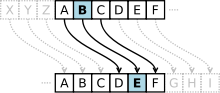
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **1** | **2** | **3** | **4** | **5** |
| **1** | [Α](http://znaimo.com.ua/) | [Β](http://znaimo.com.ua/) | [Γ](http://znaimo.com.ua/) | [Δ](http://znaimo.com.ua/) | [Ε](http://znaimo.com.ua/) |
| **2** | [Ζ](http://znaimo.com.ua/) | [Η](http://znaimo.com.ua/) | [Θ](http://znaimo.com.ua/) | [Ι](http://znaimo.com.ua/) | [Κ](http://znaimo.com.ua/) |
| **3** | [Λ](http://znaimo.com.ua/) | [Μ](http://znaimo.com.ua/) | [Ν](http://znaimo.com.ua/) | [Ξ](http://znaimo.com.ua/) | [Ο](http://znaimo.com.ua/) |
| **4** | [Π](http://znaimo.com.ua/) | [Ρ](http://znaimo.com.ua/) | [Σ](http://znaimo.com.ua/%D0%A1%D0%B8%D0%B3%D0%BC%D0%B0%20(%D0%BB%D1%96%D1%82%D0%B5%D1%80%D0%B0)) | [Τ](http://znaimo.com.ua/) | [Υ](http://znaimo.com.ua/) |
| **5** | [Φ](http://znaimo.com.ua/) | [Χ](http://znaimo.com.ua/) | [Ψ](http://znaimo.com.ua/) | [Ω](http://znaimo.com.ua/) |  |

[Квадрат Полібія](http://znaimo.com.ua/%D0%9A%D0%B2%D0%B0%D0%B4%D1%80%D0%B0%D1%82%20%D0%9F%D0%BE%D0%BB%D1%96%D0%B1%D1%96%D1%8F) з[грецьким алфавітом](http://znaimo.com.ua/%D0%93%D1%80%D0%B5%D1%86%D1%8C%D0%BA%D0%B8%D0%B9%20%D0%B0%D0%BB%D1%84%D0%B0%D0%B2%D1%96%D1%82). Для передачі, наприклад, літери " [Θ](http://znaimo.com.ua/)"спочатку показували два факела, потім три.

Під [II столітті до н.е..](http://znaimo.com.ua/II%20%D1%81%D1%82%D0%BE%D0%BB%D1%96%D1%82%D1%82%D1%8F%20%D0%B4%D0%BE%20%D0%BD%20%D0%B5.) в [Стародавній Греції](http://znaimo.com.ua/%D0%A1%D1%82%D0%B0%D1%80%D0%BE%D0%B4%D0%B0%D0%B2%D0%BD%D1%8F%20%D0%93%D1%80%D0%B5%D1%86%D1%96%D1%8F) був винайдений [Квадрат Полібія](http://znaimo.com.ua/%D0%9A%D0%B2%D0%B0%D0%B4%D1%80%D0%B0%D1%82%20%D0%9F%D0%BE%D0%BB%D1%96%D0%B1%D1%96%D1%8F). [[9]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link42) У ньому букви алфавіту записувалися в квадрат 5 на 5 (при використанні[грецького алфавіту](http://znaimo.com.ua/%D0%93%D1%80%D0%B5%D1%86%D1%8C%D0%BA%D0%B8%D0%B9%20%D0%B0%D0%BB%D1%84%D0%B0%D0%B2%D1%96%D1%82) один осередок залишалася порожньою), після чого за допомогою оптичного телеграфу передавалися номер рядка і стовпця, відповідні символу вихідного тексту (на кожну букву доводилося два сигнали: число факелів позначало розряд літери по горизонталі і вертикалі) .

Деякі дослідники вважають, що це можна розглядати як першу систему, зменшується (стискала) вихідний алфавіт, і, в деякому розумінні, як прообраз сучасної системи двійковій передачі даних.

**1.6. Шифр Цезаря**

[](http://ru.wikipedia.org/w/index.php?title=%D0%A4%D0%B0%D0%B9%D0%BB:Caesar3.svg&filetimestamp=20061227194048)

Шифр Цезаря

Згідно зі свідченням [Светонія](http://znaimo.com.ua/%D0%93%D0%B0%D0%B9%20%D0%A1%D0%B2%D0%B5%D1%82%D0%BE%D0%BD%D1%96%D0%B9%20%D0%A2%D1%80%D0%B0%D0%BD%D0%BA%D0%B2%D0%B8%D0%BB%D0%BB), Цезар використовував в листуванні [моноалфавитной шифр](http://znaimo.com.ua/%D0%9C%D0%BE%D0%BD%D0%BE%D0%B0%D0%BB%D1%84%D0%B0%D0%B2%D0%B8%D1%82%D0%BD%D0%BE%D0%B9%20%D1%88%D0%B8%D1%84%D1%80), який увійшов в історію як [Шифр Цезаря](http://znaimo.com.ua/%D0%A8%D0%B8%D1%84%D1%80%20%D0%A6%D0%B5%D0%B7%D0%B0%D1%80%D1%8F) . Книгу про шифрі написав граматик Проб . У шифрі Цезаря кожна буква алфавіту циклічно зсувається на певне число позицій. Величину зсуву можна розглядати як ключ шифрування. Сам Цезар використовував зсув на три позиції.

**2. Тайнопису**

[](http://ru.wikipedia.org/w/index.php?title=%D0%A4%D0%B0%D0%B9%D0%BB:Letter_of_Alexis_of_Russia.JPG&filetimestamp=20110402104626)

Лист царя[Олексія Михайловича](http://znaimo.com.ua/%D0%9E%D0%BB%D0%B5%D0%BA%D1%81%D1%96%D0%B9%20%D0%9C%D0%B8%D1%85%D0%B0%D0%B9%D0%BB%D0%BE%D0%B2%D0%B8%D1%87), писаний тайнописом (тарабарщиною)

Крім примітивних шифрів в історії використовувався і інший підхід - повна заміна одного алфавіту (наприклад, [кирилиці](http://znaimo.com.ua/%D0%9A%D0%B8%D1%80%D0%B8%D0%BB%D0%B8%D1%86%D1%8F)) на інший (наприклад, [грецький](http://znaimo.com.ua/%D0%93%D1%80%D0%B5%D1%86%D1%8C%D0%BA%D0%B8%D0%B9%20%D0%B0%D0%BB%D1%84%D0%B0%D0%B2%D1%96%D1%82)). Не маючи ключа, сопоставляющего вихідний і використовуваний алфавіти, прочитати напис було неможливо.  Крім цього використовувалися спеціальні техніки записи символів алфавіту таким чином, щоб ускладнити його читання. Прикладом такої техніки є "в'язані руни", коли руни записуються таким чином, що окремі їхні елементи (наприклад, вертикальні риси) збігаються. Подібні системи часто використовувалися жерцями Північно-Західної Європи аж до пізнього Середньовіччя.

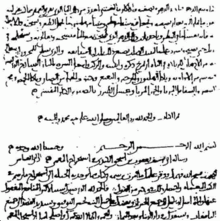
Безліч варіантів тайнопису використовувалося і на [Русі](http://znaimo.com.ua/%D0%A0%D1%83%D1%81%D1%8C). Серед них і про­сті­ [мо­но­алфа­вит­ной шифри](http://znaimo.com.ua/%D0%9C%D0%BE%D0%BD%D0%BE%D0%B0%D0%BB%D1%84%D0%B0%D0%B2%D0%B8%D1%82%D0%BD%D0%BE%D0%B9%20%D1%88%D0%B8%D1%84%D1%80) ( [проста літорея](http://znaimo.com.ua/%D0%9F%D1%80%D0%BE%D1%81%D1%82%D0%B0%20%D0%BB%D1%96%D1%82%D0%BE%D1%80%D0%B5%D1%8F), [лист у квадратах](http://znaimo.com.ua/%D0%9B%D0%B8%D1%81%D1%82%20%D0%B2%20%D0%BA%D0%B2%D0%B0%D0%B4%D1%80%D0%B0%D1%82%D0%B0%D1%85)), заміна алфавіту -[тайнопис гла­го­ли­цею](http://znaimo.com.ua/%D0%A2%D0%B0%D0%B9%D0%BD%D0%BE%D0%BF%D0%B8%D1%81%20%D0%B3%D0%BB%D0%B0%D0%B3%D0%BE%D0%BB%D0%B8%D1%86%D0%B5%D1%8E), [тайнопис грецької абеткою](http://znaimo.com.ua/%D0%A2%D0%B0%D0%B9%D0%BD%D0%BE%D0%BF%D0%B8%D1%81%20%D0%B3%D1%80%D0%B5%D1%86%D1%8C%D0%BA%D0%BE%D1%97%20%D0%B0%D0%B1%D0%B5%D1%82%D0%BA%D0%BE%D1%8E), а також особливі прийоми письма, наприклад, [моноконділ](http://znaimo.com.ua/%D0%9C%D0%BE%D0%BD%D0%BE%D0%BA%D0%BE%D0%BD%D0%B4%D1%96%D0%BB). Най­більш ранні тексти з використанням тайнопису відносяться до [XII століття](http://znaimo.com.ua/XII%20%D1%81%D1%82%D0%BE%D0%BB%D1%96%D1%82%D1%82%D1%8F).

Існує думка , що в більш пізній період тайнопис використовувалася для іконографії, нап­риклад, при написання ікони [XIV століття](http://znaimo.com.ua/XIV%20%D1%81%D1%82%D0%BE%D0%BB%D1%96%D1%82%D1%82%D1%8F) " [Донська Богоматір](http://znaimo.com.ua/%D0%94%D0%BE%D0%BD%D1%81%D1%8C%D0%BA%D0%B0%20%D1%96%D0%BA%D0%BE%D0%BD%D0%B0) ". Відповідно до іншої точ­ки зору, літерний ряд є лише шрифтовим декором, який був широко поширений як у дав­ньо­руській, так і, наприклад, в візантійського іконопису.

**3. Криптографія від**[**Середніх століть**](http://znaimo.com.ua/%D0%A1%D0%B5%D1%80%D0%B5%D0%B4%D0%BD%D1%96%20%D1%81%D1%82%D0%BE%D0%BB%D1%96%D1%82%D1%82%D1%8F)**до**[**Нового часу**](http://znaimo.com.ua/%D0%9D%D0%BE%D0%B2%D0%B8%D0%B9%20%D1%87%D0%B0%D1%81)

У Середні століття криптографія - в основному, моноалфавитной шифри - починають широ­ко використовуватися дипломатами, купцями і навіть простими громадянами. Пос­ту­по­во, у міру поширення техніки частотного криптоаналізу, шифри ускладнюються, що при­зво­дить до появи [шифрів омофоніческой заміни](http://znaimo.com.ua/%D0%A8%D0%B8%D1%84%D1%80%20%D0%BF%D1%96%D0%B4%D1%81%D1%82%D0%B0%D0%BD%D0%BE%D0%B2%D0%BA%D0%B8), а потім і [поліалфавітних шифрів](http://znaimo.com.ua/%D0%9F%D0%BE%D0%BB%D1%96%D0%B0%D0%BB%D1%84%D0%B0%D0%B2%D1%96%D1%82%D0%BD%D0%B8%D0%B9%20%D1%88%D0%B8%D1%84%D1%80).

**3.1. Розвиток криптографії в арабських країнах**

[](http://ru.wikipedia.org/w/index.php?title=%D0%A4%D0%B0%D0%B9%D0%BB:Al-kindi_cryptographic.gif&filetimestamp=20080608174535)

Перша сторінка манускрипту[Ал-Кінді](http://znaimo.com.ua/%D0%90%D0%BB-%D0%9A%D1%96%D0%BD%D0%B4%D1%96) - найраніше відома згадка про частотний криптоаналіз

З [VIII століття н.е..](http://znaimo.com.ua/VIII%20%D1%81%D1%82%D0%BE%D0%BB%D1%96%D1%82%D1%82%D1%8F) розвиток криптографії відбувається в основному в арабських країнах. Вважається, що арабський філолог [Халіль аль-Фарахіфі](http://znaimo.com.ua/%D0%A5%D0%B0%D0%BB%D1%96%D0%BB%D1%8C%20%D1%96%D0%B1%D0%BD%20%D0%90%D1%85%D0%BC%D0%B0%D0%B4%20%D0%B0%D0%BB%D1%8C-%D0%A4%D0%B0%D1%80%D0%B0%D1%85%D1%96%D1%84%D1%96) першим звернув увагу на можливість використання стандартних фраз відкритого тексту для дешифрування. Він припустив, що першими словами в листі на грецькій мові візантійського імператора будуть "В ім'я [Аллаха](http://znaimo.com.ua/%D0%90%D0%BB%D0%BB%D0%B0%D1%85) ", що дозволило йому прочитати решту повідомлення. Пізніше він написав книгу з описом методу -" Кітаб аль-Муамма "(" Книга таємного мови ").

В [855 році](http://znaimo.com.ua/855%20%D1%80%D1%96%D0%BA) виходить "Книга про великий прагненні людини розгадати загадки древньої писемності" арабського вченого [Абу Бакр Ахмед ібн Алі Ібн Вахш ан-Набат](http://znaimo.com.ua/%D0%86%D0%B1%D0%BD%20%D0%92%D0%B0%D1%85%D1%88), одна з перших книг про криптографії з описами декількох шифрів, у тому числі із застосуванням декількох алфавітів. Також до [IX століття](http://znaimo.com.ua/IX_%D1%81%D1%82%D0%BE%D0%BB%D1%96%D1%82%D1%82%D1%8F) відноситься перша відома згадка про частотний криптоаналіз - у книзі [Ал-Кінді](http://znaimo.com.ua/%D0%90%D0%BB-%D0%9A%D1%96%D0%BD%D0%B4%D1%96) " [Манускрипт про дешифрування криптографічних повідомлень](http://znaimo.com.ua/%D0%9C%D0%B0%D0%BD%D1%83%D1%81%D0%BA%D1%80%D0%B8%D0%BF%D1%82%20%D0%BF%D1%80%D0%BE%20%D0%B4%D0%B5%D1%88%D0%B8%D1%84%D1%80%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F%20%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%87%D0%BD%D0%B8%D1%85%20%D0%BF%D0%BE%D0%B2%D1%96%D0%B4%D0%BE%D0%BC%D0%BB%D0%B5%D0%BD%D1%8C) ".

У книзі [X століття](http://znaimo.com.ua/X%20%D1%81%D1%82%D0%BE%D0%BB%D1%96%D1%82%D1%82%D1%8F) "Адаб аль-Куттаб" ("Керівництво для секретарів") [ас-Сулі](http://znaimo.com.ua/%D0%A1%D1%83%D0%BB%D0%B8) є інструкції щодо шифрування записів про податки, що підтверджує поширення криптографії у звичайній, громадянського життя.

В [1412](http://znaimo.com.ua/1412) виходить 14-томна енциклопедія [Шихаб ал-Калкашанді](http://ru.wikipedia.org/en.wikipedia.org/wiki/Ahmad_al-Qalqashandi) "Субхі ал-Ааша", один з розділів якої "Щодо приховування в буквах таємних повідомлень" містив опис семи шифрів заміни та перестановки, частотного методу криптоаналізу, а також таблиці частотності букв в арабській мові на основі тексту [Корану](http://znaimo.com.ua/%D0%9A%D0%BE%D1%80%D0%B0%D0%BD). До словника криптології араби внесли такі поняття як [алгоритм](http://znaimo.com.ua/%D0%90%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC) і [шифр](http://znaimo.com.ua/%D0%A8%D0%B8%D1%84%D1%80) .

**3.2. Криптографія**[**епохи Відродження**](http://znaimo.com.ua/%D0%95%D0%BF%D0%BE%D1%85%D0%B0%20%D0%92%D1%96%D0%B4%D1%80%D0%BE%D0%B4%D0%B6%D0%B5%D0%BD%D0%BD%D1%8F)

[](http://ru.wikipedia.org/w/index.php?title=%D0%A4%D0%B0%D0%B9%D0%BB:Roger_Bacon.jpeg&filetimestamp=20090906202149)

[Роджер Бекон](http://znaimo.com.ua/%D0%91%D0%B5%D0%BA%D0%BE%D0%BD%20%D0%A0%D0%BE%D0%B4%D0%B6%D0%B5%D1%80)

Першою європейською книгою, яка описує використання криптографії, вважається праця [Роджера Бекона](http://znaimo.com.ua/%D0%91%D0%B5%D0%BA%D0%BE%D0%BD%20%D0%A0%D0%BE%D0%B4%D0%B6%D0%B5%D1%80) [XIII століття](http://znaimo.com.ua/XIII%20%D1%81%D1%82%D0%BE%D0%BB%D1%96%D1%82%D1%82%D1%8F) " [Послання ченця Роджера Бекона про таємні діях мистецтва і природи і нікчемність магії](http://znaimo.com.ua/%D0%9F%D0%BE%D1%81%D0%BB%D0%B0%D0%BD%D0%BD%D1%8F%20%D1%87%D0%B5%D0%BD%D1%86%D1%8F%20%D0%A0%D0%BE%D0%B4%D0%B6%D0%B5%D1%80%D0%B0%20%D0%91%D0%B5%D0%BA%D0%BE%D0%BD%D0%B0%20%D0%BF%D1%80%D0%BE%20%D1%82%D0%B0%D1%94%D0%BC%D0%BD%D1%96%20%D0%B4%D1%96%D1%8F%D1%85%20%D0%BC%D0%B8%D1%81%D1%82%D0%B5%D1%86%D1%82%D0%B2%D0%B0%20%D1%96%20%D0%BF%D1%80%D0%B8%D1%80%D0%BE%D0%B4%D0%B8%20%D1%96%20%D0%BD%D1%96%D0%BA%D1%87%D0%B5%D0%BC%D0%BD%D1%96%D1%81%D1%82%D1%8C%20%D0%BC%D0%B0%D0%B3%D1%96%D1%97) "( [лат.](http://znaimo.com.ua/%D0%9B%D0%B0%D1%82%D0%B8%D0%BD%D1%81%D1%8C%D0%BA%D1%83%20%D0%BC%D0%BE%D0%B2%D1%83) *"Epistola Fratris Rog. Baconis, de secretis operibus artis et naturae et nullitate magiae"* ) , що описує, серед іншого, застосування 7 методів приховування тексту.

В [XIV столітті](http://znaimo.com.ua/XIV%20%D1%81%D1%82%D0%BE%D0%BB%D1%96%D1%82%D1%82%D1%8F) співробітник таємної канцелярії [папської курії](http://znaimo.com.ua/%D0%9F%D0%B0%D0%BF%D1%81%D1%8C%D0%BA%D0%B0%20%D0%BA%D1%83%D1%80%D1%96%D1%8F) Чікко Сімонеті пише книгу про системи тайнопису, а в [XV столітті](http://znaimo.com.ua/XV_%D1%81%D1%82%D0%BE%D0%BB%D1%96%D1%82%D1%82%D1%8F) секретар папи [Климентія XII](http://znaimo.com.ua/%D0%9A%D0%BB%D0%B8%D0%BC%D0%B5%D0%BD%D1%82%20XII%20(%D0%BF%D0%B0%D0%BF%D0%B0%20%D1%80%D0%B8%D0%BC%D1%81%D1%8C%D0%BA%D0%B8%D0%B9))Габріель де Левінда, родом з міста [Парми](http://znaimo.com.ua/%D0%9F%D0%B0%D1%80%D0%BC%D0%B0), закінчує роботу над "Трактат про шифри".

Симеона де Крема (Simeone de Crema) був першим ( [1401](http://znaimo.com.ua/1401)), хто використовував таблиці [омофонів](http://znaimo.com.ua/%D0%9E%D0%BC%D0%BE%D1%84%D0%BE%D0%BD) для приховування кожного голосного в тексті за допомогою більш ніж одного еквівалента. Через більш ніж сто років ці таблиці для успішного захисту від криптоаналітичних атак використовував [Ернан Кортес](http://znaimo.com.ua/%D0%95%D1%80%D0%BD%D0%B0%D0%BD%20%D0%9A%D0%BE%D1%80%D1%82%D0%B5%D1%81).

Перша організація, що присвятила себе цілком криптографії, була створена в [Венеції](http://znaimo.com.ua/%D0%92%D0%B5%D0%BD%D0%B5%D1%86%D1%96%D1%8F) ( [Італія](http://znaimo.com.ua/%D0%86%D1%82%D0%B0%D0%BB%D1%96%D1%8F)) в [1452](http://znaimo.com.ua/1452). Три секретаря цієї організації займалися зломом і створенням шифрів за завданнями уряду.  У [1469](http://znaimo.com.ua/1469) з'являється шифр пропорційної заміни "Міланський ключ".

[](http://ru.wikipedia.org/w/index.php?title=%D0%A4%D0%B0%D0%B9%D0%BB:Leon_Battista_Alberti_1.jpg&filetimestamp=20060602022205)

Статуя [Альберти](http://znaimo.com.ua/%D0%90%D0%BB%D1%8C%D0%B1%D0%B5%D1%80%D1%82%D1%96_%D0%9B%D0%B5%D0%BE%D0%BD_%D0%91%D0%B0%D1%82%D1%82%D1%96%D1%81%D1%82%D0%B0) у дворі [Уффіци](http://znaimo.com.ua/%D0%A3%D1%84%D1%84%D1%96%D1%86%D0%B8)

Батьком західній криптографії називають ученого [епохи Відродження](http://znaimo.com.ua/%D0%95%D0%BF%D0%BE%D1%85%D0%B0%20%D0%92%D1%96%D0%B4%D1%80%D0%BE%D0%B4%D0%B6%D0%B5%D0%BD%D0%BD%D1%8F) [Леона Баттіста Альберті](http://znaimo.com.ua/%D0%90%D0%BB%D1%8C%D0%B1%D0%B5%D1%80%D1%82%D1%96_%D0%9B%D0%B5%D0%BE%D0%BD_%D0%91%D0%B0%D1%82%D1%82%D1%96%D1%81%D1%82%D0%B0). Вивчивши методи розкриття використовувалися в Європі моноалфавитной шифрів, він спробував створити шифр, який був би стійкий до частотного криптоанализу. Трактат про новий шифрі був представлений їм в папську канцелярію в [1466](http://znaimo.com.ua/1466). Альберті запропонував замість єдиного секретного алфавіту, як в моноалфавитной шифри, використовувати два або більше, перемикаючись між ними по якомусь правилу. Однак флорентійський вчений так і не зміг оформити своє відкриття в повну працюючу систему, що було зроблено вже його послідовниками.  Також Альберті запропонував пристрій із двох скріплених в центрі дисків, кожен з яких мав алфавіт, написаний по краю, і міг повертатися відносного іншого диска. Поки диски не рухаються, вони дозволяють шифрувати з використанням шифру Цезаря, однак через кілька слів диски повертаються, і змінюється ключ зсуву.

[](http://ru.wikipedia.org/w/index.php?title=%D0%A4%D0%B0%D0%B9%D0%BB:Trithemiusmoredetail.jpg&filetimestamp=20090804152148)

Фрагмент оформлення гробниці [Йоганна Трітемія](http://znaimo.com.ua/%D0%A2%D1%80%D1%96%D1%82%D0%B5%D0%BC%D1%96%D0%B9%20%D0%99%D0%BE%D0%B3%D0%B0%D0%BD%D0%BD)

Черговий відомий результат належить перу німецького абата [Йоганна Трітемія](http://znaimo.com.ua/%D0%A2%D1%80%D1%96%D1%82%D0%B5%D0%BC%D1%96%D0%B9%20%D0%99%D0%BE%D0%B3%D0%B0%D0%BD%D0%BD), якого багато істориків вважають другим батьком сучасної криптології.  У п'ятій книзі серії "Polygraphia", виданої в [1518](http://znaimo.com.ua/1518), він описав шифр, в якій кожна наступна буква шифрується своїм власним шифром зсуву. Його підхід був поліпшений Джованні Баттіста Белласе ( [італ.](http://znaimo.com.ua/%D0%86%D1%82%D0%B0%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0%20%D0%BC%D0%BE%D0%B2%D0%B0) [*Giovan Battista Bellaso*](http://ru.wikipedia.org/it.wikipedia.org/wiki/Giovan_Battista_Bellaso)), Який запропонував вибирати деякий ключове слово і записувати його над кожним словом відкритого тексту. Кожна буква ключового слова використовується для вибору конкретного шифру зсуву з повного набору шифрів для шифрування конкретної букви, тоді як в роботі Трітемія шифри вибираються просто по циклу. Для наступного слова відкритого тексту ключ починав використовуватися знову, так, що однакові слова виявлялися зашифровані однаково.  Даний спосіб зараз відомий як [шифр Віженер](http://znaimo.com.ua/%D0%A8%D0%B8%D1%84%D1%80%20%D0%92%D1%96%D0%B6%D0%B5%D0%BD%D0%B5%D1%80) (див. нижче). Крім цього, Трітемій першим помітив, що шифрувати можна і по дві букви за раз - біграм (хоча перший біграммний шифр - Playfair - був запропонований лише в [XIX столітті](http://znaimo.com.ua/XIX%20%D1%81%D1%82%D0%BE%D0%BB%D1%96%D1%82%D1%82%D1%8F)). [[38]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link87) Пізніше, в[XVII столітті](http://znaimo.com.ua/XVII%20%D1%81%D1%82%D0%BE%D0%BB%D1%96%D1%82%D1%82%D1%8F), член [ордена єзуїтів](http://znaimo.com.ua/%D0%84%D0%B7%D1%83%D1%97%D1%82%D0%B8) [Атанасіус Кірхер](http://znaimo.com.ua/%D0%90%D1%82%D0%B0%D0%BD%D0%B0%D1%81%D1%96%D1%83%D1%81%20%D0%9A%D1%96%D1%80%D1%85%D0%B5%D1%80) провів дослідження лінгвістичних аспектів робіт Трітемія, результати яких опублікував у своїй *Polygraphia nova* в [1663](http://znaimo.com.ua/1663). Одним з результатів стало створення "поліглотіческого коду на п'яти мовах", який міг використовуватися для шифрування і передачі повідомлень на [латинською](http://znaimo.com.ua/%D0%9B%D0%B0%D1%82%D0%B8%D0%BD%D1%81%D1%8C%D0%BA%D1%83%20%D0%BC%D0%BE%D0%B2%D1%83), [італійському](http://znaimo.com.ua/%D0%86%D1%82%D0%B0%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0%20%D0%BC%D0%BE%D0%B2%D0%B0), [французькою](http://znaimo.com.ua/%D0%A4%D1%80%D0%B0%D0%BD%D1%86%D1%83%D0%B7%D1%8C%D0%BA%D0%B0%20%D0%BC%D0%BE%D0%B2%D0%B0), [іспанською](http://znaimo.com.ua/%D0%86%D1%81%D0%BF%D0%B0%D0%BD%D1%81%D1%8C%D0%BA%D0%B0%20%D0%BC%D0%BE%D0%B2%D0%B0) та [німецькою](http://znaimo.com.ua/%D0%9D%D1%96%D0%BC%D0%B5%D1%86%D1%8C%D0%BA%D0%B0%20%D0%BC%D0%BE%D0%B2%D0%B0) мовами, при цьому декодування могло проводитися на кожному із зазначених мов.

[](http://ru.wikipedia.org/w/index.php?title=%D0%A4%D0%B0%D0%B9%D0%BB:GirolamoCardano.jpeg&filetimestamp=20090707103128)

[Джероламо Кардано](http://znaimo.com.ua/%D0%94%D0%B6%D0%B5%D1%80%D0%BE%D0%BB%D0%B0%D0%BC%D0%BE%20%D0%9A%D0%B0%D1%80%D0%B4%D0%B0%D0%BD%D0%BE)

В [1550](http://znaimo.com.ua/1550) італійський математик [Джероламо Кардано](http://znaimo.com.ua/%D0%94%D0%B6%D0%B5%D1%80%D0%BE%D0%BB%D0%B0%D0%BC%D0%BE%20%D0%9A%D0%B0%D1%80%D0%B4%D0%B0%D0%BD%D0%BE), перебуває на службі у [папи римського](http://znaimo.com.ua/%D0%9F%D0%B0%D0%BF%D0%B0%20%D1%80%D0%B8%D0%BC%D1%81%D1%8C%D0%BA%D0%B8%D0%B9), запропонував нову техніку шифрування - [грати Кардано](http://znaimo.com.ua/%D0%A0%D0%B5%D1%88%D1%96%D1%82%D0%BA%D0%B0%20%D0%9A%D0%B0%D1%80%D0%B4%D0%B0%D0%BD%D0%BE). Цей спосіб поєднував в собі як [стеганографія](http://znaimo.com.ua/%D0%A1%D1%82%D0%B5%D0%B3%D0%B0%D0%BD%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%8F) (мистецтво прихованого листа), так і криптографію. Утруднення становило навіть зрозуміти, що повідомлення містить зашифрований текст, а розшифрувати його, не маючи ключа (грати) в той час було практично неможливо. Грати Кардано вважають першим транспозіціонним шифром, або, як ще називають, геометричним шифром, заснованим на положенні букв в шіфротекста. [[41]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link93) Інший транспозіціонний шифр, набагато легший, використовувався в [XVII столітті](http://znaimo.com.ua/XVII%20%D1%81%D1%82%D0%BE%D0%BB%D1%96%D1%82%D1%82%D1%8F) під час втечі Джона Треваньона від сил [Кромвеля](http://znaimo.com.ua/%D0%9A%D1%80%D0%BE%D0%BC%D0%B2%D0%B5%D0%BB%D1%8C%20%D0%9E%D0%BB%D1%96%D0%B2%D0%B5%D1%80), а також під час [Другої світової війни](http://znaimo.com.ua/%D0%94%D1%80%D1%83%D0%B3%D0%B0%20%D1%81%D0%B2%D1%96%D1%82%D0%BE%D0%B2%D0%B0%20%D0%B2%D1%96%D0%B9%D0%BD%D0%B0) для спроб передачі відомостей офіцерами захопленої німецького підводного човна в листах додому.

[](http://ru.wikipedia.org/w/index.php?title=%D0%A4%D0%B0%D0%B9%D0%BB:Francis_Bacon,_Viscount_St_Alban_from_NPG_(2).jpg&filetimestamp=20090401124633)

[Френсіс Бекон](http://znaimo.com.ua/%D0%91%D0%B5%D0%BA%D0%BE%D0%BD%20%D0%A4%D1%80%D0%B5%D0%BD%D1%81%D1%96%D1%81)

[Френсіс Бекон](http://znaimo.com.ua/%D0%91%D0%B5%D0%BA%D0%BE%D0%BD%20%D0%A4%D1%80%D0%B5%D0%BD%D1%81%D1%96%D1%81) у своїй першій роботі [1580](http://znaimo.com.ua/1580) запропонував двійковий спосіб кодування латинського алфавіту, за принципом аналогічний тому, що зараз використовується в комп'ютерах.  Використовуючи цей принцип, а також маючи два різні способи накреслення для кожної з букв, відправник міг "заховати" у тексті одного довгого повідомлення короткий секретне.  Даний спосіб отримав назву " [шифр Бекона](http://znaimo.com.ua/%D0%A8%D0%B8%D1%84%D1%80%20%D0%91%D0%B5%D0%BA%D0%BE%D0%BD%D0%B0) ", хоча належить більше до [стеганографії](http://znaimo.com.ua/%D0%A1%D1%82%D0%B5%D0%B3%D0%B0%D0%BD%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%8F).

[](http://ru.wikipedia.org/w/index.php?title=%D0%A4%D0%B0%D0%B9%D0%BB:Vigenere.jpg&filetimestamp=20090225213917)

[Блез де Віженер](http://znaimo.com.ua/%D0%92%D1%96%D0%B6%D0%B5%D0%BD%D0%B5%D1%80%20%D0%91%D0%BB%D0%B5%D0%B7%20%D0%B4%D0%B5)

Найвідомішим криптографом [XVI століття](http://znaimo.com.ua/XVI%20%D1%81%D1%82%D0%BE%D0%BB%D1%96%D1%82%D1%82%D1%8F) можна назвати [Блеза де Віженер](http://znaimo.com.ua/%D0%92%D1%96%D0%B6%D0%B5%D0%BD%D0%B5%D1%80%20%D0%91%D0%BB%D0%B5%D0%B7%20%D0%B4%D0%B5). У своєму трактаті [1585](http://znaimo.com.ua/1585) він описав шифр, подібний шифру Трітемія, проте змінив систему вибору конкретного шифру заміни для кожної літери. Однією із запропонованих технік було використання букв іншого відкритого тексту для вибору ключа кожної літери початкового тексту. Описаний шифр відомий як [шифр Віженер](http://znaimo.com.ua/%D0%A8%D0%B8%D1%84%D1%80%20%D0%92%D1%96%D0%B6%D0%B5%D0%BD%D0%B5%D1%80) і, при довжині випадкового ключа дорівнює довжині відкритого тексту, є абсолютно стійким шифром, що було математично доведено багато пізніше (в [XX столітті](http://znaimo.com.ua/XX_%D1%81%D1%82%D0%BE%D0%BB%D1%96%D1%82%D1%82%D1%8F) в роботах Шеннона). Інша техніка використовувала результат шифрування для вибору наступного ключа - те, що згодом використовує [Фейстель](http://znaimo.com.ua/%D0%A4%D0%B5%D0%B9%D1%81%D1%82%D0%B5%D0%BB%D1%8C%20%D0%A5%D0%BE%D1%80%D1%81%D1%82) і [компанія IBM](http://znaimo.com.ua/IBM) при розробці шифру [DES](http://znaimo.com.ua/DES) в 1970-х роках. [[19]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link57)

[](http://ru.wikipedia.org/w/index.php?title=%D0%A4%D0%B0%D0%B9%D0%BB:Mary-cipher-code.jpg&filetimestamp=20100720102519)

Шифровка Марії Стюарт

У процесі над [Марією Стюарт](http://znaimo.com.ua/%D0%9C%D0%B0%D1%80%D1%96%D1%8F%20%D0%A1%D1%82%D1%8E%D0%B0%D1%80%D1%82) в якості доказів наводилися листи до змовників, які вдалося розшифрувати. Використовувався [шифр підстановки](http://znaimo.com.ua/%D0%A8%D0%B8%D1%84%D1%80%20%D0%BF%D1%96%D0%B4%D1%81%D1%82%D0%B0%D0%BD%D0%BE%D0%B2%D0%BA%D0%B8), з добавкою ще кілька особливих знаків, щоб утруднити розшифровку. Деякі знаки означали слова, інші не означали нічого, ще один знак означав, що подальша буква - подвійна.

До [1639](http://znaimo.com.ua/1639) відноситься перша згадка  про [рукописи Войнича](http://znaimo.com.ua/%D0%A0%D1%83%D0%BA%D0%BE%D0%BF%D0%B8%D1%81%20%D0%92%D0%BE%D0%B9%D0%BD%D0%B8%D1%87%D0%B0) - книзі, написаній невідомим автором на невідомій мові. Розшифрувати її намагалися багато відомих криптографи, але, не виключено, що рукопис є всього лише містифікацією.

Криптоаналітика Етьєн Базері ( [англ.](http://znaimo.com.ua/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0%20%D0%BC%D0%BE%D0%B2%D0%B0) [*tienne Bazeries*](http://ru.wikipedia.org/en.wikipedia.org/wiki/%C3%89tienne_Bazeries) ) (1846-1931) зміг, пропрацювавши три роки, розшифрувати архіви [Людовика XIV](http://znaimo.com.ua/%D0%9B%D1%8E%D0%B4%D0%BE%D0%B2%D0%B8%D0%BA%20XIV), зашифровані "Великому шифром ( [англ.](http://znaimo.com.ua/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0%20%D0%BC%D0%BE%D0%B2%D0%B0) [*Great Cipher*](http://ru.wikipedia.org/en.wikipedia.org/wiki/Great_Cipher) ) "За системою Россіньоло ( [англ.](http://znaimo.com.ua/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0%20%D0%BC%D0%BE%D0%B2%D0%B0) [*Rossignols*](http://ru.wikipedia.org/en.wikipedia.org/wiki/Rossignols) ) В [XVII столітті](http://znaimo.com.ua/XVII%20%D1%81%D1%82%D0%BE%D0%BB%D1%96%D1%82%D1%82%D1%8F). У паперах знайшовся наказу короля помістити на закінчення в'язня з тим, щоб вдень він з'являвся лише в масці. Їм окaзался генерал Вів'єн де Булонд ( [фр.](http://znaimo.com.ua/%D0%A4%D1%80%D0%B0%D0%BD%D1%86%D1%83%D0%B7%D1%8C%D0%BA%D0%B0%20%D0%BC%D0%BE%D0%B2%D0%B0) *Vivien de Bulonde* ), Покрили ганьбою себе і французьку армію під час[Дев'ятирічної війни](http://znaimo.com.ua/%D0%92%D1%96%D0%B9%D0%BD%D0%B0%20%D0%90%D1%83%D0%B3%D1%81%D0%B1%D1%83%D1%80%D0%B3%D1%81%D0%BA%D0%BE%D0%B9%20%D0%BB%D1%96%D0%B3%D0%B8). Судячи з усього, це і є знаменита " [Залізна маска](http://znaimo.com.ua/%D0%97%D0%B0%D0%BB%D1%96%D0%B7%D0%BD%D0%B0%20%D0%BC%D0%B0%D1%81%D0%BA%D0%B0) ". Королівський шифр протримався 200 років!

**3.3. Іспанська імперія і колонії в Америці. "Індіанська криптографія"**

В [XVI столітті](http://znaimo.com.ua/XVI%20%D1%81%D1%82%D0%BE%D0%BB%D1%96%D1%82%D1%82%D1%8F) при дипломатичному листуванні імператора [Карла I](http://znaimo.com.ua/%D0%9A%D0%B0%D1%80%D0%BB%20V%20(%D1%96%D0%BC%D0%BF%D0%B5%D1%80%D0%B0%D1%82%D0%BE%D1%80%20%D0%A1%D0%B2%D1%8F%D1%89%D0%B5%D0%BD%D0%BD%D0%BE%D1%97%20%D0%A0%D0%B8%D0%BC%D1%81%D1%8C%D0%BA%D0%BE%D1%97%20%D1%96%D0%BC%D0%BF%D0%B5%D1%80%D1%96%D1%97)) стає популярним метод *nomenclator* - покажчик географічних назв [[47]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link101). [11 березня](http://znaimo.com.ua/11%20%D0%B1%D0%B5%D1%80%D0%B5%D0%B7%D0%BD%D1%8F) [1532](http://znaimo.com.ua/1532)Родріго Ніньо, посол в [Венеції](http://znaimo.com.ua/%D0%92%D0%B5%D0%BD%D0%B5%D1%86%D1%96%D1%8F), використовував його для того, щоб нагадати імператорові про деяких засобах захисту на той випадок, якщо турецький султан захоче захопити фортецю Кліси в [Далмації](http://znaimo.com.ua/%D0%94%D0%B0%D0%BB%D0%BC%D0%B0%D1%86%D1%96%D1%8F) (близько [Спліта](http://znaimo.com.ua/%D0%A1%D0%BF%D0%BB%D1%96%D1%82%20(%D0%BC%D1%96%D1%81%D1%82%D0%BE)), [Хорватія](http://znaimo.com.ua/%D0%A5%D0%BE%D1%80%D0%B2%D0%B0%D1%82%D1%96%D1%8F)) [[48]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link102). Майже 25 років по тому те ж саме зробив маркіз де Мондехар, віце-король [Неаполя](http://znaimo.com.ua/%D0%9D%D0%B5%D0%B0%D0%BF%D0%BE%D0%BB%D1%8C), щоб сповістити [Філіпа II](http://znaimo.com.ua/%D0%A4%D1%96%D0%BB%D1%96%D0%BF%20II%20(%D0%BA%D0%BE%D1%80%D0%BE%D0%BB%D1%8C%20%D0%86%D1%81%D0%BF%D0%B0%D0%BD%D1%96%D1%97)) про можливі переговори щодо перемир'я між християнами і турками, що стало причиною кризи імперської розвідки в Середземномор'ї. Бернардіно де Мендоса ( [1541](http://znaimo.com.ua/1541) - [1604](http://znaimo.com.ua/1604)), посол Іспанії в Англії і Франції в багатьох своїх листах використовував метод *nomenclator,* де особливу роль грала заміна букв цифрами і шифр з биграмм (наприклад, BL = 23, BR = 24, y TR = 34) .

[](http://ru.wikipedia.org/w/index.php?title=%D0%A4%D0%B0%D0%B9%D0%BB:Carta-cifrada-de-25-06-1532-de-Hernan-Cortes-y-tabla-de-su-codigo.jpg&filetimestamp=20100306114303)

Закодоване лист[Ернана Кортеса](http://znaimo.com.ua/%D0%95%D1%80%D0%BD%D0%B0%D0%BD%20%D0%9A%D0%BE%D1%80%D1%82%D0%B5%D1%81) з використанням комбінованого шифру з підстановкою[омофонів](http://znaimo.com.ua/%D0%9E%D0%BC%D0%BE%D1%84%D0%BE%D0%BD) і методу*nomenclator.*

Термін *"індіанська криптографія" ("criptografa indiana"),* впроваджений дослідником Гільєрмо Ломанн Вільєна ( [ісп.](http://znaimo.com.ua/%D0%86%D1%81%D0%BF%D0%B0%D0%BD%D1%81%D1%8C%D0%BA%D0%B0%20%D0%BC%D0%BE%D0%B2%D0%B0) [*Guillermo Lohmann Villena*](http://ru.wikipedia.org/es.wikipedia.org/wiki/Guillermo_Lohmann_Villena) ), Застосовується для позначення зашифрованих документів в іспанських колоніях Америки. Першим відомим документом на території Америки, в якому використовувався шифр *("caracteres ignotos")* була депеша [Христофора Колумба](http://znaimo.com.ua/%D0%A5%D1%80%D0%B8%D1%81%D1%82%D0%BE%D1%84%D0%BE%D1%80%20%D0%9A%D0%BE%D0%BB%D1%83%D0%BC%D0%B1), адресована [Дієго Колумбу](http://znaimo.com.ua/%D0%9A%D0%BE%D0%BB%D0%BE%D0%BD%20%D0%94%D1%96%D1%94%D0%B3%D0%BE) в [1500](http://znaimo.com.ua/1500), і перехоплена губернатором [Санто-Домінго](http://znaimo.com.ua/%D0%A1%D0%B0%D0%BD%D1%82%D0%BE-%D0%94%D0%BE%D0%BC%D1%96%D0%BD%D0%B3%D0%BE), Франсиско де Бобаділья [[50]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link104).

Листи зашифровували не тільки віце-королі і вищі сановники, а й представники католицьких орденів і окремі особистості [[51]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link105) : свій шифр мав завойовник[Мексики](http://znaimo.com.ua/%D0%9C%D0%B5%D0%BA%D1%81%D0%B8%D0%BA%D0%B0) [Ернан Кортес](http://znaimo.com.ua/%D0%95%D1%80%D0%BD%D0%B0%D0%BD%20%D0%9A%D0%BE%D1%80%D1%82%D0%B5%D1%81) (використовував: комбінований шифр з підстановкою [омофонів](http://znaimo.com.ua/%D0%9E%D0%BC%D0%BE%D1%84%D0%BE%D0%BD) та кодування; а також метод *nomenclator)* [[52]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link106) і [віце-королі Перу](http://znaimo.com.ua/%D0%A1%D0%BF%D0%B8%D1%81%D0%BE%D0%BA%20%D0%B2%D1%96%D1%86%D0%B5-%D0%BA%D0%BE%D1%80%D0%BE%D0%BB%D1%96%D0%B2%20%D0%9F%D0%B5%D1%80%D1%83) [Педро де ла Гаске](http://znaimo.com.ua/%D0%93%D0%B0%D1%81%D0%BA%D0%B5%20%D0%9F%D0%B5%D0%B4%D1%80%D0%BE%20%D0%B4%D0%B5%20%D0%BB%D0%B0) [[53]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link107), [Франсиско де Толедо](http://znaimo.com.ua/%D0%A2%D0%BE%D0%BB%D0%B5%D0%B4%D0%BE%20%D0%A4%D1%80%D0%B0%D0%BD%D1%81%D0%B8%D1%81%D0%BA%D0%BE%20%D0%B4%D0%B5) [[54]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link108), адмірал Антоніо де Агуайо [[55]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link109). Іспанська Державна Рада ( [ісп.](http://znaimo.com.ua/%D0%86%D1%81%D0%BF%D0%B0%D0%BD%D1%81%D1%8C%D0%BA%D0%B0%20%D0%BC%D0%BE%D0%B2%D0%B0) [*Consejo de Estado de Espaa*](http://ru.wikipedia.org/es.wikipedia.org/wiki/Consejo_de_Estado_de_Espa%C3%B1a) ) Забезпечив [графа де Чінчон](http://znaimo.com.ua/%D0%9A%D0%B0%D0%B1%D1%80%D0%B5%D1%80%D0%B0%20%D0%9B%D1%83%D1%97%D1%81%20%D0%A5%D0%B5%D1%80%D0%BE%D0%BD%D1%96%D0%BC%D0%BE%20%D0%B4%D0%B5), губернатора Перу з [1629](http://znaimo.com.ua/1629) по [1639 роки](http://znaimo.com.ua/1639), новим винаходом в криптографії початку [XVII століття](http://znaimo.com.ua/XVII%20%D1%81%D1%82%D0%BE%D0%BB%D1%96%D1%82%D1%82%D1%8F) - покажчиком індіанських географічних назв *("nomenclator indiano");* одночасно з цим була упроваджена нова система - букви заміщалися двома цифрами (наприклад, AL - 86, BA - 31, BE - 32, BI - 33) , використовувалися також триграми.

Унікальний [складової](http://znaimo.com.ua/%D0%A1%D0%BA%D0%BB%D0%B0%D0%B4) шифр єзуїтів використаний в [Зошити Бласа Валера](http://znaimo.com.ua/Exsul%20immeritus%20blas%20valera%20populo%20suo) ( [Куско](http://znaimo.com.ua/%D0%9A%D1%83%D1%81%D0%BA%D0%BE), [1616](http://znaimo.com.ua/1616)); одночасно в документі міститься [дешифровка](http://znaimo.com.ua/%D0%94%D0%B5%D1%88%D0%B8%D1%84%D1%80%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F) інкських [стос](http://znaimo.com.ua/%D0%A1%D1%82%D0%BE%D1%81), [юпани](http://znaimo.com.ua/%D0%AE%D0%BF%D0%B0%D0%BD%D0%B0), знаків [токапу](http://znaimo.com.ua/%D0%A2%D0%BE%D0%BA%D0%B0%D0%BF%D1%83) і [секес](http://znaimo.com.ua/%D0%A1%D0%B5%D0%BA%D0%B5), багато в чому і послужили основою для створення шифру [[57]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link111); оскільки ключове значення в стос і в шифрі мав колір, то він послужив приводом для винаходу в [1749](http://znaimo.com.ua/1749) італійцем [Раймондо де Сангро](http://znaimo.com.ua/%D0%A0%D0%B0%D0%B9%D0%BC%D0%BE%D0%BD%D0%B4%D0%BE%20%D0%B4%D0%B5%20%D0%A1%D0%B0%D0%BD%D0%B3%D1%80%D0%BE) методу [кольорового друкарства](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F%20%D0%B4%D1%80%D1%83%D0%BA%D0%B0%D1%80%D1%81%D1%82%D0%B2%D0%B0%20%D0%B2%20%D0%84%D0%B2%D1%80%D0%BE%D0%BF%D1%96).

**3.4. Чорні кабінети**

[](http://ru.wikipedia.org/w/index.php?title=%D0%A4%D0%B0%D0%B9%D0%BB:Antoine_Rossignol.jpg&filetimestamp=20100109181854)

Антуан Россіньоло

[](http://ru.wikipedia.org/w/index.php?title=%D0%A4%D0%B0%D0%B9%D0%BB:John_Wallis_by_Sir_Godfrey_Kneller,_Bt.jpg&filetimestamp=20090329150833)

[Джон Валліс](http://znaimo.com.ua/%D0%94%D0%B6%D0%BE%D0%BD%20%D0%92%D0%B0%D0%BB%D0%BB%D1%96%D1%81)

В [1626](http://znaimo.com.ua/1626), при облозі міста [Реальмон](http://znaimo.com.ua/%D0%A0%D0%B5%D0%B0%D0%BB%D1%8C%D0%BC%D0%BE%D0%BD), а пізніше і в [1628](http://znaimo.com.ua/1628) при [облозі Ла-Рошелі](http://znaimo.com.ua/%D0%9E%D0%B1%D0%BB%D0%BE%D0%B3%D0%B0%20%D0%9B%D0%B0-%D0%A0%D0%BE%D1%88%D0%B5%D0%BB%D1%96), французький підданий Антуан Россіньоло ( [фр.](http://znaimo.com.ua/%D0%A4%D1%80%D0%B0%D0%BD%D1%86%D1%83%D0%B7%D1%8C%D0%BA%D0%B0%20%D0%BC%D0%BE%D0%B2%D0%B0) *Antoine Rossignol* , 1600-1682) розшифрував перехоплені повідомлення, і тим самим допоміг перемогти армію [гугенотів](http://znaimo.com.ua/%D0%93%D1%83%D0%B3%D0%B5%D0%BD%D0%BE%D1%82). Після перемоги уряд Франції кілька разів залучали його до розшифровки шифрів. Після його смерті його син ( [фр.](http://znaimo.com.ua/%D0%A4%D1%80%D0%B0%D0%BD%D1%86%D1%83%D0%B7%D1%8C%D0%BA%D0%B0%20%D0%BC%D0%BE%D0%B2%D0%B0) *Bonaventure Rossignol* ), А пізніше і онук ( [фр.](http://znaimo.com.ua/%D0%A4%D1%80%D0%B0%D0%BD%D1%86%D1%83%D0%B7%D1%8C%D0%BA%D0%B0%20%D0%BC%D0%BE%D0%B2%D0%B0) *Antoine-Bonaventure Rossignol* ), Продовжили справу батька. У той час уряд Франції приваблювало до роботи безліч криптографов, які разом утворювали так званий "Чорний кабінет" ( [фр.](http://znaimo.com.ua/%D0%A4%D1%80%D0%B0%D0%BD%D1%86%D1%83%D0%B7%D1%8C%D0%BA%D0%B0%20%D0%BC%D0%BE%D0%B2%D0%B0) *Cabinet Noir* ). [[19]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link57)

Антуану Россіньоло належить доктрина, згідно з якою стійкість шифру повинна визначатися видом зашифрованої інформації. Для військового часу достатньою буде стійкість, якщо повідомлення з наказом армійському підрозділу не буде розшифровано противником хоча б до моменту виконання одержувачем, а для дипломатичної пошти шифр повинен забезпечувати збереження на десятки років. [[1]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link33)

У Росії датою заснування першої державної шифрувальної служби можна вважати [1549](http://znaimo.com.ua/1549) - утворення "посольського наказу" з "ціферним відділенням". А як мінімум з [1702](http://znaimo.com.ua/1702) [Петра](http://znaimo.com.ua/%D0%9F%D0%B5%D1%82%D1%80%D0%BE%20I) супроводжувала похідна посольська канцелярія під керівництвом першого міністра [Ф. А. Головіна](http://znaimo.com.ua/%D0%93%D0%BE%D0%BB%D0%BE%D0%B2%D1%96%D0%BD%20%D0%A4%D0%B5%D0%B4%D1%96%D1%80%20%D0%9E%D0%BB%D0%B5%D0%BA%D1%81%D1%96%D0%B9%D0%BE%D0%B2%D0%B8%D1%87), яка з [1710](http://znaimo.com.ua/1710) набула статусу постійного представництва. У ньому зосередилася криптографічний робота з листуванням між Петром, його наближеними та різними одержувачами, а також зі створення нових шифрів.

Згодом над дешифрованием повідомлень в Росії трудилися в тому числі такі математики як [Крістіан Гольдбах](http://znaimo.com.ua/%D0%9A%D1%80%D1%96%D1%81%D1%82%D1%96%D0%B0%D0%BD%20%D0%93%D0%BE%D0%BB%D1%8C%D0%B4%D0%B1%D0%B0%D1%85), [Леонард Ейлер](http://znaimo.com.ua/%D0%9B%D0%B5%D0%BE%D0%BD%D0%B0%D1%80%D0%B4%20%D0%95%D0%B9%D0%BB%D0%B5%D1%80) та [Франц Епінус](http://znaimo.com.ua/%D0%A4%D1%80%D0%B0%D0%BD%D1%86%20%D0%95%D0%BF%D1%96%D0%BD%D1%83%D1%81). При цьому під час [Семирічної війни](http://znaimo.com.ua/%D0%A1%D0%B5%D0%BC%D0%B8%D1%80%D1%96%D1%87%D0%BD%D0%B0%20%D0%B2%D1%96%D0%B9%D0%BD%D0%B0) ( [1756](http://znaimo.com.ua/1756) - [1763](http://znaimo.com.ua/1763)) Ейлер, перебуваючи в [Пруссії](http://znaimo.com.ua/%D0%9F%D1%80%D1%83%D1%81%D1%81%D1%96%D1%8F), хоча і продовжував листуватися з вищими особами Російської імперії, також займався дешифровкою перехоплених листів російських офіцерів.

На початок [XVIII століття](http://znaimo.com.ua/XVIII%20%D1%81%D1%82%D0%BE%D0%BB%D1%96%D1%82%D1%82%D1%8F) подібні кабінети були по всій Європі, в тому числі "Die Geheime Kabinettskanzlei" у Відні, перше дешифровальной відділення в [Німеччині](http://znaimo.com.ua/%D0%9D%D1%96%D0%BC%D0%B5%D1%87%D1%87%D0%B8%D0%BD%D0%B0)під начальством графа Гронсфельда , група [Джона Валліса](http://znaimo.com.ua/%D0%92%D0%B0%D0%BB%D0%BB%D1%96%D1%81%20%D0%94%D0%B6%D0%BE%D0%BD) в Англії. До, під час і після [війни за незалежність США](http://znaimo.com.ua/%D0%92%D1%96%D0%B9%D0%BD%D0%B0%20%D0%B7%D0%B0%20%D0%BD%D0%B5%D0%B7%D0%B0%D0%BB%D0%B5%D0%B6%D0%BD%D1%96%D1%81%D1%82%D1%8C%20%D0%A1%D0%A8%D0%90) вони виявилися здатні розкрити велику частину колоніальних шифрів. Більшість з них було закрито до середини [XIX століття](http://znaimo.com.ua/XIX%20%D1%81%D1%82%D0%BE%D0%BB%D1%96%D1%82%D1%82%D1%8F), в тому числі, за однією з версій - через відсутність збройного протистояння з США.

**3.5. Криптографія в британських колоніях і США**

[](http://ru.wikipedia.org/w/index.php?title=%D0%A4%D0%B0%D0%B9%D0%BB:Benedict_arnold_illustration.jpg&filetimestamp=20070219043509)

[Бенедикт Арнольд](http://znaimo.com.ua/%D0%91%D0%B5%D0%BD%D0%B5%D0%B4%D0%B8%D0%BA%D1%82%20%D0%90%D1%80%D0%BD%D0%BE%D0%BB%D1%8C%D0%B4)

Однак у британських колоніях, найчастіше, централізованих організацій не було - перехоплення і дешифрування виконувалися звичайними службовцями, при можливості. Відомий випадок дешифрування листа [1775](http://znaimo.com.ua/1775) головного хірурга армії США ( [англ.](http://znaimo.com.ua/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0%20%D0%BC%D0%BE%D0%B2%D0%B0) [*Surgeon General of the United States Army*](http://ru.wikipedia.org/en.wikipedia.org/wiki/Surgeon_General_of_the_United_States_Army) ) Бенджаміна Черча ([англ.](http://znaimo.com.ua/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0%20%D0%BC%D0%BE%D0%B2%D0%B0) [*Benjamin Church*](http://ru.wikipedia.org/en.wikipedia.org/wiki/Benjamin_Church) ), Адресований британцям, в якому він ставив командування ворога до відома про армію США близько Бостона. Хоча в листі не містилося дійсно секретних даних, його попросили припинити подібну листування. [Бенедикт Арнольд](http://znaimo.com.ua/%D0%91%D0%B5%D0%BD%D0%B5%D0%B4%D0%B8%D0%BA%D1%82%20%D0%90%D1%80%D0%BD%D0%BE%D0%BB%D1%8C%D0%B4), генерал армії США, відомий в тому числі через використання "кодової книги", копія якої повинна бути у кожного відправника і одержувача повідомлень. Шифр полягав у вказівці позиції слова в книзі, в тому числі сторінки, рядки і номери в рядку.  Даний метод отримав назву [книжкового шифру](http://znaimo.com.ua/%D0%9A%D0%BD%D0%B8%D0%B6%D0%BA%D0%BE%D0%B2%D0%B8%D0%B9%20%D1%88%D0%B8%D1%84%D1%80).

Батьком криптографії США називають вчителя і державного діяча [Джеймса Ловелл](http://znaimo.com.ua/%D0%9B%D0%BE%D0%B2%D0%B5%D0%BB%D0%BB%20%D0%94%D0%B6%D0%B5%D0%B9%D0%BC%D1%81). Під час [війни за незалежність США](http://znaimo.com.ua/%D0%92%D1%96%D0%B9%D0%BD%D0%B0%20%D0%B7%D0%B0%20%D0%BD%D0%B5%D0%B7%D0%B0%D0%BB%D0%B5%D0%B6%D0%BD%D1%96%D1%81%D1%82%D1%8C%20%D0%A1%D0%A8%D0%90) він дешифрував безліч британських повідомлень, одне з яких заклало основу для остаточної перемоги у війні.  У майбутньому Ловелл став членом комітету з секретної кореспонденції, четвертим, після [Бенджаміна Франкліна](http://znaimo.com.ua/%D0%A4%D1%80%D0%B0%D0%BD%D0%BA%D0%BB%D1%96%D0%BD%20%D0%91%D0%B5%D0%BD%D0%B4%D0%B6%D0%B0%D0%BC%D1%96%D0%BD) (Пенсільванія), Бенджаміна Гаррісона ( [англ.](http://znaimo.com.ua/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0%20%D0%BC%D0%BE%D0%B2%D0%B0) [*Benjamin Harrison V*](http://ru.wikipedia.org/en.wikipedia.org/wiki/Benjamin_Harrison_V) ) (Віргінія) і Томаса Джонсона ( [англ.](http://znaimo.com.ua/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0%20%D0%BC%D0%BE%D0%B2%D0%B0) [*Thomas Johnson*](http://ru.wikipedia.org/en.wikipedia.org/wiki/Thomas_Johnson_(jurist)) ) (Меріленд). Саме там Джеймс заслужив своє визнання експерта [конгресу](http://znaimo.com.ua/%D0%9A%D0%BE%D0%BD%D1%82%D0%B8%D0%BD%D0%B5%D0%BD%D1%82%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D0%B9%20%D0%BA%D0%BE%D0%BD%D0%B3%D1%80%D0%B5%D1%81) з криптографії і став називатися батьком американської криптографії. [[61]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link123)

[](http://ru.wikipedia.org/w/index.php?title=%D0%A4%D0%B0%D0%B9%D0%BB:T_Jefferson_by_Charles_Willson_Peale_1791_2.jpg&filetimestamp=20060316214144)

[Томас Джефферсон](http://znaimo.com.ua/%D0%94%D0%B6%D0%B5%D1%84%D1%84%D0%B5%D1%80%D1%81%D0%BE%D0%BD%20%D0%A2%D0%BE%D0%BC%D0%B0%D1%81)

У 1790-х роках  майбутній [президент США](http://znaimo.com.ua/%D0%9F%D1%80%D0%B5%D0%B7%D0%B8%D0%B4%D0%B5%D0%BD%D1%82%20%D0%A1%D0%A8%D0%90) [Томас Джефферсон](http://znaimo.com.ua/%D0%94%D0%B6%D0%B5%D1%84%D1%84%D0%B5%D1%80%D1%81%D0%BE%D0%BD%20%D0%A2%D0%BE%D0%BC%D0%B0%D1%81) побудував одну з перших механічних роторних машин, спрощує використання поліалфавітних шифрів [[63]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link125). Серед інших авторів-винахідників варто відзначити полковника Десіуса Вадсворта ( [англ.](http://znaimo.com.ua/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0%20%D0%BC%D0%BE%D0%B2%D0%B0) [*Decius Wadsworth*](http://ru.wikipedia.org/en.wikipedia.org/wiki/Decius_Wadsworth) ), Винахідника машини з обертальними шифрувальними дисками з різною кількістю букв. Хоча він винайшов її в [1817](http://znaimo.com.ua/1817), вся слава дісталася [Чарлзу Уїтстона](http://znaimo.com.ua/%D0%A3%D1%97%D1%82%D1%81%D1%82%D0%BE%D0%BD%D0%B0%20%D0%A7%D0%B0%D1%80%D0%BB%D1%8C%D0%B7) за аналогічну машину, представлену на[Всесвітній виставці 1867 року в Парижі](http://znaimo.com.ua/%D0%92%D1%81%D0%B5%D1%81%D0%B2%D1%96%D1%82%D0%BD%D1%8F%20%D0%B2%D0%B8%D1%81%D1%82%D0%B0%D0%B2%D0%BA%D0%B0%20(1867)).  Однак поширення роторні машини отримали лише на початку [XX століття](http://znaimo.com.ua/XX_%D1%81%D1%82%D0%BE%D0%BB%D1%96%D1%82%D1%82%D1%8F).

Значний поштовх криптографії дало винахід телеграфу. Сама передача даних перестала бути секретною, і повідомлення, в теорії, міг перехопити хто завгодно. Інтерес до криптографії зріс в тому числі і серед простого населення, внаслідок чого багато спробували створити індивідуальні системи шифрування. Перевага телеграфу було явним і на полі бою, де командувач повинен був віддавати негайні накази по всій лінії фронту або хоча б на всьому полі бою, а також отримувати інформацію з місць подій. Це послужило поштовхом до розвитку польових шифрів. Спочатку армія США використовувала [шифр Віженер](http://znaimo.com.ua/%D0%A8%D0%B8%D1%84%D1%80%20%D0%92%D1%96%D0%B6%D0%B5%D0%BD%D0%B5%D1%80) з коротким ключовим словом, однак, після відкриття [методу Касіскі](http://znaimo.com.ua/%D0%9C%D0%B5%D1%82%D0%BE%D0%B4%20%D0%9A%D0%B0%D1%81%D1%96%D1%81%D0%BA%D1%96) в [1863](http://znaimo.com.ua/1863), він був замінений. [[19]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link57)

[](http://ru.wikipedia.org/w/index.php?title=%D0%A4%D0%B0%D0%B9%D0%BB:Wheatstone_Charles_drawing_1868.jpg&filetimestamp=20080926140725)

[Чарлз Уїтстона](http://znaimo.com.ua/%D0%A3%D1%97%D1%82%D1%81%D1%82%D0%BE%D0%BD%D0%B0%20%D0%A7%D0%B0%D1%80%D0%BB%D1%8C%D0%B7)

[](http://ru.wikipedia.org/w/index.php?title=%D0%A4%D0%B0%D0%B9%D0%BB:Lyon_Playfair.jpg&filetimestamp=20050818104520)

Ліон Плейфера

Подальший прогрес був пов'язаний як з індивідуальними, так і з державними дослідженнями. В [1854](http://znaimo.com.ua/1854) [Чарлз Уїтстона](http://znaimo.com.ua/%D0%A3%D1%97%D1%82%D1%81%D1%82%D0%BE%D0%BD%D0%B0%20%D0%A7%D0%B0%D1%80%D0%BB%D1%8C%D0%B7) описав, а Ліон Плейфера ( [англ.](http://znaimo.com.ua/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0%20%D0%BC%D0%BE%D0%B2%D0%B0) [*Lyon Playfair*](http://ru.wikipedia.org/en.wikipedia.org/wiki/Lyon_Playfair,_1st_Baron_Playfair) ) Домігся застосування британськими збройними силами нового шифру, як його пізніше назвуть - [шифру Плейфера](http://znaimo.com.ua/%D0%A8%D0%B8%D1%84%D1%80%20%D0%9F%D0%BB%D0%B5%D0%B9%D1%84%D0%B5%D1%80%D0%B0). Його особливістю була відносна простота використання, хоча цей шифр був одним з перших, в якому застосовувалася заміна биграмм замість окремих букв. Тому його використовували для шифрування важливою, але не дуже секретної інформації під час бою - через той час, який противник витратить на злом шифру, інформація стане вже неактуальною.  Шифр використовувався аж до Другої світової війни.

Під час [Громадянської війни в США](http://znaimo.com.ua/%D0%93%D1%80%D0%BE%D0%BC%D0%B0%D0%B4%D1%8F%D0%BD%D1%81%D1%8C%D0%BA%D0%B0%20%D0%B2%D1%96%D0%B9%D0%BD%D0%B0%20%D0%B2%20%D0%A1%D0%A8%D0%90) (1861-1865) шифри були не дуже складними. У той час як Союзні сили мали централізовані правила шифрування, командування Конфедерації залишало ці питання на розсуд польових командирів. В результаті на місцях використовувалися настільки прості схеми, що іноді противник розшифровував повідомлення швидше, ніж її номінальний одержувач. Однією з проблем було використання стандартних ключових фраз для досить хорошого шифру Віженер. Три найвідоміших були фрази "Manchester Bluff", "Complete Victory", і "Come Retribution". Їх досить швидко "відкрили" криптоаналитики союзних сил. [[19]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link57) Проблема вибору сильних паролів та ключових фраз є досить гострою і до цих пір (серед сучасних - "123456", "password" і "12345678").

**3.6. На шляху до математичної криптографії**

В [1824](http://znaimo.com.ua/1824) виходить книга [Жана-Франсуа Шампольона](http://znaimo.com.ua/%D0%A8%D0%B0%D0%BC%D0%BF%D0%BE%D0%BB%D1%8C%D0%BE%D0%BD%20%D0%96%D0%B0%D0%BD-%D0%A4%D1%80%D0%B0%D0%BD%D1%81%D1%83%D0%B0) "Prcis du systme hirogl. d. anciens Egyptiens ou recherches sur les lments de cette criture" ("Короткий нарис ієрогліфічної системи древніх єгиптян або дослідження елементів цього листа"), що містила розшифровку єгипетських ієрогліфів, приховували свої таємниці більше трьох тисяч років. [[67]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link134)

[](http://ru.wikipedia.org/w/index.php?title=%D0%A4%D0%B0%D0%B9%D0%BB:Kerkhoffs.jpg&filetimestamp=20051005185526)

[Огюст Керкгоффс](http://znaimo.com.ua/%D0%9A%D0%B5%D1%80%D0%BA%D0%B3%D0%BE%D1%84%D1%84%D1%81%20%D0%9E%D0%B3%D1%8E%D1%81%D1%82)

В [1863](http://znaimo.com.ua/1863) Фрідріх Касіскі ( [англ.](http://znaimo.com.ua/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0%20%D0%BC%D0%BE%D0%B2%D0%B0) [*Friedrich Kasiski*](http://ru.wikipedia.org/en.wikipedia.org/wiki/Friedrich_Kasiski) ) Опублікував метод, згодом названий його ім'ям, що дозволяв швидко і ефективно розкривати практично будь-які шифри того часу. Метод складався з двох частин - визначення періоду шифру і дешифрування тексту з використанням частотного криптоаналізу.

В [1883](http://znaimo.com.ua/1883) [Огюст Керкгоффс](http://znaimo.com.ua/%D0%9A%D0%B5%D1%80%D0%BA%D0%B3%D0%BE%D1%84%D1%84%D1%81%20%D0%9E%D0%B3%D1%8E%D1%81%D1%82) опублікував працю під назвою "Військова криптографія" ( [фр.](http://znaimo.com.ua/%D0%A4%D1%80%D0%B0%D0%BD%D1%86%D1%83%D0%B7%D1%8C%D0%BA%D0%B0%20%D0%BC%D0%BE%D0%B2%D0%B0) *La Cryptographie Militaire* ). У ньому він описав [шість вимог](http://znaimo.com.ua/%D0%9F%D1%80%D0%B8%D0%BD%D1%86%D0%B8%D0%BF%20%D0%9A%D0%B5%D1%80%D0%BA%D0%B3%D0%BE%D1%84%D1%84%D1%81%D0%B0), яким повинна задовольняти захищена система. Хоча до деяких з них варто ставитися з підозрою , варто відзначити працю за саму спробу:

1. шифр повинен бути фізично, якщо не математично, не розкриваються;
2. система не повинна вимагати секретності, на випадок, якщо вона потрапить до рук ворога;
3. ключ має бути простим, зберігатися в пам'яті без запису на папері, а також легко змінюваним за бажанням кореспондентів;
4. зашифрований текст повинен [без проблем] передаватися по телеграфу;
5. апарат для шифрування повинен бути легко стерпним, робота з ним не повинна вимагати допомогою декількох осіб;
6. апарат для шифрування повинен бути відносно простий у використанні, не вимагатиме значних розумових зусиль або дотримання великої кількості правил.

*Оригінальний текст* (Фр.)

1. *Le systme doit tre matriellement, sinon mathmatiquement, indchiffrable;*
2. *Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvnient tomber entre les mains de l'ennemi;*
3. *La clef doit pouvoir en tre communique et retenue sans le secours de notes crites, et tre change ou modifie au gr des correspondants;*
4. *Il faut qu'il soit applicable la correspondance tlgraphique;*
5. *Il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes;*
6. *Enfin, il est ncessaire, vu les circonstances qui en commandent l'application, que le systme soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue srie de rgles observer.*

- *Auguste Kerckhoffs.* [La Cryptographie Militaire](http://www.petitcolas.net/fabien/kerckhoffs/la_cryptographie_militaire_i.htm#desiderata)

В даний час друге з цих правил відомо як [принцип Керкгоффса](http://znaimo.com.ua/%D0%9F%D1%80%D0%B8%D0%BD%D1%86%D0%B8%D0%BF%20%D0%9A%D0%B5%D1%80%D0%BA%D0%B3%D0%BE%D1%84%D1%84%D1%81%D0%B0).

В кінці [XIX](http://znaimo.com.ua/XIX%20%D1%81%D1%82%D0%BE%D0%BB%D1%96%D1%82%D1%82%D1%8F) - початку [XX століття](http://znaimo.com.ua/XX_%D1%81%D1%82%D0%BE%D0%BB%D1%96%D1%82%D1%82%D1%8F) уряди країн знову кинули значні сили на шифрування і криптоаналіз. В [1914](http://znaimo.com.ua/1914) Великобританія відкрила ["Кімнату 40"](http://znaimo.com.ua/%D0%9A%D1%96%D0%BC%D0%BD%D0%B0%D1%82%D0%B0%2040), в [1917](http://znaimo.com.ua/1917)США - [MI-8](http://znaimo.com.ua/MI-8), що стала попередницею сучасного [АНБ](http://znaimo.com.ua/%D0%90%D0%9D%D0%91).

[](http://ru.wikipedia.org/w/index.php?title=%D0%A4%D0%B0%D0%B9%D0%BB:William-Friedman.jpg&filetimestamp=20060711205430)

[Вільям Фрідман](http://znaimo.com.ua/%D0%A4%D1%80%D1%96%D0%B4%D0%BC%D0%B0%D0%BD%20%D0%92%D1%96%D0%BB%D1%8C%D1%8F%D0%BC%20%D0%A4%D1%80%D0%B5%D0%B4%D0%B5%D1%80%D1%96%D0%BA)

В [1918](http://znaimo.com.ua/1918) вийшла монографія [американського](http://znaimo.com.ua/%D0%A1%D0%A8%D0%90) криптографа [російського](http://znaimo.com.ua/%D0%A0%D0%BE%D1%81%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0%20%D1%96%D0%BC%D0%BF%D0%B5%D1%80%D1%96%D1%8F) походження  [Вільяма Ф. Фрідмана](http://znaimo.com.ua/%D0%A4%D1%80%D1%96%D0%B4%D0%BC%D0%B0%D0%BD%20%D0%92%D1%96%D0%BB%D1%8C%D1%8F%D0%BC%20%D0%A4%D1%80%D0%B5%D0%B4%D0%B5%D1%80%D1%96%D0%BA) "Індекс збігу і його застосування в криптографії" ([англ.](http://znaimo.com.ua/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0%20%D0%BC%D0%BE%D0%B2%D0%B0) *"Index of Coincidence and Its Applications in Cryptography"* ). Робота вийшла у відкритій пресі, незважаючи на те, що була виконана в рамках військового замовлення.  Двома роками пізніше Фрідман ввів у науковий обіг терміни [криптология](http://znaimo.com.ua/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D1%8F) і [криптоаналіз](http://znaimo.com.ua/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B0%D0%BD%D0%B0%D0%BB%D1%96%D0%B7).

На початку 1920-х років практично одночасно в різних країнах з'являються патенти та електромеханічні машини, що використовують принципи криптографічного диска (ротора) і автоматизують процес шифрування. У США це був Едвард Геберн ( [англ.](http://znaimo.com.ua/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0%20%D0%BC%D0%BE%D0%B2%D0%B0) [*Edward Hebern*](http://ru.wikipedia.org/en.wikipedia.org/wiki/Edward_Hebern) ) [[7]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link141), після нього - Хьюго Кох ( [англ.](http://znaimo.com.ua/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0%20%D0%BC%D0%BE%D0%B2%D0%B0)[*Hugo Koch*](http://ru.wikipedia.org/en.wikipedia.org/wiki/Hugo_Koch) ) З Нідерландів та його "Енігма" (пізніше патент був куплений Артуром Шербіусом ( [англ.](http://znaimo.com.ua/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0%20%D0%BC%D0%BE%D0%B2%D0%B0) [*Arthur Scherbius*](http://ru.wikipedia.org/en.wikipedia.org/wiki/Arthur_Scherbius) )), [Арвід Герхард Дамм](http://znaimo.com.ua/%D0%94%D0%B0%D0%BC%D0%BC%20%D0%90%D1%80%D0%B2%D1%96%D0%B4%20%D0%93%D0%B5%D1%80%D1%85%D0%B0%D1%80%D0%B4) зі Швеції і його машина "B-1" - розробки останнього були продовжені [Борисом Хагеліним](http://znaimo.com.ua/%D0%A5%D0%B0%D0%B3%D0%B5%D0%BB%D1%96%D0%BD%20%D0%91%D0%BE%D1%80%D0%B8%D1%81) .

У 1928-1929 роках польське " [Biuro Szyfrw](http://ru.wikipedia.org/pl.wikipedia.org/wiki/Biuro_Szyfr%C3%B3w) "організувало курси для 20 математиків зі знанням німецької мови - майбутніх криптоаналітиків, троє з яких відомі роботою по злому" Енігми ". До цього на роботу брали в основному лінгвістів.

В [1929](http://znaimo.com.ua/1929) Лестер Хілл ( [англ.](http://znaimo.com.ua/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0%20%D0%BC%D0%BE%D0%B2%D0%B0) *Lester S.* *Hill* ) Опублікував в журналі "The American Mathematical Monthly" статтю " [Cryptography in an Algebraic Alphabet](http://znaimo.com.ua/%D0%A8%D0%B8%D1%84%D1%80%20%D0%A5%D1%96%D0%BB%D0%BB%D0%B0) ". У ній він описав підхід до конструювання криптографічних систем, для яких *математично* була доведена їх невразливість до частотним атакам, в тому числі до методу Касіскі. Для представлення тексту він перевів його у цифровий вигляд, а для опису шифрування використовував поліноміальні рівняння. З метою спрощення обчислення були представлені у вигляді операцій над матрицями, окремі елементи яких складалися і помножилися по модулю 26 (за кількістю літер в[латинському алфавіті](http://znaimo.com.ua/%D0%9B%D0%B0%D1%82%D0%B8%D0%BD%D1%81%D1%8C%D0%BA%D0%B8%D0%B9%20%D0%B0%D0%BB%D1%84%D0%B0%D0%B2%D1%96%D1%82)). Так як система виявилася занадто складна у використанні, він зібрав механічну шифрувальну машину, яка спрощувала ці операції. На жаль, машина могла використовувати лише обмежене безліч ключів, і навіть з машиною шифр використовувався дуже рідко - лише для шифрування деяких державних радіопередач. Тим не менш, його основний вклад - математичний підхід до конструювання надійних криптосистем. [[19]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link57)

**4. Криптографія в літературі**

Криптографія вплинула і на літературу. Згадки про криптографії зустрічаються ще за часів [Гомера](http://znaimo.com.ua/%D0%93%D0%BE%D0%BC%D0%B5%D1%80) і [Геродота](http://znaimo.com.ua/%D0%93%D0%B5%D1%80%D0%BE%D0%B4%D0%BE%D1%82), хоча вони описували мистецтво шифрування в контексті різних історичних подій. Першим вигаданим згадкою про криптографії можна вважати роман " [Гаргантюа і Пантагрюель](http://znaimo.com.ua/%D0%93%D0%B0%D1%80%D0%B3%D0%B0%D0%BD%D1%82%D1%8E%D0%B0%20%D1%96%20%D0%9F%D0%B0%D0%BD%D1%82%D0%B0%D0%B3%D1%80%D1%8E%D0%B5%D0%BB%D1%8C) "французького письменника[XVI століття](http://znaimo.com.ua/XVI%20%D1%81%D1%82%D0%BE%D0%BB%D1%96%D1%82%D1%82%D1%8F) [Франсуа Рабле](http://znaimo.com.ua/%D0%A4%D1%80%D0%B0%D0%BD%D1%81%D1%83%D0%B0%20%D0%A0%D0%B0%D0%B1%D0%BB%D0%B5), в одній із глав якого описуються спроби читання зашифрованих повідомлень. Згадка зустрічається і в " [Генріху V](http://znaimo.com.ua/%D0%93%D0%B5%D0%BD%D1%80%D1%96%D1%85%20V%20(%D0%BF'%D1%94%D1%81%D0%B0)) " [Шекспіра](http://znaimo.com.ua/%D0%A8%D0%B5%D0%BA%D1%81%D0%BF%D1%96%D1%80).

Вперше як центральний елемент художнього твору криптографія використовується в оповіданні " [Золотий жук](http://znaimo.com.ua/%D0%97%D0%BE%D0%BB%D0%BE%D1%82%D0%B8%D0%B9%20%D0%B6%D1%83%D0%BA%20(%D0%BE%D0%BF%D0%BE%D0%B2%D1%96%D0%B4%D0%B0%D0%BD%D0%BD%D1%8F)) " [Едгара Аллана По](http://znaimo.com.ua/%D0%9F%D0%BE%20%D0%95%D0%B4%D0%B3%D0%B0%D1%80%20%D0%90%D0%BB%D0%BB%D0%B0%D0%BD) [1843](http://znaimo.com.ua/1843). У ньому письменник не тільки показує спосіб розкриття шифру, а й результат, до якого може призвести подібна діяльність - знаходження захованого скарбу.

Однак, на думку [Девіда Кана](http://znaimo.com.ua/%D0%9A%D0%B0%D0%BD%20%D0%94%D0%B5%D0%B2%D1%96%D0%B4), кращим описом застосування криптографії є розповідь [1903](http://znaimo.com.ua/1903) [Артура Конан Дойля](http://znaimo.com.ua/%D0%94%D0%BE%D0%B9%D0%BB%D1%8C%20%D0%90%D1%80%D1%82%D1%83%D1%80%20%D0%9A%D0%BE%D0%BD%D0%B0%D0%BD) " [Танцюючі чоловічки](http://znaimo.com.ua/%D0%A2%D0%B0%D0%BD%D1%86%D1%8E%D1%8E%D1%87%D1%96%20%D1%87%D0%BE%D0%BB%D0%BE%D0%B2%D1%96%D1%87%D0%BA%D0%B8) ". В оповіданні великий детектив [Шерлок Холмс](http://znaimo.com.ua/%D0%A8%D0%B5%D1%80%D0%BB%D0%BE%D0%BA%20%D0%A5%D0%BE%D0%BB%D0%BC%D1%81) стикається з різновидом шифру, який не тільки ховає сенс написаного, але, використовуючи символи, схожі на дитячі малюнки, приховує сам факт передачі секретного повідомлення. В оповіданні герой успішно застосовує частотний аналіз, а також припущення про структуру та зміст відкритих повідомлень для розгадування шифру.

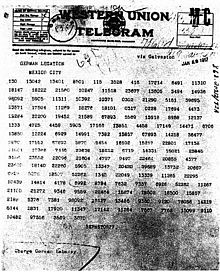
... Найбільший подвиг вигаданого криптоаналізу був здійснений, природно, найбільшим з вигаданих детективів.

*Оригінальний текст* (Англ.)

*... The greatest feat of fictional cryptanalysis was performed, naturally enough, by the greatest of fictional detectives.*

- *David Kahn.* [The Codebreakers - The Story of Secret Writing](http://znaimo.com.ua/The%20Codebreakers) ([англ.](http://ru.wikipedia.org/en.wikipedia.org/The_Codebreakers)). [[73]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link145)

**5. Криптографія Першої світової війни**

[](http://ru.wikipedia.org/w/index.php?title=%D0%A4%D0%B0%D0%B9%D0%BB:Ztel1b.jpg&filetimestamp=20051017122446)

Фотокопія [телеграми Циммермана](http://znaimo.com.ua/%D0%A2%D0%B5%D0%BB%D0%B5%D0%B3%D1%80%D0%B0%D0%BC%D0%B0%20%D0%A6%D0%B8%D0%BC%D0%BC%D0%B5%D1%80%D0%BC%D0%B0%D0%BD%D0%B0)

До Першої світової війни Росія, поряд із Францією, була лідером в області криптоаналізу на державному рівні. [Англія](http://znaimo.com.ua/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D1%8F), [США](http://znaimo.com.ua/%D0%A1%D0%A8%D0%90), [Німеччина](http://znaimo.com.ua/%D0%9D%D1%96%D0%BC%D0%B5%D1%87%D1%87%D0%B8%D0%BD%D0%B0) і менш впливові держави - ​​взагалі не мали державної дешифровальной служби, а [Австро-Угорщина](http://znaimo.com.ua/%D0%90%D0%B2%D1%81%D1%82%D1%80%D0%BE-%D0%A3%D0%B3%D0%BE%D1%80%D1%89%D0%B8%D0%BD%D0%B0) читала, в основному, листування сусідніх держав. [[74]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link149) При цьому якщо у Франції та Австро-Угорщини дешифровальной служба була військовою, то в Росії - громадянської. [[75]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link150)

Під час [Першої світової війни](http://znaimo.com.ua/%D0%9F%D0%B5%D1%80%D1%88%D0%B0_%D1%81%D0%B2%D1%96%D1%82%D0%BE%D0%B2%D0%B0_%D0%B2%D1%96%D0%B9%D0%BD%D0%B0) криптографія, і, особливо, [криптоаналіз](http://znaimo.com.ua/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B0%D0%BD%D0%B0%D0%BB%D1%96%D0%B7) стає одним з інструментів ведення війни. Відомі факти розшифровки російських повідомлень [австрійцями](http://znaimo.com.ua/%D0%90%D0%B2%D1%81%D1%82%D1%80%D1%96%D1%8F), [російськими](http://znaimo.com.ua/%D0%A0%D0%BE%D1%81%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0%20%D1%96%D0%BC%D0%BF%D0%B5%D1%80%D1%96%D1%8F) ж був розшифрований німецький шифр (завдяки знайденої водолазами копії кодової книги), після чого результати були передані союзникам. Для перехоплення радіоповідомлень були побудовані спеціальні підслуховуючі станції, в результаті роботи яких (разом з умінням дешифрувати німецький шифр, який використовували в тому числі турками) російський флот був обізнаний про склад і діях противника. В [британському адміралтействі](http://znaimo.com.ua/%D0%91%D1%80%D0%B8%D1%82%D0%B0%D0%BD%D1%81%D1%8C%D0%BA%D0%B5%20%D0%90%D0%B4%D0%BC%D1%96%D1%80%D0%B0%D0%BB%D1%82%D0%B5%D0%B9%D1%81%D1%82%D0%B2%D0%BE) було створено спеціальний підрозділ для дешифрування повідомлень ("кімната 40"), яке за час війни розшифрувало близько 15 тисяч повідомлень. Цей результат зіграв важливу роль в [битві при Доггер-банку](http://znaimo.com.ua/%D0%91%D0%B8%D1%82%D0%B2%D0%B0%20%D1%83%20%D0%94%D0%BE%D0%B3%D0%B3%D0%B5%D1%80-%D0%B1%D0%B0%D0%BD%D0%BA%D0%B8%20(1915)) і [Ютландському бою](http://znaimo.com.ua/%D0%AE%D1%82%D0%BB%D0%B0%D0%BD%D0%B4%D1%81%D1%8C%D0%BA%D0%B0%20%D0%B1%D1%96%D0%B9).

Можливо, найбільш відомим результатом роботи криптоаналітиків часу Першої світової війни є розшифровка [телеграми Циммермана](http://znaimo.com.ua/%D0%A2%D0%B5%D0%BB%D0%B5%D0%B3%D1%80%D0%B0%D0%BC%D0%B0%20%D0%A6%D0%B8%D0%BC%D0%BC%D0%B5%D1%80%D0%BC%D0%B0%D0%BD%D0%B0), що підштовхнула [США](http://znaimo.com.ua/%D0%A1%D0%A8%D0%90) до вступу у війну на стороні [Антанти](http://znaimo.com.ua/%D0%90%D0%BD%D1%82%D0%B0%D0%BD%D1%82%D0%B0).

**5.1. Росія**

До числа успішних операцій варто віднести проведене ще в мирний час викрадення кодової книги посла США в [Бухаресті](http://znaimo.com.ua/%D0%91%D1%83%D1%85%D0%B0%D1%80%D0%B5%D1%81%D1%82). Через те що посол не доповів начальству про зникнення (а дотепно користувався аналогічною кодовою книгою "сусіда" - посла США в [Відні](http://znaimo.com.ua/%D0%92%D1%96%D0%B4%D0%B5%D0%BD%D1%8C)), російська сторона змогла читати листування США зі своїми послами аж до Першої світової. Проте після її початку потік повідомлень різко знизився. Це було пов'язано з припиненням радіообміну між Німеччиною, Австро-Угорщиною і зовнішнім світом, а також зі слабкою технічною оснащеністю російських служб.

Після початку бойових дій були створені станції радіоперехоплення, особливо на Балтиці, а також організовані дешифровальной відділення при штабах армії і флоту. Однак через брак кваліфікованого персоналу повідомлення часто залишалися необробленими. Допомога армії здійснювала і власна дешифровальной служба Департаменту поліції. Проте всі ці дії були зроблені надто пізно, щоб надати скільки-небудь відчутний вплив на хід бойових дій.

**5.2. Англія**

Після успішної ліквідації німецького підводного каналу зв'язку в Північному морі і радіостанцій в [Африці](http://znaimo.com.ua/%D0%90%D1%84%D1%80%D0%B8%D0%BA%D0%B0), на [Самоа](http://znaimo.com.ua/%D0%A1%D0%B0%D0%BC%D0%BE%D0%B0) і в [Китаї](http://znaimo.com.ua/%D0%9A%D0%B8%D1%82%D0%B0%D0%B9) [Німеччина](http://znaimo.com.ua/%D0%9D%D1%96%D0%BC%D0%B5%D1%87%D1%87%D0%B8%D0%BD%D0%B0) була змушена використовувати, крім ліній союзників, [телеграф](http://znaimo.com.ua/%D0%A2%D0%B5%D0%BB%D0%B5%D0%B3%D1%80%D0%B0%D1%84), [пошту](http://znaimo.com.ua/%D0%9F%D0%BE%D1%88%D1%82%D0%B0) і [радіозв'язок](http://znaimo.com.ua/%D0%A0%D0%B0%D0%B4%D1%96%D0%BE%D0%B7%D0%B2'%D1%8F%D0%B7%D0%BE%D0%BA). Це створило добрі умови для перехоплення повідомлень, у тому числі для Англії, що згодом дало значний внесок у перемогу над [Троїстим союзом](http://znaimo.com.ua/%D0%A2%D1%80%D0%BE%D1%97%D1%81%D1%82%D0%B8%D0%B9%20%D1%81%D0%BE%D1%8E%D0%B7). Хоча Англія виявилася неготова до даної можливості, вона зуміла швидко скористатися нею.  У [1914](http://znaimo.com.ua/1914) в адміралтействі з'являється ["Кімната 40"](http://znaimo.com.ua/%D0%9A%D1%96%D0%BC%D0%BD%D0%B0%D1%82%D0%B0%2040), у створенні якої брав участь і тодішній глава адміралтейства [Уїнстон Черчілль](http://znaimo.com.ua/%D0%A7%D0%B5%D1%80%D1%87%D1%96%D0%BB%D0%BB%D1%8C%20%D0%92%D1%96%D0%BD%D1%81%D1%82%D0%BE%D0%BD).

Всі ці роки, протягом яких я обіймав офіційні посади в уряді, починаючи з осені 1914 року, я прочитував кожен з перекладів дешифрованих повідомлень і як засіб вироблення правильного рішення в галузі суспільної політики надавав їм більше значення, ніж будь-якому іншому джерелу відомостей, що знаходився в розпорядженні держави.

*Оригінальний текст* (Англ.)

*All the years I have been in office since it began in the autumn of 1914 I have read every one of these flimsies and I attach more importance to them as a means of forming a true judgement of public policy in these spheres, than to any other source of knowledge at the disposal of the state.*

- Churchill to Austen Chamberlain

Завдяки допомозі російських, які захопили кодову книгу із затонулого німецького крейсера " [Магдебург](http://znaimo.com.ua/%D0%9C%D0%B0%D0%B3%D0%B4%D0%B5%D0%B1%D1%83%D1%80%D0%B3%20(%D0%BA%D1%80%D0%B5%D0%B9%D1%81%D0%B5%D1%80)) ", а також власним подібним операціям, англійці зуміли розгадати принцип вибору шифрів Німеччиною. І хоча для надводного флоту, через погану організацію зв'язку між берегом і кораблями, це не дало великої користі, читання листування дало значний внесок у знищення німецьких підводних човнів .

Принесло користь і використання явного обману. За допомогою помилкового наказу, відправленого англійським агентом німецьким шифром, недалеко від Південної Америки була знищена ціла ескадра. За допомогою підробленого англійської коду, що потрапив в руки Антанти в травні [1915](http://znaimo.com.ua/1915), англійці на раз вводили Німеччину в оману, змусивши, наприклад, у вересні 1916 року відтягнути значні сили для відбиття міфічної десантної атаки.

19 січня [1917](http://znaimo.com.ua/1917) англійцям вдалося частково розшифрувати текст телеграми, відправленої статс-секретарем закордонних справ Німеччини [Артуром Цим мерманом](http://znaimo.com.ua/%D0%A6%D0%B8%D0%BC%D0%BC%D0%B5%D1%80%D0%BC%D0%B0%D0%BD%20%D0%90%D1%80%D1%82%D1%83%D1%80) німецькому посланнику в [Мексиці](http://znaimo.com.ua/%D0%9C%D0%B5%D0%BA%D1%81%D0%B8%D0%BA%D0%B0) Генріху фон Еккардту ( [англ.](http://znaimo.com.ua/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0%20%D0%BC%D0%BE%D0%B2%D0%B0) [*Heinrich von Eckardt*](http://ru.wikipedia.org/en.wikipedia.org/wiki/Heinrich_von_Eckardt) ). У прочитаної частини містилася інформація про плани необмеженої війни на морі. Однак тільки до середини лютого 1917 телеграма виявилася розшифрованої повністю. У телеграмі містилися плани після повернення Мексиці частини територій за рахунок США. Інформація була передана Уолтеру Пейджу ( [англ.](http://znaimo.com.ua/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0%20%D0%BC%D0%BE%D0%B2%D0%B0) [*Walter Hines Page*](http://ru.wikipedia.org/en.wikipedia.org/wiki/Walter_Hines_Page) ), Послу США в Англії. Після перевірки справжності (в тому числі - після підтвердження самого Циммермана), телеграма зіграла головну роль для виправдання в очах громадськості вступу США у [Першу світову війну](http://znaimo.com.ua/%D0%9F%D0%B5%D1%80%D1%88%D0%B0_%D1%81%D0%B2%D1%96%D1%82%D0%BE%D0%B2%D0%B0_%D0%B2%D1%96%D0%B9%D0%BD%D0%B0) проти [Четверного союзу](http://znaimo.com.ua/%D0%A6%D0%B5%D0%BD%D1%82%D1%80%D0%B0%D0%BB%D1%8C%D0%BD%D1%96%20%D0%B4%D0%B5%D1%80%D0%B6%D0%B0%D0%B2%D0%B8).

**5.3. Франція**

Найбільш драматичним моментом в криптографії Франції був червень [1918](http://znaimo.com.ua/1918), коли було життєво необхідно дізнатися напрям німецького наступу на [Париж](http://znaimo.com.ua/%D0%9F%D0%B0%D1%80%D0%B8%D0%B6). Жорж Панвен ( [фр.](http://znaimo.com.ua/%D0%A4%D1%80%D0%B0%D0%BD%D1%86%D1%83%D0%B7%D1%8C%D0%BA%D0%B0%20%D0%BC%D0%BE%D0%B2%D0%B0) [*Georges Jean Painvin*](http://ru.wikipedia.org/fr.wikipedia.org/wiki/Georges_Painvin) ) Зумів за кілька напружених днів, втративши 15 кілограм ваги, розкрити німецький шифр ADFGVX. У результаті Париж був врятований.

**5.4. Німеччина**

Кожний німецької дивізії було надано професор математики, спеціаліст з криптоаналіз, німці читали радіопередачі російських військ, що, зокрема, забезпечило нищівну перемогу німців над переважаючими силами російської армії в [Битві при Танненберг](http://znaimo.com.ua/%D0%91%D0%B8%D1%82%D0%B2%D0%B0%20%D0%BF%D1%80%D0%B8%20%D0%A2%D0%B0%D0%BD%D0%BD%D0%B5%D0%BD%D0%B1%D0%B5%D1%80%D0%B3). [[84]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link164) Втім, через нестачу криптографов, а також телефонних проводів, росіяни часто вели передачі по радіо відкритим текстом. Так чи інакше, генерал [Людендорф](http://znaimo.com.ua/%D0%9B%D1%8E%D0%B4%D0%B5%D0%BD%D0%B4%D0%BE%D1%80%D1%84) до 11 вечора мав у своєму розпорядженні всі російські депеші за день.

**6. Криптографія Другої світової війни**

Перед початком Другої світової війни провідні світові держави мали електромеханічні шифрувальні пристрої, результат роботи яких вважався розкриваються. Ці пристрої ділилися на два типи - роторні машини і машини на цевочной дисках. До першого типу відносять "Енігму", що використовувалася сухопутними військами Німеччини та її союзників, другого типу - американська [M-209](http://znaimo.com.ua/M-209).

У СРСР проводилися обидва типи машин.

**6.1. Німеччина: "Енігма", "Fish"**

[](http://ru.wikipedia.org/w/index.php?title=%D0%A4%D0%B0%D0%B9%D0%BB:Enigma.jpg&filetimestamp=20071228001247)

Трехроторная військова німецька шифрувальна машина "Енігма" [(версія з позначками)](http://ru.wikipedia.org/wiki/%D0%A4%D0%B0%D0%B9%D0%BB:Label-enigma.jpg)

Історія найвідомішої електричної роторної шифрувальної машини - "Енігма" - починається в [1917](http://znaimo.com.ua/1917) - з [патенту](http://znaimo.com.ua/%D0%9F%D0%B0%D1%82%D0%B5%D0%BD%D1%82), отриманого [голландцем](http://znaimo.com.ua/%D0%93%D0%BE%D0%BB%D0%BB%D0%B0%D0%BD%D0%B4%D1%86%D1%96) Хьюго Кохом. У наступному році патент був перекуплений Артуром Шербіусом ([*англ.*](http://ru.wikipedia.org/en.wikipedia.org/wiki/Arthur_Scherbius)), що почав комерційну діяльність з продажу примірників машини як приватним особам, так і німецьким армії і флоту.

[Німецькі](http://znaimo.com.ua/%D0%9D%D1%96%D0%BC%D0%B5%D1%87%D1%87%D0%B8%D0%BD%D0%B0) військові продовжують удосконалювати "Енігму". Без урахування настройки положення кілець ( [ньому.](http://znaimo.com.ua/%D0%9D%D1%96%D0%BC%D0%B5%D1%86%D1%8C%D0%BA%D0%B0%20%D0%BC%D0%BE%D0%B2%D0%B0) *Ringstellung* ), Кількість різних ключів становило 10. В кінці 1920-х - початку 1930 років, незважаючи на передані німецьким аристократом Хансом Тіло-Шмідтом дані по машині, що були екземпляри комерційних варіа­нтів,­ [бри­тансь­ка](http://znaimo.com.ua/%D0%91%D1%80%D0%B8%D1%82%D0%B0%D0%BD%D1%96%D1%8F) і [французька](http://znaimo.com.ua/%D0%A4%D1%80%D0%B0%D0%BD%D1%86%D1%96%D1%8F) розвідка не стали братися за завдання криптоаналізу. Ймовірно, на той час вони вже визнали, що шифр є невзламиваемим. Проте група з трьох [польських](http://znaimo.com.ua/%D0%9F%D0%BE%D0%BB%D1%8C%D1%89%D0%B0) математиків так не вважала, і, аж до [1939](http://znaimo.com.ua/1939), вела роботи по "боротьбі" з "Енігмой", і навіть вміла читати багато повідомлення, зашифрованими "Енігмой" ​​(у варіанті до внесення змін до протоколу шифрування від грудня 1938 року). В одного з них, [Маріана Реевского](http://znaimo.com.ua/%D0%A0%D0%B5%D0%B5%D0%B2%D1%81%D0%BA%D1%96%D0%B9%20%D0%9C%D0%B0%D1%80%D1%96%D0%B0%D0%BD)зародилася ідея боротися з криптографічного машиною за допомогою іншої машини. Ідея осяяла Реевского в кафе, і він дав машині ім'я "Бомба" за назвою круглого тістечка.

Серед результатів, переданих британським розвідникам перед захопленням Польщі Німеччиною, були і "живі" екземпляри "Енігми", і електромеханічна машина "Bomba", складалася з шести  спарених "Енігма" і допомагала в розшифровці (прототип для пізнішої "Bombe" [Алана Тьюрінга](http://znaimo.com.ua/%D0%A2%D1%8C%D1%8E%D1%80%D0%B8%D0%BD%D0%B3%20%D0%90%D0%BB%D0%B0%D0%BD%20%D0%9C%D0%B0%D1%82%D1%96%D1%81%D0%BE%D0%BD%D0%B0)), а також унікальні методики криптоаналізу.

Подальша робота по злому була організована в [Блетчлі-парку](http://znaimo.com.ua/%D0%91%D0%BB%D0%B5%D1%82%D1%87%D0%BB%D1%96-%D0%BF%D0%B0%D1%80%D0%BA), сьогодні є одним із предметів національної гордості [Великобританії](http://znaimo.com.ua/%D0%91%D1%80%D0%B8%D1%82%D0%B0%D0%BD%D1%96%D1%8F). У розпал діяльності центр "Station X" налічував 12 тисяч чоловік, але, незважаючи на це, німці не дізналися про нього до самого кінця війни.  Повідомлення, розшифровані центром, мали гриф секретності "Ultra" - вище, ніж використовувався до цього "Top Secret" (за однією з версій звідси і назва всієї британської операції - "Операція Ультра"). Англійці робили підвищені заходи безпеки, щоб Німеччина не здогадалася про розкриття шифру. Яскравим епізодом є випадок з бомбардуванням [Ковентрі](http://znaimo.com.ua/%D0%9A%D0%BE%D0%B2%D0%B5%D0%BD%D1%82%D1%80%D1%96) [14 лютого](http://znaimo.com.ua/14%20%D0%BB%D1%8E%D1%82%D0%BE%D0%B3%D0%BE) [1940](http://znaimo.com.ua/1940), про яку прем'єр-міністрові Великоб­ри­та­нії­[Уїнстону Черчиллю](http://znaimo.com.ua/%D0%A7%D0%B5%D1%80%D1%87%D1%96%D0%BB%D0%BB%D1%8C%20%D0%92%D1%96%D0%BD%D1%81%D1%82%D0%BE%D0%BD) було відомо заздалегідь завдяки розшифровці наказу. Однак Черчілль, спи­раючись на думку аналітиків про можливості Німеччини здогадатися про операцію "Ульт­ра", прийняв рішення про неприйняття заходів до захисту міста і евакуації жителів.

Війна змушує нас все більше і більше грати в Бога. Не знаю, як би я вчинив ...

*Оригінальний текст* (Англ.)

*War is forcing us more and more to play God. I don't know what I should have done.*

- Президент США [Франклін Рузвельт](http://znaimo.com.ua/%D0%A0%D1%83%D0%B7%D0%B2%D0%B5%D0%BB%D1%8C%D1%82%20%D0%A4%D1%80%D0%B0%D0%BD%D0%BA%D0%BB%D1%96%D0%BD%20%D0%94%D0%B5%D0%BB%D0%B0%D0%BD%D0%BE) про бомбардування [Ковентрі](http://znaimo.com.ua/%D0%9A%D0%BE%D0%B2%D0%B5%D0%BD%D1%82%D1%80%D1%96) [[89]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link175) [[90]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link177) [[91]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link178)

Хоча для [СРСР](http://znaimo.com.ua/%D0%A1%D0%A0%D0%A1%D0%A0) існування і навіть результати роботи "Station X" секрету не представляли. Саме з результатів повідомлень, дешифрованих в "Station X", СРСР дізнався про намічений "реванш" [Гітлера](http://znaimo.com.ua/%D0%93%D1%96%D1%82%D0%BB%D0%B5%D1%80%20%D0%90%D0%B4%D0%BE%D0%BB%D1%8C%D1%84) за [Сталінградську битву](http://znaimo.com.ua/%D0%A1%D1%82%D0%B0%D0%BB%D1%96%D0%BD%D0%B3%D1%80%D0%B0%D0%B4%D1%81%D1%8C%D0%BA%D0%B0%20%D0%B1%D0%B8%D1%82%D0%B2%D0%B0) і зміг підготуватися до операції на Курськом напрямку, що отримав назву " [Курська дуга](http://znaimo.com.ua/%D0%9A%D1%83%D1%80%D1%81%D1%8C%D0%BA%D0%B0%20%D0%B4%D1%83%D0%B3%D0%B0) ".

З сучасної точки зору шифр "Енігми" був не дуже надійним, але тільки поєднання цього фактора з наявністю безлічі перехоплених повідомлень, кодових книг, донесень розвідки, результатів зусиль військових і навіть [терористичних](http://znaimo.com.ua/%D0%A2%D0%B5%D1%80%D0%BE%D1%80%D0%B8%D0%B7%D0%BC) атак дозволило "розкрити" шифр.

[](http://ru.wikipedia.org/w/index.php?title=%D0%A4%D0%B0%D0%B9%D0%BB:Lorenz-SZ42-2.jpg&filetimestamp=20050715221339)

Німецька кріптомашіна Lorenz

Однак з [1940](http://znaimo.com.ua/1940) вища німецьке командування почало використовувати новий метод шифрування, названий британцями "Fish". Для шифрування використовувалося новий пристрій "Lorenz SZ 40", розроблене на замовлення військових. Шифрування грунтувалося на принципі одноразового блокнота ([шифр Вернама](http://znaimo.com.ua/%D0%A8%D0%B8%D1%84%D1%80%20%D0%92%D0%B5%D1%80%D0%BD%D0%B0%D0%BC%D0%B0), одна з модифікацій [шифру Віженер](http://znaimo.com.ua/%D0%A8%D0%B8%D1%84%D1%80%20%D0%92%D1%96%D0%B6%D0%B5%D0%BD%D0%B5%D1%80), описана в [1917](http://znaimo.com.ua/1917)) і при правильному використанні гарантувало абсолютну крипостійкість (що було доведено пізніше в роботах Шеннона). Проте для роботи шифру потрібний "надійний" генератор випадкової послідовності, який би синхронізуватися на передавальної та приймаючої сторони. Якщо криптоаналітика зуміє передбачити наступне число, що видається генератором, він зможе розшифрувати текст.

На жаль для Німеччини, генератор, який використовується в машинах "Lorenz SZ 40" виявився "слабким" . Проте його злом все одно не можна було здійснити вручну - криптоаналітика з Блетчлі-парку потрібно було створити пристрій, який би перебирав всі можливі варіанти і рятувало б криптоаналітиків від ручного перебору. Таким пристроєм стала одна з перших програмованих обчислювальних машин "Colossus", створена Максом Ньюменом ( [англ.](http://znaimo.com.ua/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0%20%D0%BC%D0%BE%D0%B2%D0%B0) [*Max Newman*](http://ru.wikipedia.org/en.wikipedia.org/wiki/Max_Newman) ) І Томмі Флауерс ( [англ.](http://znaimo.com.ua/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0%20%D0%BC%D0%BE%D0%B2%D0%B0) [*Tommy Flowers*](http://ru.wikipedia.org/en.wikipedia.org/wiki/Tommy_Flowers) ) За участю [Алана Тьюрінга](http://znaimo.com.ua/%D0%A2%D1%8C%D1%8E%D1%80%D0%B8%D0%BD%D0%B3%20%D0%90%D0%BB%D0%B0%D0%BD%20%D0%9C%D0%B0%D1%82%D1%96%D1%81%D0%BE%D0%BD%D0%B0) в [1943](http://znaimo.com.ua/1943) (хоча деякі джерела [[93]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link183) [[94]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link184) вказують, що вона була зроблена для злому "Енігми"). Машина включає 1600 [електронних ламп](http://znaimo.com.ua/%D0%95%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%20%D0%BB%D0%B0%D0%BC%D0%BF%D0%B0) і дозволила скоротити час, необхідний на злом повідомлень, з шести тижнів [[92]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link181) до кількох годин.

**6.2. Японія**

На озброєнні [Японії](http://znaimo.com.ua/%D0%AF%D0%BF%D0%BE%D0%BD%D1%96%D1%8F) стояло кілька систем шифром різного ступеня складності, найбільш витончена система, введена в дію в [1939](http://znaimo.com.ua/1939) - ["Пурпуровий годинника"](http://znaimo.com.ua/Purple%20(%D1%88%D0%B8%D1%84%D1%80%D1%83%D0%B2%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%20%D0%BC%D0%B0%D1%88%D0%B8%D0%BD%D0%B0)) ([англ.](http://znaimo.com.ua/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0%20%D0%BC%D0%BE%D0%B2%D0%B0) *Purple* ), Використовувала електромеханічну машину, як і в німців. Неабияким зусиллям і практично поодинці американський криптограф російського походження [Вільям Фрідман](http://znaimo.com.ua/%D0%A4%D1%80%D1%96%D0%B4%D0%BC%D0%B0%D0%BD%20%D0%92%D1%96%D0%BB%D1%8C%D1%8F%D0%BC%20%D0%A4%D1%80%D0%B5%D0%B4%D0%B5%D1%80%D1%96%D0%BA) зміг зламати японський код та реконструювати саму японську машину. Відомості з розшифрованої листування отримали кодову назву "Меджік". Одним з перших важливих повідомлень через "Меджік" було, що японці збираються напасти на США, до чого останні не встигли підготуватися. У подальшому ході війни американці отримували за допомогою "Меджік" багато корисних відомостей, у тому числі і про стан справ у союзників японців -[нацистської](http://znaimo.com.ua/%D0%9D%D0%B0%D1%86%D0%B8%D1%81%D1%82) Німеччини.  Непомірне напруга підірвало здоров'я Фрідмана, і в [1941](http://znaimo.com.ua/1941) він змушений був демобілізуватися, хоча продовжив роботу і далі як цивільна особа, а після війни знову став військовим.

**6.3. СРСР**

В армії і флоті [СРСР](http://znaimo.com.ua/%D0%A1%D0%A0%D0%A1%D0%A0) використовувалися шифри з кодами різної довжини - від двох символів (фронт) до п'яти (стратегічні повідомлення). Коди мінялися часто, хоча іноді і повторювалися на іншій ділянці фронту. За [ленд-лізом](http://znaimo.com.ua/%D0%9B%D0%B5%D0%BD%D0%B4-%D0%BB%D1%96%D0%B7) СРСР отримав кілька [M-209](http://znaimo.com.ua/M-209), які використовувалися як основа для створення своїх власних шифрувальних машин, хоча про їх використання невідомо.

Також для зв'язку вищих органів управління країною (в тому числі [Ставки Верховного Головнокомандування](http://znaimo.com.ua/%D0%A1%D1%82%D0%B0%D0%B2%D0%BA%D0%B0%20%D0%92%D0%B5%D1%80%D1%85%D0%BE%D0%B2%D0%BD%D0%BE%D0%B3%D0%BE%20%D0%93%D0%BE%D0%BB%D0%BE%D0%B2%D0%BD%D0%BE%D0%BA%D0%BE%D0%BC%D0%B0%D0%BD%D0%B4%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F)) і фронтами використовувалася [ВЧ-зв'язок](http://znaimo.com.ua/%D0%92%D0%A7-%D0%B7%D0%B2'%D1%8F%D0%B7%D0%BE%D0%BA). Вона представляла собою технічні засоби для запобігання прослуховування телефонних розмов, які [модулювали](http://znaimo.com.ua/%D0%90%D0%BC%D0%BF%D0%BB%D1%96%D1%82%D1%83%D0%B4%D0%BD%D0%B0%20%D0%BC%D0%BE%D0%B4%D1%83%D0%BB%D1%8F%D1%86%D1%96%D1%8F) високочастотний сигнал звуковим сигналом від мембрани мікрофону. Вже під час Другої світової війни механізм замінили на більш складний, який розбивав сигнал на відрізки по 100-150 мс і три-чотири частотних смуги, після чого спеціальний шифратор їх перемішував. На приймальному кінці аналогічний пристрій виробляло зворотні маніпуляції для відновлення мовного сигналу. Криптографічного захисту не було, тому використовуючи [спектрометр](http://znaimo.com.ua/%D0%A1%D0%BF%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BC%D0%B5%D1%82%D1%80) можна було виділити використовувані частоти і межі часових відрізків, після чого повільно, по складах, відновлювати сигнал.

Під час [радянсько-фінської війни (1939-1940)](http://znaimo.com.ua/%D0%A0%D0%B0%D0%B4%D1%8F%D0%BD%D1%81%D1%8C%D0%BA%D0%BE-%D1%84%D1%96%D0%BD%D1%81%D1%8C%D0%BA%D0%B0%20%D0%B2%D1%96%D0%B9%D0%BD%D0%B0%20(1939-1940)) [Швеція](http://znaimo.com.ua/%D0%A8%D0%B2%D0%B5%D1%86%D1%96%D1%8F) успішно дешіфровивала сполучення СРСР і допомагала [Фінляндії](http://znaimo.com.ua/%D0%A4%D1%96%D0%BD%D0%BB%D1%8F%D0%BD%D0%B4%D1%96%D1%8F). Так, наприклад, під час [битви при Суо­мус­салмі](http://znaimo.com.ua/%D0%91%D0%B8%D1%82%D0%B2%D0%B0%20%D0%BF%D1%80%D0%B8%20%D0%A1%D1%83%D0%BE%D0%BC%D1%83%D1%81%D1%81%D0%B0%D0%BB%D0%BC%D1%96)­успі­шне перехоплення повідомлень про просування радянської [44-ї стрілецької ди­ві­зії](http://znaimo.com.ua/44-%D1%82%D0%B0%20%D1%81%D1%82%D1%80%D1%96%D0%BB%D0%B5%D1%86%D1%8C%D0%BA%D0%B0%20%D0%B4%D0%B8%D0%B2%D1%96%D0%B7%D1%96%D1%8F) допоміг [Карлу Маннергейму](http://znaimo.com.ua/%D0%9C%D0%B0%D0%BD%D0%BD%D0%B5%D1%80%D0%B3%D0%B5%D0%B9%D0%BC%20%D0%9A%D0%B0%D1%80%D0%BB%20%D0%93%D1%83%D1%81%D1%82%D0%B0%D0%B2%20%D0%95%D0%BC%D1%96%D0%BB%D1%8C) вчасно вислати підкріплення, що стало запорукою перемоги. Успіш­не дешифрування наказів про бомбових ударах по [Гельсінкі](http://znaimo.com.ua/%D0%93%D0%B5%D0%BB%D1%8C%D1%81%D1%96%D0%BD%D0%BA%D1%96) дозволяло часто включити сис­тему оповіщення про повітряне ударі ще до того, як літаки стартують з те­ри­то­рії [Латвії](http://znaimo.com.ua/%D0%9B%D0%B0%D1%82%D0%B2%D1%96%D1%8F) та [Естонії](http://znaimo.com.ua/%D0%95%D1%81%D1%82%D0%BE%D0%BD%D1%96%D1%8F).

[30 грудня](http://znaimo.com.ua/30%20%D0%B3%D1%80%D1%83%D0%B4%D0%BD%D1%8F) [1937](http://znaimo.com.ua/1937) був утворено 7-е відділення (надалі - 11-й відділ) Управління розвідки Наркомату ВМФ, завданням якого було керівництво і організація дешифровальной роботи. У роки війни на дешифровальной-розвідувальної службі СРСР складалося не більше 150 чоловік, проте все одно, на думку Вадима Тимофійовича Кулінченко - капітана 1 рангу у відставці, ветерана-підводника, ДРС показала "дивовижну результативність та ефективність". У 1941-1943 роках ДРС Балтійського флоту було зламано 256 німецьких і фінляндських шифрів, прочитано 87 362 повідомлення. ДРС Північного флоту (всього - 15 осіб) зламала 15 кодів (в 575 варіантах) і прочитала більше 55 тис. повідомлень від літаків і авіабаз противника, що, за оцінкою Кулінченко, "дозволило повністю контролювати всю закриту листування ВПС Німеччини". ДРС СФ також розкрито 39 шифрів і кодів використовуваних аварійно-рятувальної, маякової і радіонавігаційної службами і берегової оборони противника і прочитано близько 3 тис. повідомлень. Важливі результати були отримані і в інших напрямках. ДРС Чорноморського флоту мало інформацію і про поточну бойовій обстановці, і навіть перехоплювало деякі стратегічні повідомлення.

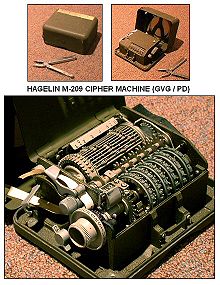
Якби не було розвідки Чорноморського флоту, я не знав би обстановки на Півдні.

- Верховний головнокомандувач Сталін, літо 1942 року

Успішні результати з читання зашифрованою японської дипломатичної переписки дозволили зробити висновок про те, що [Японія](http://znaimo.com.ua/%D0%AF%D0%BF%D0%BE%D0%BD%D1%96%D1%8F) не має наміру починати військові дії проти СРСР. Це дало можливість перекинути велику кількість сил на німецький фронт.

У передачах радіозв'язку з радянськими ядерними шпигунами в США (див. [створення радянської атомної бомби](http://znaimo.com.ua/%D0%A1%D1%82%D0%B2%D0%BE%D1%80%D0%B5%D0%BD%D0%BD%D1%8F%20%D1%80%D0%B0%D0%B4%D1%8F%D0%BD%D1%81%D1%8C%D0%BA%D0%BE%D1%97%20%D0%B0%D1%82%D0%BE%D0%BC%D0%BD%D0%BE%D1%97%20%D0%B1%D0%BE%D0%BC%D0%B1%D0%B8)) Центр в Москві використовував теоретично невразливу криптографічну система з одноразовим ключем. Тим не менш, в ході реалізації глибоко засекреченого [проекту "Венона"](http://znaimo.com.ua/%D0%9F%D1%80%D0%BE%D0%B5%D0%BA%D1%82%20%D0%92%D0%B5%D0%BD%D0%BE%D0%BD%D0%B0) контррозвідці США вдавалося розшифрувати передачі, в деякі періоди близько половини з них. Причиною цього було те, що у воєнні роки через нестачу ресурсів деякі ключі використовувалися повторно, особливо в 1943-1944 роках. Крім того, ключі не були по-справжньому випадковими, так вироблялися друкарками вручну.

**6.4. США**

[](http://ru.wikipedia.org/w/index.php?title=%D0%A4%D0%B0%D0%B9%D0%BB:Hagelin_M-209.jpg&filetimestamp=20060603155929)

Криптографічний машина [M-209](http://znaimo.com.ua/M-209)

Американська шифрувальна машина [M-+209](http://znaimo.com.ua/M-209) (CSP-1 500) була заміною M-94 ([*англ.*](http://ru.wikipedia.org/en.wikipedia.org/wiki/M-94)) (CSP-885) для передачі тактичних повідомлень. Була розроблена­ [шведсь­ким](http://znaimo.com.ua/%D0%A8%D0%B2%D0%B5%D1%86%D1%96%D1%8F) вина­хід­ни­ком [російського](http://znaimo.com.ua/%D0%A0%D0%BE%D1%81%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0%20%D1%96%D0%BC%D0%BF%D0%B5%D1%80%D1%96%D1%8F) походження [Борисом Хагеліним](http://znaimo.com.ua/%D0%A5%D0%B0%D0%B3%D0%B5%D0%BB%D1%96%D0%BD%20%D0%91%D0%BE%D1%80%D0%B8%D1%81) в кінці 1930-х років. Кілька примірників бу­ло придбано для армії США, після чого дизайн був спрощений, а механічні частини – укріп­лені. Вперше машина була використана в [Північноафриканської кампанії](http://znaimo.com.ua/%D0%9F%D1%96%D0%B2%D0%BD%D1%96%D1%87%D0%BD%D0%BE%D0%B0%D1%84%D1%80%D0%B8%D0%BA%D0%B0%D0%BD%D1%81%D1%8C%D0%BA%D0%B0%20%D0%BA%D0%B0%D0%BC%D0%BF%D0%B0%D0%BD%D1%96%D1%8F) під час насту­пу в листопаді [1942](http://znaimo.com.ua/1942). До початку 1960-х років компанією Smith Corona ([*англ.*](http://ru.wikipedia.org/en.wikipedia.org/wiki/Smith_Corona)) було виго­тов­ле­но близько 125 тисяч пристроїв.

Машина складалася з 6 коліс, комбінація виступів яких давала значення зсуву для літе­ри тексту.  Період криптографічного послідовності становив 101 405 850 букв. Хоча маши­на не могла використовуватися для шифрування серйозного трафіку (не була криптографічно стійкою), M-209 була популярна в армії з-за малої ваги, розміру і легкості в навчанні.

Також [США](http://znaimo.com.ua/%D0%A1%D0%A8%D0%90) під час Другої світової війни набирали зв'язківців з індіанського пле­ме­ні [Навахо](http://znaimo.com.ua/%D0%9D%D0%B0%D0%B2%D0%B0%D1%85%D0%BE%20(%D0%BD%D0%B0%D1%80%D0%BE%D0%B4)), [мова якого](http://znaimo.com.ua/%D0%9D%D0%B0%D0%B2%D0%B0%D1%85%D0%BE%20(%D0%BC%D0%BE%D0%B2%D0%B0)) за межами США ніхто не знав.  При цьому була врахована проб­ле­ма, що виникла ще під час Першої світової війни з використанням мови племені [Чокто](http://znaimo.com.ua/%D0%A7%D0%BE%D0%BA%D1%82%D0%BE%20(%D0%BD%D0%B0%D1%80%D0%BE%D0%B4)) для схо­жих цілей - в обох мовах просто не було достатньої кількості військових термінів. Тому був складений словник з 274 військових термінів, а також 26 слів алфавітного коду. Останній був згодом розширений для запобігання частотних атак. Як вказує [Сінгх](http://znaimo.com.ua/%D0%A1%D1%96%D0%BD%D0%B3%D1%85%20%D0%A1%D0%B0%D0%B9%D0%BC%D0%BE%D0%BD), саме відсутність знан­ня мови племені Навахо стало причиною того, що даний код так і залишився нероз­шиф­ро­ваним японцями. Інформація про використання настільки екзотичного засоби шифрування радіо­переговорів була розсекречена лише в [1968](http://znaimo.com.ua/1968).

Великим успіхом американських криптоаналітиків з'явився [проект "Венона"](http://znaimo.com.ua/%D0%9F%D1%80%D0%BE%D0%B5%D0%BA%D1%82%20%D0%92%D0%B5%D0%BD%D0%BE%D0%BD%D0%B0) ( [англ.](http://znaimo.com.ua/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0%20%D0%BC%D0%BE%D0%B2%D0%B0) [*Venona project*](http://ru.wikipedia.org/en.wikipedia.org/wiki/Venona_project) ) По розшифровці переговорів радянської розвідки зі своїми агентами в ядерному " [проекті Манхеттен](http://znaimo.com.ua/%D0%9C%D0%B0%D0%BD%D1%85%D0%B5%D1%82%D1%82%D0%B5%D0%BD%D1%81%D1%8C%D0%BA%D0%B8%D0%B9%20%D0%BF%D1%80%D0%BE%D0%B5%D0%BA%D1%82) ". Перші відомості про проект для публіки чи з'явилися в 1986 і остаточно в 1995 роках. Тому результати перехоплення не могли бути використані на таких судових процесах як [справа Розенбергів](http://znaimo.com.ua/%D0%AE%D0%BB%D1%96%D1%83%D1%81%20%D1%96%20%D0%95%D1%82%D0%B5%D0%BB%D1%8C%20%D0%A0%D0%BE%D0%B7%D0%B5%D0%BD%D0%B1%D0%B5%D1%80%D0%B3%D0%B8). Деякі шпигуни так і залишилися безкарними.

Розшифровка стала можливою через недосконалість реалізації протоколу - повторне використання ключа і неповна випадковість при створенні ключа. Якби ключ відповідав би всім вимогам алгоритму, злом коду був би неможливий.

**7. Математична криптографія**

Після Першої світової війни уряди країн засекретили всі роботи в області криптографії. На початок 1930-х років остаточно сформувалися розділи математики, які є основою для майбутньої науки - загальна [алгебра](http://znaimo.com.ua/%D0%90%D0%BB%D0%B3%D0%B5%D0%B1%D1%80%D0%B0), [теорія чисел](http://znaimo.com.ua/%D0%A2%D0%B5%D0%BE%D1%80%D1%96%D1%8F%20%D1%87%D0%B8%D1%81%D0%B5%D0%BB), [теорія ймовірностей](http://znaimo.com.ua/%D0%A2%D0%B5%D0%BE%D1%80%D1%96%D1%8F%20%D0%B9%D0%BC%D0%BE%D0%B2%D1%96%D1%80%D0%BD%D0%BE%D1%81%D1%82%D0%B5%D0%B9) і [математична статистика](http://znaimo.com.ua/%D0%9C%D0%B0%D1%82%D0%B5%D0%BC%D0%B0%D1%82%D0%B8%D1%87%D0%BD%D0%B0%20%D1%81%D1%82%D0%B0%D1%82%D0%B8%D1%81%D1%82%D0%B8%D0%BA%D0%B0). До кінця 1940-х років побудовані перші програмовані рахункові машини, закладені основи [теорії алгоритмів](http://znaimo.com.ua/%D0%A2%D0%B5%D0%BE%D1%80%D1%96%D1%8F%20%D0%B0%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC%D1%96%D0%B2), [кібернетики](http://znaimo.com.ua/%D0%9A%D1%96%D0%B1%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B8%D0%BA%D0%B0) . Тим не менш, в період після Першої світової війни і до кінця 1940-х років у пресі було опубліковано зовсім небагато робіт і монографій, а й ті відбивали далеко не найактуальніше стан справ. Найбільший прогрес в криптографії досягається у військових відомствах.

Ключовий віхою у розвитку криптографії є ​​фундаментальна праця [Клода Шеннона](http://znaimo.com.ua/%D0%A8%D0%B5%D0%BD%D0%BD%D0%BE%D0%BD_%D0%9A%D0%BB%D0%BE%D0%B4_%D0%95%D0%BB%D0%B2%D1%83%D0%B4) "Теорія зв'язку в секретних системах" ( [англ.](http://znaimo.com.ua/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0%20%D0%BC%D0%BE%D0%B2%D0%B0) *Communication Theory of Secrecy Systems* ) - Секретна доповідь, представлений автором у [1945](http://znaimo.com.ua/1945), і опублікований ним в "Bell System Technical Journal" в [1949](http://znaimo.com.ua/1949). У цій роботі, на думку багатьох сучасних криптографов [[9]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link42) [[93]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link183) [[106]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link209), був вперше показаний підхід до криптографії в цілому як до [математичної](http://znaimo.com.ua/%D0%9C%D0%B0%D1%82%D0%B5%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0) науки. Були сформульовані її теоретичні основи і введені поняття, з пояснення яких сьогодні починається вивчення криптографії студентами.

У 1960-х роках почали з'являтися різні [блокові шифри](http://znaimo.com.ua/%D0%91%D0%BB%D0%BE%D0%BA%D0%BE%D0%B2%D0%B8%D0%B9%20%D1%88%D0%B8%D1%84%D1%80), які володіли більшою криптостійкості в порівнянні з результатом роботи роторних машин. Однак вони припускали обов'язкове використання цифрових електронних пристроїв - ручні або напівмеханічними способи шифрування вже не використовувалися.

[](http://ru.wikipedia.org/w/index.php?title=%D0%A4%D0%B0%D0%B9%D0%BB:David_Kahn_2009.jpg&filetimestamp=20091129012857)

[Девід Кан](http://znaimo.com.ua/%D0%9A%D0%B0%D0%BD%20%D0%94%D0%B5%D0%B2%D1%96%D0%B4)

В [1967](http://znaimo.com.ua/1967) виходить книга [Девіда Кана](http://znaimo.com.ua/%D0%9A%D0%B0%D0%BD%20%D0%94%D0%B5%D0%B2%D1%96%D0%B4) " [Зломщики кодів](http://znaimo.com.ua/%D0%97%D0%BB%D0%BE%D0%BC%D1%89%D0%B8%D0%BA%D0%B8%20%D0%BA%D0%BE%D0%B4%D1%96%D0%B2) ". Хоча книга не містила скільки-небудь нових відкриттів, вона детально описувала наявні на той момент результати в області криптографії, великий історичний матеріал, включаючи успішні випадки використання криптоаналізу, а також деякі відомості, які уряд США вважало все ще секретними.  Але головне - книга мала помітний комерційний успіх і познайомила з криптографією десятки тисяч людей. З цього моменту почали потроху з'являтися роботи і у відкритій пресі.

Приблизно в цей же час [Хорст Фейстель](http://znaimo.com.ua/%D0%A4%D0%B5%D0%B9%D1%81%D1%82%D0%B5%D0%BB%D1%8C%20%D0%A5%D0%BE%D1%80%D1%81%D1%82) переходить з [Військово-повітряних сил США](http://znaimo.com.ua/%D0%92%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%BE%D0%B2%D0%BE-%D0%BF%D0%BE%D0%B2%D1%96%D1%82%D1%80%D1%8F%D0%BD%D1%96%20%D1%81%D0%B8%D0%BB%D0%B8%20%D0%A1%D0%A8%D0%90) на роботу в лабораторію [корпорації IBM](http://znaimo.com.ua/IBM). Там він займається розробкою нових методів в криптографії і розробляє [клітинку Фейстеля](http://znaimo.com.ua/%D0%9C%D0%B5%D1%80%D0%B5%D0%B6%D0%B0%20%D0%A4%D0%B5%D0%B9%D1%81%D1%82%D0%B5%D0%BB%D1%8F), що є основою багатьох сучасних шифрів, у тому числі шифру [Lucifer](http://znaimo.com.ua/Lucifer%20(%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%8F)), що став прообразом шифру[DES](http://znaimo.com.ua/DES) - стандарту шифрування США з [23 листопада](http://znaimo.com.ua/23%20%D0%BB%D0%B8%D1%81%D1%82%D0%BE%D0%BF%D0%B0%D0%B4%D0%B0) [1976](http://znaimo.com.ua/1976), першого у світі відкритого державного стандарту на шифрування даних, що не становлять державної таємниці [[107]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link213). При цьому за рішенням [Агентства національної безпеки США (АНБ)](http://znaimo.com.ua/%D0%90%D0%B3%D0%B5%D0%BD%D1%82%D1%81%D1%82%D0%B2%D0%BE%20%D0%BD%D0%B0%D1%86%D1%96%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D1%97%20%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8) при прийнятті стандарту довжина ключа була зменшена з 112 до 56 [біт](http://znaimo.com.ua/%D0%91%D1%96%D1%82).  Незважаючи на знайдені уразливості (пов'язані, втім, у першу чергу, саме із зменшеною довжиною ключа), він використовувався, в тому числі зі змінами, до[2001](http://znaimo.com.ua/2001).  На основі осередку Фейстеля були створені й інші шифри, в тому числі [TEA](http://znaimo.com.ua/TEA) ( [1994](http://znaimo.com.ua/1994)), [Twofish](http://znaimo.com.ua/Twofish) ( [1998](http://znaimo.com.ua/1998)), [IDEA](http://znaimo.com.ua/IDEA) ( [2000](http://znaimo.com.ua/2000)), а також [ГОСТ 28147-89](http://znaimo.com.ua/%D0%93%D0%9E%D0%A1%D0%A2%2028147-89), який є стандартом шифрування в [Росії](http://znaimo.com.ua/%D0%A0%D0%BE%D1%81%D1%96%D1%8F) як мінімум з [1989](http://znaimo.com.ua/1989).

[](http://ru.wikipedia.org/w/index.php?title=%D0%A4%D0%B0%D0%B9%D0%BB:Whitfield_Diffie.png&filetimestamp=20070524191741)

[Уітфілд Діффі](http://znaimo.com.ua/%D0%94%D1%96%D1%84%D1%84%D1%96%20%D0%A3%D1%96%D1%82%D1%84%D1%96%D0%BB%D0%B4)

[](http://ru.wikipedia.org/w/index.php?title=%D0%A4%D0%B0%D0%B9%D0%BB:Martin-Hellman.jpg&filetimestamp=20060515160905)

[Мартін Хеллман](http://znaimo.com.ua/%D0%A5%D0%B5%D0%BB%D0%BB%D0%BC%D0%B0%D0%BD%20%D0%9C%D0%B0%D1%80%D1%82%D1%96%D0%BD)

В [1976](http://znaimo.com.ua/1976) публікується робота [Уитфилда Діффі](http://znaimo.com.ua/%D0%94%D1%96%D1%84%D1%84%D1%96%20%D0%A3%D1%96%D1%82%D1%84%D1%96%D0%BB%D0%B4) і [Мартіна Хеллмана](http://znaimo.com.ua/%D0%A5%D0%B5%D0%BB%D0%BB%D0%BC%D0%B0%D0%BD%20%D0%9C%D0%B0%D1%80%D1%82%D1%96%D0%BD) "Нові напрямки в криптографії" ( [англ.](http://znaimo.com.ua/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0%20%D0%BC%D0%BE%D0%B2%D0%B0) *"New Directions in Cryptography"* ) . Дана робота відкрила нову область в криптографії, тепер відому як [криптографія з відкритим ключем](http://znaimo.com.ua/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%8F_%D0%B7_%D0%B2%D1%96%D0%B4%D0%BA%D1%80%D0%B8%D1%82%D0%B8%D0%BC_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%BC). Також у роботі містився опис [алгоритму Діффі - Хеллмана](http://znaimo.com.ua/%D0%90%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC%20%D0%94%D1%96%D1%84%D1%84%D1%96%20-%20%D0%A5%D0%B5%D0%BB%D0%BB%D0%BC%D0%B0%D0%BD%D0%B0), що дозволяв сторонам згенерувати загальний секретний ключ використовуючи тільки відкритий канал. Крім цього одним з результатів публікації стало значне зростання числа людей, що займаються криптографією.

Хоча робота Діффі-Хеллмана створила великий теоретичний доробок для відкритої криптографії, першою реальною криптосистемою з відкритим ключем вважають алгоритм [RSA](http://znaimo.com.ua/RSA) (названий по імені авторів - [Rivest](http://znaimo.com.ua/%D0%A0%D0%B8%D0%B2%D0%B5%D1%81%D1%82%20%D0%A0%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%B4%20%D0%9B%D1%96%D0%BD%D0%BD), [Shamir](http://znaimo.com.ua/%D0%A8%D0%B0%D0%BC%D1%96%D1%80%20%D0%90%D0%B4%D1%96) і [Adleman](http://znaimo.com.ua/%D0%90%D0%B4%D0%BB%D0%B5%D0%BC%D0%B0%D0%BD%20%D0%9B%D0%B5%D0%BE%D0%BD%D0%B0%D1%80%D0%B4%20%D0%9C%D0%B0%D0%BA%D1%81)). Опублікована в серпні [1977](http://znaimo.com.ua/1977) робота дозволила сторонам обмінюватися секретною інформацією не маючи заздалегідь обраного секретного ключа. Побоюючись поширення системи в недержавних структурах, [АНБ](http://znaimo.com.ua/%D0%90%D0%9D%D0%91) безуспішно вимагало припинення розповсюдження системи. RSA використовується в усьому світі і, на [1996](http://znaimo.com.ua/1996), був стандартом де-факто для шифрування з відкритим ключем. Чернетки стандарту [ISO](http://znaimo.com.ua/ISO) для цифрового підпису та банківського стандарту ANSI засновані на RSA, також він служить інформаційним додатком для ISO 9796, прийнятий як стандарт у Французькому банківському співтоваристві і в [Австралії](http://znaimo.com.ua/%D0%90%D0%B2%D1%81%D1%82%D1%80%D0%B0%D0%BB%D1%96%D1%8F). В [США](http://znaimo.com.ua/%D0%A1%D0%A8%D0%90), через тиск АНБ, стандарти на шифрування з відкритим ключем або цифровий підпис відсутні, хоча більшість компаній використовує стандарт [PKCS # 1](http://znaimo.com.ua/PKCS), заснований на RSA.

Варто відзначити, що і [RSA](http://znaimo.com.ua/RSA), і [алгоритм Діффі - Хеллмана](http://znaimo.com.ua/%D0%90%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC%20%D0%94%D1%96%D1%84%D1%84%D1%96%20-%20%D0%A5%D0%B5%D0%BB%D0%BB%D0%BC%D0%B0%D0%BD%D0%B0) були вперше відкриті в англійських спецслужбах у зворотному порядку, але не були ні опубліковані, ні запатентовані через секретність.

В [Росії](http://znaimo.com.ua/%D0%A0%D0%BE%D1%81%D1%96%D1%8F) для шифрування з відкритим ключем стандарт відсутня, однак для­ [елек­трон­но­го цифрового підпису](http://znaimo.com.ua/%D0%95%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B8%D0%B9_%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B8%D0%B9_%D0%BF%D1%96%D0%B4%D0%BF%D0%B8%D1%81) (органічно пов'язаної з шифруванням з відкритим ключем) прий­ня­тий стандарт [ГОСТ Р 34.10-2001](http://znaimo.com.ua/%D0%93%D0%9E%D0%A1%D0%A2%20%D0%A0%203410-2001), що використовує [криптографію на еліптичних кривих](http://znaimo.com.ua/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%8F%20%D0%BD%D0%B0%20%D0%B5%D0%BB%D1%96%D0%BF%D1%82%D0%B8%D1%87%D0%BD%D0%B8%D1%85%20%D0%BA%D1%80%D0%B8%D0%B2%D0%B8%D1%85).

**8. Відкрита криптографія і держава**

Починаючи з 1970-х років інтерес до криптографії зростає з боку окремих дослідників, бізнесу та приватних осіб. Цьому сприяли в тому числі і публікації у відкритій пресі - книга [Девіда Кана](http://znaimo.com.ua/%D0%9A%D0%B0%D0%BD%20%D0%94%D0%B5%D0%B2%D1%96%D0%B4) " [Зломщики кодів](http://znaimo.com.ua/%D0%97%D0%BB%D0%BE%D0%BC%D1%89%D0%B8%D0%BA%D0%B8%20%D0%BA%D0%BE%D0%B4%D1%96%D0%B2) ", готовність наукової (створення осередку Фейстеля, роботи Діффі і Хеллмана, шифрів DES і RSA) і технічної бази (обчислювальної техніки), а також наявність" замовлення "з боку бізнесу - вимог до надійної передачі інформації в рамках окремої країни і по всьому світу. Одночасно з цим з'явилося й опір з боку держави розвитку *відкритої криптографії (цивільної криптографії* ), що видно на прикладі історії протидії з [АНБ](http://znaimo.com.ua/%D0%90%D0%9D%D0%91). Серед причин негативного ставлення уряду вказують на неприпустимість потрапляння надійних систем шифрування в руки терористів, організованої злочинності або ворожої розвідки.

Після зростання суспільного інтересу до криптографії в [США](http://znaimo.com.ua/%D0%A1%D0%A8%D0%90) в кінці 1970-х і початку 1980-х років [АНБ](http://znaimo.com.ua/%D0%90%D0%9D%D0%91) зробило ряд спроб придушити інтерес суспільства до криптографії. Якщо з компанією IBM вдалося домовитися (у тому числі з питання зниження криптостійкості шифру [DES](http://znaimo.com.ua/DES)), то наукове співтовариство довелося контролювати через систему грантів - [Національний науковий фонд США](http://znaimo.com.ua/%D0%9D%D0%B0%D1%86%D1%96%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D0%B9%20%D0%BD%D0%B0%D1%83%D0%BA%D0%BE%D0%B2%D0%B8%D0%B9%20%D1%84%D0%BE%D0%BD%D0%B4%20(%D0%A1%D0%A8%D0%90)). Представники фонду погодилися направляти роботи з криптографії на перевірку в АНБ і відмовляти у фінансуванні певних наукових напрямів. Також АНБ контролювала і бюро патентів, що дозволяло накласти гриф секретності в тому числі на винаходи цивільних осіб. Так, в [1978](http://znaimo.com.ua/1978) гриф "таємно", відповідно до закону [Invention Secrecy Act](http://ru.wikipedia.org/en.wikipedia.org/wiki/Invention_Secrecy_Act) про засекречування винаходів, які могли бути використані для вдосконалення техніки військового призначення, отримало винахід "Phaserphone"  групи під керівництвом Карла Микола ( [англ.](http://znaimo.com.ua/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0%20%D0%BC%D0%BE%D0%B2%D0%B0) *Carl R.* *Nicolai* ), Що дозволяє шифрувати голос. Після того як історія отримала значний розголос у пресі, АНБ довелося відмовитися від спроб засекретити і монополізувати винахід. Також в [1978](http://znaimo.com.ua/1978) цивільний співробітник АНБ Джозеф Мейер ( [англ.](http://znaimo.com.ua/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0%20%D0%BC%D0%BE%D0%B2%D0%B0) *Joseph Meyer* ) Без узгодження з начальством послав у [IEEE](http://znaimo.com.ua/IEEE), членом якого він також був, лист з попередженням , що публікація матеріалів щодо шифрування і криптоаналіз порушує Правила з регулювання міжнародного трафіку озброєнь ( [англ.](http://znaimo.com.ua/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0%20%D0%BC%D0%BE%D0%B2%D0%B0)[*International Traffic in Arms Regulations, ITAR*](http://ru.wikipedia.org/en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations) ). Хоча Мейер виступав як приватна особа, лист було розцінено як спроба АНБ припинити цивільні дослідження в області криптографії. Тим не менш, його точка зору не знайшла підтримки, але саме обговорення створило рекламу як відкритої криптографії, так і симпозіуму з теорії інформації [1977](http://znaimo.com.ua/1977) - науки, тісно пов'язаної з шифруванням і криптоаналізу завдяки роботам Шеннона.

[](http://ru.wikipedia.org/w/index.php?title=%D0%A4%D0%B0%D0%B9%D0%BB:Len-mankin-pic.jpg&filetimestamp=20100326141455)

[Леонард Макс Адлеман](http://znaimo.com.ua/%D0%9B%D0%B5%D0%BE%D0%BD%D0%B0%D1%80%D0%B4%20%D0%9C%D0%B0%D0%BA%D1%81%20%D0%90%D0%B4%D0%BB%D0%B5%D0%BC%D0%B0%D0%BD), один з авторів [RSA](http://znaimo.com.ua/RSA)

Після провалів, пов'язаних з листом Мейєра і справи групи Ніколаї, директор АНБ опублікував кілька статей, в яких закликав академічні кола до спільного вирішення проблем, пов'язаних з відкритим вивченням криптографії та національною безпекою. В результаті утворилася деяка структура самоцензури - попередньої перевірки наукових публікацій в особливому державному комітеті. У той же час АНБ отримує можливість розподіляти кошти на криптографічні дослідження, "відокремивши" від [Національного наукового фонду](http://znaimo.com.ua/%D0%9D%D0%B0%D1%86%D1%96%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D0%B9%20%D0%BD%D0%B0%D1%83%D0%BA%D0%BE%D0%B2%D0%B8%D0%B9%20%D1%84%D0%BE%D0%BD%D0%B4%20(%D0%A1%D0%A8%D0%90)) свій власний, в 2-3 мільйони доларів США. Тим не менше, після конфлікту з [Леонардо Адлеманом](http://znaimo.com.ua/%D0%90%D0%B4%D0%BB%D0%B5%D0%BC%D0%B0%D0%BD%20%D0%9B%D0%B5%D0%BE%D0%BD%D0%B0%D1%80%D0%B4%20%D0%9C%D0%B0%D0%BA%D1%81) в [1980](http://znaimo.com.ua/1980) було вирішено, що заявку на фінансування криптографічних досліджень можна подавати як у національний, так і в спеціалізований фонд АНБ.

Законодавчо в [США](http://znaimo.com.ua/%D0%A1%D0%A8%D0%90) було зроблено обмеження на використання відкритої криптографії. Висувалася вимога навмисне забезпечити ослаблену захист від злому, щоб державні служби при необхідності (у тому числі - за рішенням суду) могли прочитати або прослухати зашифровані повідомлення. Однак через кілька інцидентів злому комерційних систем від цього довелося відмовитися, оскільки заборона на використання сильної криптографії всередині країни став завдавати шкоди економіці. У результаті до кінця 1980-х років в США залишився єдиний заборона - на експорт "сильної" криптографії, в результаті якого, а також через розвиток персональної обчислювальної техніки, до початку 1990-х років вся експортована із США криптографія стала "повністю слабкою ".

Тим не менш, [АНБ](http://znaimo.com.ua/%D0%90%D0%9D%D0%91) і [ФБР](http://znaimo.com.ua/%D0%A4%D0%91%D0%A0) кілька разів піднімали питання про заборону або дозвільному механізмі для приватних компаній займатися роботами в області криптографії, але ці ініціативи завжди зустрічали опір суспільства та бізнесу. На даний момент можна сказати, що зараз АНБ відмовилася від усіх претензій і вважає за краще виступати експертної стороною. До цього (а ФБР і до цих пір) кілька разів змінювало свою позицію, пропонуючи різні схеми використання сильної криптографії в бізнесі та приватними особами.

[](http://ru.wikipedia.org/w/index.php?title=%D0%A4%D0%B0%D0%B9%D0%BB:PRZ_closeup.jpg&filetimestamp=20100117164707)

[Філіп Циммерман](http://znaimo.com.ua/%D0%A6%D0%B8%D0%BC%D0%BC%D0%B5%D1%80%D0%BC%D0%B0%D0%BD%20%D0%A4%D1%96%D0%BB%D1%96%D0%BF), автор [PGP](http://znaimo.com.ua/PGP)

В [1991](http://znaimo.com.ua/1991) законопроект № 266 включив в себе необов'язкові вимоги, які, якщо б вони були прийняті, змусили б усіх виробників захищеного телекомунікаційного обладнання залишати "чорні ходи" ( [англ.](http://znaimo.com.ua/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0%20%D0%BC%D0%BE%D0%B2%D0%B0) *trap doors* ), Які б дозволили уряду отримувати доступ до незашифрованому повідомленнями. Ще до того як законопроект провалився, [Філіп Циммерман](http://znaimo.com.ua/%D0%A6%D0%B8%D0%BC%D0%BC%D0%B5%D1%80%D0%BC%D0%B0%D0%BD%20%D0%A4%D1%96%D0%BB%D1%96%D0%BF) виклав в Інтернет [PGP](http://znaimo.com.ua/PGP) - пакет безкоштовного програмного забезпечення з відкритим кодом для шифрування і електронного підпису повідомлень. Спочатку він планував випустити комерційну версію, але ініціатива уряду щодо просування законопроекту спонукала його випустити програму безкоштовно. У зв'язку з цим проти Циммермана було порушено кримінальну справу за "експорт озброєнь", яке було припинено тільки в[1996](http://znaimo.com.ua/1996), коли світ побачила вже 4-а версія програми.

Наступною ініціативою став проект Clipper Chip ([*англ.*](http://ru.wikipedia.org/en.wikipedia.org/wiki/Clipper_Chip)), запропонований в [1993](http://znaimo.com.ua/1993). Чіп містив сильний, згідно із заявою [АНБ](http://znaimo.com.ua/%D0%90%D0%9D%D0%91), алгоритм шифрування [Skipjack](http://znaimo.com.ua/Skipjack), який, тим не менш, дозволяв третій стороні (тобто уряду США) отримати доступ до закритого ключа і прочитати зашифроване повідомлення. Даний чіп пропонувалося використовуватися як основу для захищених телефонів різних виробників. Однак дана ініціатива не була прийнята бізнесом, який вже мав досить сильні та відкриті програми на зразок [PGP](http://znaimo.com.ua/PGP). В [1998](http://znaimo.com.ua/1998) шифр був розсекречений, після чого [Біхам](http://znaimo.com.ua/%D0%91%D1%96%D1%85%D0%B0%D0%BC%20%D0%95%D0%BB%D1%96), [Шамір](http://znaimo.com.ua/%D0%A8%D0%B0%D0%BC%D1%96%D1%80%20%D0%90%D0%B4%D1%96) і [Бірюков](http://ru.wikipedia.org/en.wikipedia.org/wiki/Alex_Biryukov) протягом одного дня провели успішні атаки на варіант шифру c 31 раундом (з 32-х).

Проте, ідея депонування ключів поширювалася. В [Великобританії](http://znaimo.com.ua/%D0%91%D1%80%D0%B8%D1%82%D0%B0%D0%BD%D1%96%D1%8F) її намагалися впровадити кілька років, а під [Франції](http://znaimo.com.ua/%D0%A4%D1%80%D0%B0%D0%BD%D1%86%D1%96%D1%8F) вона почала діяти в [1996](http://znaimo.com.ua/1996). Однак, незважаючи на значні зусилля США, і, зокрема, її уповноваженого з криптографії - [Девіда Аарона](http://znaimo.com.ua/%D0%90%D0%B0%D1%80%D0%BE%D0%BD%20%D0%94%D0%B5%D0%B2%D1%96%D0%B4), багато країн, у тому числі входять до [Організацію економічного співробітництва та розвитку](http://znaimo.com.ua/%D0%9E%D1%80%D0%B3%D0%B0%D0%BD%D1%96%D0%B7%D0%B0%D1%86%D1%96%D1%8F%20%D0%B5%D0%BA%D0%BE%D0%BD%D0%BE%D0%BC%D1%96%D1%87%D0%BD%D0%BE%D0%B3%D0%BE%20%D1%81%D0%BF%D1%96%D0%B2%D1%80%D0%BE%D0%B1%D1%96%D1%82%D0%BD%D0%B8%D1%86%D1%82%D0%B2%D0%B0%20%D1%82%D0%B0%20%D1%80%D0%BE%D0%B7%D0%B2%D0%B8%D1%82%D0%BA%D1%83), в цілому відмовилися від цієї ідеї на користь захисту недоторканності приватного життя. Також експерти (наприклад, в доповіді Європейської Комісії "До європейської інфраструктурі цифрових підписів та криптографії" COM (97) 503 ) відзначили наявність безлічі невирішених проблем, пов'язаних зі структурою централізованого депонування ключів, в тому числі: зниження загальної захищеності системи, потенційно високу вартість і потенційну легкість обману з боку користувачів. [[112]](http://znaimo.com.ua/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97#link223) Останнє легко пояснити на прикладі системи Clipper, коли користувач мав можливість згенерувати неправдиву інформацію для відновлення ключа (разом з коротким хеш-кодом) так, що система працювала без технічної можливості відновити ключ третя стороною.

У грудні [1998](http://znaimo.com.ua/1998) на засіданні учасників [Вассенаарської угоди](http://znaimo.com.ua/%D0%92%D0%B0%D1%81%D1%81%D0%B5%D0%BD%D0%B0%D0%B0%D1%80%D1%81%D1%8C%D0%BA%D1%96%20%D1%83%D0%B3%D0%BE%D0%B4%D0%B8) США спробувала отримати послаблення в правилах експорту для систем з депонуванням ключів, проте сторони не дійшли згоди. Це можна назвати датою остаточної поразки подібних систем на сьогоднішній день. Після цього Франція в січні [1999](http://znaimo.com.ua/1999) оголосила про відмову від системи депонування ключів. [Тайвань](http://znaimo.com.ua/%D0%A2%D0%B0%D0%B9%D0%B2%D0%B0%D0%BD%D1%8C), в [1997](http://znaimo.com.ua/1997) оголосив про плани по створенню такої системи, також відмовився від них в [1998](http://znaimo.com.ua/1998). В [Іспанії](http://znaimo.com.ua/%D0%86%D1%81%D0%BF%D0%B0%D0%BD%D1%96%D1%8F), незважаючи на передбачену можливість депонування ключів в прийнятому в 1998 році законі про телекомунікації, система так і не запрацювала.

Після відмови від технічних засобів доступу до ключів, уряду звернулися до ідеї законодавчого регулювання цього питання - коли людина сама зобов'язується надати заздалегідь або на вимогу ключ для читання повідомлень. Даний варіант можна назвати "законний доступ". У різних країнах до нього ставляться по-різному. ОЕСР залишає за своїми членами свободу у використанні або відмову від даного способу. У липні [1997](http://znaimo.com.ua/1997) на саміті в [Денвері](http://znaimo.com.ua/%D0%94%D0%B5%D0%BD%D0%B2%D0%B5%D1%80) учасники " [Великої Вісімки](http://znaimo.com.ua/%D0%92%D0%B5%D0%BB%D0%B8%D0%BA%D0%B0%20%D0%B2%D1%96%D1%81%D1%96%D0%BC%D0%BA%D0%B0)"ідею підтримали. В [Малайзії](http://znaimo.com.ua/%D0%9C%D0%B0%D0%BB%D0%B0%D0%B9%D0%B7%D1%96%D1%8F) і [Сінгапурі](http://znaimo.com.ua/%D0%A1%D1%96%D0%BD%D0%B3%D0%B0%D0%BF%D1%83%D1%80) за відмову надання ключів слідству людині загрожує кримінальне покарання. В [Великобританії](http://znaimo.com.ua/%D0%91%D1%80%D0%B8%D1%82%D0%B0%D0%BD%D1%96%D1%8F) і [Індії](http://znaimo.com.ua/%D0%86%D0%BD%D0%B4%D1%96%D1%8F) схожі закони розглядаються. В [Ірландії](http://znaimo.com.ua/%D0%86%D1%80%D0%BB%D0%B0%D0%BD%D0%B4%D1%96%D1%8F) прийнятий закон з положеннями про розкриття відкритого тексту, але і з рекомендаціями проти насильницького розкриття ключів. В[Бельгії](http://znaimo.com.ua/%D0%91%D0%B5%D0%BB%D1%8C%D0%B3%D1%96%D1%8F), [Нідерландах](http://znaimo.com.ua/%D0%9D%D1%96%D0%B4%D0%B5%D1%80%D0%BB%D0%B0%D0%BD%D0%B4%D0%B8) і [США](http://znaimo.com.ua/%D0%A1%D0%A8%D0%90) розглядаються пропозиції про розкриття відкритого тексту, але з поправками про необов'язковість свідчення проти самого себе. Деякі країни, такі як [Данія](http://znaimo.com.ua/%D0%94%D0%B0%D0%BD%D1%96%D1%8F), відхилили подібну ініціативу.

В [2000](http://znaimo.com.ua/2000) США зняли практично всі обмеження на експорт криптографічного продукції, за винятком 7 країн з "терористичними режимами". Ще одним кроком до відкритої криптографії став [конкурс AES](http://znaimo.com.ua/AES%20(%D0%BA%D0%BE%D0%BD%D0%BA%D1%83%D1%80%D1%81)), в якому брали участь вчені всього світу.

У Росії на даний момент діяльність з розробки та виробництва криптографічних засобів є ліцензованої.

**9. Сучасна криптографія**

З кінця 1990 років починається процес відкритого формування державних стандартів на криптографічні протоколи. Мабуть, найвідомішим є розпочатий в [1997](http://znaimo.com.ua/1997)[конкурс AES](http://znaimo.com.ua/AES%20(%D0%BA%D0%BE%D0%BD%D0%BA%D1%83%D1%80%D1%81)), в результаті якого в [2000](http://znaimo.com.ua/2000) державним стандартом США для криптографії з секретним ключем був прийнятий шифр [Rijndael](http://znaimo.com.ua/Rijndael), зараз вже більш відомий як AES.  Аналогічні ініціативи носять назви [NESSIE](http://znaimo.com.ua/NESSIE) ( [англ.](http://znaimo.com.ua/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0%20%D0%BC%D0%BE%D0%B2%D0%B0) *New European Schemes for Signatures, Integrity, and Encryptions* ) В [Європі](http://znaimo.com.ua/%D0%84%D0%B2%D1%80%D0%BE%D0%BF%D0%B0) і [CRYPTREC](http://znaimo.com.ua/CRYPTREC) ([англ.](http://znaimo.com.ua/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0%20%D0%BC%D0%BE%D0%B2%D0%B0) *Cryptography Research and Evaluation Committees* ) В [Японії](http://znaimo.com.ua/%D0%AF%D0%BF%D0%BE%D0%BD%D1%96%D1%8F).

У самих алгоритмах як операцій, покликаних утруднити [лінійний](http://znaimo.com.ua/%D0%9B%D1%96%D0%BD%D1%96%D0%B9%D0%BD%D0%B8%D0%B9_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B0%D0%BD%D0%B0%D0%BB%D1%96%D0%B7) і [диференціальний криптоаналіз](http://znaimo.com.ua/%D0%94%D0%B8%D1%84%D0%B5%D1%80%D0%B5%D0%BD%D1%86%D1%96%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D0%B9_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B0%D0%BD%D0%B0%D0%BB%D1%96%D0%B7) крім випадкових функцій (наприклад, S-блоків, використовуваних в шифрах [DES](http://znaimo.com.ua/DES) і [ГОСТ](http://znaimo.com.ua/%D0%93%D0%9E%D0%A1%D0%A2%2028147-89)) стали використовувати більш складні математичні конструкції, такі як обчислення [в полі Галуа](http://znaimo.com.ua/%D0%9A%D1%96%D0%BD%D1%86%D0%B5%D0%B2%D0%B5%20%D0%BF%D0%BE%D0%BB%D0%B5) в шифрі [AES](http://znaimo.com.ua/Advanced%20Encryption%20Standard). Принципи вибору алгоритмів (криптографічних примітивів) поступово ускладнюються. Пред'являються нові вимоги, часто не має прямого відношення до математики, такі як стійкість до [атакам по сторонніх каналах](http://znaimo.com.ua/%D0%90%D1%82%D0%B0%D0%BA%D0%B0%20%D0%BF%D0%BE%20%D1%81%D1%82%D0%BE%D1%80%D0%BE%D0%BD%D0%BD%D1%96%D0%BC%20%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%B0%D1%85). Для вирішення завдання захисту інформації пропонуються все нові механізми, у тому числі організаційні та законодавчі.

Також розвиваються принципово нові напрямки. На стику [квантової фізики](http://znaimo.com.ua/%D0%9A%D0%B2%D0%B0%D0%BD%D1%82%D0%BE%D0%B2%D0%B0%20%D1%84%D1%96%D0%B7%D0%B8%D0%BA%D0%B0) і математики розвиваються [квантові обчислення](http://znaimo.com.ua/%D0%9A%D0%B2%D0%B0%D0%BD%D1%82%D0%BE%D0%B2%D1%96%20%D0%BE%D0%B1%D1%87%D0%B8%D1%81%D0%BB%D0%B5%D0%BD%D0%BD%D1%8F) і [квантова криптографія](http://znaimo.com.ua/%D0%9A%D0%B2%D0%B0%D0%BD%D1%82%D0%BE%D0%B2%D0%B0%20%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%8F). Хоча квантові комп'ютери лише справа майбутнього, вже зараз запропоновані алгоритми для злому існуючих "надійних" систем (наприклад, [алгоритм Шора](http://znaimo.com.ua/%D0%90%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC%20%D0%A8%D0%BE%D1%80%D0%B0)). З іншого боку, використовуючи квантові ефекти, можливо побудувати і принципово нові способи надійної передачі інформації. Активні дослідження в цій області йдуть з кінця 1980-х років.

У сучасному світі криптографія знаходить безліч різних застосувань. Крім очевидних - власне, для передачі інформації, вона використовується [в стільникового зв'язку](http://znaimo.com.ua/A5%20(%D1%88%D0%B8%D1%84%D1%80)), платному цифровому телебаченні при підключенні до [Wi-Fi](http://znaimo.com.ua/WPA) і на транспорті для захисту квитків від підробок , і в банківських операціях , і навіть [для захисту електронної пошти від спаму](http://znaimo.com.ua/DomainKeys%20Identified%20Mail).

**10)** **Механізми та протоколи керування ключами в ІВК інформаційної  
системи**

**1**.

У фізичному світі нескладно розпізнати хто ким є, коли бачиш, чуєш або упізнаєш людину за її почерком. Проте у світі цифровому все ще спілкуються одне з одним на екрані комп’ютера. Коли організації переводять свої бізнес-операції в режим онлайн, то найважливішими вимогами стають безпека і довіра. А значить, розпізнання особистості індивіду або ж цілої організації виходить на перший план. Цифровий підпис як механізм, що прискорює операції, зберігає кошти, зменшує обсяг використовуваного паперу і покращує безпеку здійснення тієї чи іншої операції, широко застосовується як фундаментальний компонент ведення бізнесу в кіберпросторі. Цифровий підпис забезпечує цілісність даних і доказ оригіналу (неможливість відмовитися від авторства). Одержувач може зберегти його з метою використання для вирішення спорів у випадку, якщо відправник відкидатиме зміст повідомлення або навіть заперечуватиме факт надіслання його ним самим. Цифровий підпис також застосовують для розпізнання користувача у системах або додатках.

2. Що таке ідентифікація?

Архітектура безпеки OSI (OSI Security Architecture) (ISO7498-2) дає визначення двом видам ідентифікації: ідентифікації особи та ідентифікації походження даних.

1. Ідентифікація особи здійснюється шляхом перевірки одної автентичної особи іншою. Це операція, орієнтована на зв’язок. Ідентифікація особи зазвичай відбувається за допомогою використання ідентифікаційного механізму обміну. Суть його становить процес обміну повідомленнями між парою осіб і найчастіше називається протоколом ідентифікації. Ідентифікація особи включає в себе односторонню ідентифікацію, котра забезпечить доказ справжності одної особи іншій особі. Але без зворотного процесу, а також двостороння ідентифікація, за допомогою якої обидві сторони отримують доказ справжності протилежної особи.

2. Ідентифікація походження даних надає будь-якій особі підтвердження того, що джерелом отриманих даних є саме заявлене джерело. Але така система сама по собі не дає захисту від дуплікації або модифікації одиниць інформації. Цифровий підпис є особливою технікою розпізнання, яку можна застосовувати для встановлення походження повідомлення, щоб вирішити спір щодо того, яке повідомлення було надіслано (і чи було воно надіслано взагалі).

3. Основа для ідентифікації

У світі, повному мереж зв’язку, неможливо ідентифікувати особу так само, як це робиться у світі фізичному. Тому для ідентифікації потребується основа, на якій необхідно створити протокол. Взагалі процес ідентифікації відбувається за допомогою обміну криптографічнимиІнформаційна страктура: Ідентифікація і Цифровий підпис

Електронне управління – Що необхідно знати лідеру у сфері управління Сторінка 2 із 10 повідомленнями, які є спільним секретом між двома особами. Так званий спільний секрет можна віднести до однієї з трьох наступних областей:

1. Щось, що ви знаєте, PIN-код або пароль. Така ідентифікація ґрунтується на знанні. В цьому випадку особа та IT-система имають спільний PIN-код або пароль. Людині пропонується ввести такий PIN-код або пароль під час ідентифікації, і вінкон вертується у криптографічний ключ. Цей ключ потім використовується у протоколі ідентифікації. Якщо PIN-код або пароль, що вводиться людиною, співпадає з аналогом, який зберігається системою, то ідентифікація людини проходить успішно.

2. Щось, що ви маєте, безпечне посвідчення особи або будь-який інший упізнавальний знак, за яким можлива генерація одноразового паролю; ключ, що вставляється у «безпечну зону» приймаючого апарата; або смарт-карта (яка може містити ключі і здійснювати криптографічні операції від імені користувача). Така ідентифікація ґрунтується на упізнавальних знаках. В цьому випадку у безпечну розпізнавальну систему вводиться ключ. Маючи розпізнавальні знаки, ви маєте ключ доступу. Таким чином, будь-яка особа, яка розпоряджається розпізнавальним знаком, вважається власником такого розпізнавального знаку.

3. Щось, чи ви є, як, наприклад, фізіологічна риса або спосіб поведінки. Така ідентифікація заснована на біометриці. І в цьому випадку біометричні параметри перетворюються на профіль, зміст якого співставляється зі зразком, що зберігається. Сьогодні технології, які застосовуються в такому виді інформації, включають в себе статистичну біометрику, а саме відбитки пальців, розпізнання сітківки, райдужної оболонки ока, обличчя і геометрії руки; а також динамічну біометрику, до якої відноситься голосі і перевірка підпису. При отриманні подібності біометричних даних, які в необхідній мірі наближаються до їх зразків, відбувається аутентифікація конкретної особи. Таким чином, необхідний захист особистих файлів (при їх криптографічній конвертації) при обміні між пристроєм, що фіксує біометричну інформацію, і сервером, який проводить перевірку отриманих даних. Цю інформацію необхідно захищати від перехоплення третіми особами, які можуть використати її для завдання шкоди, вводячи у мережу.

Об’єкти ідентифікації, заснованої на наявності розпізнавальних знаків і на знаннях, для проведення розпізнавання не грунтуються на будь-якому притаманному індивіду атрибуті. Є ряд недоліків, що пов’язані з цими двома видами ідентифікації. Розпізнавальний знак може бути втрачено, загублено, забуто, невірно розташовано або добровільно передано шахраю. PIN-коди і паролі можна забути, вгадати, підгледіти або розкрити добровільно. Біометричні способи за своєю природою є надійнішими для ідентифікації і не мають впливу вказаних недоліків. Проте, в них наявні недоліки іншого року, такі як складність реєстрації, активації та використання; вони також зазнають впливу оточуючого середовища і стану здоров’я. Але всі ці «секрети» дуже вразливі при передачі по відкритій мережі; навіть звичний PIN-код або пароль піддаються словарному пошуку і всебічним атакам. Паролі є прикладом слабкого мехінузму ідентифікації; людина демонструє знання паролю, який відповідає його/її ідентифікації користувача, а сервер порівнює заявлений пароль із тим, що міститься у файлі паролю. В такому типі методу пароль є секретом, і сам пароль або його відтворення відкриваються. На противагу йому, в ефективних методах ідентифікації одна особа доводить свою ідентифікацію іншій шляхом демонстрації зняння секрету, що асоціюється з цією особою, без розкриття самого секрету під час протоколу. Для сторін-учасників немає потреби знати точний пароль; можливо одній особі отримати інформацію, що асоціюється з цим паролем дляІнформаційна страктура: Ідентифікація і Цифровий підпис Електронне управління – Що необхідно знати лідеру у сфері управління Сторінка 3 із 10 підтвердження факту знання ним/нею цього паролю. Це так званий протокол «питання – відповідь». Він заснований на шифруванні, механізмі цілісності (МАС) або цифровому підписі.

4. PKI/CA

Криптографічні технології можна використовувати для забезпечення повного спектру послуг по безпеці. Вони повинні братися до уваги при здійсненні захисту секретної або важливої інформації та систем. Криптографія є галуззю прикладної математики, що займається питаннями безпеки передачі даних. У криптографії відправник переводить незахищену інформацію (звичайний текст) у закодований текст (шифровий текст). Одержувач використовує засоби криптографії для переведення отриманного цифрового тексту назад у звичайний текст, для перевірки особистості відправника, цілісності даних або кількох із названих показників одночасно. Цифровий підпис є одним із механізмів, які можна застосовувати для захисту автентичності і цілісності електронних документів. Його можна використовувати для документу будь-якої форми, що обробляється в електронному вигляді. Цифровий підпис вживається за допомогою методу криптографії на основі унікальної зв’язаної пари ключів, в якій один з них використовується для створення підпису (приватний ключ), а другий – для перевірки підпису (відкритий ключ). Щоб захистити конфіденційність приватного ключа, необхідно ретельно над цим працювати.

Цей ключ повинен зберігатися у таємниці, оскільки будь-хто, хто має до нього доступ, може підписувати документи. На доповнення до цього, захист цілісності відкритого ключа також є важливим. Такий захист здійснюється шляхом використання сертифікату відкритого ключа. Одною з головних проблем, пов’язаних із криптографією, є процес відкриття доступу користування приватними ключами для уповноважених користувачів, при цьому зберігаючи їх секретність для всіх інших осіб. Серед інших важливих завдань стоять зв’язування відкритих ключів з організаціями, відкриття можливості для інших організацій перевірки зв’язків відкритого ключа, а також забезпечення послуг, що необхідні для поточного управління ключами у поширюваній системі. Підхід до задоволення потреб безпеки, що виникає, використовує шасштабовані і поширювані характеристики Інфраструктури Відкритого Ключа (ІВК). ІВК може прискорити і спростити доставку продуктів і надання послуг шляхом використання електронних підходів.Термін «інфраструктура відкритого ключа» походить від криптографії відкритого ключа, технології, на якій базується ІВК. Вона має унікальні характеристики, що роблять її безцінною як основу для функцій безпеки у поширюваних системах. Інфраструктура відкритого ключа є поєднанням програмного забезпечення, шифрувальних технологій і послуг, які допомагають захистити безпеку її комунікацій і бізнес-операцій у мережах. ІВК об’єднує цифрові сертифікати, криптографію відкритого ключа та органи сертифікування у повний спектр загальної архітектури безпеки організації.

Типова ІВК включає в себе видачу цифрових сертифікатів індивідуальним користувачам і серверам, програмне забезпечення по реєстрації кінцевого користувача; інтеграцію із сертифікатами; інструменти для управління, оновлення та скасування сертифікатів, а також інші послуги і підтримку, пов’язані з ними.

5. Компоненти ІВК

До функціональних елементів інфраструктури відкритого ключа відносяться органи сертифікації, органи реєстрації, сховища та архіви. Інформаційна страктура: Ідентифікація і Цифровий підпис.

Електронне управління – Що необхідно знати лідеру у сфері управління Сторінка 4 із 10

• Орган сертифікації (ОС), як нотаріус, видає або скасовує сертифікати.

• Орган реєстрації (ОР) – організація, якій ОС довіряє зареєструвати або ручатися

перед ОС за зв’язок між відкритими ключами та ідентифікацією власників сертифікатів.

• Сховище – це база даних активних сертифікатів і список анульованих сертифікатів (САС) для системи ОС.

• Архів є базою даних, яку використовують при вирішенні майбутніх спорів.

• Користувачі ІВК – це організації або фізичні особи, які використовують ІВК, але не видають сертифікати.

ОС є базовим складовим компонентом для ІВК, сукупністю комп’ютерних технічних засобів, програмного забезпечення і людей, які управляють ними. Він має своє ім.’я і відкритий ключ. ОС виконує такі 4 основні функцій ІВК:

1. Видає сертифікати.

2. Має інформацію про статус сертифікату і видає САС.

3. Видає свої поточні сертифікати і САС.

4. Містить архіви даних про статус виданих ним сертифікатів, що втратили юридичну силу.

ОС випускає цифровий сертифікат для ідентифікації кожної окремої особи, підтверджуючи, що особа має відповідні повноваження. Цифровий сертифікат зазвичай містить відкритий ключ, інформацію про особу власника відповідного приватного ключа, термін дії сертифікату, а також власний цифровий підпис ОС. ОС також повинен видавати та обробляти списки анульованих сертифікатів САС, які містять перелік усіх сертифікатів, дію яких скасовано. ОР створено для перевірки даних сертифікату для ОС. Як і ОС, ОР є системою комп’ютерних технічних засобів, програмного забезпечення і людей, які управляють ними. На відміну від ОС, ОР часто управляється одною людиною. Кожен ОС має список акредитованих ОР; ОС знає ОР за назвою і відкритим ключем.

Додатки ІВК у значній мірі залежать від служби каталогів із дистрибуції сертифікатів і статусних даних про сертифікати, що лежать в їх основі. Каталог забезпечує засоби для зберігання і розповсюдження сертифікатів, а також управління процесом внесення оновлень у сертифікати.

Архів відповідає за тривале зберігання інформації від імені ОС. Архів встановлює те, що інформація була коректною в момент її отримання і не піддавалася модифікації в період її зберігання в архіві. Архів захищає інформацію за допомогою технічних механізмів і відповідних процедур під час її перебування в архіві. Якщо в майбутньому виникає спір щодо підпису, цю інформацію можна використовувати для встановлення факту застосування для підписання документу приватного ключа, пов’язаного із сертифікатом. Користувачі ІВК залежать від інших компонентів ІВК для отримання сертифікатів, а також для перевірки сертифікатів для інших організацій, що є їхніми партнерами. Кінцеві організації включають в себе сторону, яка з упевненістю покладається на сертифікат у своєму знанніІнформаційна страктура: Ідентифікація і Цифровий підпис

Електронне управління – Що необхідно знати лідеру у сфері управління Сторінка 5 із 10 відкритого ключа іншої організації і власника сертифікату, якому видано сертифікат і який може підписувати документи.

6. Архітектури ІВК

Власники сертифікату отримують інші сертифікати від ОС в залежності від організації або спільноти, членами якої вони є. ІВК зазвичай складається з багатьох ОС, пов’язаних вивіреними каналами. Вивірений канал пов’язує сторону з одною або кількома вивіреними третіми особами, такими, щоб сторона, яка покладається, могла мати упевненість в дійсності використовуваного сертифікату. Є дві традиційні архітектури ІВК для досягнення цієї мети, а саме: ієрархічна і переплетена. Третій підхід, з’єднана архітектура ОС, був розроблений з метою вирішення проблеми, що стоїть перед організаціями, які шукають шляхів з’єднання своєї ІВК з ІВК їхніх ділових партнерів.

6.1 Ієрархічна

Органи організовані за ієрархією під «кореневим» ОС, який видає сертифікати підлеглим ОС. Ці ОС можуть видавати сертифікати іншим ОС або користувачам, які знаходяться нижче за них в ієрархії зв’язків. В ієрархічній ІВК кожна сторона, яка покладається, знає відкритий ключ свого кореневого ОС. Будь-який сертифікат можна перевірити, перевіривши канали сертифікації для сертифікатів, починаючи з кореневого ОС.

6.2 Переплетена

Незалежні ОС сертифікують один одного (тобто видають сертифікати один одному), що дає результат загального переплетіння вивірених зв’язків між рівними ОС. Сторона, яка покладається, знає відкритий ключ ОС «біля» неї, і, як правило, того, хто видав її сертифікат.

Сторона, яка полагающаяся, здійснює перевірку сертифікату шляхом перевірки каналу сертифікації, який походить від вивіреного ОС.

6.3 З’єднувальний ОС

Архітектура з’єднувального ОС була розроблена для зв’язку організаційних ІВК, незалежно від їх архітектури. Вона досягається шляхом введення нового ОС, що нази­ває­ть­ся з’єднувальним, єдиною метою якого є встановлення зв’язків з організаційними ІВК.

На відміну від переплетеного ОС, з’єднувальний ОС не видає сертифікатів прямо користувачам. На відміну від кореневого ОС в ієрархічній структурі, з’єднувальний ОС не призначений для використання в якості точки довіри. Всі користувачі ІВК сприймають з’єдну­вального ОС як посередника. З’єднувальний ОС встановлює однакові відносини з інши­ми організаційними ІВК (малюнок 1.2). Ці відносини можуть об’єднуватися для формування мосту довіри, що пов’язує користувачів у різних ІВК. Якщо для домену довіри використано ієрархічну ІВК, з’єднувальний ОС встановить зв’язок із кореневим ОС. Якщо ж домен працює у вигляді переплетеної ІВК, з’єднувальний ОС вступить у зв’язок тільки з одним з ОС цього домену. В обох випадках ОС, що вступає у вивірені зв’язки із з’єднувальним ОС, називається головним ОС.

**Ідентифікаційні дані Центру**

Повне найменування: Центр сертифікації ключів Приватного акціонерного товариства "Інфраструктура відкритих ключів".

Місце знаходження: 61058, м. Харків, пр-т Леніна, 5.

Тел./факс: (057) 760-12-60.

Електронна поштова скринька (e-mail): csk@ivk.org.ua.

Електронна адреса електронного інформаційного ресурсу (web-сайту): www.іvk.org.ua

Центр сертифікації ключів Приватного акціонерного товариства "Інфраструктура відкритих ключів" (далі - ПрАТ "ІВК") в м. Харкові є відокремленим структурним, не госпрозрахунковим підрозділом. Фінансове та матеріальне утримання Центру здійснюється ПрАТ "ІВК".

***Ідентифікаційні дані ПрАТ "ІВК":***

Повне найменування: Закрите акціонерне товариство "Інфраструктура відкритих ключів".

Скорочене найменування: ПрАТ "ІВК".

Юридична адреса: 04050, м. Київ, вул. Мельникова, 12.

Тел./факс: (044) 524-98-58.

Код ЄДРПОУ: 33406085.

П/р № 260093017732 у АКБ "Промінвестбанк" (ПрАТ), МФО 300012.

**2. ПЕРЕЛІК СУБ'ЄКТІВ, ЗАДІЯНИХ В ОБСЛУГОВУВАННІ І ВИКОРИСТАННІ СЕРТИФІКАТІВ КЛЮЧІВ**

***2.1. Обслуговування сертифікатів ключів***

Під послугами ЕЦП розуміється надання у користування засобів ЕЦП, допомога при генерації відкритих та особистих ключів, обслуговування сертифікатів ключів (формування, розповсюдження, скасування, зберігання, блокування та поновлення), надання інформації щодо чинних, скасованих і блокованих сертифікатів ключів, послуги фіксування часу, консультації та інші послуги, визначені Законом України "Про електронний цифровий підпис".

Центр забезпечує надання повного переліку послуг ЕЦП, передбачених політикою сертифікації, зокрема:

1) реєстрація заявників;

2) надання у користування засобів криптографічного захисту інформації (далі - КЗІ), у тому числі надійних засобів ЕЦП;

3) допомога при генерації відкритих та особистих ключів;

4) обслуговування сертифікатів ключів заявників, що включає:

* сертифікацію відкритих ключів заявників;
* розповсюдження та зберігання сертифікатів ключів;
* управління статусом сертифікатів ключів та розповсюдження інформації про статус сертифікатів ключів;

5) надання послуги фіксування часу.

Окрім надання послуг ЕЦП, Центр надає консультаційні послуги за зверненням заявників (підписувачів, користувачів).

Надання вищезазначених послуг здійснюється Центром відповідно до цього Регламенту та на підставі укладених письмових договорів або договорів приєднання, укладених шляхом прийняття заяви-приєднання.

Для наближення послуг ЕЦП до місцезнаходження заявників та підписувачів, Центр створює відокремлені пункти реєстрації. Відокремлені пункти реєстрації є відособленими підрозділами без правового статусу юридичної особи, що реалізують функції Центру з реєстрації заявників та їх подальшого обслуговування на відповідній території (крім формування сертифікатів). Відокремлені пункти реєстрації не є юридичними особами, вони наділяються майном юридичної особи, діють на підставі Положення про відокремлений пункт реєстрації юридичної особи та цього Регламенту.

Безпосереднє управління відокремленими пунктами реєстрації здійснюється Центром.

До складу відокремлених пунктів реєстрації входять:

* керівник;
* адміністратор реєстрації;
* оператор реєстрації (діловод).

Функції та завдання відокремлених пунктів реєстрації:

* встановлення осіб, які звернулися до Центру з метою формування сертифіката ключа;
* перевірка даних, обов'язкових для формування сертифіката ключа, а також даних, які вносяться у сертифікат ключа на вимогу заявника;
* проведення процедур реєстрації заявників (підписувачів);
* отримання від заявників (підписувачів) заявок на формування, скасування, блокування та поновлення сертифікатів ключів;
* надання допомоги підписувачам під час генерації особистих та відкритих ключів у разі отримання від них відповідного звернення та вживання заходів щодо забезпечення безпеки інформації під час генерації;
* перевірка законності звернень про блокування, поновлення та скасування сертифікатів ключів;
* надання заявникам, підписувачам, користувачам консультацій щодо умов та порядку надання послуг ЕЦП;
* представництво інтересів ПрАТ "ІВК" у відповідному регіоні.

***2.2. Використання сертифікатів ключів***

Використання сертифікатів ключів, сформованих Центром здійснюється підписувачами, а також користувачами.

Користувачі можуть не мати договірних відносин з Центром.

Підписувачами можуть бути:

* фізичні особи, у тому числі посадові особи та наймані працівники;
* фізичні особи-підприємці;
* юридичні особи, у тому числі органи державної влади, органи місцевого самоврядування у випадках, встановлених законодавством.

**3. Сфера використання сертифіката ключа**

***3.1. Перелік сфер, у яких дозволяється використання сертифікатів ключів***

Сертифікати ключів, сформовані Центром, використовуються для підтвердження ЕЦП, який задовольняє вимогам щодо підпису, застосованого до даних в електронній формі, у такий же спосіб, як власноручні підписи задовольняють вимогам стосовно документу на папері.

Центр здійснює обслуговування сертифікатів ключів, сформованих для органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій всіх форм власності, фізичних осіб, незалежно від сфери використання сертифікатів ключів.

***3.2. Обмеження щодо використання сертифікатів ключів***

Центр має право встановлювати обмеження сфери використання сформованих ним сертифікатів ключів. Інформація щодо обмеження сфери використання доводиться до заявника (підписувача) та зазначається у сформованому Центром сертифікаті ключа.

***3.3. Центр має право:***

* вимагати від заявника або його уповноваженого представника надавати повну та дійсну інформацію, необхідну для реєстрації заявника та формування сертифіката ключа підписувача, а також здійснювати перевірку наданої інформації;
* не приймати запит на формування сертифіката ключа, що виконаний в електронному вигляді, якщо використаний заявником для формування запиту на сертифікат ключа засіб криптографічного захисту інформації не підтримується Центром;
* скасовувати, блокувати, поновлювати сертифікати ключі заявника у порядку, визначеному цим Регламентом;
* вимагати від заявника дотримуватись умов цього Регламенту та умов договору про надання послуг ЕЦП;
* припинити надання заявнику послуг ЕЦП у разі несплати ним вартості послуг, порушення умов цього Регламенту або договору про надання послуг ЕЦП;
* вимагати від заявника відшкодування в повному обсязі майнової та моральної шкоди у разі, якщо така шкода була завдана Центру з вини заявника;
* вимагати від заявника укладення Акту виконаних робіт.

***3.4. Центр зобов'язаний:***

* забезпечити можливість цілодобового вільного доступу з використанням телекомунікаційних мереж загального користування до сертифікатів ключів інших заявників (підписувачів), даних про статус сертифікатів ключів, сертифіката ключа Центру, нормативних документів з питань надання послуг ЕЦП;
* використовувати програмно-технічний комплекс (далі - ПТК), засоби криптографічного захисту інформації, у тому числі засоби ЕЦП, що відповідають вимогам нормативних документів у галузі криптографічного та технічного захисту інформації та мають позитивний експертний висновок у галузі КЗІ і атестат відповідності комплексної системи захисту інформації;
* забезпечувати розташування засобів ПТК, за допомогою яких здійснюється надання послуг в спеціальних приміщеннях, здійснювати їх охорону для запобігання безконтрольному проникненню в приміщення Центру сторонніх осіб;
* забезпечувати захист персональних даних підписувача, отриманих від заявника, згідно діючого законодавства, за виключенням персональних даних підписувача, які є загальновідомими, містяться у відкритих інформаційних джерелах або після формування сертифіката ключа стають його частиною;
* забезпечувати реєстрацію заявників та підписувачів відповідно до порядку реєстрації, визначеного цим Регламентом;
* перевіряти унікальність реєстраційної інформації заявників, що використовується для ідентифікації підписувачів;
* забезпечувати формування сертифікатів ключів зареєстрованого підписувача відповідно до порядку, визначеного даним Регламентом;
* забезпечувати унікальність реєстраційних номерів сертифікатів ключів, що формуються Центром;
* встановлювати належність відкритого ключа та відповідного особистого ключа підписувача;
* забезпечувати унікальність значень відкритих ключів у сертифікатах ключів, що формуються Центром;
* інформувати заявників (підписувачів) про необхідність здійснення перевірки чинності сертифіката ключа з використанням інформації про його статус та врахування всіх визначених у сертифікаті ключа обмежень щодо його використання;
* своєчасно попереджувати підписувача та додавати до сертифіката ключа підписувача інформацію про обмеження використання ЕЦП;
* своєчасно блокувати сертифікат ключа підписувача за заявою на блокування, що надходить від заявника (підписувача) або за іншими умовами, які визначені чинним законодавством, в усній формі чи у електронному вигляді, та протягом 2 годин занести відомості про блокований сертифікат ключа у список відкликаних сертифікатів із зазначенням дати та часу занесення;
* своєчасно поновлювати сертифікат ключа підписувача за заявою на поновлення, що надходить від заявника або за іншими умовами, які визначені чинним законодавством, не пізніше одного робочого дня, наступного за робочим днем, протягом якого була подана заява, та виключити відомості про блокований сертифікат зі списку відкликаних сертифікатів;
* своєчасно скасовувати сертифікат ключа підписувача за заявою на скасування, що надходить від заявника або за іншими умовами, які визначені чинним законодавством, та протягом 2 годин занести відомості про скасований сертифікат ключа у список відкликаних сертифікатів із зазначенням дати, часу занесення та причини скасування;
* перевіряти законність звернень про скасування, блокування та поновлення сертифікатів ключів та зберігати документи, на підставі яких були скасовані, блоковані та поновлені сертифікати ключів;
* забезпечити зберігання сформованих сертифікатів ключів протягом строку, передбаченого законодавством для зберігання відповідних документів на папері;
* публікувати відомості щодо відкликаних сертифікатів на електронному інформаційному ресурсі Центру з періодичністю 1 раз у 2 години;
* надавати заявникам (підписувачам, користувачам) консультації з питань, пов'язаних з ЕЦП.

***3.5. Відповідальність***

У разі невиконання своїх обов'язків за даним Регламентом Центр або заявник (далі разом та окремо - Сторони), повинні в повному обсязі відшкодувати збитки, заподіяні іншій стороні, у порядку, встановленому чинним законодавством.

Сторони несуть відповідальність за дії своїх співробітників, а також інших осіб, які мають або мали доступ (незалежно від того, був цей доступ санкціонований Стороною, або виник з її провини) до апаратних засобів, програмного, інформаційного забезпечення, криптографічних ключів та інших засобів ЕЦП, як за свої особисті.

Сторони не відповідають за невиконання або неналежне виконання своїх обов'язків за даним Регламентом, а також за збитки, які виникли у зв'язку з цим, у випадках, якщо це є наслідком зустрічного невиконання (неналежного виконання) Сторонами своїх обов'язків.

Центр не несе відповідальності за майнову та моральну шкоду, що була спричинена неналежною роботою програмного забезпечення Центру у разі, якщо неналежна робота програмного забезпечення була викликана "мережевими атаками", дією "вірусних програм" або іншим неякісним (не ліцензованим) програмним забезпеченням заявника, підписувача, користувача.

Центр не несе відповідальності за майнову та моральну шкоду, що може бути спричинена заявнику або третім особам, у разі невиконання або неналежного виконання заявником вимог цього Регламенту та договору про надання послуг ЕЦП.

Центр не відповідає за невиконання або неналежне виконання своїх обов'язків за даним Регламентом, а також за збитки, що виникли у зв'язку із цим, у випадках:

* якщо Центр обґрунтовано покладався на відомості, зазначені заявником;
* підробки, підміни або іншого перекручування заявником або його уповноваженим представником відомостей, що містяться у реєстраційних або в інших документах, наданих Центру.

Центр несе відповідальність за збитки, спричинені заявнику у випадку, якщо такі збитки виникли внаслідок:

* внесення в сертифікат невірних відомостей, відмінних від вказаних у заяві на формування сертифіката;
* невірного встановлення заявника, наприклад, унаслідок технічних помилок, недотримання процедур перевірки документів тощо;
* несвоєчасної публікації списків відкликаних сертифікатів;
* помилкового скасування або блокування сертифікатів;
* компрометації особистого ключа Центру;
* відмови та збою технічних і програмних засобів ПТК;
* помилкових або протиправних дій обслуговуючого персоналу Центру;
* несанкціонованого розголошення персональних даних підписувачів.

Відповідальність Сторін, яка не врегульована положеннями даного Регламенту, регулюється чинним законодавством України.

Сторони звільняються від відповідальності за повне або часткове невиконання своїх зобов'язань, якщо таке невиконання сталося внаслідок настання форс-мажорних обставин, таких, як пожежа, повінь, землетрус, інше стихійне лихо, військові дії, дія надзвичайного стану, блокада, громадські масові зворушення, страйків, аварій на транспорті, диверсій, розпоряджень Державних органів влади, або інших обставин, які не залежать від волі Сторін, за умови, що дані обставини безпосередньо впливають на виконання їх зобов'язань, і їх неможливо було передбачити на момент укладання договору про надання послуг ЕЦП.

Сторона, що через зазначені вище обставини не може в повному обсязі виконувати свої зобов'язання, повинна в строк не більше п'яти днів письмово сповістити про це іншу Сторону, а в строк до десяти днів надати відповідні документи, які це підтверджують.

Несвоєчасне (пізніше 5-ти днів) повідомлення про існування обставин форс-мажору позбавляє відповідну Сторону права посилатися на них для виправдання.

Достатнім доказом існування обставин форс-мажору є довідки компетентних органів влади.

У випадку, якщо вищезгадані обставини будуть діяти більше трьох місяців, кожна зі Сторін може письмово сповістити іншу про повне або часткове припинення дії договору про надання послуг ЕЦП, що звільняє Сторони від взаємних зобов'язань, за винятком проведення взаєморозрахунків у частині вже виконаних Сторонами зобов'язань.

***3.6. Порядок розв'язання спорів та вирішення конфліктних ситуацій***

Будь-яка конфліктна ситуація вирішується шляхом переговорів із дотриманням претензійного порядку.

У разі виникнення непорозумінь щодо виконання вимог даного Регламенту та договору про надання послуг ЕЦП, які не вирішено мирним шляхом, або інших спірних питань, Сторона, яка вважає, що її права порушуються, зобов'язана в місячний строк з моменту, коли вона дізналась або повинна була дізнатись про таке порушення, направити іншій Стороні обґрунтовану претензію.

Претензія, направлена з порушенням зазначеного строку, не розглядається.

Усі спірні ситуації, за якими не досягнуто згоди в претензійному порядку, вирішуються у господарському або загальному суді.

**4. Порядок розповсюдження (публікації) інформації**

***4.1. Інформаційний ресурс Центру***

Інформаційний ресурс Центру призначений для розміщення на ньому відкритої інформації, яка структурно поділяється на:

* довідкову інформацію (режими роботи Центру, положення Регламенту, нормативні документи, договори на надання послуг, форми заяв тощо);
* сертифікат ключа Центру;
* сертифікати ключів серверів Центру;
* сертифікати ключів підписувачів;
* списки відкликаних сертифікатів, що містять інформацію про статуси сертифікатів ключів Центру та підписувачів.

Електронна адреса (DNS-ім'я) електронного інформаційного ресурсу: www.іvk.org.ua.

Технічною основою інформаційного ресурсу Центру є сервери взаємодії, що входять до складу ПТК Центру.

Довідкова інформація розміщується на HTTP-сервері сервера взаємодії у вигляді набору web-сторінок.

Сертифікат ключа Центру, сертифікати ключів серверів Центру та підписувачів, а також списки відкликаних сертифікатів розміщуються:

* у складі web-сторінок на HTTP-сервері сервера взаємодії;
* у інформаційному дереві LDAP-каталога на LDAP-сервері сервера взаємодії.

Доступ до HTTP-сервера здійснюється за DNS-ім'ям www.іvk.org.ua за протоколом HTTP (номер TCP-порта 80).

Доступ до LDAP-сервера здійснюється за DNS-ім'ям www.іvk.org.ua за протоколом LDAP (номер TCP-порта 389).

***4.2 Порядок публікації сертифіката ключа Центру та сертифікатів ключів серверів Центру***

Після формування сертифіката ключа Центру виконується його публікація на інформаційному ресурсі. На інформаційному ресурсі також здійснюється публікація сертифікатів ключів серверів Центру:

* сервера обробки запитів (CMP-сервера);
* сервера позначок часу (TSP-сервера);
* сервера визначення статусу сертифікатів ключів (OCSP-сервера).

Публікація сертифікатів ключів серверів Центру виконується після формування сертифіката ключа відповідного сервера.

***4.3 Порядок публікації сертифікатів ключів підписувачів***

Публікація сертифікатів ключів підписувачів на інформаційному ресурсі Центру здійснюється за згодою заявника (підписувача). Інформація про необхідність публікації сертифікатів ключів кожного окремого підписувача вноситься у склад реєстраційних даних під час реєстрації.

Публікація сертифікатів ключів підписувачів у інформаційному дереві LDAP-каталога здійснюється автоматично з інтервалом синхронізації п'ятнадцять (15) хв.

***4.4 Порядок публікації списків відкликаних сертифікатів***

Публікація списків відкликаних сертифікатів на інформаційному ресурсі Центру (на HTTP-сервері) здійснюється одразу після його випуску.

Центр виконує випуск списків відкликаних сертифікатів (далі - список) двох типів:

* повний список;
* частковий список.

Повний список випускається один (1) раз на тиждень та місить інформацію про всі відкликані сертифікати ключів, які були сформовані Центром на діючому особистому ключеві.

Частковий список випускається кожні дві (2) години та місить інформацію про всі відкликані сертифікати ключів, статус яких був змінений в інтервалі між часом випуску останнього повного списку та часом формування поточного часткового списку.

ПУБЛІКАЦІЯ СПИСКІВ ВІДКЛИКАНИХ СЕРТИФІКАТІВ У ІНФОРМАЦІЙНОМУ ДЕРЕВІ LDAP-КАТАЛОГА ЗДІЙСНЮЄТЬСЯ АВТОМАТИЧНО З ІНТЕРВАЛОМ СИНХРОНІЗАЦІЇ П'ЯТЬ (5) ХВ.

**5. Порядок ідентифікації та автентифікації (під час реєстрації)**

***5.1. Організаційні вимоги щодо встановлення заявника під час реєстрації***

***5.1.1. Загальні положення***

Перед формуванням вперше сертифікатів ключів юридичним особам (ЕЦП використовується в якості печатки) або фізичним особам (ЕЦП використовується як аналог власноручного підпису) Центр здійснює встановлення заявника (фізичної або юридичної особи). Встановлення заявника здійснюється при його особистій присутності або його уповноваженого представника в Центрі або відокремленому пункті реєстрації.

Заявник (уповноважений представник) повинен ознайомитися із умовами обслуговування сертифікатів ключів, передбачених політикою сертифікації, а також Регламентом, зокрема:

* зобов'язання та підстави відповідальності Центру стосовно обслуговування сертифікатів ключів;
* зобов'язання та підстави відповідальності заявника (підписувача) стосовно використання сертифіката ключа і зберігання особистого ключа;
* сфери використання підписувачем сертифіката ключа;
* строки зберігання Центром даних про заявників (підписувачів), що були отримані ним під час реєстрації;
* відомості про засоби ЕЦП, що можуть використовуватися для формування та перевірки ЕЦП.

***5.1.2. Встановлення юридичної особи***

Встановлення заявника - юридичної особи здійснюється за установчими документами юридичної особи або копіями таких документів, які нотаріально засвідчені відповідно до законодавства. Крім цього, під час реєстрації встановлюється представник юридичної особи та його повноваження.

Під час реєстрації уповноважена особа заявника надає такі документи:

***Обов'язкові документи***

* заповнена та підписана заява на реєстрацію для отримання посиленого сертифіката ключа встановленого зразка;
* заповнена та підписана заява приєднання до договору "Про надання послуг електронного цифрового підпису" у двох примірниках;
* оригінал статуту юридичної особи (положення про установу) або його нотаріально засвідчена копія (виключно для ознайомлення);
* оригінал або копія свідоцтва про державну реєстрацію, засвідчена підписом керівника та печаткою юридичної особи або підписом та печаткою посадової особи Центру;
* документи, що підтверджують повноваження керівника заявника;
* копії паспортів підписувачів (копії 1-4 сторінок), засвідчені власноручними підписами власників паспортів.

***Додаткові документи***

* копія довідки про присвоєння ідентифікаційного коду ДРФО керівника та головного бухгалтера (у разі, якщо формуються сертифікати для керівника та бухгалтера);;
* копія свідоцтва про реєстрацію платника податку на додану вартість (у разі, якщо особа є платником ПДВ).

У разі, якщо заявником є бюджетна установа, замість заяви приєднання до договору "Про надання послуг електронного цифрового підпису" надаються два примірники договору.

Копії та витяги, крім нотаріально засвідчених, засвідчуються підписом керівника та печаткою юридичної особи. Якщо заявником подано оригінал документу, копія такого документу може бути засвідчена підписом та печаткою посадової особи Центру.

**для відокремлених підрозділів (філії, представництва) юридичних осіб:**

***Обов'язкові документи***

* заповнена та підписана заява на реєстрацію для отримання сертифіката ключа встановленого зразку;
* заповнена та підписана заява приєднання до договору "Про надання послуг електронного цифрового підпису" у двох примірниках;
* оригінал або копія положення про відокремлений підрозділ, засвідчена підписом та печаткою керівника відокремленого підрозділу;
* довідка управління статистики по внесення відомостей про відокремлений підрозділ до ЄДРПОУ;
* документи, що підтверджують повноваження керівника заявника;
* копія довіреності керівника відокремленого підрозділу, засвідчена підписом та печаткою керівника відокремленого підрозділу.

***Додаткові документи***

* копія довідки про присвоєння ідентифікаційного коду ДРФО керівника та головного бухгалтера (у разі, якщо формуються сертифікати для керівника та бухгалтера);
* копія свідоцтва про реєстрацію платника податку на додану вартість (у разі, якщо особа є платником ПДВ).

Копії та витяги, крім нотаріально засвідчених, засвідчуються підписом керівника та печаткою відокремленого підрозділу. Якщо заявником подано оригінал документу, копія такого документу може бути засвідчена підписом та печаткою посадової особи Центру.

Бланки реєстраційних документів (договір та заява приєднання, заява на реєстрацію, довіреність, тощо) встановленої форми розміщуються на інформаційному ресурсі Центру.

***5.1.3. Встановлення фізичної особи***

Встановлення фізичної особи здійснюється за паспортом (або іншим документом, який засвідчує особу відповідно до законодавства України). Встановлення фізичної особи - підприємця здійснюється на підставі свідоцтва про державну реєстрацію або його належно засвідченої копії та документа, що посвідчує особу (паспорт).

У разі, якщо під час реєстрації встановлюється підписувач - фізична особа як представник юридичної особи, заявником виступає юридична особа. Реєстрація заявника здійснюється відповідно до п. 5.1.2 Регламенту.

Під час реєстрації заявник (фізична особа) надає такі документи:

***для фізичних осіб - підприємців:***

***Обов'язкові документи***

* заповнена та підписана заява на реєстрацію для отримання сертифіката ключа встановленого зразку;
* заповнена та підписана заява приєднання до договору "Про надання послуг електронного цифрового підпису" у двох примірниках;
* оригінал або копія свідоцтва про державну реєстрацію фізичної особи - підприємця, засвідчена підписом підприємця з прикладенням його печатки або підписом та печаткою посадової особи Центру;
* паспорт громадянина.

***Додаткові документи***

* копія свідоцтва про реєстрацію платника податку на додану вартість (в разі, якщо особа є платником ПДВ);

Копії та витяги, крім нотаріально засвідчених, засвідчуються підписом підприємця та його печаткою. Якщо заявником подано оригінал документу, копія такого документу може бути засвідчена підписом та печаткою посадової особи Центру;

Бланки реєстраційних документів (договір та заява приєднання, заява на реєстрацію, довіреність, тощо) встановленої форми розміщуються на інформаційному ресурсі Центру.

***для фізичних осіб:***

***Обов'язкові документи***

* заповнена та підписана заява на реєстрацію для отримання сертифіката ключа встановленого зразку;
* заповнена та підписана заява приєднання до договору "Про надання послуг електронного цифрового підпису" у двох примірниках;
* паспорт фізичної особи;
* копія довідки про присвоєння ідентифікаційного коду ДРФО.

Бланки реєстраційних документів (договір та заява приєднання, заява на реєстрацію, довіреність, тощо) встановленої форми розміщуються на інформаційному ресурсі Центру.

Заявник може бути представлений довіреною особою - представником, якщо немає можливості його особистої присутності у Центрі. У цьому випадку заявник надає довіреність відповідного зразка. Встановлення представника здійснюється за паспортом або іншими документами відповідно до законодавства.

Довіреність представника засвідчується:

* для юридичних осіб - підписом керівника з прикладенням печатки юридичної особи;
* для фізичних осіб-підприємців - підписом підприємця з прикладенням його печатки або у разі відсутності печатки - нотаріально;
* для фізичних осіб - нотаріально.

Адміністратор реєстрації Центру виконує процедуру встановлення особи заявника (його довіреної особи), що проходить процедуру реєстрації.

Надані заявником (представником) документи розглядаються протягом однієї години з моменту їх надходження.

До розгляду не приймаються документи, які мають підчистки, дописки, закреслені слова, інші незастережні виправлення або написи олівцем, а також мають пошкодження, внаслідок чого їх текст неможливо прочитати.

За результатом розгляду наданих документів адміністратор реєстрації приймає рішення про відмову в реєстрації у разі:

* відсутності всіх необхідних для реєстрації документів;
* подання неналежно засвідчених копій документів;
* встановлення невідповідності даних, що визначені наданими документами, фактичним.

У випадку відмови у реєстрації, надані документи повертаються заявнику (представнику) з позначкою адміністратора реєстрації на заяві про підстави відмови.

При ухваленні позитивного рішення, після оформлення договірних документів та виконання заявником необхідних умов надання послуг ЕЦП (попередня оплата, внесення авансу, подання додаткових документів тощо) адміністратор реєстрації виконує дії по занесенню реєстраційної інформації до реєстру користувачів Центру.

Всі документи, що були надані заявникам під час реєстрації, беруться на облік шляхом формування справи підписувача, уведення необхідних ідентифікаційних даних підписувачів до бази даних Центру. Справа підписувача реєструється в журналі, який ведеться в паперовому або електронному вигляді.

Реєстрація заявника є підставою для генерації ключів заявника, створення запиту на сертифікацію та формування сертифіката ключа підписувача.

***5.1.4. По завершенню процедури реєстрації, заявнику надаються:***

* оформлені договірні документи;
* надійні засоби ЕЦП разом з інструкцією користувача;
* носій, що містить чинні сертифікати ключів центрального засвідчувального органу, Центру, підписувача;
* носій інформації, що містить особистий ключ підписувача (у випадку генерації ключів у Центрі).

***5.1.5. Захист персональних даних підписувачів забезпечується шляхом вжиття:***

* організаційних заходів щодо обліку та зберігання справ підписувачів, зокрема формування справи підписувачів та їх облік, призначення відповідальної особи за зберігання справ підписувачів, обмежений доступ обслуговуючого персоналу до приміщення (шаф), де зберігаються справи підписувачів;
* організаційно-технічних та технічних заходів реалізованих комплексною системою захисту інформації автоматизованої системи Центру (далі - КСЗІ), у тому числі: використанням надійних засобів ЕЦП, веденням журналів роботи системи у захищеному вигляді, розмежування та контролю інформаційних потоків між внутрішньою локальною мережею Центру та підсистемою відкритого доступу, використанням антивірусних засобів, міжмережевих екранів тощо.

***5.1.6. Підтвердження володіння заявником (підписувачем) особистим ключем, відповідний якому відкритий ключ надається заявником на сертифікацію***

Запит на сертифікацію в електронному вигляді містить відкритий ключ, що надається на сертифікацію та засвідчується ЕЦП за допомогою відповідного йому особистого ключа. Підтвердження володіння заявником (підписувачем) особистим ключем, відповідний якому відкритий ключ надається на сертифікацію, здійснюється шляхом перевірки Центром (відокремленим пунктом реєстрації) ЕЦП запиту на формування сертифіката ключа.

У випадку, якщо термін дії сертифіката закінчився, для формування сертифіката використовується процедура автентифікації підписувача, що передбачена для реєстрації.

***5.1.7. Автентифікація підписувача під час звернення щодо блокування, скасування та поновлення сертифіката ключа***

В залежності від порядку звернення щодо блокування, скасування та поновлення сертифіката ключа передбачені різні форми автентифікації підписувача та перевірки законності такого звернення:

* у разі письмового звернення підписувача, законність звернення встановлюється за власноручним підписом та печатки юридичної особи (для юридичних осіб);
* у разі звернення шляхом направлення запиту на блокування або скасування сертифіката в електронному вигляді, законність звернення встановлюється шляхом перевірки ЕЦП на запиті за допомогою чинного сертифіката підписувача;
* у разі звернення щодо блокування сертифіката ключа по телефону, законність звернення встановлюється за парольною фразою, що вказується підписувачем під час реєстрації.

**6. Процедури та механізми, пов'язані із формуванням, блокуванням, скасуванням та використанням сертифіката ключа**

***6.1.ПОРЯДОК ГЕНЕРАЦІЇ КЛЮЧІВ ПІДПИСУВАЧА***

Відкритий та особистий ключі підписувача можуть бути згенеровані:

* на робочому місці підписувача;
* на робочій станції генерації ключів підписувачів у Центрі.

***6.1.1. Генерація на робочому місці підписувача***

Для генерації відкритого та особистого ключів на робочому місці підписувача застосовуються надійні засоби ЕЦП, що надаються Центром. При цьому генерація здійснюється з використанням технічних засобів заявника.

Згенерований особистий ключ підписувача захищається паролем та записується на носій ключової інформації. Відповідальність за забезпечення конфіденційності та цілісності особистого ключа несе заявник.

Надійні засоби ЕЦП, що надаються заявнику, формують відкритий ключ підписувача у відповідному форматі.

Передача до Центру (відокремлених пунктів реєстрації) сформованого підписувачем відкритого ключа здійснюється на носії інформації особисто підписувачем або довіреною особою заявника.

У випадку генерації ключів на робочому місці підписувача, при отриманні відкритого ключа у відповідному форматі, адміністратор реєстрації перевіряє формат наданого ключа засобами програмного забезпечення "ІІТ ЦСК-1. Віддалений адміністратор реєстрації", і у разі його невідповідності - відмовляє у формуванні сертифіката ключа. При цьому надані раніше документи повертаються заявнику з позначкою адміністратора реєстрації на заяві.

Під час обробки запиту на формування сертифіката ключа підписувача здійснюється перевірка належності особистого ключа підписувача відкритому ключу, який міститься у запиті. Перевірка здійснюється з використанням АРМ адміністратора реєстрації автоматично, шляхом перевірки ЕЦП, накладеного на запит на формування сертифіката, з використанням відкритого ключа, що міститься у запиті. Тобто запит на формування сертифіката є самопідписаним. Формування сертифіката ключа підписувача можливе за умов успішної перевірки.

***6.1.2. Генерація ключів на робочій станції Центру***

Ключі підписувача генеруються ним особисто або довіреною особою заявника на робочій станції генерації ключів, що входить до складу ПТК Центру.

По закінченні процедури генерації, особистий ключ підписувача автоматично записується на носій ключової інформації та залишається у підписувача, а відкритий ключ передається через службовий носій інформації на робочу станцію адміністратора реєстрації.

Особисті ключі підписувачів не зберігаються у Центрі. Після генерації та запису на носій ключової інформації вони автоматично знищуються надійним способом.

Генерація ключів довіреною особою здійснюється на робочій станції генерації ключів. По закінченні процедури генерації, носій ключової інформації та парольна фраза вкладається у непрозорий конверт, який запечатується, скріплюється печаткою ПрАТ "ІВК", підписами довіреної особи та адміністратора реєстрації у випадку, якщо адміністратором надавалась допомога при генерації ключів.

Після передачі конверта з носієм ключової інформації довіреній особі заявника, відповідальність за забезпечення конфіденційності та цілісності особистого ключа несе заявник.

У разі, якщо генерація ключів здійснювалась довіреною особою, підписувач при отриманні особистого ключа зобов'язаний перевірити цілісність конверта. Якщо цілісність не порушена, то невідкладно, до першого використання особистого ключа, підписувач зобов'язаний змінити пароль доступу до нього.

У разі, якщо неможливо змінити пароль шляхом перезапису ключа на той самий носій ключової інформації (наприклад ключ записаний на CD-R), після зміни паролю на новому носії необхідно знищити надійним способом особистий ключ зі старим паролем.

Якщо цілісність конверта порушена, заявник (підписувач) невідкладно зобов'язаний звернутись до Центру із заявою про скасування сертифіката відповідного ключа.

Строк дії особистого ключа підписувача не може перевищувати 2 (двох) років. Початком перебігу строку дії особистого ключа підписувача вважається дата та час формування сертифіката, що містить відкритий ключ, відповідний до особистого.

***6.2. Порядок формування сертифікатів ключів підписувачів***

Формування сертифіката ключа підписувачу здійснюється на підставі даних, отриманих від заявника або його представника під час реєстрації.

Підписувач на один і той самий момент часу може мати і використовувати лише один особистий ключ, якому відповідає відкритий ключ із чинним сертифікатом ключа, отриманим заявником - юридичною особою (фізичною особою - підприємцем). Це обмеження не стосується електронної печатки.

Формат сертифіката відповідає вимогам Закону України "Про електронний цифровий підпис" та визначається відповідними технічними специфікаціями форматів представлення базових об'єктів національної системи ЕЦП.

Якщо процедуру реєстрації виконано успішно, адміністратор реєстрації надсилає електронний запит на формування сертифіката та реєстраційні дані підписувача до серверу обробки запитів Центру.

Після формування сертифіката ключа Центром адміністратор реєстрації виготовляє три примірника сертифіката у вигляді документа у паперовій формі, які засвідчуються печаткою ПрАТ "ІВК", власноручним підписом заявника або підписом його представника, а також власноручним підписом адміністратора реєстрації.

Сертифікат ключа підписувача в електронній формі записується на носій інформації заявника та у реєстр сертифікатів Центра.

Строк чинності сертифіката ключа не може перевищувати двох (2) років. Початком строку чинності сертифіката ключа вважається дата та час його формування.

***6.3 Повторне формування сертифіката ключа***

Повторне формування сертифіката ключа полягає у формуванні нового сертифіката ключа підписувачу, у разі завчасного (протягом дії договору) скасування чинного сертифіката, з підстав компрометації особистого ключа або зміни відомостей про заявника (підписувача), зазначених у сертифікаті ключа, який скасований.

При повторному формуванні сертифіката ключа адміністратором реєстрації здійснюється перевірка дійсності даних, які надавалися заявником раніше під час реєстрації.

При виникненні необхідності зміни даних, зазначених у сертифікаті ключа, Центр може здійснити переформування сертифіката ключа підписувачу із використанням попередньо засвідченого відкритого ключа підписувача у разі, якщо відповідний йому особистий ключ не був скомпрометований. При цьому строк чинності особистого ключа не може перевищувати двох (2) років.

***6.4. Надання сформованого сертифіката ключа підписувачу та визнання сертифіката ключа його власником***

Після отримання сертифіката ключа підписувач повинен перевірити правильність відомостей, що в ньому містяться. При виявленні некоректних даних (помилки в реквізитах), підписувач повинен повідомити про зазначене Центр (відокремлений пункт реєстрації) у порядку, встановленому для скасування сертифіката ключа. В такому випадку сертифікат ключа скасовується та формується новий сертифікат ключа.

***6.5. Використання сертифіката та особистого ключа***

***6.5.1 Права та обов'язки заявника***

Заявник зобов'язаний:

* ознайомитись з умовами надання послуг ЕЦП, визначених цим Регламентом та відповідними нормативними документами, та дотримуватись них;
* надавати повну та дійсну інформацію під час реєстрації, необхідну для формування сертифіката ключа підписувача;
* зберігати у таємниці особистий ключ ЕЦП та вживати усіх можливих заходів для запобігання його втрати, розкриття, перекручування чи несанкціонованого використання;
* не розголошувати та не повідомляти іншим особам пароль доступу до особистого ключа та ключову фразу голосової автентифікації;
* не розголошувати та не повідомляти іншим особам пароль доступу до захищеного носія ключової інформації, на якому знаходиться особистий ключ ЕЦП;
* використовувати особистий ключ виключно для мети, визначеної у сертифікаті, та додержуватися інших обмежень щодо сфери використання сертифіката ключа;
* використовувати надійні засоби ЕЦП для генерації особистих та відкритих ключів, формування та перевірки ЕЦП;
* негайно інформувати Центр про наступні події, що трапилися до закінчення строку чинності сертифіката ключа: компрометацію особистого ключа; компрометацію паролю захисту особистого ключа; виявлені неточності або зміни даних, зазначених у сертифікаті;
* не використовувати особистий ключ у разі його компрометації;
* не використовувати особистий ключ, відповідний до сертифіката ключа, заява на скасування чи блокування якого подана до Центру, протягом часу з моменту подання заяви і до моменту офіційного повідомлення про скасування сертифіката ключа;
* не використовувати для накладання ЕЦП особистий ключ, відповідний до сертифіката ключа, що скасований або блокований.

Якщо заявник та підписувач є різними суб'єктами, заявник повинен зобов'язати підписувача виконувати вимоги цього Регламенту.

Заявник має право:

* своєчасно отримувати якісні послуги ЕЦП;
* цілодобового вільного доступу з використанням телекомунікаційних мереж загального користування до сертифікатів ключів інших підписувачів, даних про статус сертифікатів ключів, сертифіката ключа Центру, нормативних документів з питань надання послуг ЕЦП;
* одержувати сертифікати ключів Центру;
* одержувати список відкликаних сертифікатів, сформований Центром;
* застосовувати сертифікати ключів Центру для перевірки справжності ЕЦП сертифікатів ключів, сформованих Центром;
* застосовувати список відкликаних сертифікатів, сформований Центром, для перевірки статусу власного сертифіката ключа та сертифікатів ключів інших підписувачів;
* ознайомлюватись з інформацією щодо діяльності Центру та надання послуг ЕЦП;
* подавати заяви, скарги, претензії, позови;
* вимагати скасування, блокування або поновлення свого сертифіката ключа.
* вимагати від Центру усунення порушень умов даного Регламенту та договору про надання послуг ЕЦП;
* вимагати від Центру виконання вимог захисту персональних даних підписувача;
* оскаржити дії чи бездіяльність Центру у судовому порядку.

***6.5.2. Обов'язки користувача***

Користувач зобов'язаний:

* використовувати надійні засоби ЕЦП;
* підтверджувати ЕЦП з використанням чинних посилених сертифікатів ключів Центру;
* під час перевірки ЕЦП використовувати посилений сертифікат ключа, чинний на момент накладення ЕЦП.

***6.6 Підстави та порядок скасування, блокування та поновлення сертифікатів ключів***

***6.6.1. Підстави та порядок скасування сертифікатів ключів підписувачів***

Під скасуванням розуміється відміна чинності сертифіката ключа. Центр негайно скасовує сформований сертифікат ключа підписувача у разі:

* набрання законної сили рішенням суду про скасування посиленого сертифіката ключа;
* смерті підписувача або оголошення його померлим за рішенням суду;
* визнання підписувача недієздатним за рішенням суду;
* припинення діяльності суб'єкта господарювання - заявника;
* розірвання підписувачем трудового договору з юридичною особою - заявником;
* надання заявником недостовірних даних;
* не поновлення заявником заблокованого сертифіката протягом 30 календарних днів;
* припинення (розірвання) договору приєднання "Про надання послуг електронного цифрового підпису";
* за заявою заявника або його уповноваженого представника.

***6.6.2. Обставини, за яких сертифікат повинен бути скасований заявником.***

Підписувач (заявник - юридична особа) зобов'язаний звернутися до Центру щодо скасування сертифіката ключа у разі:

* компрометації особистого ключа підписувача (факт або обґрунтована підозра того, що особистий ключ став відомий іншим особам, втрата можливості подальшого використання особистого ключа із будь-яких обставин, зокрема, втрата або пошкодження носія ключової інформації тощо);
* зміни відомостей, зазначених у сертифікаті ключа: переведення на іншу посаду або звільнення з роботи підписувача (для сертифікатів, в яких зазначено посада його власника); зміна прізвища; виявлення помилок у реквізитах сертифіката ключа тощо.

Документи, що були підставою для скасування, блокування або поновлення сертифіката ключа, фіксуються та зберігаються у Центрі.

***6.6.3. Порядок скасування сертифікатів ключів***

Скасування припиняє чинність сертифіката ключа. Скасовані сертифікати ключів поновленню не підлягають.

Для скасування сертифіката ключа заявник зобов'язаний подати до Центру або відокремленого пункту реєстрації письмову заяву встановленого зразка, засвідчену його особистим підписом. Якщо заявником є юридична особа, заява засвідчується підписом уповноваженого представника та печаткою юридичної особи.

Подача заяви на скасування сертифіката ключа здійснюється тільки протягом робочого дня Центру.

Обробка заяви на скасування сертифіката ключа та інформування заявника (підписувача) про скасування здійснюється протягом одного робочого дня, що йде за робочим днем, протягом якого була подана заява.

Часом скасування сертифіката ключа вважається час зміни його статусу в реєстрі користувачів Центру.

Підписувач не має права використовувати особистий ключ для накладення ЕЦП, сертифікат ключа якого скасовано.

У випадку, якщо необхідне термінове скасування сертифіката ключа через об'єктивні обставини, з метою недопущення спричинення майнової шкоди, заявник (підписувач) має право заблокувати сертифікат ключа такого особистого ключа в усній формі та протягом строку блокування подати відповідні заяви про блокування та скасування сертифіката ключа.

***6.6.4. Порядок блокування сертифікатів ключів***

Під блокуванням сертифіката ключа розуміється тимчасове припинення чинності сертифіката ключа.

Після блокування сертифіката ключа, заявник зобов'язаний протягом 30 календарних днів поновити строк чинності сертифіката ключа або подати заяву про його скасування. У випадку, якщо протягом зазначеного строку заявник не поновить чинність блокованого сертифіката ключа та не подасть заяви про його скасування, по закінченню вищезазначеного строку такий сертифікат ключа автоматично скасовується Центром.

Блокування сертифіката ключа здійснюється на підставі заяви заявника: в усній, письмовій формі, чи у вигляді електронного документа.

Часом блокування сертифіката ключа вважається час зміни його статусу у реєстрі користувачів Центру.

***6.6.5. Блокування сертифіката за заявою в усній формі***

Заява в усній формі подається заявником (підписувачем) до Центру засобами телефонного зв'язку за номером, який опублікований Центром на власному інформаційному ресурсі, при цьому заявник повинен повідомити адміністратору реєстрації наступну інформацію:

* ідентифікаційні дані власника сертифіката;
* ключову фразу голосової автентифікації;
* реєстраційний номер сертифіката ключа.

Заява в усній формі приймається тільки у випадку позитивної автентифікації (збігу голосової фрази та ідентифікаційних даних підписувача з інформацією в реєстрі користувачів).

Усна заява може бути подана цілодобово. Обробка усної заяви на блокування сертифіката та інформування власника сертифіката здійснюється протягом тридцяти хвилин з моменту подачі заяви. Усна заява повинна бути підтверджена письмовою заявою на протязі 7 (семи) робочих днів з часу прийняття усної заяви.

***6.6.5.1. Блокування сертифіката за заявою у письмовій формі***

Письмова заява подається до Центру або до відокремленого пункту реєстрації за встановленою формою та засвідчується власноручним підписом заявника.

У разі якщо власником сертифіката є юридична особа, підпис уповноваженого представника юридичної особи засвідчується печаткою.

Подача письмової заяви на блокування сертифіката до Центру та її розгляд здійснюється протягом робочого дня.

Обробка такої заяви та інформування заявника про блокування повинні бути здійснені протягом одного робочого дня, що йде за робочим днем, протягом якого була подана заява.

***6.6.5.2. Блокування сертифіката ключа за електронним запитом***

Електронний запит на блокування сертифіката ключа передається до ПТК Центру у вигляді вкладення у вигляді HTTP-запиту.

Електронний запит формується підписувачем за допомогою програмних засобів, які надаються Центром.

Електронний запит на блокування сертифіката ключа засвідчується ЕЦП відповідного сертифіката ключа підписувача.

У разі передачі запиту на блокування сертифіката ключа у вигляді HTTP-запиту, обробка запиту та інформування підписувача про блокування здійснюються в режимі реального часу.

У разі передачі запиту на блокування сертифіката ключа засобами електронної пошти, обробка запиту та інформування підписувача про блокування повинні бути здійснені протягом 2 (двох) годин після отримання запиту Центром.

Заява у вигляді електронного запиту повинна бути підтверджена письмовою заявою на протязі 7 (семи) робочих днів з часу прийняття Центром електронного запиту.

***6.6.6. Порядок поновлення чинності сертифікатів ключів***

Поновлення чинності сертифіката ключа можливе лише для заблокованих сертифікатів ключів, термін блокування яких не скінчився.

Для здійснення поновлення чинності сертифіката ключа, заявник подає до Центру або відокремленого пункту реєстрації, письмову заяву встановленого зразка.

Подача письмової заяви на поновлення чинності сертифіката ключа до Центру та її розгляд здійснюється тільки протягом робочого дня.

Обробка письмової заяви на поновлення чинності сертифіката ключа та інформування заявника про поновлення повинні бути здійснені протягом одного робочого дня, що йде за робочим днем, протягом якого була подана заява.

Часом поновлення чинності сертифіката ключа вважається час зміни його статусу у реєстрі користувачів Центру.

***6.6.7. Розповсюдження інформації про статус сертифікатів ключів***

Для розповсюдження інформації про статус сертифіката ключа Центру використовується механізм списку відкликаних сертифікатів.

Список відкликаних сертифікатів випускається один раз на добу та місить ідентифікаційні дані скасованих (блокованих) сертифікатів ключів до закінчення строку їх дії.

У разі скасування (блокування, поновлення) сертифіката, оновлений список відкликаних сертифікатів випускається та публікується не пізніше двох годин після отримання запиту на відкликання сертифіката.

***6.6.8. Закінчення строку чинності сертифіката ключа підписувача***

Термін дії особистого ключа дорівнює даті і часу початку та закінчення дії відповідного сертифіката ключа. Термін дії відкритого ключа встановлено рівним терміну дії відповідного сертифіката ключа.

Після закінчення строку чинності сертифіката ключа, він вилучається з інформаційного ресурсу Центру та поміщається в архів. Центр зберігає сертифікат та пов'язані з ним списки відкликаних сертифікатів безстроково. За запитом користувачів, Центр надає доступ до необхідного сертифіката та пов'язаних з ним списків відкликаних сертифікатів з архівних записів Центру у строки, встановлені законодавством України для відповідей на звернення громадян.

**МОДУЛЬ №2**

**2.11) Основні види атак, принципи криптоаналізу. Основи криптографії**

**Базові поняття криптографії**  
 Припустимо, що одна особа збирається відіслати іншій особі повідомлення і хоче бути впевненою в тому, що ніхто інший не зможе його прочитати навіть тоді, коли воно буде перехоплене.  
  
 У криптографії повідомлення називають *вихідним текстом*(plaintext), зміну вмісту повідомлення так, що воно стає недоступним для сторонніх, —*шифруванням*(encryption), зашифроване повідомлення — *шифрованим текстом*(ciphertext), а процес отримання вихідного тексту із шифрованого —*дешифруванням*(decryption).

Криптогра́фія (від грецького kryptós — прихований і gráphein — писати) — наука про математичні методи забезпечення конфіденційності (неможливості прочитання інформації стороннім) і автентичності (цілісності і справжності авторства) інформації.

Криптографічний захист (шифрування) інформації — це вид захисту, який реалізується за допомогою перетворень інформації з використанням спеціальних (ключових) даних з метою приховування змісту інформації, підтвердження її справжності, цілісності, авторства тощо

Дешифрування — це зворотній процес відтворення інформації із шифротексту.

Криптоаналіз — розділ криптології, що займається математичними методами порушення конфіденційності і цілісності інформації без знання ключа.

Криптографічна система (криптосистема) — сукупність засобів криптографічного захисту, необхідної ключової, нормативної, експлуатаційної, а також іншої до-кументації (зокрема й такої, що визначає заходи безпеки).

Ключ — це деяка величина, що, працюючи в сполученні з криптоалгоритмом, робить визначений шифртекст. Ключі, як правило, — це дуже великі числа. Розмір ключа виміряється в бітах.

Зв’язка ключів (keyring) — (криптографія) сукупність ключів. Кожен користувач має два типи зв’язок ключів — приватну, яка містить один або кілька приватних ключів цього користувача, і публічну — сукупність його публічних ключів.

Приватний ключ — складова пари ключів, яка має зберігатись у секреті одним або всіма учасниками комунікацій. Приватний ключ використовується для створення цифрових підписів та дешифрування повідомлень, зашифрованих за допомогою відповідного публічного ключа.

Публічний ключ — один із пари ключів, який вільно надається кореспондентам і використовується для шифрування і верифікації цифрових підписів. Знання публічного ключа не дає змоги розкрити пов’язаний із ним приватний ключ.

**Криптографія** – наука про математичні методи забезпечення конфіденційності та автентичності інформації.

**Відкритий текст** – масив даних ( необов’язково текст )який передається по ненадійній, незахищеній мережі з використанням алгоритмів криптографії.

**Шифрований текст** - масив даних отриманий після застосування криптосистеми із визначеним ключем для наступної розшифровки.

**Криптосистема (шифр)**- сімейство оборотних перетворень вихідного тексту в шифрований.

**Ключ** - параметр, що визначає вибір конкретного перетворення для шифрування даного тексту. У сучасних шифрах алгоритм шифрування відомий і стійкість шифру цілком визначається таємністю ключа (принцип Кірхгофа)

**Криптоаналіз** — наука, що вивчає математичні методи порушення конфіденційності, аутентичності і цілісності інформації .

**Криптоаналітик** – людина, що створює і використовує методи крипто аналізу.

**Криптологія** - наука, що займається методами шифрування і дешифрування масиву даних Криптологія складається з двох частин - криптографія і крипто аналіз

**Криптографічний атака** - спроба криптоаналітиків викликати відхилення в захищеній системі обміну інформацією. Успішну криптографічну атаку називають взломом.

**Розшифрування** - процес нормального застосування криптографічного перетворення шифрованого тексту у відкритий

**Дешифрування** - процес витягу відкритого тексту без знання криптографічного ключа на основі відомого, шифрованого.

**Криптографічна стійкість** - здатність криптографічного алгоритму протистояти криптоаналізу.

**Емітозахист** - захист від нав'язування хибної інформації ,досягається за рахунок включення в пакет даних емітовставки. ключа і даних. , які як правило генеруються в процесі шифрування.

***Методи шифрування***  
Залежно від структури використання ключів методи шифрування поділяють:

***Тайнопись***

* стороннім особам невідомий алгоритм шифрування
* закон перетворення повідомлень знає тільки відправник та одержувач

***Симетричне шифрування***

* стороннім особам може бути відомий алгоритм шифрування
* невідомою частиною є невелика порція інформації яку називають ключем
* ключ є однаковим для відправника і одержувача

Переваги

* Метод шифрування є швидко застосованим із зі відомого алгоритма шифрування та може бути реалізований в апаратно програмних комплексах.
* Уніфікація систем криптографічного захисту для всієї організації.
* Стандартні підходи до захисту каналів зв’язку , спрощують систему навчання персоналу.

Недоліки

* Потрібна додаткова система аутентичної передачі ключа шрифтосистемами усім учасникам захищеного інформаційного середовища
* Симетричні шрифти використовують для шифрування оборотні математичні перетворення, які окремо піддаються криптоаналізу.

***Асиметричне шифрування***

* Стороннім особам відомий алгоритм шифрування.
* Система складається з n+1 ключів.Де один з ключів завжди є відомим(інші ключі передаються одному або декільком користувачам)
* Властивості ключів та їх вплив на криптосистему є асиметричним.
* В деяких варіантах асиметричної системи використовують пари ключів відомий і закритий.
* Асиметричні алгоритми використовують різні ключі у різних напрямках шифрування і розшифрування інформації.
* Асиметричні системи для генерації ключів, а також для їх застосування використовують необоротні математичні перетворення.

Переваги

1. Висока криптостійкість системи зі за того що використовується n+1 ключів
2. Використовується в системах з невідомою архітектурою інформаційних систем для початкової аутентифікації користувача або створення захищеного каналу аутентифікації.
3. Широка область застосування в різних галузях передачі інформації, де кількість донорів і акцепторів заздалегідь невідома.
4. Асиметричні шифри системи стійкі до підміни інформації в процесі передачі із за n – вимірності використовуваних ключів.

Недоліки

1. Асиметричні системи використовують складні функції математичних перетворень, а отже іде значне навантаження на програмні апаратні комплекси
2. Складне впровадження асиметричних систем в організаціях де можливий сильний плив кадрів тому, шо системи вимагають значних капіталовкладень у навчанні персоналу.

Асимнтричні системи аутентифікують тільки процес передачі інформації, а не самого користувача. Асиметричні шифри: [RSA](http://uk.wikipedia.org/wiki/RSA/), [Elgamal](http://ru.wikipedia.org/wiki/%D0%A1%D1%85%D0%B5%D0%BC%D0%B0_%D0%AD%D0%BB%D1%8C-%D0%93%D0%B0%D0%BC%D0%B0%D0%BB%D1%8F/), Elliptic curve cryptography, Симетричні шифри: DES, DESX, Triple DES, IDEA

**Методи криптоаналізу**

***Класичний криптоаналіз***

1. Частотний аналіз – аналіз зашифрованого тексту на частоту появи тих чи інших символів.
2. [Метод Казіскі](http://wiki.univ.uzhgorod.ua/index.php/%D0%9C%D0%B5%D1%82%D0%BE%D0%B4_%D0%9A%D0%B0%D0%B7%D1%96%D1%81%D0%BA%D1%96)
3. Метод індексних співпадань. До шифрованого тексту використовують просте математичне перетворення, після якого перевіряють текст на індексні спів падання.

***Симетричнний алгоритм***

1. диференціальний криптоаналіз
2. лінійний криптоаналіз
3. різницевий криптоаналіз
4. статистичний криптоаналіз.

Структура симетричних і асиметричних алгоритмів шифрування Симетричний алгоритм DES – один ключ який використовується як для шифрування так і для розшифрування DES тримає інформацію в блоках по 64 біти, а ткож використовує 16 циклову мережу перетворень Фейстеля

Для шифрування використовується ***ключ 56 біт***. Даний алгоритм шифрує вхідне пові­дом­лення методом комбінування нелінійної і лінійної перестановки перетворень. Сімейство алгоритмів DES-х створене в 1984р. Використовує для перетворення блоків по 64 біта кожен, методом складання по модулю 2 ключа та блока.

***Другий ключ*** використовується для шифрування тексту із блоків по 64 бітиза допомогою лінійних перестановок. Алгоритм перестановок може регулвати користувач.

***Третій ключ*** використовується для перетворення уже шифрованого тексту методом складання по модулю 2. DES-х використовується для захисту ліній зв’язку. Асиметричні алгоритми. RSA (1977) розроблений в Масачусецькому технологічному інституті. Алгортм використовується у великій кількості криптографічних додатків з0 метою створення електронного підпису або як додатковий алгоритм аутентифікації, досих пір не реалізований апаратно. Безпека алгоритму RSA заснована на труднощі задання множини розкладу на множники. Алгоритм використовує 2 ключа відкритий (public) і закритий (private).

**Опис основних видів атак**

Розглянемо спочатку типові атаки на відмову, тобто атаки що можуть здійснюватися з одного комп’ютера.

**Прямі атаки**

В даному пункті будуть описані атаки, які можуть бути ефективно здійснені з одного

джерела. Ці атаки використовують певні особливості побудови протоколів мережі Інтернет.

Часто такого роду атаки використовуються в якості елементів для конструювання складних

розподілених нападів.

1.1. Націлені на ресурси цілі

1.1.1. Спрямовані HTTP Flood.

Найпопулярнішою та найбільшою компонентою мережі Інтернет являється World Wide Web (www) – або Всесвітня Павутина. www-програми, як правило, використовують протокол Hypertext Transfer Protocol (HTTP), який ініціює запит шляхом встановлення Transmission Control Protocol (TCP) з’єднання з певним портом (як правило 80 порт). Через це більшість захисного програмного забезпечення залишає TCP порт 80 відкритим для вільного проходження HTTP трафіка. Широка розповсюдженість WWW систем зробила HTTP чудовою мішенню для нападників. Власне кажучи, атака HTTP flood пов’язана з бомбар­ди­ров­кою Веб сервера звичайними HTTP запитами. Згідно з недавніми дос­ліджен­ня­ми [14], HTTP flood атака входить у функціональний набір абсолютної більшості ботнет. Для того щоб надіслати HTTP запит необхідно спочатку встановити дійсне TCP з’єднання, що вимагає наявності дійсної IP адреси. Нападник тут може використати IP адресу ботів. Більше того, нападник може сконструювати особливий запит для збільшення сили атаки або для того, щоб уникнути виявлення. Наприклад, видати боту інструкцію надіслати HTTP запит на завантаження великого файлу. Тоді комп’ютеру жертви необхідно зчитати цей файл з диску, завантажити у пам'ять, загрузити в пакети та надсилати їх у ботнет. Отже, навіть простий HTTP запит може привести до значного завантаження процесору, пам’яті, пристроїв вводу/виводу та лінії з’єднання з Інтернет. Однак така поведінка трафіка, як у попередньому прикладі є підозрілою. Повторні запити на завантаження можуть бути виявлені та блоковані. Більш складною стратегією є імітація звичайного трафіка. Нападник може задати ботам

програму пересилки HTTP запитів, аналізу відповідей і рекурсивного відкриття

посилань. В цьому разі HTTP запити від атакуючої мережі дуже подібні до нормального

веб трафіка, що ускладнює фільтрацію атак цього типу. 19 ICMP атаки. В атаках цього типу використовуються особливості реалізації протокола ICMP. Оскільки цей протокол є внутрішнім механізмом підтримки працездатності IP-мереж, то він природно викликав підвищену увагу нападників. Виділяють [15] декілька типів. Перший тип – атака розрива з’єднання (connection-reset attacks) використовує ICMP-повідомлення, що сигналізують про фатальну помилку і спричиняють до припинення TCP-з’єднання. Якщо нападник сфальшує такий пакет і надішле його жертві, то її з’єднання з сервером буде розірвано. Для формування такого пакету йому потрібно знати IP адреси жертви і сервера, порт і унікальне число, яке ідентифікує з’єднання. Для підбору останньої величини йому достатньо надіслати всього 65536 пакетів. Ця слабкість була виявлена 13 березня 2005 року і зачепила велику кількість операційних систем, маршрутизаторів і свічів. Зокрема, Windows XP, Windows 2000, Windows 2000 Server, Windows 98. Другий тип [16] полягає в звуженні пропускної здатності (throughput-reduction attacks), при цьому використовуються ICMP-повідомлення, що вимагають від джерела зменшення пропускного каналу. Це службові пакети, що надсилаються мережею в разі її перевантаження. Для їх фальшування використовується аналогічний наведеному вище набір параметрів. Нарешті третій тип [16] пов'язаний з пакетами ICMP, які відповідають за допустиму фрагментацію пакетів. Надсилаючи сфальшований пакет на адресу джерела нападник добивається ситуації коли великий файл надсилається мізерними шматочками, що, звичайно, знижує швидкість передачі.

1.1.2. Поглинаючі SYN Flood. Перед тим як перейти до опису SYN flood атаки потрібно згадати послідовність встановлення TCP з’єднань. TCP з’єднання встановлюється між клієнтом, що ініціює з’єднання і сервером, який отримує запит. На початку кожного TCP з’єднання клієнт звертається до сервера для виконання процедури, яка називається потрійне рукостискання (a three-way handshake) [17]. По-перше, клієнт надсилає серверу SYN пакет, запитуючи про з’єднання (рис. 7).

Потім сервер відповідає на запит пакетом SYN-ACK та зберігає інформацію про запит на з’єднання у стеці пам’яті. Структури, що створюються у пам’яті, як правило, досягають 280 Байт. В цей момент часу з’єднання знаходиться в напіввідчиненому стані, або в стані SYN RECVD (очікування). Для попередження вичерпання ресурсів кожна операційна сис­те­ма має певний ліміт з’єднань, що можуть перебувати в стані SYN RECVD. Після отримання SYN-ACK пакету клієнт підтверджує свій запит за допомогою пакету ACK. Коли сервер отримує пакет ACK він перевіряє стек в пошуках з’єднання, яке підтверджується цим паке­том. Якщо таке з’єднання існує, то воно переводиться зі стану SYN RECVD в стан ESTABLISHED (встановлене). Після цього потрійне рукостискання 20 завершене і почи­наєть­ся передача даних. Крім описаного «природного» способу видалення з’єднання, що знаходиться в стані SYN RECVD також можна надіслати пакет RST (рестарт) або чекати поки час очікування перевищить певний ліміт, відведений на встановлення з’єднання.

Атака SYN flood використовує вразливості TCP потрійного рукостискання, а саме, ту особливість, що сервер повинен розміщувати в пам’яті дані для будь-якого вхідного SYN пакета, незалежно від його аутентифікації. При проведенні SYN flood атаки нападник посилає SYN пакети з сфальшованою IP адресою, тобто вказує IP адресу, якої не існує. В цьому разі під час виконання потрійного рукостискання сервер поміщає запит на з’єднання в пам’ять і чекає на підтвердження запиту від клієнта.

Оскільки сфальшованої нападником адреси може просто не існувати, то пакетів підтвердження сервер не отримує і запит залишається в пам’яті протягом певного часу. За короткий час ці запити заповнюють стек пам’яті, що призначений для їх зберігання (як правило його об’єм не дуже великий). В результаті нові запити на з’єднання від користувачів не можуть бути оброблені і сервіси системи виявляються заблокованими. Мож­ли­вою модифікацією цієї атаки (стійкою до фільтрації адрес) є ситуація, коли атака здійснюється з ботів з використанням дійсної IP адреси. При цьому система налаштовується ігнорувати SYN/ACK пакети жертви. SYN floods залишається однією з найбільш потужних методів поглинаючих атак. 21 ACK Flood. ACK Flood це шлях обійти захист від SYN flood атаки. Більшість мереж налаштовані на захист від атаки SYN пакетів, в той час як ACK пакети можуть безперешкодно проходити через мережу. Це створює додаткові можливості по завантаженню ресурсів жертви, оскільки отримавши пакет ACK, система має виконати

пошук відповідного йому TCP з’єднання. Не знайшовши такого (оскільки нападник і не намагався його встановити) система відповідає пакетом RST. Таким чином ресурси цілі завантажуються прийомом та надсиланням пакетів. Reset (RST) Flood. Атаки типу SYN flood використовують вразливості встановлення з’єднання. На відміну від них, атаки RSR Flood спрямовані на вже встановлені з’єднання.

Пакети з міткою RST використовуються для перевстановлення з’єднання (наприклад в разі коли на одній з машин відбувася збій). Якщо дві машини С і В обмінюються даними через встановлене з’єднання, і нападник А вирішує атакувати С, то для здійснення атаки йо­му потрібно обчислити/підібрати правильне число ідентифікації з’єднання (при розриві з’єднан­ня підтвердження пакетом АСК не використовується). Тепер нападник може перер­ва­ти з’єднання В і С шляхом надсилання сфальшованого пакета. Більше того, він може за­ван­та­жувати машину пакетами від імені В оскільки С не підозрює, що з’єднання розірване.

FIN Attack: Атака FIN attack використовує пакети FIN, які відповідають за закінчення TCP з’єднання. Нападник намагається встановити серію нових з’єднань та відразу по встановленні закрити їх не надіславши ніяких даних. Ідея полягає в тому, щоб заван­тажу­ва­ти сервер великою кількістю з’єднань. Перевага цієї атаки для напалника по­ля­гає в тому, що оскільки на пакет FIN машина повинна відповісти пакетом ACK він може відразу визначити чи успішні його дії.

1.1.3. Експлойтні WinNuke. Одним з перших і класичних випадків експлойтної атаки на відмову являється WinNuke, який з’явився 7 травня 1997 року. Автор методу розмістив опис і текст програми на декількох сайтах новин, що зумовило швидке його розповсюдження.

Першою жертвою став сервер www.microsoft.com, який був недосяжний для користу­ва­чів з 9 по 12 травня. Звичайно, що і багато інших серверів, які працювали на системі Windows NT також стали жертвами атак. Сутність WinNuke дуже проста. Поряд зі зви­чай­ни­ми даними стандарт включає можливість пересилки по TCP-з’єднанню і термінових (Out Of Band, OOB) службових даних. На рівні форматів пакетів TCP це виражається в ненульовому значенні відповідного поля (urgent pointer). Більшість комп’ютерів, що працю­ють­ під Windows використовують протокол NetBIOS, якому для роботи потрібно три IP-пор­ти: 137, 138, 139. Виявилось, що якщо з’єднатися з Windows-машиною через 139 порт і надіс­лати туди декілька байт OOB-даних, то NetBIOS не22 знаючи як їх обробляти просто підвисить машину. Під дію цієї атаки підпадають системи Windows 95, Windows NT до 4.0. Ping of Death. В цій атаці використовується особливості реалізації протокола ICMP.

Оскільки цей протокол є внутрішнім механізмом підтримки працездатності IP-мереж, то він природно викликав підвищену увагу нападників. Особливість полягає в тому, що ICMP-пакети мають певні привілеї в обробці, тому ping великого розміру може паралізувати роботу комп’ютера або навіть усієї мережі. Існує багато реалізацій програм, що використовують цю помилку: Ping of Death, SPing, Jolt, SSPing, IceNuke, IcePing, та інші. Як виявилося, Windows-системи неадекватно реагують на отримання сильно фрагментованого ICMP-пакета (шматочками до одного кілобайта) великого розміру (трохи більше 64 кілобайт). Реакція полягає в повному повисанні комп’ютера. В кінці червня 1997 року жертвою Ping of Death став сервер Майкрософт. На відміну від WinNuke жертвами цієї атаки можуть стати не тільки Windows-системи а й Mac OS і деякі версії Unix. Teardrop. Даний тип атак на відмову використовує експлойт реалізації протоколу, згідно з яким якщо пакет занадто великий для обробки, то він мусить розбиватися на два фрагмента. Ці фрагменти містять інформацію про відносне зміщення початку другого пакета. При прийомі пакетів система опрацьовує інформацію про зміщення і формує цілий пакет. При атаці teardrop нападник фальшує значення зміщень другого або наступних пакетів і призводить до того, що довжина пакета стає менш за нуль або у машинній логіці дуже великим числом. Це приводить до копіювання величезного блока пам’яті, що затирає системні області. Після появи атаки Teardrop виникло декілька модифікацій, які були здатні пробивати Windows NT з встановленим патчем від звичайного Teardrop. Найбільш відомі з них Bonk (Boink), NewTear, SynDrop. Вказані атаки можуть застосовуватися проти систем Windows 3.1/95/NT, Linux (до 2.0.32 і2.1.63). LanD. Наступний метод атаки, який називається lanD відомий тим, що в свій час вражав велику кількість систем. Крім Windows NT, під його дію підпадали Mac OS та багато варіантів Unix (від безкоштовних до комерційних), і такі екзотичні системи, як QNX і BeOS, і навіть апаратні маршрутизатори (в тому числі Cisco і 3Com). Суть атаки land полягає в наступному: при встановленні TCP з’єднання посилається SYN-пакет задресою відправника, що співпадає з адресою. Пакет посилається на будь-який відкритий порт. Реакцією Windows-комп’ютера на land є повне зависання. Атака була ефективна проти операційних систем Windows 9х/NT. В 2005 році була виявлена вразли­вість в системах Windows XP і Windows 2003 Server, яка призвела до появи модифі­ка­ції атаки lanD - Remote LanD. 23

1.2. Націлені на ресурси мережі

Під ресурсами мережі в цьому пункті розуміються канали зв’язку, граничні маршрутизатори, кореневі DNS сервери та інші пристрої, що забезпечують роботу мережі. Атаки на інфраструктуру мережі спрямовані на сервіси, функціонування яки критичне для роботи мережі Інтернет. Такі атаки можуть вплинути на роботу всієї мережі. Наприклад кореневі DNS сервери містять інформацію про сервери головних доменів, таких, як .com. У разі успішної атаки на відмову всі ці домени стали б недосяжні для користувачів. Однак, такі пристрої як правило мають додаткові резерви для випадків пікових навантажень, тому прості поглинаючі атаки не можуть бути застосовані (вони можуть створювати порівняно невеликі об’єми трафіку). Що стосується спрямованих та експлойтних атак на інфраструктуру, то в силу важливості цих об’єктів для функціонування всієї мережі будь-яку знайдену вразливість досить швидко виправляють. Тому особливих типів атак, характерних саме для даного розділу не зафіксовано.

**Віддзеркалені атаки**

В основі здійснення віддзеркалених атак лежить використання фальшування адреси та

особливостей протоколів TCP-з’єднання, а саме – момент коли один комп’ютер відповідає на запит іншого. Схема виконання атаки наступна: пакет-запит фальшується від імені жертви та надсилається на велику кількість машин. Потім всі ці машини відповідають жертві пакетами-відповідями, завантажуючи його канал беззмістовним (хоча й законним) трафіком. Як випливає з опису схеми найбільш сильно ефект віддзеркалення проявляється при здійсненні поглинаючих атак.

1.3. Націлені на ресурси цілі

1.3.1. Поглинаючі Smurf. Може бути здійснена з допомогою звичайної команди ‘ping’. В багатьох системах існує можливість опитувати мережу за допомогою пакетів ICMP echo.

При отриманні такого пакета комп’ютер повинен вернути пакет ICMP echo reply по вказаній адресі. Однак базові ICMP пакети можуть мати сфальшовану зворотну адресу (це спрямовано для ускладнення від слідкування джерела атаки).Фактором посилення такої атаки є існування так званої адреси широкотрансльованих запитів (broadcast address). Ці адреси використовуються в службових цілях для визначення поточної конфігурації мережі (опитування активних вузлів). Відсилка пакета на цю адресу приводить до його розсилання по всій мережі, причому всі активні комп’ютери повинні відповісти на адресу машину, що послала пакет. Атака відбувається наступним чином: нападник спрямовує пакет на адресу широко трансльованого запиту і він розсилається по24 всій мережі. При цьому зворотну адресу сфальшовано і всі відповіді – пакети ICMP echo reply приходять на машину жертви. Таким чином один надісланий пакет викликає цілий шторм відповідей, посилюючи початкову силу атаки в сотні раз. Fraggle. Одним з варіантів описаної вище атаки є атака fraggle (осколочна граната). Ця атака базується smurf, але використовує пакети UDР замість ICМР.

Нападник надсилає сфальшовані пакети UDР на адресу широко трансльованого запиту, як правило на порт 7. Кожна система мережі, в якій дозволена відповідь на такі UDР echo пакети відповість жертві, в результаті буде згенеровано великий об’єм трафіку DNS Amplification Attacks. Досить ефективною формою віддзеркаленої атаки є використання серверів Доменної Системи Імен (Domain Name System (DNS) servers). Ці сервери потрібні для зберігання і надання за вимогою різних записів (resource records (RR)) з іменами доменів Інтернет. В такому записі можуть бути дані типу TXT RR, в які адміністратор може внести довільний текст, типу A RR, де визначається відображення імені в 32-бітну IP адресу та типу SOA1 RR, де визначається ім’я домена Інтернет та інша супутня інформація. Найважливішою функцією DNS серверів є транслювання імен доменів в IP адреси. Після отримання запиту на IP адресу DNS сервер намагається знайти відповідний запис у своїй базі даних. Якщо це не вдалося, то запит розсилається по всіх відомих йому DNS серверах. Ця процедура називається рекурсивним запитом. Розміри запиту і відповіді можуть суттєво відрізнятись. Зазвичай, відповідь містить початковий запит та відповідь. Це означає, що відповідь завжди більша за запит. Більше того, відповідь може містити різні типи RR даних і деякі з них можуть мати значний обсяг. Приклад атаки, що відбувалася на початку 2006 року [18].

Сценарий атаки наступний: на початку нападник отримує права доступу на DNS сервер та розміщує максимальну можливу (4000 Б) типу TXT RR. Далі нападник видає команду контрольованій ботнет надсилати сфальшований DNS запит з зворотною адресою жертви на всі DNS сервери з вимогою даних, які розмістив нападник. В кінці кінців всі запити вертаються на машину жертви значно посиленими. Теоретично, початковий трафік потужністю 140 Mb/s з ботнет може призвести до потоку DNS відповідей потужністю 10 Gb/s.

1.4. Націлені на ресурси мережа

1.4.1. Поглинаючі25 ICMP flood. Виникає при завантаженні мережі жертви пакетами ICMP\_ECHO та ICMP\_ECHO\_REPLY. Ці пакети можуть бути сфальшовані і наповнюють мережу віддзеркаленими відповідями, завантажуючи пропускну здатність жертви.

**Приховані атаки**

Мабуть, першою роботою, присвяченою опису і характеристиці проблеми прихова­них­ або низькочастотних атак була стаття Кузмановича і Найтлі [19]. В роботі досліджена причина появи прихованих атак (в статті shrew attack – «атака землерийки») та їх вплив на роботу TCP потоків. Дослідники відмічають обмеженість існуючих механізмів захисту проти атак такого типу, але не пропонують алгоритму ефективної протидії. В чому ж полягає така атака? Атакуючий комп’ютер A встановлює з’єднання з жертвою та надсилає велику кількість пакетів, на короткий час завантажуючи канал. Отримавши переповнення каналу протокол TCP вмикає механізм RTO (retransmission timeout) певний час не приймаючи пакети від А. Оцінивши цей час, протягом нього нападник не надсилає пакетів.

Після того як час RTO пройшов і до того як з’єднання буде закрите (оскільки воно не активне) нападни надсилає наступну порцію пакетів. В результаті підтримується порожнє з’єднання, яке завантажує пам'ять і ресурси машини. Такі атаки також отримали назву пульсуючих атаки (pulse attacks). Крім того, що один атакуючий комп’ютер може підтримувати декілька десятків таких з’єднань, атаку може бути запущено з декількох десятків тисяч комп’ютерів. За своєю природою приховані атаки є поглинаючими, однак вони також використовують особливості реалізації протоколів, тому їх також можна віднести до спрямованих.

В результаті якість зв’язку суттєво знижується, оскільки доводиться обслуговувати

беззмістовні потоки даних (хоча й цілком законні з точки зору роботи протоколу). Механізми захисту від звичайних прихованих атак запропоновані в роботах [20, 21]. Також ця задача частково вирішується системами захисту на основі виявлення великої кількоті

нових IP адрес [5].

Однак проблема залишається відкритою, якщо атака використовує несинхронні потоки або атаки з змінним періодом. При цьому агенти атаки можуть ускладнювати поведінку імітуючи дії користувача, що ставить складні задачі по виявленню самого факту атаки. Даний розділ атак з’явився нещодавно і ще знаходиться у розвитку.

**Розподілені атаки**

Розподілені атаки на відмову – це найпотужніші за об’ємом трафіка види нападу. Сучасний стан розвитку мереж дозволяє набрати цілу армію ботів та кинути їх в атаку на певний сервер-жертву. При цьому в якості методу атаки може використовуватися будь-який з описаних вище. Однак справжня сила розподілених атак проявляється при здійсненні поглинаючих атак (особливо якщо при цьому імітується звичайний трафік). Події остан­ніх 26 років показують зрощення таких видів діяльності як виконання атак на відмову, розсилка спама та написання комп’ютерних черв’яків (computer worm). Черв’як розповсюджується по мережі, захоплюючи комп’ютери і розмножуючись. При цьому він встановлює на захоплені комп’ютери програму-агент, яка чекає на інструкції від керуючої машини. В залежності від

команд програма може розсилати спам або приймати участь в здійсненні атаки. Опишемо

декілька найбільш відомих розподілених атак.

Distributed DDoS attack of October 22, 2002. Скоординована розподілена атака на відмову була здійснення 22 Жовтня з 20.45 по 22.00 [22]. Ціллю атака були всі тринадцять кореневих DNS серверів. Потужність атаки коливалась від 50 до 100 Mbits/sec на кожен сервер, загальна потужність можна оцінити числом 900 Mbits/sec (1.8 Mpkts/sec).

Відповідно до повідомлень Пола Віксі, оператора сервера F, атака 21 жовтня складалась з пакетів ICMP Echo Request, тобто пакетів, що вимагали відповіді. Найпростіше рішення проти такої атаки полягає в обмеженні або заблокуванні всіх ICMP пакетів до закінчення атаки (оскільки атака тривала недовго це було непомітно). Якщо б атака тривала весь день, це б вплинуло на загальну роботу мережі, оскільки протягом атаки деякі сервери обробляли лише 50 % запитів [23]. Загальний трафік атаки містив пакети ICMP, TCP SYN, fragmented TCP і UDP flood атак. Джерела атаки були в основному сфальшовані випадковим чином, але зі значень, присутніх в таблицях маршрутизації (тобто дійсних).

В результаті атаки деякі сервери були недосяжні для багатьох областей мережі Інтернет. При цьому робота серверів не була перервана – просто велика частина ресурсів тратилася на обробку порожніх запитів. Незвичність атаки полягала в тому, що вона була спрямована на всі сервери одночасно, чого раніше не траплялось. MyDoom worm. Черв’як Mydoom, також відомий як W32.MyDoom@mm, Novarg, Mimail.R і Shimgap використовує вразливості операційних систем Microsoft Windows. Вперше був помічений 26 січня 2004 року. Він став найшвидшим поштовим черв’яком на той момент по швидкості розпов­сю­джен­­ня.­

Як правило, Mydoom (або MyDoom.A) поширювався через електронну пошту з темою повідомлення «Помилка», «Служба доставки пошти» та подібні. При цьому лист містив файли, що зазвичай генеруються поштовими серверами при помилці доставки. При перегляді цих додатків черв’як розсилав себе по всім поштовим адресам з адресної книги. Він також намагався поширитись через популярну файлообмінну peer-to-peer мережу KaZaA. При цьому Mydoom уникав адрес певних університетів таких як Rutgers, MIT, Stanford і UC Berkeley, та великих компаній як Microsoft і Symantec. Перша версія Mydoom.A встановлювала засіб віддаленого контролю комп’ютера. 1 лютого 2004 року всі боти повинні були розпочати розподілену атаку на відмову вебсайта компанії SCO Group. Далі події розгортались наступним чином: 25- 26 січня 2004: Перша зареєстрована поява Mydoom на початку робочого дня в Америці. За декілька годин черв’як почав швидко поширюватися мережею Інтернет. Це поширення спричинило зменшення загальної швидкодії Інтернет на 10 відсотків. Веб-сторінки завантажувалися в півтора раза довше. За оцінками кожний десятий електронний лист в цей час був надісланий Mydoom. Хоча атака повинна була розпочатися 1 лютого, сайт SCO Group був вимкнено через декілька годин після появи черв’яка. Досі немає певності, чи відповідальний за це Mydoom.

28 січня: Перші відомості про другу версію черв’яка - Mydoom.B. Нова версія включала заплановану атаку SCO Group та ідентичну атаку проти сайта Microsoft.com, яка повинна була початися 3 лютого. Поширення MyDoom досягло піку – за оцінками кожний п’ятий електронний лист був надісланий з його участю. 29 січня: Поширення Mydoom поча­ло сповільнюватися.

1 лютого: Приблизно один мільйон комп’ютерів, заражених черв’яком Mydoom почали найпотужнішу в світі атаку на відмову. Напередодні сайт www.sco.com було відключено самою компанією (незалежної інформації чи атака насправді досягла цілі немає досі).

2 лютого: The SCO Group moves its site to www.thescogroup.com. 3 лютого: Почалась розподілена атака Mydoom.B на сайт Microsoft. Однак її сила була незначною оскільки по-перше розповсюдження Mydoom.B було значно меншим за його попередника, по-друге адміністратори були заздалегідь попереджені про атаку.

9 лютого: Паразитичний червяк Doomjuice, який використовував для розповсю­дже­ня­ комп’ютери заражені Mydoom почав своє розповсюдження. Він заражав комп’ютери та по­чинав атаку сайта Microsoft. 26 липня: З’явився новий варіант Mydoom - W32/MyDoom-O. Після захоплення комп’ютера цей черв’як шукав на дисках адресні книги і формував на їх основі пошукові запити для отримання нових адрес. Розміщення запитів було наступним –

www.google.com (45%) search.lycos.com (22.5%) search.yahoo.com (20%) www.altavista.com (12.5%). В результаті вказані сервери потрапили під неспрямовану атаку на відмову. Практично весь день сервіс Google був недоступний для користувачів. Інші сервіси значно вповільнили роботу. Distributed DDoS attack of February 6/7, 2007.

На початку 2007 року кореневі DNS сервери знову потрапили під дію розподіленої атаки на відмову. Цілями атаки були сервери F-Root, G-Root, L-Root і M-Root. Ці сервери 28 обслуговують домен .org і інші. Протягом 6/7 числа 90 відсотків запитів не було оброблено.

Атака на кореневі сервери, найбільша з 2002 року, продовжувалась 12 годин. По резу­ль­­татам досліджень було виявлено, що в атаці приймало участь: 4000-5000 ботів з опера­цій­ною системою Microsoft Windows ~65% з Південної Кореї; ~19% з США; ~3.5% з Канади; ~2.5% з Китаю; інші з різних місць;

Атака складалась з наступних дій:

Боти виконували по одному DNS запиту на кожен сервер;

Боти встановлювали по три з’єднання з жертвами;

По кожному з’єднанню починали передаватися UDP пакети випадкової довжини на порт 53 (який відповідає за роботу DNS сервера);

Зворотні адреси не фальшувались;

Після 12 годин боротьби атаку вдалося відбити. Нападник залишився невідомим.

Проведення настільки довгої і потужної атаки було повною несподіванкою для дослідників.

Таким чином, існує потенційна можливість вивести з ладу всю всесвітню мережу шляхом прямої атаки на кореневі сервери.

*Тенденції розвитку*

Слід зазначити, що організація атак на відмову давно займає значне місце серед зловмисної діяльності в мережі Інтернет. Деякий спад, (точніше незростання) кількості атак на відмову в 2006 році, що був пов'язаний з бурхливим розвитком інших видів діяльності, таких як спам і фітинг схоже закінчився. Початок 2007 року був ознаменований потужною атакою на кореневі сервери. Згідно з дослідженнями Лабораторії Касперского [24] cпам і DoS-атаки – одні з основних тем новин інформаційної безпеки 2007 року. Починаючи з жовтня 2006 року, коли черв’як Warezov почав створювати гігантські зомбі-мережі в мережі Інтернет почався новий виток розвитку спама. Ці події взаємопов’язані і вказують на зрощення цих двох явищ: Warezov збирав бази адрес і відправляв їх зловмисникам. Крім того він встановлював на заражені комп’ютери модулі для організації спам-розсилок. Цим же займались і два інших активних поштових черв’яка – Zhelatin і Bagle.

Організація атак на відмову перенесла пік популярності в 2002 – 2003 роках, після чого на досить довгий період ця сфера діяльності була дещо призабута. Можливо це було пов’язано з тим, що відбувалась своєрідна зміна поколінь кіберзловмисників. Ті люди, що займались атаками на відмову 4-5 років назад поступово переключились на більш «тонкі» способи зловмисної діяльності: розсилку спама, кражу даних, встановлення реклами. Нове покоління29 script-kiddies, які поки що нічого не вміють, використовують чужі розробки і діяти методами грубої сили. Звідси і нинішній сплеск різних DoS-програм (+209%), які дозволяють організовувати атаки по всьому світу. Хотя кількісні показники цієї поведінки поки що невеликі, тенденція спостерігається досить чітка.

Пірингові мережі (Peer-to-peer networks), що використовуються для обміну інформацією і можуть включати сотні тисяч комп’ютерів останнім часом стають базою для здійснення надпотужних розподілених атак. Цей тип атак почав з’являтися на початку 2007 ро­ку. За даними фірми Prolexic Technologies в атаках брало участь до 100.000 машин. Су­дя­чи­ з усього, потужність таких атак буде зростати.

Іншим напрямком можна вважати появу прихованих атак. Ці атаки поглинають пропускну здатність каналу жертви і можуть імітувати звичайних трафік. Поточні реалізації

використовують досить прості моделі поведінки агентів-ботів, тому їх можливо протестувати та виявити. Але подальше ускладнення схеми дій може привести до появи нових небезпечних модифікацій. 30

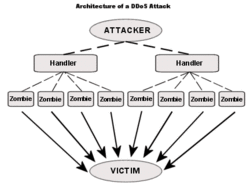
**Атака на відмову в обслуговуванні, розподілена атака на відмову в обслуговуванні** ([англ.](http://uk.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0_%D0%BC%D0%BE%D0%B2%D0%B0) *DoS attack, DDoS attack, (Distributed) Denial-of-service attack*) — напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними до користувачів, для яких комп'ютерна система була призначена.

Одним із найпоширеніших методів нападу є насичення атакованого комп'ютера або мережевого устаткування великою кількістю зовнішніх запитів (часто безглуздих або невірно сформульованих) таким чином атаковане устаткування не може відповісти користувачам, або відповідає настільки повільно, що стає фактично недоступним. Взагалі відмова сервісу здійснюється :

* примусом атакованого устаткування до зупинки роботи програмного забезпечення/устаткування або до витрат наявних ресурсів, внаслідок чого устаткування не може продовжувати роботу;
* заняттям комунікаційних каналів між користувачами і атакованим устаткуванням, внаслідок чого якість сполучення перестає відповідати вимогам.

Якщо атака відбувається одночасно з великої кількості [IP-адрес](http://uk.wikipedia.org/wiki/IP-%D0%B0%D0%B4%D1%80%D0%B5%D1%81%D0%B0), то її називають *розподіленою* (**DDoS**).

Анатомія DoS-атак

[](http://uk.wikipedia.org/wiki/%D0%A4%D0%B0%D0%B9%D0%BB:Dos.gif)

DDoS-атака

DoS-атаки поділяються на локальні та віддалені. До локальних відносяться різні [експлойти](http://uk.wikipedia.org/wiki/%D0%95%D0%BA%D1%81%D0%BF%D0%BB%D0%BE%D0%B9%D1%82): [форк-бомби](http://uk.wikipedia.org/w/index.php?title=%D0%A4%D0%BE%D1%80%D0%BA-%D0%B1%D0%BE%D0%BC%D0%B1%D0%B0&action=edit&redlink=1) і програми, що відкривають по мільйону файлів або запускають якийсь циклічний алгоритм, який "з'їдає" пам'ять та процесорні ресурси. Для локальної DoS атаки необхідно мати, або якимось чином отримати доступ до атакованої машини на рівні, що буде достатнім для захоплення ресурсів.

Розглянемо віддалені DoS-атаки. Вони поділяються на два види:

1. Віддалена експлуатація помилок в ПЗ з метою довести його до неробочого стану.
2. Flood — посилка на адресу жертви величезної кількості безглуздих (рідше — осмислених) пакетів. Метою флуду може бути канал зв'язку або ресурси машини. У першому випадку потік пакетів займає весь пропускний канал і не дає машині, що атакується, можливості обробляти легальні запити. У другому — ресурси машини захоплюються за допомогою багаторазового і дуже частого звернення до якого-небудь сервісу, що виконує складну, ресурсоємну операцію. Це може бути, наприклад, тривале звернення до одного з активних компонентів (скрипту) web-сервера. Сервер витрачає всі ресурси машини на обробку запитів, що атакують, а користувачам доводиться чекати.

У традиційному виконанні (один атакувальний — одна жертва) зараз залишається ефективним лише перший вид атак. Класичний флуд — даремний. Просто тому що при сьогоднішній ширині каналу серверів, рівні обчислювальних потужностей і повсюдному використанні різних анти-DoS прийомів в ПЗ (наприклад, затримки при багаторазовому виконанні тих самих дій одним клієнтом), атакувальний перетворюється на докучливого комара, не здатного завдати будь-якого збитку. Але якщо цих "комарів" наберуться сотні, тисячі або навіть сотні тисяч, вони легко покладуть сервер на лопатки. Розподілена атака типу «відмова в обслуговуванні» (DDoS), зазвичай здійснювана за допомогою безлічі «зазомбованих» [хостів](http://uk.wikipedia.org/wiki/%D0%A5%D0%BE%D1%81%D1%82), може відрізати від зовнішнього світу навіть найстійкіший сервер, і єдиним ефективним захистом при цьому є організація розподіленої системи серверів ([кластера](http://uk.wikipedia.org/wiki/%D0%9A%D0%BB%D0%B0%D1%81%D1%82%D0%B5%D1%80)).

Є два варіанти організації DDoS атак:

* [Ботнет](http://uk.wikipedia.org/wiki/%D0%91%D0%BE%D1%82%D0%BD%D0%B5%D1%82) - зараження певного числа комп'ютерів програмами, які в певний момент починають здійснювати запити до атакованого сервера.
* [Флешмоб](http://uk.wikipedia.org/wiki/%D0%A4%D0%BB%D0%B5%D1%88%D0%BC%D0%BE%D0%B1) - домовленість великого числа користувачів інтернету почати здійснювати певні типи запитів до атакованого сервера.

Методи боротьби

Небезпека більшості DDoS-атак — в їх абсолютній прозорості і «нормальності». Адже якщо помилка в ПЗ завжди може бути виправлена, то повна витрата ресурсів — явище майже буденне. З ними стикаються багато адміністраторів, коли ресурсів машини (ширини каналу) стає недостатньо, або web-сайт піддається [слешдот-ефекту](http://uk.wikipedia.org/w/index.php?title=%D0%A1%D0%BB%D0%B5%D1%88%D0%B4%D0%BE%D1%82-%D0%B5%D1%84%D0%B5%D0%BA%D1%82&action=edit&redlink=1). І, якщо різати трафік і ресурси для всіх підряд, то можна врятуватися від DDoS, у той же час, втративши велику частину клієнтів.

Виходу з цієї ситуації фактично немає, проте наслідки DDoS-атак і їх ефективність можна істотно понизити за рахунок правильного налаштування маршрутизатора, брандмауера і постійного аналізу аномалій в мережевому трафіку.

Боротьба з flood-атаками

Отже, існує два типи DoS/DDoS-атак, і найпоширеніша з них заснована на ідеї флуда, тобто завалення жертви величезною кількістю пакетів. Флуд буває різним: [ICMP-флуд](http://uk.wikipedia.org/w/index.php?title=ICMP-%D1%84%D0%BB%D1%83%D0%B4&action=edit&redlink=1), [SYN-флуд](http://uk.wikipedia.org/w/index.php?title=SYN-%D1%84%D0%BB%D1%83%D0%B4&action=edit&redlink=1),[UDP-флуд](http://uk.wikipedia.org/w/index.php?title=UDP-%D1%84%D0%BB%D1%83%D0%B4&action=edit&redlink=1) і [HTTP-флуд](http://uk.wikipedia.org/w/index.php?title=HTTP-%D1%84%D0%BB%D1%83%D0%B4&action=edit&redlink=1). Сучасні DoS-боти можуть використовувати всі ці види атак одночасно, тому слід заздалегідь поклопотатися про адекватний захист від кожної з них.

**Icmp-флуд**

Дуже примітивний метод забивання смуги пропускання і створення навантажень на мережевий стек через монотонну посилку запитів ICMP ECHO ([пінг](http://uk.wikipedia.org/wiki/%D0%9F%D1%96%D0%BD%D0%B3)). Легко виявляється за допомогою аналізу потоків трафіку в обидві сторони: під час атаки типу Icmp-флуд вони практично ідентичні.

**Виконання**

# ping -i 0 -s 10000 -l 100 -q ya.ru

-i задає інтервал надсилання пакетів. Інтервал менше 200 мс дозволений тільки суперкористувачу. -s задає розмір пакету. Стандартний 54, найбільший 65507 байт. -l задає кількість пакетів що відправляються без очікування на відповідь, і -q робить так щоб утиліта вивела лише підсумки.

**Захист**

Майже безболісний спосіб абсолютного захисту заснований на відключенні відповідей на запити ICMP ECHO:

# sysctl net.ipv4.icmp\_echo\_ignore\_all=1

Або за допомогою брандмауера:

# iptables -A INPUT -p icmp -j DROP --icmp-type 8

**SYN-флуд**

Один з поширених способів не лише забити канал зв'язку, але і ввести мережевий стек операційної системи в такий стан, коли він вже не зможе приймати нові запити на підключення. Заснований на спробі ініціалізації великого числа одночасних TCP-з'єднань через посилку SYN-пакету з неіснуючою зворотною адресою. Після декількох спроб відіслати у відповідь ACK-пакет на недоступну адресу більшість операційних систем ставлять невстановлене з'єднання в чергу. І лише після n-ої спроби закривають з'єднання. Оскільки потік ACK-пакетів дуже великий, незабаром черга виявляється заповненою, і ядро дає відмову на спроби відкрити нове з'єднання. Найрозумніші DoS-боти ще й аналізують систему перед початком атаки, щоб слати запити лише на відкриті життєво важливі порти. Ідентифікувати таку атаку просто: досить спробувати підключитися до одного з сервісів. Оборонні заходи зазвичай включають:

Збільшення черги «напіввідкритих» tcp-з'єднань:

# sysctl -w net.ipv4.tcp\_max\_syn\_backlog=1024

Зменшення часу утримання «напіввідкритих» з'єднань:

# sysctl -w net.ipv4.tcp\_synack\_retries=1

Включення механізму TCP syncookies:

# sysctl -w net.ipv4.tcp\_syncookies=1

Обмеження максимального числа «напіввідкритих» з'єднань з одного IP до конкретного порту:

# iptables -i INPUT -p tcp --syn --dport 80 -m iplimit --iplimit-above 10 -j DROP

**UDP-флуд**

Типовий метод захаращення смуги пропускання. Заснований на нескінченній посилці udp-пакетів на порти різних udp-сервісів. Легко усувається за рахунок відрізання таких сервісів від зовнішнього світу і установки ліміту на кількість з'єднань в одиницю часу до dns-сервера на стороні шлюзу:

# iptables -i INPUT -p udp --dport 53 -j DROP -m iplimit --iplimit-above 1

**HTTP-флуд**

Один з найпоширеніших на сьогоднішній день способів флуду. Заснований на нескінченному посиланні http-повідомлень GET на 80-й порт з метою завантажити web-сервер настільки, щоб він виявився не в змозі обробляти всю решту запитів. Часто, метою флуду стає не корінь web-сервер, а один із скриптів, що виконують ресурсоємні завдання або що працює з базою даних. У будь-якому разі, індикатором атаки, що почалася, служитиме аномально швидке зростання логів web-сервера.

Методи боротьби з Http-флудом включають тюнинг web-сервера і бази даних з метою понизити ефект від атаки, а також відсіювання DoS-ботів за допомогою різних прийомів. По-перше, слід збільшити максимальне число з'єднань до бази даних одночасно. По-друге, встановити перед web-сервером [Apache](http://uk.wikipedia.org/wiki/Apache) легкий і продуктивний [nginx](http://uk.wikipedia.org/wiki/Nginx) — він кешуватиме запити і видаватиме статику. Це рішення із списку «Must have», яке не лише понизить ефект DoS-атак, але і дозволить серверу витримати величезні навантаження. Невеликий приклад:

# vi /etc/nginx/nginx.conf

# Збільшує максимальну кількість використовуваних файлів worker\_rlimit\_nofile 80000;

events {

# Збільшує максимальну кількість з'єднань

worker\_connections 65536;

# Використовувати ефективний метод метод epoll для обробки з'єднань

use epoll;

}

http {

gzip off;

# Відключаємо таймаут на закриття keep-alive з'єднань

keepalive\_timeout 0;

# Не віддавати версію nginx в заголовку відповіді

server\_tokens off;

# Скидати з'єднання після таймауту

reset\_timedout\_connection on;

}

# Стандартні налаштування для роботи в якості проксі

server {

listen 111.111.111.111 default deferred;

server\_name host.com www.host.com;

log\_format IP $remote\_addr;

location / {

proxy\_pass http://127.0.0.1/;

}

location ~\* \.(jpeg|jpg|gif|png|css|js|pdf|txt|tar)$ {

root /home/www/host.com/httpdocs;

}

}

Частіше за все HTTP DDoS атака проводиться за допомогою [ботнету](http://uk.wikipedia.org/wiki/%D0%91%D0%BE%D1%82%D0%BD%D0%B5%D1%82), розподіленої роботизованої системи, що об’єднується за допомогою комп'ютерної мережі та віддалено керується зловмисником. Учасниками такої спілки, як правило стають заражені [вірусом](http://uk.wikipedia.org/wiki/%D0%92%D1%96%D1%80%D1%83%D1%81_%D0%BA%D0%BE%D0%BC%D0%BF%27%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B8%D0%B9), або [троянською програмою](http://uk.wikipedia.org/wiki/%D0%A2%D1%80%D0%BE%D1%8F%D0%BD%D1%81%D1%8C%D0%BA%D0%B8%D0%B9_%D0%B2%D1%96%D1%80%D1%83%D1%81) комп'ютери звичайних користувачів, які навіть про це не підозрюють. Виключенням є використання для атаки фреймів (тег frame) або посилань (тег link, або script), що розміщуються на одному або декількох web-ресурсах з великою кількістю користувачів та посилаються на web-сервер, що атакується. В деяких випадках, атаку проводять користувачі, що усвідомлено формують чисельну групу та об’єднані ціллю нанести шкоду обраному web-ресурсу. Як правило, група координується організатором за допомогою соціальних мереж або інших засобів зв’язку, що дають змогу передавати повідомлення великій кількості користувачів одночасно. Розставимо види HTTP DDoS атак в залежності від ступеня складності захисту від них (від найменшого до найбільшого): атака з використанням фреймів та посилань; атака з використанням мережі ботів; атака, що організована чисельною групою користувачів. Вразливим місцем атаки з використанням фреймів або посилань є обов’язкова наявність в HTTP запиті заголовка referer, що встановлюється браузером користувача і містить URL ресурсу, з котрого перейшов по посиланню користувач. Сформувавши на основі статистики за кількістю переходів перелік і виключивши з нього сайти, на котрих офіційно розміщені рекламні або інші посилання на ресурс (каталоги, прайс агрегатори) можна відфільтрувати та заблоковувати шкідливий трафік. Захист атак з використанням мережі ботів – задача що завжди потребує нетривіальних рішень. Один із основних способів базується на недосконалості роботизованих систем, найчастіше на неможливості інтерпретації скриптів на мові Javascript. Користувач, що невідомий web-серверу отримує в відповідь на запит скрипт на мові Javascript та лише після правильного виконання коду скрипту – отримує доступ до запрошених ним даних. Проблемою даної реалізації є організація безперешкодного доступу пошукових ботів до даних web-сервера. Захист від атак, що організовані чисельною групою користувачів найскладніше завдання, так як неможливо відрізнити їх від звичайних користувачів ресурсу. Для захисту потрібен постійний збір статистики доступу користувачів до ресурсу та при перевищені порогу частоти відвідувань з однієї IP-адреси просити користувача ввести перевірочні символи. Основна проблема даної реалізації — блокування локальних мереж, що працюють через одну IP адресу (за допомогою технології NAT).

У разі потреби можна задіювати nginx-модуль ngx\_http\_limit\_req\_module[[1]](http://uk.wikipedia.org/wiki/DoS-%D0%B0%D1%82%D0%B0%D0%BA%D0%B0#cite_note-1), що обмежує кількість одночасних підключень з однієї адреси.

UDP та торенти

З кінця січня (стабільна µTorrent версія 2.0 з µTP вийшла якраз 25 січня, офіційно доступна з 3 лютого) в статистичних звітах операторів зв'язку виявлено безперервне зростання UDP-трафіку і одночасне зменшення середньої величини пакетів, які істотно збільшували навантаження на мережеве устаткування. Спостереження показали, що чим сильніше завантажений канал клієнта, тим дрібніші пакети, довша черга і вище навантаження на [роутерах](http://uk.wikipedia.org/wiki/%D0%A0%D0%BE%D1%83%D1%82%D0%B5%D1%80).

У всіх випадках причиною що відбувається був названий МікроТоррент (µTorrent), з версії 1.8.1 що почав освоювати протокол обміну µTP (Micro Transport Protocol, до речі, що так і не дістав схвалення IETF). І провайдерам просто пощастило, що через низку обставин клієнти до версії µTorrent v2.0 не оновилися одночасно. (У ній, за умовчанням, UDP-завантаження стартує першим, а якщо не вийде, то лише тоді — по TCP). Інакше наростання проблем в мережі замість плавного носило б миттєвий характер і, можливо, відразу «повалило» до третини вітчизняних провайдерів. Останні могли б трактувати поведінку як DDoS-атаки на провайдерське устаткування з відповідним недемократичним «закручуванням гайок» в аварійному порядку.

Остаточний аналіз ситуації був ускладнений тим, що у відкритому доступі повного опису протоколу, який став займати значну долю UDP трафіку, немає: цей опис застарілий і не дає повної картини, а стаття у Вікіпедії досить поверхневий описує характер проблем.

Реінженеринг дозволив не лише переконатися, що згідно з алгоритмами µTP в процесі обміну зменшується довжина пакету із зростанням завантаження каналу, але і передбачити, що для підтвердження використовуються udp-пакети квитування (з функцією, типа ACK) розміром в 2 десятки байт.

Логіка розробників протоколу і алгоритмів µTorrent може виправдовуватися тим, що вони не вважають розумними чекати TCP-ACK від доставки пакету. Адже tcp-потік формується послідовно, і якщо в стеку, наприклад, вже знаходиться 50 пакетів, але немає два, то передачу вони не здійснюватимуть, поки втрачені не прийдуть. А ось пірингове застосування за своєю суттю якраз і не критично до строгої послідовності у вступі інформації, адже воно запрошує і складає файли зі шматочків.

І що виходить насправді? Додаток, відповідно, зменшує розмір пакету, тому що у нього зростає час між відсиланням пакету і приходом квитанції. Але зростає-то воно тому, що пакети стоять в переповненій черзі на «шейпері». І замість того що б спочатку зменшити кількість посланих, алгоритм … далі зменшує їх розмір. В результаті, при даному агресивному алгоритмі використання UDP-протоколу МікроТоррентом результуючий трафік (ємкість каналу) на клієнтові практично не змінюється. Тобто вихідна мрія творців даного ПЗ — завантажити канал «під зав'язку» від цього ближче не стає. Змінюється лише структура трафіку — з'являється більше дрібних пакетів, що для провайдера насправді небезпечніше, ніж зростання трафіку.

Давайте порахуємо: якщо в ходу пакети по 150 байт, то при швидкості 100 мегабіт операторові потрібно буде обробити в секунду … 87 тисяч пакетів! Не кожен провайдер зможе оперативно відреагувати на виниклу проблему: замінити ті ж сервери доступа/роутери на високопродуктивних не всім по кишені. В результаті, багато провайдерів вимушено було для своїх клієнтів ввести на додаток до обмежень по Mbps, ще і по pps.

Але, навіть якщо провайдерське устаткування зможе впоратися з цим алогічним алгоритмом обміну, замість вичавлених з провайдера декількох зайвих відсотків смуги, клієнт ризикує втратити значно більше завдяки збільшеному пакетному навантаженню . на свій домашній шлюз і, можливо навіть — на свій не дуже сучасний ПК! А що він зробить, побачивши, що швидкість закачування знизилася? Правильно, без тіні сумніву звернеться в технічну підтримку і звалить свої проблеми на провайдера.

Оскільки локальна ситуація моделюється досить нескладно, я провів невеликий експеримент з наявним ADSL-Wi-Fi-шлюзом, який можу запропонувати прогресивним користувачам µTorrenta. Особливо вражаючим тест виглядатиме на давніх роутерах з Wifi. У моєму циклі випробувань пристрій почав «сповільнюватися» приблизно вже при 30-40 активних сесіях «звичайного» закачування, але при агресивній роботі по UDP (всього 5 роздач) втратив відразу майже третину смуги. Поза сумнівом, причина — в перевищенні можливої кількості коректно оброблюваних пакетів за одиницю часу.

**2.12)** **Алгоритми з секретним ключем**

**Криптографічні алгоритми з секретним ключем**

Алгоритми із секретним ключем або симетричні алгоритми — це такі алгоритми, для яких ключ для шифрування повідомлення збігається із ключем для його дешифрування.

Наведемо деякі приклади симетричних алгоритмів

Алгоритм *DES* (Data Encryption Standard) був прийнятий як національний стандарт США1977 року. Головним його недоліком є довжина ключа (56 біт), що робить DES недостатньо надійним у сучасних умовах (ключ може бути знайдений за скінчений час перебором усіх можливих ключів). Як альтернативу сьогодні використовують *потрійний DES* (послідовне шифрування трьома різними ключами).  
  
 У 2001 році було прийнято новий стандарт на симетричний криптографічний алгоритм. Він (як і сам алгоритм) дістав назву *AES* (Advanced Encryption Standard). За довжиною ключ AES значно перевищує DES (стандарт визначає ключі на 128, 192 і 256 біт), крім того, він відрізняється високою продуктивністю.  
  
**Обмін повідомленнями із використанням криптографії із секретним ключем**  
  
Подамо у вигляді протоколу обмін повідомленнями у разі використання криптографічного алгоритму із секретним ключем.

1. Аліса і Боб погоджуються, що вони використовуватимуть систему із секретним ключем.
2. Вони доходять згоди щодо спільного ключа.
3. Аліса шифрує вихідний текст ключем і посилає його Бобові.
4. Боб розшифровує повідомлення тим самим ключем.

Другий крок потрібно робити секретно через деякий альтернативний канал передавання даних. Якщо Аліса і Боб не можуть використати такий канал, вони змушені передавати ключ незашифрованим, інакше інша сторона не зможе ним скористатися. Якщо при цьому ключ перехопить зловмисник, то він далі зможе читати всю інформацію, яку передають каналом.

Цю проблему неможливо вирішити, залишаючись у межах традиційних симетричних алгоритмів. Потрібен принципово інший підхід. Він отримав назву *крипто­графії із відкритим ключем*(public key cryptography).

**2.13) Криптографічні алгоритми з відкритим ключем**

Алгоритми з відкритим ключем розроблено таким чином, що ключ, використаний для шифрування, відрізняється від ключа для дешифрування. Ці два ключі працюють у парі: текст, який шифрують одним ключем, дешифрують іншим відповідно до формул

Ці алгоритми так називаються тому, що один із цих ключів може бути відкритий для всіх (наприклад, опублікований у пресі), даючи змогу будь-якій особі шифрувати цим ключем, але таке повідомлення може прочитати тільки справжній адресат (що володіє другим ключем).

Ключ, що відкривають для інших осіб для виконання шифрування, називають відкритим ключем (public key), парний до нього ключ для дешифрування — закритим ключем (private key).

Алгоритми із секретним ключем працюють швидше за алгоритми з відкритим ключем, тому, якщо не потрібні специфічні властивості, забезпечувані відкритим ключем (наприклад, не передбачене пересилання даних відкритим каналом зв'язку), достатньо обмежитися алгоритмом із секретним ключем.

Найвідомішим алгоритмом із відкритим ключем є *RSA.*

**Обмін повідомленнями з використанням криптографії із відкритим ключем**

Обмін повідомленнями у разі використання криптографії з відкритим ключем наведемо у вигляді протоколу

1. Аліса і Боб погоджуються використовувати систему з відкритим ключем.
2. Боб надсилає Алісі свій відкритий ключ.
3. Аліса шифрує повідомлення відкритим ключем Боба і відсилає його Бобові.
4. Боб розшифровує це повідомлення своїм закритим ключем.

Ця послідовність кроків позбавлена недоліків, властивих для процедури обміну секретним ключем. Перехоплення відкритого ключа зловмисником не спричиняє порушення безпеки каналу, а закритий ключ між сторонами не передають

**2.14) Протоколи аутентифікації**

**Автентифікáція** (з [грец.](http://uk.wikipedia.org/wiki/%D0%93%D1%80%D0%B5%D1%86%D1%8C%D0%BA%D0%B0_%D0%BC%D0%BE%D0%B2%D0%B0) *αυθεντικός*; реальний або істинний) — процедура встано­влен­ня належності користувачеві інформації в системі пред'явленого ним [ідентифікатора](http://uk.wikipedia.org/wiki/%D0%86%D0%B4%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D1%96%D0%BA%D0%B0%D1%82%D0%BE%D1%80).

З позицій [інформаційної безпеки](http://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0) Автентифікація є частиною [процедури](http://uk.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%86%D0%B5%D0%B4%D1%83%D1%80%D0%B0) надання дос­ту­­­пу для роботи в [інформаційній системі](http://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0), наступною після [ідентифікації](http://uk.wikipedia.org/wiki/%D0%86%D0%B4%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D1%96%D0%BA%D0%B0%D1%86%D1%96%D1%8F_(%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0)) і пе­ре­дує­ [авто­ри­за­ції](http://uk.wikipedia.org/wiki/%D0%90%D0%B2%D1%82%D0%BE%D1%80%D0%B8%D0%B7%D0%B0%D1%86%D1%96%D1%8F).

Механізм Автентифікації

Один із способів автентифікації в інформаційній системі полягає у попе­ред.­ній [ідентифікації](http://uk.wikipedia.org/wiki/%D0%86%D0%B4%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D1%96%D0%BA%D0%B0%D1%86%D1%96%D1%8F) на основі користувацького [ідентифікатора](http://uk.wikipedia.org/wiki/%D0%86%D0%B4%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D1%96%D0%BA%D0%B0%D1%82%D0%BE%D1%80) ([«логіна»](http://uk.wikipedia.org/wiki/%D0%9B%D0%BE%D0%B3%D1%96%D0%BD) ([англ.](http://uk.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0_%D0%BC%D0%BE%D0%B2%D0%B0) *login* — реє­стра­цій­ного імені користувача) і [пароля](http://uk.wikipedia.org/wiki/%D0%9F%D0%B0%D1%80%D0%BE%D0%BB%D1%8C) — певної конфіденційної інформації, знання якої пере­дба­чає володіння певним ресурсом в мережі. Отримавши введений користувачем логін и па­роль, комп'ютер порівнює їх зі значенням, яке зберігається в спеціальній захищеній [базі да­них](http://uk.wikipedia.org/wiki/%D0%91%D0%B0%D0%B7%D0%B0_%D0%B4%D0%B0%D0%BD%D0%B8%D1%85) і, у випадку успішної автентифікації проводить [авторизацію](http://uk.wikipedia.org/wiki/%D0%90%D0%B2%D1%82%D0%BE%D1%80%D0%B8%D0%B7%D0%B0%D1%86%D1%96%D1%8F) з подальшим допуском ко­рис­тувача до роботи в системі.

Види Автентифікації

**Слабка Автентифікація**

Традиційну автентифікацію за допомогою пароля називають ще однофакторною або слабкою. Оскільки за наявності певних ресурсів перехоплення або підбір пароля є справою часу. Не останню роль в цьому грає людський чинник — чим стійкішим до взлому методом підбору є пароль, тим важче його запам'ятати людині і тим вище ймовірність що він буде додатково записаний, що підвищить ймовірність його перехоплення або викрадення. І навпаки — легкі для запам'ятовування паролі (наприклад часто вживані слова або фрази, як приклад, дати народження, імена близьких, назви моніторів чи найближчого обладнання) в плані стійкості до злому є дуже не вдалими. Як вихід, впроваджуються одноразові паролі, проте їхнє перехоплення також можливе.

**Сильна Автентифікація**

Паралельно, за необхідності, використовується сильна або багатофакторна автентифікація — на основі двох чи більше факторів. В цьому випадку для автентифікації використостовується не лише інформація відома користувачеві, а й додаткові фактори. Наприклад:

* властивість, якою володіє суб'єкт;
* знання — інформація, яку знає суб'єкт;
* володіння — річ, якою володіє суб'єкт.

Способи Аутентифікації

**Парольна**

Здійснюється на основі володіння користувачем певної конфіденційної інформації.

**Біометрична**

Біометрична аутентифікація основана на унікальності певних антропометричних характеристик людини. У галузі інформаційних технологій термін біометрія застосовується в значенні технології ідентифікації особистості. Біометричний захист ефективніший ніж такі методи як, використання смарт-карток, паролів, PIN-кодів. Найчастіше використовуються:

1. Параметри [голосу](http://uk.wikipedia.org/wiki/%D0%93%D0%BE%D0%BB%D0%BE%D1%81).
2. Візерунок [райдужної оболонки](http://uk.wikipedia.org/wiki/%D0%A0%D0%B0%D0%B9%D0%B4%D1%83%D0%B6%D0%BD%D0%B0_%D0%BE%D0%B1%D0%BE%D0%BB%D0%BE%D0%BD%D0%BA%D0%B0) ока і карта [сітківки](http://uk.wikipedia.org/wiki/%D0%A1%D1%96%D1%82%D0%BA%D1%96%D0%B2%D0%BA%D0%B0) ока.
3. Риси [обличчя](http://uk.wikipedia.org/wiki/%D0%9E%D0%B1%D0%BB%D0%B8%D1%87%D1%87%D1%8F).
4. Форма [долоні](http://uk.wikipedia.org/wiki/%D0%94%D0%BE%D0%BB%D0%BE%D0%BD%D1%8F).
5. [Відбитки пальців](http://uk.wikipedia.org/wiki/%D0%94%D0%B0%D0%BA%D1%82%D0%B8%D0%BB%D0%BE%D1%81%D0%BA%D0%BE%D0%BF%D1%96%D1%8F).
6. Форма і спосіб особистого [підпису](http://uk.wikipedia.org/wiki/%D0%9F%D1%96%D0%B4%D0%BF%D0%B8%D1%81).

**Етапи**

Основні етапи проектування системи біометричної аутентифікації на основі динамічного підпису в цілому. Розробка математичної моделі динамічного підпису і методів його обробки. Реалізація алгоритму роботи модуля аутентифікації системи на основі створеної математичної моделі і методів обробки. Реалізація системи аутентифікації у складі інформаційної системи. Тестування системи аутентифікації. Модифікація коду фрагментів системи у процесі функціонування системи.

Перший етап — проектування, полягає у аналізі вимог, які ставляться до системи і на їх основі проектується архітектура системи аутентифікації в цілому. Враховується сфера застосування системи, зокрема задається її точність, надійність, зручність; операційна система (ОС) у якій буде функціонувати ПЗ та інші параметри. У випадку розробки універсальної системи необхідно передбачити можливість зміни цих параметрів інтегратором (адміністратором) системи, а також бажано розробляти кросплатформенне ПЗ, незалежне від ОС. Розробити рольову модель роботи системи — скористатися апаратом об'єктно-орієнтованого аналізу і об'єктно-орієнтованого проектування. Рекомендується використовувати уніфіковану мову програмування UML для проектування і моделювання інформаційної системи, а також дотримуватися наступних принципів: модульність — кожна компонента системи є модулем, який просто модифікується, замінюється і виконує відведену йому специфічну роль; підтримка відкритих стандартизованих протоколів для передачі даних, взаємодії об'єктів і форматів збереження файлів; документованість — усі методи (функції), класи, об'єкти детально і доступно документувати.

Другий етап — розробка математичної моделі є ключовим. Необхідно вдало підібрати підхід до побудови моделі: стохастичний чи детермінований, на думку авторів це стохастичний підхід. Розробка математичної моделі передбачає: розробку моделі, яка враховувала б ключові особливості об'єкта дослідження і вибір діагностичних ознак; проведення аналізу цих діагностичних ознак і розробка методів для попередньої обробки. У випадку використання статистичного підходу — дослідити статистичні характеристики діагностичних ознак. Ці дослідження дозволяють зробити висновки про адекватність моделі.

Третій етап — на основі математичної моделі розробляється алгоритм, який реалізується на деякій мові програмування. Особливу увагу слід привернути на реалізацію системи вводу підпису

**За допомогою унікального предмета**

Здійснюється за допомогою додаткових предметів ([токен](http://uk.wikipedia.org/w/index.php?title=%D0%A2%D0%BE%D0%BA%D0%B5%D0%BD_(%D0%B0%D0%B2%D1%82%D0%BE%D1%80%D0%B8%D0%B7%D0%B0%D1%86%D1%96%D1%8F)&action=edit&redlink=1), [смарт-карта](http://uk.wikipedia.org/wiki/%D0%A1%D0%BC%D0%B0%D1%80%D1%82-%D0%BA%D0%B0%D1%80%D1%82%D0%B0)) або атрибутів (криптографічний [сертифікат](http://uk.wikipedia.org/wiki/%D0%A1%D0%B5%D1%80%D1%82%D0%B8%D1%84%D1%96%D0%BA%D0%B0%D1%82)).

Автентифікація в ОС

Протоколи Автентифікації

Протоколи автентифікації — категорія [криптографічних протоколів](http://uk.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%87%D0%BD%D0%B8%D0%B9_%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB), які забезпечують надійну автентифікацію особи.

Існує багато різноманітних протоколів автентифікації:

* [AKA](http://uk.wikipedia.org/w/index.php?title=AKA_(security)&action=edit&redlink=1)
* [CAVE-based authentication](http://uk.wikipedia.org/w/index.php?title=CAVE-based_authentication&action=edit&redlink=1)
* [Challenge-handshake authentication protocol](http://uk.wikipedia.org/w/index.php?title=Challenge-handshake_authentication_protocol&action=edit&redlink=1) (CHAP)
* [CRAM-MD5](http://uk.wikipedia.org/wiki/CRAM-MD5)
* [Diameter](http://uk.wikipedia.org/w/index.php?title=Diameter_(protocol)&action=edit&redlink=1)
* [EAP](http://uk.wikipedia.org/wiki/EAP) (EAP)
* [Host Identity Protocol](http://uk.wikipedia.org/w/index.php?title=Host_Identity_Protocol&action=edit&redlink=1) (HIP)
* [Кербер](http://uk.wikipedia.org/wiki/%D0%9A%D0%B5%D1%80%D0%B1%D0%B5%D1%80_(%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB))
* [MS-CHAP](http://uk.wikipedia.org/w/index.php?title=MS-CHAP&action=edit&redlink=1) і [MS-CHAPv2](http://uk.wikipedia.org/w/index.php?title=MS-CHAPv2&action=edit&redlink=1) різновиди CHAP
* [LAN Manager](http://uk.wikipedia.org/w/index.php?title=LAN_Manager&action=edit&redlink=1)
* [NTLM](http://uk.wikipedia.org/wiki/NTLM), також відомий як NT LAN Manager
* [Password-authenticated key agreement](http://uk.wikipedia.org/w/index.php?title=Password-authenticated_key_agreement&action=edit&redlink=1) протоколи
* [Password Authentication Protocol](http://uk.wikipedia.org/w/index.php?title=Password_Authentication_Protocol&action=edit&redlink=1) (PAP)
* [Protected Extensible Authentication Protocol](http://uk.wikipedia.org/w/index.php?title=Protected_Extensible_Authentication_Protocol&action=edit&redlink=1) (PEAP)
* [RADIUS](http://uk.wikipedia.org/wiki/RADIUS)
* [Secure Remote Password protocol](http://uk.wikipedia.org/w/index.php?title=Secure_Remote_Password_protocol&action=edit&redlink=1) (SRP)
* [TACACS](http://uk.wikipedia.org/w/index.php?title=TACACS&action=edit&redlink=1) і [TACACS+](http://uk.wikipedia.org/w/index.php?title=TACACS%2B&action=edit&redlink=1)
* [RFID-Authentication Protocols](http://uk.wikipedia.org/w/index.php?title=RFID-Authentication_Protocols&action=edit&redlink=1)
* [Woo Lam 92 (protocol)](http://uk.wikipedia.org/w/index.php?title=Woo_Lam_92_(protocol)&action=edit&redlink=1)
* [Протокол Нідхема-Шредера](http://uk.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D0%9D%D1%96%D0%B4%D1%85%D0%B5%D0%BC%D0%B0-%D0%A8%D1%80%D0%B5%D0%B4%D0%B5%D1%80%D0%B0)

Розширення кола користувачів розподілених систем і ускладнення завдань, що вирі­шують­ся за допомогою подібних мереж, привели до усвідомлення першорядної важливості проб­лем, пов'язаних із забезпеченням інформаційної безпеки при міжмережевої взаємодії, перш за все з використанням відкритих каналів передачі даних, що створюють потенційну мож­ливість для дій як пасивного порушника, що має можливість тільки переглядати дос­ту­п­ні йому повідомлення, так і активного порушника, який поряд з прослуховуванням може мо­ди­фікувати доступні йому повідомлення.

Ось чому одним з найважливіших завдань забезпечення безпеки є розробка методів і засобів, що дозволяють одній стороні (перевіряючому) переконатися в ідентичності іншого боку (що доводить). Широко поширеними механізмами вирішення даної проблеми є спеціальні прийоми, що дають можливість перевірити коректність повідомлень, які демонструють, що доводить володіє певним секретом. Зазвичай такі методи і засоби називаються ідентифікацією (аутентифікацією) користувачів, або перевіркою ідентичності, Існує також особливий різновид подібних протоколів, звана аутентифікації повідомлень (або аутентифікацією джерела даних), яка реалізується за допомогою симетричних алгоритмів або / і цифрового підпису.

Основна відмінність між аутентифікації користувача та аутентифікації повідомлення полягає в тому, що остання не забезпечує тимчасових гарантій того, коли це повідомлення було створено, а аутентифікація користувачів дає можливість доводить ідентифікувати себе в ході сесії.

Існують також інструментарії, що реалізують одночасно аутентифікацію та розподіл ключів; здійснення деяких з них полягає в проведенні аутентифікації повідомлень, які представляють собою ключ (це питання детально розглядається в наступному розділі).  
Автентифікація користувача - процес, за допомогою якого одна сторона переконується в ідентичності іншого боку, при цьому інша сторона теж активно бере участь у процесі обміну інформацією.

В рамках цієї книги ми будемо вважати, що терміни ідентифікація, аутентифікація користувачів і аутентифікація є синонімами.

Всі протоколи аутентифікації можуть бути розділені на такі категорії:

- На основі знання чого-небудь. Прикладом можуть служити стандартні паролі, персональні ідентифікаційні номери (PIN), а також секретні та відкриті ключі, знання яких демонструється в протоколах типу «запит-відповідь».

- На основі володіння чим-небудь. Звичайно це магнітні картки, смарт-карти, touch memory і персональні генератори, які використовуються для створення одноразових паролів.  
- На основі яких-небудь невід'ємних характеристик. Ця категорія включає методи, що базуються на перевірці призначених для користувача біометричних характеристик (голос, сітківка ока, відбитки пальців).

У даній категорії не використовуються криптографічні методи і засоби. Аутентифікація на основі біометричних характеристик застосовується для контролю доступу в приміщення або до будь-якої техніки.

**Ідентифікація і автентифікація**

КЗЗ повинен реалізувати рівень НИ-2.

Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особу суб’єкта, що намагається одержати доступ до захищених об’єктів WEB-сторінки.

Політика ідентифікації і автентифікації стосується: всіх користувачів WEB-сторінки, які намагаються одержати доступ до системного та функціонального програмного забезпечення, що використовується для актуалізації, захисту публічної інформації та супроводження WEB-сторінки; створеної в процесі супроводження WEB-сторінки технологічної інформації КСЗІ та технологічної інформації щодо управління АС; задіяного для цього периферійного обладнання.

КЗЗ повинен однозначно ідентифікувати категорії користувачів WEB-сторінки і за атрибутами кожної з цих категорій визначати послуги, що їм доступні. Ідентифікація здійснюється на підставі особистого імені та/або ІР-адреси користувача.

КЗЗ повинен автентифікувати адміністратора WEB-сторінки, співробітників СЗІ та користувачів, які мають повноваження щодо управління АС, з використанням захищеного механізму на підставі особистого пароля. Автентифікація користувачів, що мають виключне право доступу тільки до публічної інформації, не здійснюється.

Дозвіл на виконання будь-яких дій з інформацією та обладнанням WEB-сторінки, що контролюються КЗЗ, надається користувачу тільки після успішного завершення процедур ідентифікації та/або автентифікації його КЗЗ відповідно до категорії користувача.

КЗЗ повинен забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування.

**Ідентифікація і автентифікація при обміні**

КЗЗ повинен реалізувати рівень НВ-1.

Ця послуга дозволяє у разі використання технології Т2 компонентам КЗЗ WEB-сервера і віддаленої робочої станції здійснити взаємну ідентифікацію, перш ніж розпочати взаємодію.

Послуга ідентифікації і автентифікації при обміні стосується адміністратора безпеки та користувачів, яким надані повноваження щодо супроводження WEB-сторінки, технологічної інформації КСЗІ.

КЗЗ повинен надавати доступ до процесів, що забезпечують ініціалізацію обміну даними, тільки адміністратору безпеки і користувачам, яким надано повноваження щодо супроводження WEB-сторінки.

Обмін інформацією між компонентами КЗЗ повинен здійснюватися тільки після ідентифікації і автентифікації КЗЗ-відправником КЗЗ-отримувача інформації. Результати процедури ідентифікації і автентифікації є дійсними протягом всього сеансу обміну (незалежно від кількості об’єктів, що експортуються) і втрачають свою силу після його закінчення.

Процедура ідентифікації і автентифікація компонентів КЗЗ повинна здійснюватися на підставі їхніх імен, ІР-адрес і паролів.

Підтвердження ідентичності має виконуватися на підставі затвердженого в АС протоколу автентифікації.

**Поняття криптографічного алгоритму і протоколу**

**Криптографічні алгоритми**  
  
*Криптографічний алгоритм,*який ще називають *шифром*(cipher), — це математична функція, яку використовують для шифрування і дешифрування.  
  
Сучасні криптографічні алгоритми проблему безпеки вирішують виключно за допомогою *ключа*(key). Ключ — це значення, яке використовують для шифрування і дешифрування, при цьому без знання ключа дешифрування має бути технічно неможливим (тобто неможливим за наявності будь-яких доступних ресурсів). Ключ має належати до множини зі значною кількістю елементів: її розмір повинен бути таким, щоб забезпечити технічну неможливість підбору ключа повним перебором усіх елементів цієї множині.  
  
Сукупність алгоритму і множини всіх можливих вихідних текстів, шифрованих текстів і ключів називають *криптосистемою.*  
  
Криптографічні алгоритми, засновані на ключі, поділяють на дві основні групи: *симетричні*(або *алгоритми із секретним ключем)*і *алгоритми із відкритим ключем.*Далі докладніше про особливості цих двох груп.  
  
**Криптографічні протоколи**  
  
*Криптографічний протокол —*це послідовність кроків, розроблена для виконання деякої задачі із забезпечення криптографічного захисту даних.  
  
Такий протокол обов'язково включає дві або більше сторін і розглядається як обмін діями між сторонами. Для позначення сторін прийнято використовувати такі імена: *Аліса —*учасник, що робить перший крок; *Боб*— учасник, що робить крок у відповідь.  
  
На окремих етапах протоколів використовують різні криптографічні алгоритми.

**Гібридні криптосистеми**

На практиці алгоритми із відкритим ключем не можуть цілковито замінити алгоритми із секретним ключем, насамперед через те, що вони працюють значно повільніше, і шифрувати ними великі обсяги даних неефективно.  
  
Для того щоб об'єднати переваги двох категорій алгоритмів, використовують гібридні криптосистеми, де алгоритми із відкритим ключем використовують для шифрування не самих повідомлень, а ключів симетричних алгоритмів, якими далі (після обміну) шифрують весь канал. Такі ключі називають сесійними ключами, бо їх звичайно створюють за допомогою генераторів випадкових чисел для конкретної сесії.  
  
Протокол роботи гібридної криптосистеми наведемо нижче.

1. Боб відсилає Алісі свій відкритий ключ.
2. Аліса генерує випадковий сесійний ключ, шифрує його відкритим ключем Боба і відсилає Бобові.
3. Боб розшифровує сесійний ключ своїм закритим ключем.
4. Обидві сторони далі обмінюються повідомленнями, зашифрованими сесійним ключем.

Гібридні криптосистеми забезпечують якісний захист ключів і прийнятну продуктивність. Про різні застосування цієї технології йтиметься далі.

Ще одна галузь застосування криптографії із відкритим ключем — *цифрові підписи.*Протокол створення і перевірки цифрового підпису при цьому складається з таких кроків.

1. Аліса шифрує документ своїм закритим ключем, тим самим підписуючи його.
2. Аліса відсилає шифрований документ Бобові.
3. Боб розшифровує документ відкритим ключем Аліси, підтверджуючи цифровий підпис.

Цей протокол забезпечує підтримку основних характеристик цифрових підписів, до яких належить, зокрема, неможливість приховати зміну підписаного документа. У цьому разі спроба змінити документ без використання закритого ключа призводить до того, що документ не дешифрується після перевірки підпису.  
  
Алгоритми із відкритим ключем, однак, неефективні для підписування повідомлень великого обсягу. Щоб підвищити продуктивність, цифрові підписи реалізують із використанням односторонніх хеш-функцій.

**Односторонні хеш-функції**  
  
*Хеш-функція —*функція, що приймає на вхід рядок змінної довжини, який називають *вхідним образом,*а повертає рядок фіксованої (звичайно меншої) довжини — *хеш.*  
  
За значенням *односторонньої функції*важко віднайти аргумент. *Одностороння хеш-функція*також працює в одному напрямку: легко отримати хеш із вихідного рядка, але технічно неможливо знайти вхідний образ, із якого походить цей хеш.  
  
Односторонній хеш-функції властива свобода від колізій: технічно неможливо створити два вхідних образи з одним і тим самим значенням хеша.  
  
Найрозповсюдженшшми односторонніми хеш-функціями є MD5 і SHA-1. Крім цифрових підписів, їх можна використати для розв'язання різних задач, які потребують такого відображення важливої інформації, що заслуговує на довіру.  
  
  
**Підписи із відкритим ключем і односторонніми хеш-функціями**  
  
У разі використання односторонніх хеш-функцій для цифрових підписів замість документа підписують його хеш (значно менший за обсягом). Протокол набуває такого вигляду.

1. Аліса отримує односторонній хеш документа.
2. Аліса шифрує хеш своїм закритим ключем, тим самим підписуючи документ.
3. Аліса відсилає Бобові документ і зашифрований хеш.
4. Боб розшифровує хеш, переданий Алісою, її відкритим ключем.
5. Боб отримує односторонній хеш переданого Алісою документа.
6. Боб порівнює хеші, отримані під час виконання кроків 4 і 5. Якщо вони збігаються, підпис Аліси можна вважати вірним.

Цей протокол грунтується на тому, що підпис хеша можна прирівняти до підпису документа, що випливає із властивості свободи від колізій односторонніх хеш-функцій (неможливо створити два документи, які були б перетворені на один хеш).

**2.15)** **Цифрові підписи**

**Організаційне забезпечення електронного цифрового підпису**

Організаційне забезпечення електронного цифрового підпису (ЕЦП) здійснюється відповідно до законодавства держави, на території якої використовується такий засіб ЕЦП. Якщо такого законодавства немає, правове регулювання в галузі застосування засобів ЕЦП здійснюється на основі нормативних актів адміністративних органів.

Необхідність сертифікації засобів ЕЦП

Засіб ЕЦП — це програмне і/чи апаратне забезпечення, призначене для генерації пари ключів (закритого й відкритого) та їх автоматизованого застосування під час шифрування або дешифрування електронного підпису. Оскільки від алгоритмів, на основі яких діє засіб ЕЦП, залежить надійність і стійкість документообігу, до засобів ЕЦП існують спеціальні вимоги.

Необхідність сертифікації відкритих ключів

Відкритий ключ тому й називається відкритим, що він доступний кожному з партнерів власника закритого ключа. Якщо в разі звертання від партнера Oksanlia до партнера Магу потрібен захищений канал зв'язку, то партнер Oksanka може скористатися відкритим ключем партнера Магу. Тоді він може бути відносно впевнений, що в каналі зв'язку повідомлення не перехоплять. Але залишається відкритим питання, чи веде цей канал справді до партнера Маrу! Є дуже простий прийом підміни відкритого ключа для створення помилкового каналу зв'язку. Припустімо, сторона Artu.ro бажає перехопити чужі дані. У цьому разі вона може за допомогою засобу ЕЦП створити собі пари ключів й опублікувати відкритий ключ нібито від імені партнера Маrу. Тоді всі повідомлення від партнера Oksanka до партнера Маrу перехоплюватимуться і читатимуться стороною Artиrо, причому ні Oksanka, ні Магу навіть не здогадуватимуться про те, що Arturo бере участь у "договірних" відносинах.

Наведений приклад ілюструє лише найпростішу форму зловживання, бо хоча у відкритому ключі й наводяться дані про його власника, у ньому немає засобів, які засвідчують справжність цих даних. Без вирішення цього питання механізм ЕЦП не можна використовувати ні в електронній комерції, ні в електронному документообігу.

Значна частина державних законодавчих актів, що стосуються електронних цифрового підпису, комерції та документообігу, присвячена механізму посвідчення особи власника відкритого ключа. В усіх випадках цей механізм ґрунтується на тому, що вводиться (призначається) додаткова сторона, яка засвідчує належність відкритого ключа конкретній юридичній або фізичній особі.

Хто саме має право засвідчувати відкриті ключі, коли і як, у законодавствах різних держав вирішується по-різному. Зокрема, це може бути державний орган або організація, уповноважена державою для ведення такої діяльності. Можливо, що для внутрішнього документообігу підприємства цю функцію можна доручити особі, призначеній керівництвом, а для документообігу всередині відомства -- уповноваженому підрозділу.

Поняття електронного сертифіката

На практиці сертифікація відкритих ключів виконується в такий спосіб.

Особа (юридична або фізична), що створила собі пару ключів (відкритий і закритий) за допомогою засобу ЕЦП, має звернутися в орган, уповноважений виконати сертифікацію. Цей орган називається Центром сертифікації (Certification Authority, СА).

Центр сертифікації перевіряє належність відкритого ключа заявнику і засвідчує цей факт додаванням до відкритого ключа свого підпису, зашифрованого власним закритим ключем.

Будь-який партнер, що бажає вступити в контакт із власником відкритого ключа, може прочитати засвідчувальний запис за допомогою відкритого ключа центру сертифікації. Якщо цілісність цього запису не порушена і він довіряє центру сертифікації, то може використовувати відкритий ключ партнера для зв'язку з ним.

Слід звернути увагу, що центр сертифікації завіряє тільки факт належності відкритого ключа конкретній особі чи організації. У літературі існують некоректні твердження про те, що центр сертифікації нібито завіряє сумлінність власника відкритого ключа. Насправді, сертифікація відкритого ключа не стосується сумлінності, платоспроможності, ретельності й будь-яких інших ділових якостей його власника. Приклад — загальногромадянський паспорт. Це засіб посвідчення тільки особи його власника. Паспорт не може і не має містити які-небудь дані, що характеризують свого власника. Для цього є інші засоби. Наявність повноцінного сертифіката відкритого ключа говорить про те, що ключ можна використовувати для посвідчення особи партнера. Але доцільність цих відносин центром сертифікації не засвідчується.

**Технічне забезпечення режиму електронного цифрового підпису. Поняття електронного цифрового підпису**

**Особливості рукописного підпису**

Власноручний підпис під документом віддавна вважається доказом того, що людина, яка підписала цей документ, ознайомилася з ним і згодна з його змістом. Тобто рукописний підпис є одним із засобів ідентифікації особи, в основу якого покладено гіпотезу про унікальність особистих біометричних параметрів людини. Чому ж підпис заслужив таку довіру? Основні причини такі:

дійсність підпису можна перевірити (його наявність у документі дає змогу переконатися, чи справді він був підписаний людиною, що володіє правом ставити цей підпис);

підпис не можна підробити (справжній підпис - доказ того, що саме та людина, якій він належить, поставила цей підпис під документом);

підпис, що вже стоїть під одним документом, не може бути використаний ще раз для підписання іншого документа (підпис — невід'ємна частина документа і його не можна перенести в інший документ);

підписаний документ не підлягає ніяким змінам;

від підпису неможливо відректися (той, хто поставив підпис, не може згодом заявити, що він не підписував цей документ).

Насправді жодна з перерахованих властивостей підпису на всі 100 % не виконується. У нашому сучасному криміналізованому суспільстві підписи підробляють і копіюють, від них відрікаються, а в уже підписані документи вносять довільні зміни. Тобто застосування рукописного підпису не позбавлене недоліків:

недостатній ступінь захисту (коли необхідна підвищена достовірність відомостей, що містяться у документі, використовують додаткові засоби захисту: наявність додаткових рукописних підписів, печатки юридичних осіб, засвідчення у нотаріуса, спеціальні бланки тощо);

нерозривний фізичний зв'язок з матеріальним носієм (рукописний підпис можливий тільки на документах з матеріальною природою, тому особа, що підписує документ, має безпосередньо контактувати з матеріальним носієм цього документа);

розбіжності між оригіналом та копіями, отриманими засобами копіювально-миожильної техніки (копії не мають тієї юридичної сили, яку має оригінал документа);

ніяким чином не забезпечує аутентифікацію документа, тобто його цілісність і незмінність (без додаткових засобів захисту рукописний підпис не гарантує незмінності вмісту документа під час його збереження або транспортування).

Особливості електронного цифрового підпису

Застосування глобальних комунікацій в економічній діяльності та повсякденному житті зумовило появу принципово нового виду відносин, пов'язаних з обміном інформацією без використання паперових носіїв, тобто за допомогою електронних документів. Під електронним документом мають на увазі документ, в якому інформацію подано в електронній формі та який містить необхідні реквізити (у тому числі електронний цифровий підпис).

Електронний цифровий підпис (ЕЦП) є реквізитом електронного документа і призначений для його захисту від підробки. ЕЦП має не фізичну, а логічну природу. Під час побудови цифрового підпису замість звичайного зв'язку між печаткою або рукописним підписом та аркушем паперу простежується складна залежність між документом в електронному вигляді, секретним і загальнодоступним (відкритим) ключами, а також цифровим підписом. Складність підробки ЕЦП зумовлена дуже великим обсягом математичних обчислень.

ЕЦП може мати цілком "буквений" вигляд, але частіше він поданий у вигляді послідовності довільних символів. Цифровий підпис може зберігатися разом з документом, наприклад, стояти на його початку, в кінці або в окремому файлі (природно, що в останньому випадку, перевіряючи підпис, необхідно мати у своєму розпорядженні як сам документ, так і файл, що містить підпис).

***Електронний цифровий підпис*** — це засіб, що дає змогу на основі використання криптографічних методів визначити авторство і дійсність документа. При цьому електронний цифровий підпис має такі переваги:

дематеріалізація документів (незалежність ЕЦП від носія дає можливість використовувати його в електронному документообігу й установлювати договірні взаємовідносини без безпосереднього контакту між фізичними або юридичними особами);

рівнозначність копій (логічна природа ЕЦП дає змогу не розрізняти копії одного документа та зробити їх рівнозначними);

додаткова функціональність: в основі механізму ЕЦП лежить криптографія, тому ЕЦП є не тільки засобом ідентифікації, а й засобом аутентифікації документа (в електронний документ, підписаний ЕЦП, не можна внести зміни, не порушивши підпису);

автоматизація (створення, застосування, засвідчення та перевірка ЕЦП виконується із застосуванням програмних та апаратних засобів обчислювальної техніки, тому добре автоматизується);

порівнянність захисних властивостей (об'єктивна оцінка сертифікованих програмних та апаратних засобів обчислювальної техніки, призначених для створення ЕЦП (далі — засобів ЕЦП), базується на чіткому математичному аналізі, а не на гіпотезі про унікальність біометричних параметрів людини);

— масштабованість (виходячи з оцінки захисних властивостей ЕЦП, у цивільному документообігу можна використовувати найпростіші засоби ЕЦП, у службовому — сертифіковані для секретної інформації — спеціальні засоби ЕЦП).

Усі наведені властивості ЕЦП широко використовуються в електронній комерції. Однак у використанні ЕЦП є й недоліки. Хоча електронний документообіг з електронним підписом сприяє підвищенню продуктивності праці, але виводить механізм підпису з-під контролю звичайними методами (візуальними) та може створювати ілюзію благополуччя. Тому для використання ЕЦП необхідне спеціальне технічне, організаційне та правове забезпечення.

Криптографічні основи застосування електронного цифрового підпису

У подальшому застосування електронного цифрового підпису розглядатиметься в договірних відносинах між віддаленими сторонами, що не мають між собою прямого або опосередкованого контакту через матеріальні носії інформації. Цей випадок найбільш загальний і відповідає двом основним моделям електронної комерції, що розвиваються сьогодні: Виробник — Виробник і Виробник — Споживач.

Важливою проблемою договірних відносин, що відбуваються в електронній формі, є можливість відмови (repudiation) однієї зі сторін від умов угоди і/чи свого підпису. З неї випливає потреба в засобах об'єктивної ідентифікації партнерів. Якщо таких засобів немає або вони недосконалі, договірні сторони одержують можливість відмови від своїх зобов'язань, що випливають з умов договору.

Важливо мати на увазі, що за такими відмовами не обов'язково стоїть злий намір. Відмова цілком виправдана, якщо партнер установив зловживання своїми реквізитами з боку не-вповноважених осіб чи факт однобічного внесення змін у зміст договору. Такі події можливі як з боку кожного з партнерів, так і на шляхах транспортування.

Для спрощення технічної сторони питання слід перейти від використання понять договір і документ до поняття повідомлення. Це дає змогу формально підійти до розгляду документів зважаючи тільки на зміст повідомлення. Такий методологічний прийом характерний для інформатики. Далі ми будемо розглядати документи як унікальні послідовності символів. Вимога унікальності пов'язана з тим, що, коли хоча б один символ у послідовності буде якось змінено, це буде вже зовсім інший документ, не адекватний вихідному.

Ще одне припущення, яке слід зробити, стосується способу транспортування повідомлення. Будь-які види транспортування: звичайна кур'єрська, електронна або інша пошта — замінимо терміном канал зв'язку.

Для того щоб послідовність символів, тобто повідомлення, могло однозначно ідентифікувати її автора, необхідно, аби воно мало унікальні ознаки, відомі тільки його відправнику й одержувачу. З незапам'ятних часів це досягається застосуванням засобів шифрування (більш загальний термін — криптографія). Якщо обидві сторони використовують той самий метод шифрування повідомлень, відомий тільки їм, то можна сказати, що вони спілкуються в захищеному каналі, де кожна зі сторін матиме відносну впевненість у тому, що:

автором повідомлення справді є партнер (ідентифікація партнера);

повідомлення не було змінено в каналі зв'язку (аутентифікація повідомлення).

Ця впевненість відносна, тому що стороннім особам можуть стати відомі метод шифрування і його ключ.

Метод і ключ шифрування

Метод шифрування — це формальний алгоритм, що описує порядок перетворення вихідного повідомлення в результуюче. Ключ шифрування — набір параметрів (даних), необхідних для застосування методу. Є безліч методів (алгоритмів) шифрування. За історичними джерелами, Юлій Цезар для зв'язку зі своїми воєначальниками використовував метод підстановки з ключем, що дорівнював 3. У вихідному повідомленні кожен символ заміщався іншим, віддаленим від нього в алфавіті на 3 позиції

Такий метод, як і ключ шифрування, дуже простий, тому на його захищеність можна розраховувати тільки тоді, коли канал обслуговують особи (посильні), які не мають елементарної грамотності. Трохи підвищити захист можна, якщо використовувати довший ключ шифрування, наприклад: 3—5—7. У цьому випадку перший символ повідомлені! -і зміщується на три позиції, другий — на п'ять, третій — на сім позицій, після чого процес циклічно повторюється. Послідовність символів ключа можна розглядати як ключове слово. Якщо ключ містить кілька ключових слів, його називають ключовою фразою.

Коли той самий ключ використовується багаторазово для роботи з різними повідомленнями, його називають статичним, а якщо для кожного повідомлення використовується новий ключ, то — динамічним. У цьому випадку повідомлення має нести зашифровану інформацію про те, який ключ з відомого набору було у ньому використано.

Симетричні та несиметричні методи шифрування

Розглянутий вище метод підстановки — класичний приклад симетричного шифрування. Симетричність полягає в тому, що обидві сторони використовують той самий ключ. Яким ключем повідомлення шифрувалося, тим воно і дешифрується. Тому цей ключ секретний. Перевагою симетричних методів шифрування є їх достатня теоретична вивченість та висока криптостійкість, тому вони можуть використовуватися для впевненої аутентифікації повідомлень. До основних недоліків цих методів слід зарахувати додаткові заходи таємності під час поширення ключів і пов'язані з цим проблеми, можливі витрати, а також той факт, що методи з секретним ключем працюють тільки в умовах повної довіри партнерів один до одного.

Таким чином, для електронної комерції традиційні методи шифрування, що базуються на симетричних ключах, застосовувати незручно.

Лише в останні три десятиліття з'явилися й набули розвитку нові методи, що одержали назву методів несиметричної криптографії. Несиметрична криптографія використовує спеціальні математичні методи, розроблені в результаті розвитку нових галузей математики. На цих методах ґрунтується електронна комерція взагалі та програмні засоби, які отримали назву засоби ЕЦП. Після застосування одного з таких засобів утворюється пара взаємозалежних ключів, що мають унікальну властивість: те, що зашифровано одним ключем, може бути дешифровано тільки іншим, і навпаки. Власник пари ключів може залишити один ключ собі, а інший — поширити (опублікувати). Публікація відкритого ключа відбувається прямим розсиланням через незахищений канал, наприклад, електронною поштою. Зручніше виставити відкритий ключ на своєму (або орендованому) web-сервері, де його зможе одержати кожен бажаючий. Ключ, залишений для себе, називається закритим, або особистим ключем {private), а опублікований ключ — відкритим, або публічним (public).

Повідомлення (замовлення, договори тощо), котрі надсилаються власникові ключової пари, шифруються його відкритим ключем, а дешифруються за допомогою закритого. Якщо власник ключової пари захоче звернутися з повідомленням до своїх клієнтів, він зашифрує його закритим ключем, а одержувачі прочитають його за допомогою відповідного відкритого ключа.

Застосування несиметричних методів шифрування надає такі можливості.

Використання закритого ключа дає змогу ідентифікувати відправника. Під час використання несиметричного шифрування досягається можливість ідентифікації відправника. Якщо клієнт звернувся із замовленням до фірми МКС, що торгує програмними засобами, й одержав у відповідь зашифрований файл, то він може застосувати до нього відкритий ключ фірми. Якщо цей файл направила йому не фірма МКС, а невідома особа, то ключ не підійде, повідомлення не буде дешифровано і шкідливі наслідки від використання невідомого програмного забезпечення не настануть.

Використання відкритого ключа дає можливість аутентифікувати повідомлення. Якщо клієнт фірми МКС разом із замовленням указує конфіденційні дані, наприклад, про свою платіжну карту, то він може бути впевнений у тому, що ніхто сторонній цю інформацію не прочитає, тому що повідомлення, зашифроване відкритим ключем, може прочитати тільки власник закритого ключа.

Обмін відкритими ключами між партнерами уможливлює створення ними спрямованого каналу зв'язку між собою. Якщо два партнери, які ніколи раніше не зустрічалися, бажають почати листування, вони можуть зробити це, обмінявшись своїми відкритими ключами. Тоді кожний з них відправлятиме своє повідомлення, зашифрувавши його своїм закритим ключем, а партнер читатиме його відповідним відкритим ключем. При цьому одержувач повідомлення може бути впевнений у тому, що одержав листа від партнера, а не від особи, що побажала залишитися невідомою.

Подвійне послідовне шифрування спочатку своїм особистим ключем, потім відкритим ключем іншої сторони дає змогу партнерам створити захищений спрямований канал зв'язку. У попередній схемі шифрування використовується не для захисту інформації, що міститься в повідомленні, а тільки для ідентифікації відправника. Можна поєднати обидві ці функції. Для цього відправник мусить застосувати до повідомлення два ключі. Спочатку він шифрує повідомлення своїм закритим ключем, а потім те, що вийде, шифрується відкритим ключем одержувача. Той діє в зворотному порядку. Спочатку він дешифрує повідомлення своїм закритим ключем і робить його таким, що можна прочитати; потім дешифрує повідомлення відкритим ключем відправника і переконується в особі того, хто надіслав цей лист.

У найпростішому вигляді електронний цифровий підпис — це деякі відомості про себе, наприклад, прізвище, ім'я, по батькові та посада, зашифровані особистим ключем. Кожен, хто має відкритий ключ, зможе ці відомості прочитати і переконатися, хто є автором повідомлення. Таким чином, у найпростішому розумінні ЕЦП — це засіб ідентифікації відправника. Однак на практиці в ЕЦП включають не тільки відомості про відправника, а й додаткові дані.

Поняття про компрометацію ЕЦП

ЕЦП як засіб ідентифікації партнера більш надійний, ніж традиційний рукописний підпис. Однак і його можна фальсифікувати. Це може статися, коли зловмисник у той чи інший спосіб одержить доступ до закритого ключа. Тоді говорять про компрометацію закритого ключа, з якої випливає компрометація електронного підпису, створеного з його допомогою.

Закритий ключ може бути скомпрометовано традиційними і нетрадиційними способами.

Традиційні способи компрометації, як правило, пов'язані з протизаконними діями:

викрадення ключа шляхом копіювання в результаті несанкціонованого прямого фізичного або віддаленого мережного доступу до устаткування, на якому він зберігається;

одержання ключа в результаті відповіді на запит, виконаний з ознаками шахрайства чи підробки;

викрадення ключа разом з устаткуванням, на якому він зберігався (навіть, якщо викрадення устаткування здійснюється не для доступу до ключа);

викрадення ключа в результаті змови з особами, що мають право на його використання (навіть факт звільнення співробітника, який мав доступ до закритого ключа організації, теж розглядається як компрометація ключа).

Незаконність традиційних методів компрометації ключа дає змогу деякою мірою розраховувати на те, що захист ключа, хоча й опосередковано, забезпечує законодавство. На жаль, це не стосується нетрадиційних способів компрометації, що базуються на реконструкції закритого ключа за вихідними даними, отриманими легально, зокрема за відкритим ключем. Зараз довести незаконність дій щодо реконструкції чужого закритого ключа практично неможливо (принаймні поки не відбудеться подія незаконного використання реконструйованого ключа).

Передумови можливої реконструкції такі:

реконструктор має легальний доступ до відкритого ключа, а він, як відомо, пов'язаний із закритим ключем певними математичними співвідношеннями, оскільки разом вони утворюють ключову пару;

він може експериментувати не на випадкових, а на спеціально підібраних повідомленнях, підготовлених власноручно так, як йому зручно;

він має повний доступ до зашифрованих повідомлень, оскільки сам може створити їх за допомогою відкритого ключа;

йому відомий метод шифрування і дешифрування, за яким працює програмний засіб ЕЦП (у загальному випадку алгоритм не ховається, а навпаки, широко публікується для загального тестування).

Криптостійкість засобів ЕЦП

Теоретично знання методу шифрування, відкритої половини ключа, вихідного і зашифрованого текстів дають зловмисникові повну можливість реконструкції закритого ключа. На практиці процес реконструкції стикається з наявністю спеціальних апаратних і програмних засобів, а також з величезними витратами обчислювального часу.

Окрім криптографії, с криптоаналіз — наука про методи розкриття і/або підробки даних. Вона розробляє метоли, що дають змогу:

— відтворювати зашифровану інформацію, тобто знімати з

неї захист;

— оцінювати якість захисту інформації, тобто давати

об'єктивну оцінку прийнятим методам захисту.

Під час використання криптографії якість захисту визначається одночасно як методами, так і даними. Метод у цьому разі закладено в алгоритмі шифрування. Дані полягають у вихідному повідомленні та в ключі шифрування. Зашифроване повідомлення може слабко протистояти методам криптоаналізу з двох причин: у зв'язку із "слабкістю" алгоритму, що лежить в основі дії засобу ЕЦП, та характерними рисами ключа (невдалі властивості ключової пари).

До проблеми оцінки криптостійкості алгоритмів є два підходи. Перший — централізований, ґрунтується на закритості алгоритмів шифрування, і другий — децентралізований, базується на їх відкритості.

За централізованого підходу відповідальність за надійність засобів шифрування взагалі та засобів ЕЦП зокрема бере на себе держава в особі органу, уповноваженого розробляти засоби ЕЦП або давати оцінку засобам, виконаним іншими розробниками. У цьому разі захист може ґрунтуватися на "закритості" алгоритму.

З погляду держави, це найпростіший, найдешевший і легко контрольований шлях. Уповноважений адміністративний орган може зробити секретним алгоритм, що рекомендується до загального застосування, а використання інших алгоритмів законодавчо заборонити. Це, звичайно, ускладнить реконструкцію закритих ключів і підробку ЕЦП, але багато споживачів так і не знатимуть про справжні властивості захисту запропонованого ("нав'язаного") алгоритму. їм залишиться тільки довіряти адміністративному органові, що запевняє у надійності алгоритму.

У разі децентралізації алгоритм шифрування робиться відкритим. Він широко публікується і кожен може самостійно перевірити його криптостійкість. Зрозуміло, звичайний користувач не стане цього робити, але він може бути впевненим у тому, що безліч фахівців, озброєних і належною технікою, і належними методами, активно цим займаються. Якщо вони неспроможні що-небудь зробити, то на цьому етапі розвитку технології алгоритм можна вважати надійним: йому можна довіряти, поки у відкритій пресі не з'являться повідомлення про його спростування.

На практиці водночас у різних сферах можуть застосовуватися різні підходи. Одна справа — захист цивільної електронної пошти, інша — службовий і фінансовий документообіг підприємств і, нарешті, зовсім інша справа — спецзасоби, що використовуються там, де є загроза безпеці держави.

На криптостійкість ЕЦП впливають також властивості пари ключів. Ключі створюються в результаті застосування засобу ЕЦП — програмного чи апаратного забезпечення, що генерує пару ключів за запитом користувача. В основі цього засобу також лежить деякий алгоритм. Є кілька різновидів алгоритмів, за допомогою яких створюються пари ключів, однак не всі вони мають однакові властивості. Деякі, на перший погляд, бездоганні алгоритми можуть не завжди генерувати повноцінні криптостійкі ключі, причому користувач, що створив собі пару ключів за допомогою придбаного ним засобу ЕЦП, ніколи не довідається про дефекти ключа, поки не зазнає збитку внаслідок незаконного використання його ЕЦП чи втрати важливих даних.

На державному рівні можливі два підходи до забезпечення стійкості ключів, що перебувають в обігу. По-перше, можлива сертифікація засобів ЕЦП уповноваженим органом. У цьому разі засоби ЕЦП, що не пройшли експертизу, не одержують відповідного сертифіката і забороняються до застосування. Недолік цього методу в тому, що подібна сертифікація пов'язана зі значними витратами фінансів і часу. Не кожен розробник засобів ЕЦП має можливість вкласти необхідні кошти в їх сертифікацію. Проте це страхує суспільство від використання засобів ЕЦП, виконаних некваліфікованими кадрами.

Другий підхід може полягати в сертифікації не засобів ЕЦП, а конкретних ключів, створених з їх допомогою. У такому разі пару ключів (закритий і відкритий) потрібно подавати органу, що виконує сертифікацію. Він приймає рішення з огляду як на відносну криптостійкість ключів, так і на характер діяльності заявника. Те, що допустиме для малого торговельного підприємства, може бути неприйнятним для банківської структури. Недоліком такого підходу є наявність копій закритих ключів у державному органі, де їх захист від неправомочного використання (чи втрати) сумнівний.

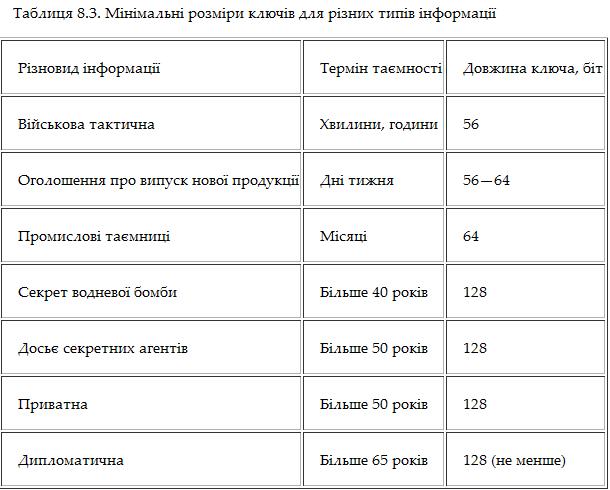
Можливі й комбіновані рішення, що поєднують сертифікацію засобів ЕЦП з сертифікацією ключів.

Вплив розміру ключів на їх криптостійкість

Цікаво, що чим досконалішими стають системи шифрування і пов'язані з ними засоби ЕЦП, тим рідше з'являються повідомлення про незаперечні шифри та "абсолютні захисти". Чим вища криптографічна культура суспільства, тим очевидніший факт, що абсолютних засобів захисту немає, і питання зняття будь-якого захисту зводиться лише до питання про технічні засоби, що використовуються, витрати часу й економічної доцільності.

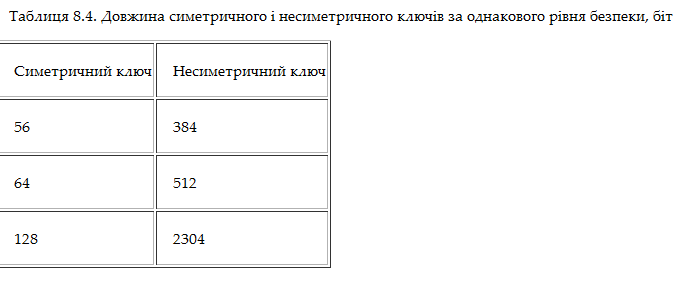
Початкових даних для реконструкції закритого ключа більше ніж досить. Якщо важко знайти оригінальні методи, що ґрунтуються на криптоаналізі, можна скористатися методом простого перебирання, який завжди веде до розв'язування завдання, хоча заздалегідь невідомо, коли це відбудеться. Тривалість реконструкції визначається, по-перше, продуктивністю використовуваної обчислювальної техніки, а по-друге, розміром ключа.

Розмір ключа вимірюється в бітах (двійкових розрядах). Чим він більший, тим, відповідно, більше часу потрібно на перебирання можливих значень, тим довше працює алгоритм. Тому вибір оптимальної довжини ключа — це питання балансу. Знов-таки воно вирішується по-різному залежно від характеру діяльності організації (табл. 8.3). Те, що необхідне для цивільного листування, не підходить для банківських організацій і тим більше не може бути застосовано в діяльності служб, пов'язаних з державною безпекою.



Криптостійкість симетричних ключів оцінюється просто. Наприклад, якщо довжина симетричного ключа становить 40 біт (таке шифрування називають слабким), то для його реконструкції треба перебрати числа. Використовуючи для цього декілька сучасних передових комп'ютерів, задачу можна розв'язати швидше, ніж за добу. Це недешевий, але цілком можливий захід. Якщо довжина ключа становить 64 біти, то необхідно мати мережу з кількох десятків спеціалізованих комп'ютерів, і задача розв'язується протягом кількох тижнів. Це вкрай дорогий захід, але технічно він можливий за сучасного рівня розвитку техніки. Сильним називають шифрування з довжиною симетричного ключа 128 біт. На будь-якому сучасному устаткуванні реконструкція такого ключа займає часу в мільйони разів більше, ніж вік Всесвіту. Це технічно неможливий захід, якщо немає яких-небудь додаткових даних, наприклад, відомостей про характерні настроювання засобу ЕЦП, що використовувався під час генерації ключа. Теоретично такі дані у "зломщика" можуть бути (наприклад, отримані агентурними методами), і тоді реконструкція навіть сильного ключа стане технічно можливою.

Для ключів несиметричного шифрування одержати таку просту формулу, як для симетричних ключів, зазвичай не вдається. Алгоритми несиметричного шифрування ще не до кінця вивчено. Тому під час використання несиметричного шифрування говорять про відносну криптостійкість ключів. Зрозуміло, що їх криптостійкість, як і для симетричних ключів, залежить від довжини (табл. 8.4), але виразити це співвідношення простою формулою для більшості алгоритмів поки що не вдалося. Звичайно відносну криптостійкість оцінюють за емпіричними даними, отриманими дослідним шляхом.



Підсумки багатовікового протистояння розробника шифру — криптограми, і його опонента — криптоаналітика, підбив голландець Керкхгофф (1835—1903), який сформулював правила цього протистояння. Основне з них полягає в тому, що під час розробки і застосування шифру треба зважати на те, що весь механізм шифрування, множина правил чи алгоритмів рано або пізно стає відомою опонентові, а стійкість шифру визначається тільки таємністю ключа, яка, у свою чергу, визначається його довжиною.

Принцип достатності захисту

Теоретична оцінка трудомісткості реконструкції дуже довгих несиметричних ключів показує неможливість розв'язання цього завдання в розумний термін, проте не слід розглядати це як привід для зайвого самозаспокоєння.

З часом може бути виявлено які-небудь нові властивості алгоритмів несиметричного шифрування, що спрощують реконструкцію закритого ключа. Змінюється і рівень розвитку техніки, і середній рівень продуктивності комп'ютерів. Тому в основі використання засобів ЕЦП лежить базовий принцип достатності шифрування, відповідно до якого:

ніякі засоби шифрування не вважаються абсолютними;

повідомлення вважається досить захищеним, якщо для його реконструкції необхідні матеріальні витрати, які значно перевищують цінність інформації, що є в повідомленні;

захист повідомлення, що вважається достатнім для сучасного стану науки і техніки, може виявитися недостатнім у найближчому майбутньому.

Таким чином, в основі принципу достатності захисту лежить принцип економічної доцільності.

Поняття про дайджест повідомлення. Електронна печатка. Хеш-функція

Дотепер ми вважали, що електронний підпис містить інформацію про автора, зашифровану за допомогою його закритого ключа. Це дає змогу власнику відкритого ключа переконатися в тому, що автором повідомлення є та особа, від імені якої воно надійшло. Разом з тим є технічна можливість включити до складу ЕЦП і дані, що характеризують саме повідомлення, щоб виключити ймовірність внесення в нього змін під час передачі каналами зв'язку. Для цього використовується поняття дайджесту повідомлення.

Дайджест повідомлення — це унікальна послідовність символів, що однозначно відповідає змісту повідомлення. Зазвичай дайджест має фіксований розмір, наприклад, 128 або 168 біт, що не залежить від довжини самого повідомлення. Дайджест вводиться до складу ЕЦП з відомостями про автора і шифрується разом з ними.

Найпростіший прийом створення дайджесту можна розглянути на прикладі контрольної суми. Оскільки кожен символ повідомлення становить числовий код (наприклад, за таблицею ASCII), то можна підсумувати всі коди послідовності й визначити числовий параметр, що відповідає такому повідомленню, назвемо його контрольною сумою. Передбачається, що у разі зміни змісту повідомлення в каналі зв'язку зміниться і контрольна сума, що буде встановлено приймаючою стороною. Про справжню контрольну суму вона довідається з підпису і, порівнявши їх, знайде стороннє втручання. Однак такий механізм не можна вважати задовільним, оскільки в ньому немає однозначної відповідності між текстом повідомлення і величиною контрольної суми. За належного старання можна виконати ряд взаємозалежних змін у повідомленні, за яких контрольна сума не зміниться. Є й інші механізми обчислення контрольних сум, але вони не можуть вважатися прийнятними. їхній основний недолік полягає в оборотності. Можна запропонувати алгоритм, що дасть змогу за відомою контрольною сумою створити нове повідомлення, яке відрізнятиметься від вихідного, але матиме таку саму контрольну суму.

Сучасній математиці відомі спеціальні функції, що не мають властивості оборотності. Вони дають можливість з однієї послідовності чисел (з одного повідомлення) одержати іншу (інше повідомлення) таким чином, що зворотне перетворення буде неможливим. Такі функції використовують у криптографії і називають хеш-функціями.

З принципом дії хеш-функцій зручно познайомитися на прикладі того, як на комп'ютерах організовано зберігання паролів. Пароль — це секретна послідовність символів, які клієнт має повідомити системі, щоб вона почала його обслуговувати. Перевірку паролів виконують шляхом їх порівняння з деякими контрольними записами, але в цьому випадку ми мали б припустити, що десь у системі зберігаються справжні паролі всіх її зареєстрованих клієнтів. Це зовсім неприйнятно з погляду безпеки. Насправді справжні паролі клієнтів спочатку обробляються хеш-функцією і тільки після такого шифрування закладаються на зберігання. Викрадені зашифровані паролі не стануть корисними зловмисникові, оскільки хеш-функція необоротна і реконструювати справжній пароль за його хеш-кодом — занадто складне завдання. Коли до системи підключається законний користувач і вводить свій пароль, то цей пароль теж обробляється хеш-функцією, після чого отриманий хеш-код порівнюється з контрольними кодами, що зберігаються в системі. Якщо збіг установлено, то пароль було введено правильно.

Схожий метод використовується і для автентифікації документів засобами ЕЦП. Вихідне повідомлення обробляється хеш-функцією, після чого утворюється деякий хеш-код. Він так само унікальний для такого повідомлення, як відбитки пальців для людини. Це і є дайджест повідомлення. Його нерідко називають відбитком, за аналогією до відбитків пальців, електронною печаткою, або штампом. Дайджест (електронна печатка) повідомлення приєднується до електронного підпису і далі є його складовою.

Приймаюча сторона розшифровує повідомлення (якщо воно було зашифровано), перевіряє електронний підпис за допомогою своєї половини ключа, потім обробляє повідомлення тією самою хеш-функцією, що й відправник, після чого звіряє отриманий дайджест із тим, що містився у підписі. Якщо дайджести збіглися, то повідомлення не було змінено в каналі зв'язку.

Таким чином, ми познайомилися з двома компонентами електронного підпису: відомостями, що вважав за потрібне подати про себе автор (власне підпис), і дайджестом повідомлення. Вони становлять два поля у форматі електронного підпису. У принципі, їх уже досить для двобічного зв'язку, але до них додається ще низка полів, пов'язаних з деякими реєстраційними й організаційними аспектами механізму електронного підпису.

**2.16) Використання паролів і механізмів контролю за доступом**

***Побудова захищених AC***

*У розділі розглянуто основні принципи та методи побудови СЗІ, деякі аспекти захисту на різних стадіях створення АС та аналізу захищеності СЗІ.*

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

* невизначеністю, яка, в свою чергу, зумовлена наявністю «людського фактора», оскільки невідомо, хто, коли, де і яким чином може порушити безпеку об'єкта захисту;
* неможливістю створення ідеальної системи захисту (СЗ), тобто може йтися тільки про той або інший ступінь забезпечення безпеки об'єктів захисту;
* використанням при організації захисту вимог мінімальності ризику та мінімальності можливих витрат;
* необхідністю організації захисту від усіх і всього.

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

**2.1. Організаційні принципи побудови СЗІ**

Серед організаційних принципів відзначимо такі:

1. **Принцип законності,** тобто додержання всіх законодавчих та нормативних актів, які мають відношення до забезпечення інформаційної безпеки. Важко переоцінити важливість цього принципу, хоча додержуватися його дуже непросто, особливо зважаючи на недосконалість та відставання від життя нашого відповідного законодавства.
2. **Принцип персональної відповідальності,** відповідно до якого кожен співробітник підприємства, фірми або їхній партнер несе персональну відповідальність за збереження режиму безпеки в рамках своїх повноважень. СЗІ має будуватися таким чином, щоб при будь-яких порушеннях було чітко відоме або хоча б мінімізоване коло осіб, що мають відношення до порушень. Це не тільки полегшує процес розслідування порушень, а також є ефективним засобом

сумлінного виконання службових обов'язків і утримання потенційних ЗЛ від несанкціонованих дій.

1. **Принцип обмеження повноважень,** який має відношення як до персоналу, так і до засобів захисту та обробки інформації; відповідно до нього, по-перше, ніхто не повинен знайомитись із конфіденційною інформацією, якщо це не потрібно для виконання його службових обов'язків; по-друге, повинна бути реалізована заборона на фізичний доступ до вразливих об'єктів для осіб, яким це не потрібно за родом їхньої діяльності; по-третє, для виконання функціональних обов'язків персоналу слід надавати мінімум будь-яких засобів.
2. **Принцип взаємодії та співпраці усіх служб АС,** спрямований на створення в АС сприятливої внутрішньої та зовнішньої атмосфери безпеки. Внутрішня атмосфера безпеки досягається довірчими відносинами між співробітниками СБ та персоналом, допоміжними заходами та стимулюванням, у тому числі і матеріальним. Діюча служба безпеки не повинна перетворюватися в засіб тотального стеження за персоналом з боку керівництва. В довірчій атмосфері набагато складніше подолати СЗІ. Створення зовнішньої атмосфери полягає в необхідності налагоджування співробітництва із зацікавленими особами та організаціями. Тобто йдеться про робочі контакти з місцевими органами влади, міліції, пожежної служби й іншими контролюючими організаціями, а також із службами безпеки сусідніх організацій - так створюються елементи колективної безпеки, що набагато підвищує її ефективність.

**2.2. Принципи реалізації СЗІ**

Реалізація СЗІ базується на принципах:

* системності та комплексності;
* централізованого управління СЗ;
* неможливості обминути захисні засоби;
* рівноміцності і рівнопотужності рубежів захисту;
* ешелонованості оборони;
* неможливості переходу до безпечного стану;
* мінімальних привілеїв;
* розподілу обов'язків;
* простоти, гнучкості та керованості;
* захисту засобів СЗ;
* неперервності захисту;
* розумної достатності;
* відкритості алгоритмів та засобів захисту;
* економічної ефективності СЗ.

Коротко пояснимо зміст наведених принципів.

**Системність та комплексність** включають необхідність урахування усіх елементів, умов і чинників, які є взаємозалежні, взаємодіють і змінюються в часі, а також є істотно значимі для розуміння і вирішення проблеми забезпечення безпеки АС. При створенні системи захисту необхідно враховувати всі слабкі, найбільш вразливі місця системи обробки інформації, а також характер, можливі об'єкти і на- прямки атак на систему з боку порушників (особливо висококваліфікованих зловмисників), шляхи проникнення в АС і НСД до інформації.

У розпорядженні фахівців з комп'ютерної безпеки є широкий спектр заходів, методів і засобів захисту комп'ютерних систем. їх комплексне і використання передбачає узгоджене застосування різнорідних засобів при побудові цілісної системи захисту, що перекриває всі відомі канали реалізації загроз і не містить слабких місць на стиках окремих її компонентів.

**Централізоване управління СЗ** необхідно планувати внаслідок наявності в будь-якій АС цілого комплексу різнорідних технічних і нетехнічних заходів і засобів захисту АС. Крім того, централізоване управління дозволяє відстежувати виконання прийнятої ПБ.

**Неможливість обминути захисні засоби** полягає в тому, що внаслі- док якісного та надійного інформаційного обстеження АС повинна бути впевненість у відсутності різного роду «обхідних шляхів» захис- них засобів.

**Рівноміцність і рівнопотужність рубежів захисту** передбачають виявлення в рубежах захисту незахищених (або слабозахищених) ділянок і планування посилення найслабкішої ланки, а також однако- вого відносного рівня захищеності кожного рубежу захисту - більш потужний захист там, де більша загроза, і менш потужний у протилежному випадку. Крім того, рівноміцність передбачає найбільш ефек- тивний розподіл захисних ресурсів по рубежах.

**Ешелонованість оборони** означає, що не слід покладатися на один захисний рубіж, яким би надійним він не здавався. За засобами фізичного захисту повинні слідувати програмно-технічні засоби, за ідентифікацією та автентифікацією - управління доступом і т. п. Засоби захисту на рівні ОС повинні забезпечувати одну з найбільш укріплених ліній оборони, оскільки ОС - це саме та частина КС, яка керує використанням усіх її ресурсів. Зовнішній захист повинен

Забезпечуватися фізичними, організаційними і правовими засобами. **Неможливість переходу до безпечного стану** передбачає, що за будь-яких обставин, в тому числі і нештатних, захисний засіб або виконує свої функції, або повністю блокує доступ. Образно кажучи,

такий стан має бути подібним до наступного: якщо в фортеці механізм під'ємного мосту ламається, то міст має залишатися в піднятому стані. **Принцип мінімальних привілеїв** наказує виділяти персоналу тільки ті права доступу, які необхідні йому для виконання службових обов'язків, зменшуючи тим самим збитки від випадкових або навми- сних некоректних дій персоналу.

**Принцип розподілу обов'язків** передбачає такий розподіл ролей *і* відповідальності, щоб лише одна людина не могла порушити ***і*** критично важливий для організації процес або створити пролом у захисті на замовлення зловмисника. Зокрема, його реалізація може попередити зловмисні або некваліфіковані дії персоналу.

**Простота** означає, що механізми захисту повинні бути інтуїтивно зрозумілі і прості у використанні. Застосування засобів захисту не повинно бути пов'язане зі знанням спеціальних мов або виконанням дій, що вимагають значних додаткових трудовитрат при звичній роботі законних користувачів, а також не повинно вимагати від користувача виконання рутинних малозрозумілих йому операцій (наприклад, запровадження декількох паролів та імен і т. п.). Крім того, простота дає можливість формально або неформально доводити коректність захисту.

Майже завжди вжиті заходи і встановлені засоби захисту, особливо в початковий період їхньої експлуатації, можуть забезпечувати як надмірний, так і недостатній рівень захисту. Природно, що для забезпечення можливості варіювання рівня захищеності засоби захисту повинні мати певну **гнучкість.** Особливо важливою ця властивість є в тих випадках, коли встановлення засобів захисту необхідно здійсню вати на працюючій системі, не порушуючи процесу її нормальногс функціонування. Крім того, зовнішні умови і вимоги з часом змінюють ся. В таких ситуаціях властивість гнучкості може врятувати власники АС від необхідності вжиття кардинальних заходів для повної заміни за собів захисту на нові. **Керованість** дозволяє перевіряти узгодженісті конфігурацій різних компонентів і здійснювати централізоване адмініс трування.

**Принцип захисту засобів СЗ** вимагає, щоб будь-який захисний захід або засіб був, у свою чергу, забезпечений захистом. При цьом; в основі принципу повинні лежати правила: «захист від усіх», «все що незрозуміле - небезпечне», «довіряй, але перевіряй».

**Неперервність захисту** означає, що захист інформації - це не разовий захід і навіть не певна сукупність проведених заходів і вста новленого засобу захисту, а безперервний цілеспрямований процес що передбачає вжиття відповідних заходів на всіх етапах життєвого циклу АС, починаючи з ранніх стадій проектування, а не тільки на етапі її експлуатації. Розробка СЗ повинна вестися паралельно з розроб кою самої АС. Це дозволить врахувати вимоги безпеки при проектуван ні архітектури і, у кінцевому рахунку, дозволить створити більш ефек тивну (як за затратами ресурсів, так і за невразливістю) захищену систему. Більшості фізичних і технічних засобів захисту для ефективно го виконання своїх функцій необхідна постійна організаційна (адмініст-ративна) підтримка (своєчасна зміна і забезпечення правильного збере ження і застосування імен, паролів, ключів шифрування, перевизначен ня повноважень і т. ін.). Перерви в роботі засобів захисту можуть бути використані ЗЛ для аналізу застосованих методів і засобів захисту; для впровадження спеціальних програмних і апаратних «закладок» *і* інших засобів подолання СЗ після відновлення її функціонування.

**Розумна достатність** передбачає, що створити абсолютно непереборну СЗ принципово неможливо - при достатній кількості часу і засобів можна перебороти будь-який захист. Однак високоефективна СЗ коштує дорого, використовує при роботі суттєву частину потужності і ресурсів КС і може створювати істотні додаткові незручності користувачам. Отже, СЗ має бути організована ефективно, тобто обсяг застосованих заходів повинен бути розумним і відповідати існуючим загрозам. **Відкритість алгоритмів** та **засобів захисту** полягає в тому, що застосовані для організації захисту методи, алгоритми та інші засоби не обов'язково мають бути засекреченими. Наприклад, відкритість алгоритму роботи СЗ не повинна давати можливість подолати її (навіть його автору). Як показує досвід, засекреченість розробок із захисту аж ніяк не підвищує рівень захищеності системи, а іноді навіть провокує підвищену увагу до неї, фактично підвищуючи ризик подолання СЗ.

**Економічна ефективність СЗ** означає, що слід вести мову тільки про деякий прийнятний рівень безпеки. Він має досягатися мінімумом витрат, тобто важливо правильно обрати той достатній рівень захисту, при якому поточні економічні витрати, ризик і розмір можливих майбутніх витрат були б прийнятними.

**2.3. Методи побудови захищених АС**

Методи побудови захищених АС умовно можна розділи-

Іти на дві групи [6]:

1) що стосуються довільного ПЗ АС: ієрархічний метод розробки; дослідження коректності і верифікація.

2) специфічні тільки для систем захисту (теорія безпечних систем). Спочатку розглянемо **ієрархічний метод розробки ПЗ АС.** Відповідно до принципу абстракції при проектуванні АС розробники можуть іти щонайменше двома шляхами: від апаратури «вгору» - до віртуальної машини, яку являє собою АС, чи від віртуальної машини «униз» - до реального устаткування. Це і є два основні методи проектування - метод знизу вгору і метод зверху вниз. Інші методи по своїй суті зводяться до цих двох чи є їх комбінацією. **Метод знизу вгору** передбачає початок проектування з основного апаратного устаткування системи. При проектуванні модулі розби-ваються на ряд шарів, причому нульовий шар віртуальної системи утворює апаратура. Шари, що реалізують одну чи кілька необхідних властивостей, додаються послідовно, поки не буде отримана бажана віртуальна машина.

До недоліків методу проектування знизу вгору відносять: • необхідність із самого початку приймати рішення про вибір способу реалізації компонентів АС - за допомогою апаратури, мікропрограм чи програм,- який зробити дуже важко; • можливість проектування АС тільки після розробки апаратури;

• розбіжність між реальною АС і визначеною в ТЗ.

При використанні **методу зверху вниз (ієрархічний метод)** виходять від віртуальної машини, що представляє АС, з необхідними властивостями і послідовно розробляють шари віртуальної системи апаратури. У цьому випадку проектування відбувається в такій послідовності. Визначається рівень абстракції опису компонентів АС вищого шару. Далі систематично проводиться аналіз того, чи достатньо визначені компоненти, щоб можна було їх реалізувати, використовуючи деякі примітивні поняття. Якщо ні, то кожна функція кожного компонента представляється функціями компонентів наступного шару, якому відповідає більш низький рівень абстракції, і знову проводиться аналіз на можливість їхньої реалізації. В ієрархічному методі доцільно використовувати структурний принцип і принцип модульного проектування.

Структурний принцип має фундаментальне значення і є основою більшості реалізацій. Відповідно до цього принципу, для побудови ПЗ вимагаються тільки три основні конструкції:

* функціональний блок;
* конструкція узагальненого циклу;

• конструкція ухвалення двоїчного рішення. Функціональний блок можна представити як окремий обчислювальний оператор чи як будь-яку іншу реальну послідовність обчислень з єдиним входом і єдиним виходом, як у підпрограмі. Організація циклу в літературі часто згадується як елемент DO-WHILE. Конструкція ухвалення двоїчного рішення називається IF-THEN-ELSE.

Зауважимо, що ці конструкції можуть самі розглядатися як функціональні блоки, оскільки вони мають тільки один вхід і однн вихід. Таким чином, можна ввести перетворення операції циклу у функціональний блок і в подальшому розглядати всякий такий оператор циклу еквівалентом (трохи більш складного) функціонального блоку. Аналогічно можна ввести перетворення конструкції ухвалення рішення до функціонального блоку. Нарешті, можна привести будь-яку послідовність функціональних елементів до одного функціонального елемента. У той же час зворотна послідовність перетворень може бути використана в процесі проектування програми за спадною схемою, тобто виходячи з єдиного функціонального блоку, що поступово розкладається в складну структуру основних елементів.

Принцип модульного проектування полягає в поділі програм на функціонально самостійні частини (модулі), що забезпечують замінність, кодифікацію, видалення і доповнення складових.

Переваги використання модульного принципу такі:

• спрощується налагодження програм, тому що обмежений доступ до модуля й однозначність його зовнішнього прояву виключають вплив помилок в інших, зв'язаних з ним, модулях на  
його функціонування;

* забезпечується можливість організації спільної роботи великих колективів розробників, тому що кожен програміст має справу з незалежною від інших частиною програми;
* підвищується якість програми, тому що відносно малий розмір модулів і, як наслідок, невелика складність їх дають змогу провести більш повну перевірку програми.

Іншою проблемою є **дослідження коректності реалізації і верифікація АС.** Під поняттям коректності чи правильності розуміється відповідність об'єкта, що перевіряється, певному еталонному об'єкту чи сукупності формалізованих еталонних характеристик і правил. Коректність ПЗ при розробці найбільш повно визначається ступенем відповідності висунутим до неї формалізованим вимогам програмної специфікації. У специфікаціях відбивається сукупність еталонних характеристик, властивостей і умов, яким повинна відповідати програма. Основну частину специфікації складають функціональні критерії і характерис- тики. Вихідною програмною специфікацією, якій повинна відповідати програма, є ТЗ. У разі відсутності такої цілком формалізованої специфікації вимог, як ТЗ, якому повинна відповідати АС і результати її функціонування, іноді використовуються неформалізовані представлення роз- робника чи користувача-замовника програм. Однак поняття корект- ності програм стосовно запитів користувача чи замовника пов'язане з невизначеністю самого еталона, якому повинна відповідати АС. Для складних програм завжди існує ризик знайти їхню некоректність (на думку користувача чи замовника) при формальній коректності щодо специфікацій унаслідок неточності самих специфікацій. Традиційний погляд на специфікацію вимог полягає в тому, що І вона являє собою документ, написаний природною мовою, що є ін-терфейсом між замовником і виготовлювачем. Хоча підготовці доку- мента може передувати деяка взаємодія, саме цей документ значною  *м*ірою виступає як «точка відліку» для виготовлювача програм. Таким чином, можна зробити висновок про те, що створення су-купності взаємопов'язаних несуперечливих специфікацій є необхідною базою для забезпечення коректності проектованої програми. При цьому специфікації повинні: • бути формальними;

•дозволяти перевіряти несуперечність і повноту вимог замовника;  
 • бути основою для подальшого формалізованого проектування ОС.  
 Існує кілька підходів до визначення специфікацій вимог.

**Специфікація як опис.** Замовник видає специфікацію, щоб виробники могли постачити його тим виробом, що він бажає, тому замов-н**ик** бачить цей документ головним чином як опис системи, яку він

бажав би мати. У принципі, в описі має бути зазначено, що повинна і Що не повинна робити система. На практиці звичайно по умовчанню передбачається, що система повинна робити те, що уточнюється в

специфікації, і не повинна робити нічого іншого. У цьому полягає головна проблема з описовою стороною специфікації. Передбачається, що замовник завжди точно знає все, що система повинна і не повинна робити. Більше того, надалі передбачається, що замовник цілком переніс це знання у специфікований документ.

**Специфікація як розпорядження.** Виробник дивиться на специфікований документ як на набір складових, що підлягають збиранню, щоб розв'язати проблему замовника. Такий директивний підхід обумовлюється не тільки труднощами створення описового документа (як зазначалося вище), а й відомостями, що навмисно чи ненавмисно розширюють чи обмежують волю виробника.

**Договірна методологія.** У рамках «опис замовника - розпорядження виробнику» специфікація розглядається як формальний поділ між сторонами. Що стосується замовника, то він обумовлює мінімально прийнятне, тоді як виготовлювач - максимально необхідне. Договір пропонується і приймається при зародженні системи і закінчується після завершення системи, коли замовник приймає систему, яка відповідає його мінімальним вимогам. Під час виготовлення системи в принципі не передбачається ніяких взаємодій, навіть якщо виробник підозрює, що наказуване не зовсім відповідає тому, що замовник бажає бачити насправді.

**Специфікація як модель.** Сучасні більш строгі уявлення про специфікацію трактують її як модель системи. За умови, що покладена в основу моделі семантика достатньою мірою обґрунтована, така специфікація забезпечує чітке формулювання вимог.

Відповідні моделі підходять також для автоматизованого контролю цілісності й іншого прогнозного аналізу, що, зокрема, забезпечить припинення розробки системи, у принципі не здатної задовольнити вимоги.

Моделі як опис системи мають такі відмітні риси порівняно з іншими способами формального опису:

* добре сполучення спадного і висхідного підходів до їхньої розробки з можливістю вибору абстрактного опису;
* можливість опису рівнобіжної, розподіленої і циклічної роботи;
* можливість вибору різних формалізованих апаратів для опису систем.

Основна перевага використання формальної моделі полягає в можливості дослідження з її допомогою особливостей системи, що моделюється. Покладаючи в основу формального методу розробки математичну модель і потім досліджуючи модель, можна виявити такі грані поводження системи, що в іншому разі не були б очевидні до більш пізніх стадій.

Оскільки цільовим об'єктом проектування є АС, то модель може описувати або саму АС, або її поводження, тобто зовнішні прояви функціонування АС. Модель, що описує поводження АС у порівнянні з моделлю АС, має одну важливу перевагу - вона може бути перевірена й

оцінена як виконавцями, так і замовниками, оскільки замовники не знають, як повинна працювати АС, але зате вони уявляють, що вона повинна робити. У результаті такого моделювання може бути перевірена коректність специфікацій щодо вихідної постановки задачі, тобто ТЗ. Крім того, критерії правильності вважаються достатніми за умови, що специфікація являє собою вичерпний опис «зовнішнього» поводження об'єкта в усіх можливих (чи запланованих) ситуаціях його використання.

Як було відзначено вище, при розробці АС, особливо її компонентів, що представляють СЗІ, для забезпечення високих гарантій відсутності несправностей і наступного доказу того, що система функціонує відповідно до вимог ТЗ, використовуються формальні підходи до її проектування.

Формальне проектування алгоритмів базується, в основному, на мовах алгоритмічних логік, що включають висловлення виду

Q{S}R,

що читається в такий спосіб: «якщо до виконання оператора S була виконана умова Q, то після нього буде R». Тут Q називається перед-

: умовою, a R - постумовою. Ці мови були винайдені практично одно-

часно Р. У. Флойдом (1967 p.), С. А. Р. Хоаром (1969 р.) і вченими

польської логічної школи (А. Сальвіцький та ін., 1970 p.). Як переду-

мова, так і постумова є предикатами.

Розгляд програм як деяких «перетворювачів предикатів» дає змо-

гу прямо визначити зв'язок між початковими і кінцевими станами без яких-небудь посилань на проміжні стани, що можуть виникнути під

час виконання програми.

Перевага представлення алгоритму у вигляді перетворювача пре-

дикатів полягає в тому, що воно дає можливість:

• аналізувати алгоритми як математичні об'єкти;

• дати формальний опис алгоритму, що дозволяє інтелектуально

охопити алгоритм;

• синтезувати алгоритми за представленими специфікаціями;

• провести формальне верифікування алгоритму, тобто довести  
 коректність його реалізації.

Методологія формальної розробки і доведення коректності в да-

ний час добре розроблена і викладена в цілому ряді робіт. Коротко

викладемо суть цих методів:

• розробка алгоритму проводиться методом послідовної деком-позиції, з розбивкою загальної задачі, розв'язуваної алгоритмом, на ряд дрібніших підзадач;

• критерієм деталізації підзадач є можливість їхньої реалізації за  
допомогою однієї конструкції чи розгалуження циклу;

• розбивка загальної задачі на підзадачі передбачає формулю-  
вання перед-і постумов для кожної підзадачі з метою їхнього  
коректного проектування і подальшої верифікації.

Для доведення коректності алгоритму (верифікація) формулюється математична теорема Q{S}R, що потім доводиться. Доведення теореми про коректність прийнято розбивати на дві частини. Одна частина служить для доведення того, що розглянутий алгоритм може завершити роботу (проводиться аналіз усіх циклів). В іншій частині доводиться коректність постумови в припущенні, що алгоритм завершує роботу.

Дуже важливим напрямком є **теорія довірених безпечних систем (ТСВ).** Поняття «довірене обчислювальне середовище» (trusted computing base - ТСВ) з'явилося у закордонній практиці забезпечення інформаційної безпеки досить давно. Зміст характеристики «довірена» можна пояснити в такий спосіб.

Дискретна природа характеристики «безпечний» (у тому сенсі, що або щось є безпечним, цілком задовольняючи ряд пропонованих вимог, або не є, якщо одна чи кілька вимог не виконані) у сполученні з твердженням «ніщо не буває безпечним на сто відсотків» підштовхують до того, щоб увести більш гнучкий термін, який дає можливість оцінювати те, наскільки розроблена захищена АС відповідає очікуванням замовників. У цьому відношенні характеристика «довірений» більш адекватно відбиває ситуацію, де оцінка, виражена цією характеристикою (безпечний чи довірений), грунтується не на думці розробників, а на сукупності факторів, включаючи думку незалежної експертизи, досвід попереднього співробітництва з розробниками, і, в остаточному підсумку, є прерогативою замовника, а не розробника.

Довірене обчислювальне середовище (ТСВ) включає сукупність усіх компонентів і механізмів захищеної АС, що відповідають за реалізацію політики безпеки. Всі інші частини АС, а також її замовник покладаються на те, що ТСВ коректно реалізує задану політику безпеки навіть у тому випадку, якщо окремі модулі чи підсистеми АС розроблені висококваліфікованими ЗЛ для того, щоб втрутитися у функціонування ТСВ і порушити підтримувану нею політику безпеки.

Мінімальний набір компонентів, що утворюють довірене обчислювальне середовище, забезпечує такі функціональні можливості:

* взаємодію з апаратним забезпеченням АС;
* захист пам'яті;
* функції файлового виведення-введення-висновку;
* керування процесами.

Доповнення і модернізація існуючих компонентів АС з урахуванням вимог безпеки можуть призвести до ускладнення процесів супроводу і документування. З іншого боку, реалізація всіх перелічених функціональних можливостей у рамках централізованого довіреного обчислювального середовища в повному обсязі може викликати розростання розмірів ТСВ і, як наслідок, ускладнення доведення коректності реалізації політики безпеки. Так, операції з файлами можуть бути реалізовані в ТСВ у деякому обмеженому обсязі, достатньому для підтримки політики безпеки, а розширене введення-виведення у

такому випадку реалізується в тій частині АС, що перебуває за межами ТСВ. Крім того, необхідність упровадження пов'язаних з безпекою функцій у багато компонентів АС, які реалізовані в різних модулях АС, призводить до того, що захисні функції розподіляються по всій АС, викликаючи аналогічну проблему.

**2.4. Передпроектні аспекти створення СЗІ**

У процесі проектування захищеної АС необхідно проектувати і СЗІ, причому потрібно враховувати два основні параметри: стан АС і рівень витрат на створення АС. Щодо стану АС, то слід зазначити, що під станами АС маються на увазі такі ситуації: АС уже функціонує, є готовий проект, система тільки проектується. Витрати ж можна задавати або поки що вважати їх необмеженими. Таким чином, глобальне завдання створення СЗІ - це створення оптимальних механізмів захисту і управління ними. Цю загальну мету можна ви-разити у вигляді послідовності наступних дій або концепції захисту:

* аналіз цілей і умов проектування;
* обґрунтування вимог до ЗІ; • вибір варіанта проекту;

• реалізація варіанта проекту.

Як обґрунтувати вимоги до ЗІ? Тут слід зазначити, що формаль- них методів розв'язання цієї задачі не існує і її доводиться розв'язу- вати неформально, у вигляді деяких рекомендацій, пропозицій і т. п., ; які формуються на основі наведених вище принципів. Складно, користуючись лише інженерною інтуїцією, одержати оптимальні проектні рішення. Часто доводиться залучати досить **і** складні наукові методи, що вимагають розробки і застосування комп'ютерних систем.

Нижче розглядається приклад можливої послідовності дій щодо створення захищеної АС [27].

Отже, загальні цілі і задачі для даного об'єкта звичайно визначаються в процесі діалогу замовника і проектанта. У ході розробки проекту вони постійно будуть уточнюватися, тобто в процесі спільної роботи підвищується взаєморозуміння замовника і проектанта і шукається розумний компроміс.

На передпроектних стадіях робіт зі створення АС повинні бути вирішені два такі основні завдання:

• сформульовано вимоги до забезпечення режиму ІБ при реалізації функцій і задач проектованої АС;

•розроблено концепцію політики ІБ.

Важливо відзначити те, що вимоги формулюються щодо задач і функцій у термінах:

•доступності (період недоступності, час доступу, інші показни-  
 ки, обумовлені предметною областю);

* цілісності (показники надійності збереження, доставки);
* конфіденційності (градації конфіденційності чи грифів таємності). Розробка концепції політики ІБ відбувається на етапі «Розробка варіантів концепції АС і вибір варіанта концепції АС» після вибору варіанта концепції створюваної АС і здійснюється на основі аналізу таких груп факторів:
* правові і договірні вимоги;
* вимоги до забезпечення режиму ГБ щодо функцій і задач АС;
* загрози (класи ризиків), яким піддаються інформаційні ресурси. У результаті аналізу формулюються загальні положення ІБ, що стосуються організації в цілому:
* цілі і пріоритети, які має організація в області ІБ;
* загальні напрямки в досягненні цих цілей;

• аспекти програми ІБ, що повинні зважуватися на рівні організації в цілому;

• посадові особи, відповідальні за реалізацію програми ІБ.  
Розробку самої політики ІБ варто здійснювати на стадії «Технічне завдання» і при цьому виконати такі етапи:

* аналіз ризиків;
* визначення вимог до засобів захисту;
* вибір основних рішень щодо забезпечення режиму ІБ;
* розробка планів забезпечення безперебійної роботи організації;
* документальне оформлення політики ІБ. Розглянемо один за одним зазначені етапи.

Аналіз ризиків передбачає вивчення і систематизацію загроз ІБ, визначення вимог до засобів забезпечення ІБ. Вивчення і систематизація загроз ІБ передбачає такі етапи:

1. **Вибір елементів АС і інформаційні ресурси, для яких буде застосовано аналіз.** Повинні бути обрані критичні елементи АС і критичні інформаційні ресурси, що можуть бути об'єктами атаки чи самі є потенційним джерелом порушення режиму ІБ.
2. **Ідентифікація загроз і формування їх списку.** Формується детальний список загроз, складається матриця загрози/елементи АС чи інформаційні ресурси. До кожного елемента матриці потрібно скласти опис можливого впливу загрози на відповідний елемент АС чи інформаційний ресурс. У процесі складання матриці уточнюється список загроз і виділених елементів.
3. **Розробка методології оцінки ризику.** Повинні бути отримані оцінки гранично припустимого й існуючого ризику здійснення загрози протягом деякого часу. В ідеалі для кожної із загроз має бути отримане значення ймовірності її здійснення протягом деякого часу. Це допоможе співвіднести оцінку можливого збитку з витратами на захист. На практиці для більшості загроз неможливо одержати достовірні дані про ймовірність реалізації загрози і доводиться обмежуватися якісними оцінками.
4. **Оцінка збитку, пов'язаного з реалізацією загроз.** Здійснюється оцінка збитку, що може завдати діяльності організації реалізація загроз безпеки, з урахуванням можливих наслідків порушення конфіденційності, цілісності і доступності інформації.
5. **Оцінка витрат на заходи, пов'язані із захистом і залишковим ризиком.** Здійснюється попередня оцінка прямих витрат по кожному заходу без урахування витрат на заходи комплексного характеру.
6. **Аналіз вартість/ефективність.** Витрати на систему захисту інформації необхідно співвіднести з цінністю інформації, що захищається, й інших інформаційних ресурсів, що піддаються ризику, а також зі збитком, який може бути завдано організації внаслідок реалізації загроз. У результаті аналізу уточнюються припустимі залишкові ризики і витрати на заходи, пов'язані із захистом інформації.
7. **Підсумковий документ.** За результатами проведеної роботи складається документ, що містить:

* переліки загроз ІБ, оцінки ризиків і рекомендації для зниження ймовірності їхнього виникнення;
* захисні заходи, що необхідні для нейтралізації загроз;
* аналіз вартість/ефективність, на підставі якого робляться висновки про припустимі рівні залишкового ризику і доцільність застосування конкретних варіантів захисту.

При визначенні вимог до засобів захисту вихідними даними є:

* аналіз функцій і задач АС;
* аналіз ризиків.

На основі цих даних обирається профіль захисту (клас захищеності АС від НСД) і у разі потреби в технічному завданні формулюються додаткові вимоги, специфічні (пов'язані, наприклад, зі специфікою ІБ у сучасних розподілених АС) для даної АС.

Для всіх функцій і задач АС потрібно дати визначення відповідних функцій безпеки. Функції безпеки з однаковими назвами можуть мати різні визначення для різних функцій і задач АС.

Потім визначаються механізми безпеки, що реалізують ці функції. Як відомо, основні механізми ІБ такі:

* керування доступом до інформації;
* ідентифікація й автентифікація;
* криптографія;
* екранування;
* забезпечення цілісності і доступності даних;
* підтримка працездатності АС при збоях, аваріях, НП;
* відстеження подій, що становлять загрозу ІБ;
* керування доступом в АС;
* протоколювання дій і подій.

Вибір основних рішень щодо забезпечення режиму ІБ повинен бути розглянутий на трьох рівнях:

* адміністративному (система підтримки керівництвом організації робіт із забезпечення ІБ);
* організаційному (конкретні організаційні заходи щодо забезпечення режиму ІБ);
* технічному (реалізація механізмів захисту програмно-технічними засобами).

**2.5. Забезпечення режиму ІБ на подальших стадіях створення АС**

Подальшими стадіями створення АС є «Ескізний проект» і «Технічний проект». На цих стадіях повинні бути розроблені проектні рішення, що реалізують механізми ІБ. Проектні рішення мають включати розділи:

* основні технічні рішення по системі в цілому;
* опис автоматизованих функцій і задач;
* основні технічні рішення за видами забезпечення;
* заходи щодо підготовки об'єкта автоматизації до введення системи в дію.

У процесі **підготовки до експлуатації** АС повинні бути вирішені питання навчання користувачів і персоналу, організації фізичного захисту і контролю за дотриманням режиму ІБ, організації доступу користувачів до роботи в АС.

Користувачів і персонал мають навчити дотриманню режиму ІБ, правильному поводженню з інформаційними ресурсами. Вони повинні знати про загрози порушення режиму ІБ і мати необхідні навички для роботи в АС. Рекомендується затвердити права й обмеження на доступ користувачам у письмовій формі.

Для організації фізичного захисту і контролю за дотриманням режиму ІБ повинні бути розглянуті такі питання.

1. **Контроль доступу в приміщення.** Контроль доступу в приміщення і загальні заходи для захисту устаткування є складовою заходів для забезпечення ІБ. Устаткування, критично важливі чи вразливі елементи системи, повинні бути розміщені в захищених ділянках, обмежених периметром безпеки, з належним контролем доступу в приміщення. Для зменшення ризику НСД чи ушкодження документації і носіїв інформації рекомендується задати правила використання робочого столу.
2. **Забезпечення конфіденційності.** Користувачі інформаційних ресурсів організації повинні підписати зобов'язання про збереження конфіденційності (нерозголошення). Особливу увагу варто приділити процедурі надання доступу до інформаційних ресурсів користувачам зі сторонніх організацій. Для цього повинні бути розроблені спеціальні правила.
3. **Журнали реєстрації подій.** Необхідно підготувати журнал реєстрації виконуваних завдань, що будуть вести оператори АС.

**4.Забезпечення захисту документації по АС.** Документація по АС може містити опис прикладних процесів, структур даних і процесів підтвердження повноважень. У цьому випадку вона повинна бути за  
хищена від НСД. Рекомендується застосовувати такі засоби контролю:

* список осіб із правом доступу до документації повинен бути максимально обмежений, а дозвіл на її використання має видаватися власником додатка;
* друковані матеріали, створювані в процесі роботи АС, які стосуються документації, варто зберігати окремо від інших матеріалів і поширювати на них правила обмеження доступу.

**5.Доступ до носіїв інформації і їхній захист.** Необхідно організувати контроль доступу до носіїв інформації і забезпечити їхній фізичний захист. Для доступу до носіїв інформації з конфіденційною  
інформацією необхідно мати затверджені правила. При організації системи доступу слід враховувати таке:

* система ідентифікації носіїв повинна бути така, щоб за мітками, використовуваними для ідентифікації носіїв, не можна було визначити, яка саме інформація зберігається;
* необхідно вчасно стирати вміст повторно використовуваних носіїв інформації, якщо вони більше не потрібні;
* винесення носіїв інформації зі сховища необхідно фіксувати в контрольному журналі;
* збереження всіх носіїв інформації в надійному, захищеному місці відповідно до інструкцій.

На етапі **підготовчої роботи з організації доступу** в АС рекомендується розглянути такі питання.

**1.Реєстрація користувачів.** Повинні існувати документи з описом доступних користувачу сервісів, допустимих правил роботи в АС **і** правил забезпечення режиму ІБ. Сервіси АС не повинні надавати  
доступ, поки не будуть закінчені процедури визначення повноважень.  
Для керування доступом до багатокористувацьких сервісів має бути розроблена процедура реєстрації користувачів. Ця процедура повинна:

* перевіряти, чи надано користувачеві дозвіл на використання сервісу відповідальним за його використання;
* вести облік усіх зареєстрованих осіб, що використовують АС;
* перевіряти, чи достатній рівень доступу користувача до системи і чи не суперечить він політиці безпеки, прийнятій в організації, наприклад, чи не компрометує він принцип поділу обов'язків;
* вчасно вилучати права доступу в користувачів, що залишили організацію;
* періодично перевіряти і видаляти застарілі ідентифікатори й облікові записи, що більше не потрібні.

**2.Керування привілеями.** Використання спеціальних привілеїв варто обмежити і контролювати, оскільки це один з основних факторів, Що сприяють порушенню режиму ІБ. У багатокористувацьких АС повинна існувати система контролю надання привілеїв. При організації такої системи рекомендується:

* ідентифікувати привілеї, пов'язані з кожним програмним продуктом чи сервісом, підтримуваним системою, а також категорії співробітників, яким їх необхідно надати;
* надавати привілеї окремим особам тільки у випадку крайньої необхідності і залежно від ситуації, тобто тільки коли вони потрібні для виконання ними своїх функцій;
* реалізувати автоматичний процес визначення повноважень і вести облік усіх наданих привілеїв;
* по можливості використовувати системні програми, для яких немає необхідності надавати спеціальні привілеї користувачам;
* користувачі, що мають великі привілеї для спеціальних цілей, повинні використовувати інший ідентифікатор користувача для звичайної роботи.

**3.Керування паролями користувачів.** Надання паролів необхідно контролювати. Зразкові вимоги до системи контролю повинні бути такими:

* зобов'язати користувачів зберігати персональні паролі і паролі робочих груп у секреті;
* коли користувачі повинні самі вибирати свої паролі, видати їм надійні тимчасові паролі, що вони зобов'язані негайно замінити. Тимчасові паролі також видаються у випадку, коли користувачі забувають свої паролі;
* передавати тимчасові паролі користувачам надійним способом. Варто уникати передачі паролів через посередників чи за допомогою незахищених (незашифрованих) повідомлень електронної пошти. Користувачі повинні підтвердити одержання паролів.

**4.Перегляд прав доступу користувачів.** Для забезпечення ефективного контролю за дотриманням режиму ІБ необхідно організувати процес перегляду прав доступу користувачів через регулярні проміжки  
часу. Такий процес має забезпечувати:

* перегляд повноважень доступу користувачів через регулярні проміжки часу (наприклад, 6 місяців);
* перегляд дозволу на надання спеціальних привілейованих прав доступу через більш короткі проміжки часу (наприклад, 3 місяці).

Підтримка режиму ІБ **при експлуатації** АС вимагає постійного контролю за реалізацією політики ІБ. Основними напрямками є контроль за роботою користувачів, захист цілісності даних і програм, керування доступом до додатків.

Контроль за роботою користувачів включає такі аспекти:

* керування доступом до робочих місць в АС;
* контроль за використанням паролів;
* контроль за устаткуванням, залишеним без нагляду;
* відстеження часу простою терміналів;
* обмеження доступу до сервісів.

Користувачі повинні знати свої обов'язки щодо забезпечення контролю доступу, особливо що стосується використання паролів. Доступ користувача до ресурсів АС повинен надаватися відповідно до політики керування доступом. Зокрема, рекомендується надати користувачам тільки прямий доступ до сервісів, використання яких їм дозволено. Особливу увагу адміністраторам безпеки слід приділяти контролю мережних підключень до конфіденційних чи критично важливих додатків, а також контролю за роботою користувачів у зонах підвищеного ризику, наприклад, у загальнодоступних місцях, що знаходяться поза організацією. Слід контролювати такі аспекти.

**1. Керування доступом до робочих місць в АС.** Доступ до робочих місць в АС слід надавати тільки зареєстрованим користувачам.  
Системи керування доступом повинні забезпечувати:

* ідентифікацію й автентифікацію користувачів, а також при необхідності термінала і місцезнаходження кожного зареєстрованого користувача;
* ведення журналу обліку спроб доступу (успішних і невдалих) до АС;
* у разі потреби обмежувати підключення користувачів у неви-значений час.

**2.Використання паролів.** Користувачі повинні слідувати встановленим процедурам підтримки режиму ІБ при виборі і використанні паролів. Пропонуються такі рекомендації з вибору і використання паролів:

* рекомендується вибирати паролі, що містять не менше як шість символів;
* при виборі паролів не слід використовувати: місяці року, дні тижня і т. п., прізвища, ініціали, реєстраційні номери автомобілів; назви й ідентифікатори організацій; номери телефонів чи групи символів, що складаються з одних цифр; більш як два однакових символи, що слідують один за одним; групи символів, що складаються з одних цифр чи одних букв;
* змінювати паролі через регулярні проміжки часу (приблизно через місяць) і уникати повторного чи «циклічного» використання старих паролів;
* частіше змінювати паролі для привілейованих системних ресурсів, наприклад, паролі доступу до певних системних утиліт;
* змінювати тимчасові паролі при першому вході в системи;
* не включати паролі в процедури автоматичного входу в системи, наприклад у макроси чи функціональні клавіші;
* не допускати використання одного пароля кількома користувачами;
* забезпечувати збереження паролів у секреті;
* змінювати паролі кожного разу, коли є ознаки можливої компрометації паролів;

• якщо користувачам необхідний доступ до кількох сервісів, за

хи­ще­них паролями, то їм рекомендується використовувати один надійний пароль.

**3.Користувацьке устаткування, залишене без нагляду.** Користувачі повинні забезпечити належний захист устаткування, залишеного без нагляду. Устаткування, встановлене на робочих місцях користувачів  
(наприклад, робочі станції чи файлові сервери), може потребувати організації захисту від НСД. Користувачі повинні знати процедури захисту устаткування, залишеного без нагляду, а також свої обов'язки із забезпечення такого захисту.

Пропонуються такі рекомендації:

* завершувати сеанси зв'язку по закінченні роботи, якщо їх не можна захистити за допомогою відповідного блокування;
* використовувати логічне відключення від серверів по закінченні сеансу зв'язку, не обмежуватися тільки вимиканням ПК чи термінала;
* захищати невикористовувані ПК чи термінали шляхом блокування ключем чи іншим засобом контролю доступу.

1. **Відстеження часу простою терміналів.** Для недіючих терміналів у зонах з підвищеним ризиком порушення ІБ (у загальнодоступних місцях чи місцях, що знаходяться поза межами досяжності адміністраторів безпеки організації) необхідно встановити допустимий час простою для запобігання доступу незареєстрованих користувачів. Після закінчення цього часу екран термінала має очищатися, а сеанси зв'язку з додатками і мережними сервісами завершуватися. Допустимий час простою повинен задаватися виходячи з аналізу ризику НСД до користувацького термінала.
2. **Обмеження періоду підключення.** Додатковий захист сервісів від НСД можна забезпечити за допомогою обмеження допустимого періоду підключення. Обмеження дозволеного періоду підключення термінала до АС дає змогу зменшити імовірність НСД до ресурсів АС. Можливість застосування такого засобу контролю варто розглянути для АС з терміналами, встановленими в зонах підвищеного ризику порушення ІБ (у загальнодоступних місцях чи місцях, що знаходяться поза межами досяжності адміністраторів безпеки). Прикладами таких обмежень є:

* використання визначених інтервалів часу дозволеного доступу, наприклад, для пакетної передачі файлів, регулярних чи інтерактивних сеансів зв'язку невеликої тривалості;
* обмеження часу підключення звичайних годин роботи організації і одержання спеціального дозволу для роботи в понаднормовий час.

**6.Обмеження доступу до сервісів.** Користувачам і обслуговуючому персоналу АС слід надавати доступ до сервісів відповідно до прийнятої політики керування доступом до інформації. Рекомендується розглянути можливість використання таких засобів контролю:

* доступ до додатків (сервісів) через систему меню, що забезпечує контроль повноважень доступу користувачів;
* обмеження доступу користувачів до інформації про структури даних і функції АС, доступ до яких їм не дозволено, за допомогою відповідного редагування документації користувачів;
* контроль за вихідною інформацією додатків на предмет наявності в них конфіденційної інформації. Така інформація повинна надсилатися тільки на визначені термінали і комп'ютери. Повинен проводитися періодичний аналіз вихідної інформації і за потреби зайва інформація повинна вилучатися.

Адміністратори АС і користувачі повинні бути завжди готові до можливості проникнення шкідливого ПЗ в АС і вживати заходів для виявлення його впровадження та ліквідації наслідків його атак.

В основі захисту від вірусів повинні лежати знання і розуміння правил безпеки, належні засоби керування доступом до систем. Зокрема:

* організація повинна проводити політику, що вимагає установки тільки ліцензованого ПЗ;
* противірусні програмні засоби повинні регулярно обновлятися і використовуватися для профілактичних перевірок (бажано щоденних);
* необхідно проводити регулярну перевірку цілісності критично важливих програм і даних. Наявність зайвих файлів і слідів несанкціонованого внесення змін повинні бути зареєстровані в журналі і розслідувані;
* дискети невідомого походження слід перевіряти на наявність вірусів до їхнього використання;
* необхідно суворо дотримуватися встановлених процедур повідомлення про випадки ураження АС комп'ютерними вірусами і вживання заходів з ліквідації наслідків їхньвго проникнення;
* слід мати плани забезпечення безперебійної роботи організації для випадків вірусного зараження, у тому числі плани резервного копіювання всіх необхідних даних і програм і їхнього відновлення. Ці заходи особливо важливі для мережних файлових серверів, що підтримують велику кількість робочих станцій.

Крім того, розглянемо особливості керування доступом до сервісів.

**1. Електронна пошта.** В організації повинні бути задані чіткі правила, що стосуються статусу і використання електронної пошти. Для зменшення ризику порушення ІБ, пов'язаного із застосуванням

електронної пошти, рекомендується:  
 • враховувати вразливість електронних повідомлень стосовно

несанкціонованого перехоплення і модифікації;

• враховувати можливість неправильної адресації чи направлен-

ня повідомлень не за призначенням, а також надійність і

. доступність сервісу в цілому.

**2. Системи електронного документообігу.** При використанні систем електронного документообігу слід взяти до уваги виконання вимог ІБ:

* необхідність виключення деяких категорій конфіденційної інформації у випадку, якщо в даній системі не забезпечується належний рівень захисту;
* необхідність визначення правил і засобів контролю для адміністрування колективно використовуваної інформації, наприклад використання електронних дощок оголошень;
* використання засобів обмеження доступу до інформації, що належить різним робочим групам;
* визначити категорії персоналу і представників сторонніх організацій, яким дозволено використовувати систему, і місця, з яких можна одержати доступ до неї.

**3. Керування доступом до додатків.** Для запобігання несанкціонованому доступу до інформації в АС необхідно використовувати логічні засоби контролю доступу. Логічний доступ до додатків варто надавати тільки зареєстрованим користувачам. Додатки повинні:

* контролювати доступ користувачів до даних і додатків відповідно до політики керування доступом, прийнятої в організації;
* забезпечувати захист від НСД до системних програм, що здатні обійти засоби контролю і забезпечують можливість НСД;
* не порушувати захисту інших систем, з якими вони розділяють інформаційні ресурси.

**4. Використання системних програм.** В АС можуть використовуватися системні програми, здатні обійти засоби контролю ОС і додатків. Необхідно обмежити і ретельно контролювати використан  
ня таких системних утиліт. Рекомендується використовувати такі  
засоби контролю (по можливості):

* захист системних утиліт за допомогою паролів;
* ізоляція системних утиліт від прикладного ПЗ;
* надання доступу до системних утиліт мінімальному числу користувачів;
* надання спеціального дозволу на використання системних утиліт;
* обмеження доступності системних утиліт, наприклад, часом внесення санкціонованої зміни;
* реєстрація усіх випадків використання системних утиліт;
* визначення і документування рівнів повноважень доступу до системних утиліт;
* видалення всіх непотрібних утиліт і системних програм.

**5. Керування доступом до бібліотек вихідних текстів програм.**Для зведення ризику ушкодження ПЗ до мінімуму необхідно здійснювати суворий контроль за доступом до бібліотек вихідних текстів програм. Рекомендується дотримуватися таких правил:

• не зберігати бібліотеки вихідних текстів програм в АС;

* призначити відповідального за збереження бібліотеки вихідних текстів програм;
* роздруківки програм слід зберігати в бібліотеках вихідних текстів;
* обмежити доступ до бібліотек вихідних текстів програм;
* не зберігати розроблювані програми в бібліотеках вихідних текстів робочих програм;
* відновлення бібліотек вихідних текстів програм і видача текстів програм програмістам повинні виконуватися тільки призначеним відповідальним співробітником після одержання дозволу на доступ до додатка у встановленій формі;
* необхідно фіксувати всі випадки доступу до бібліотек вихідних текстів програм у контрольному журналі;
* застарілі версії вихідних текстів програм слід архівувати із зазначенням дати закінчення їхнього використання разом із усім допоміжним програмним забезпеченням і інформацією про організацію виконання завдань для цієї версії ПЗ;
* супровід і копіювання бібліотек вихідних текстів програм необхідно здійснювати відповідно до процедур керування процесом внесення змін.

**6. Ізоляція вразливих місць у захисті АС.** При наявності вразливих місць у захисті АС може знадобитися організація виділеного (ізольованого) обчислювального середовища. Можливе застосування  
інших спеціальних заходів: запуск додатка на виділеному комп'ютері чи поділ ресурсів тільки з надійними прикладними системами. У загаль ному випадку рекомендується дотримуватись таких правил:

* вразливі місця в АС повинні бути явно визначені і задокументовані;
* коли вразливий додаток запускається в колективно використовуваному середовищі, необхідно явно вказати прикладні процеси, з якими він може працювати одночасно.

**7. Відстеження подій, що становлять загрозу ІБ.** Для виявлення несанкціонованих дій і забезпечення відповідності політиці керування доступом рекомендується дотримуватись встановлених правил.

**8. Реєстрація подій.** Усі надзвичайні ситуації і події, що пов'язані **з** порушенням режиму ІБ, необхідно реєструвати в журналі. Журнал слід зберігати протягом заданого проміжку часу. Крім невдалих спроб входу в систему, доцільно також реєструвати випадки успіш- ного доступу. Контрольний журнал повинен включати таке:

* ідентифікатори користувачів;
* дата і час входу і виходу із системи;

• ідентифікатор чи місцезнаходження термінала (по можливості).  
**9. Спостереження за використанням сервісів.** Необхідно вста  
новити процедури спостереження за використанням сервісів АС.  
Користувачі повинні використовувати тільки явно дозволені сервіси.

Рівень контролю слід визначити за допомогою оцінки ризиків. Рекомендується стежити за такими подіями:

* невдалі спроби доступу в АС;
* спроби несанкціонованого використання відновлених користувацьких ідентифікаторів;
* використання ресурсів із привілейованим доступом;
* окремі дії, потенційно небезпечні з погляду порушення режиму ІБ;
* використання конфіденційних ресурсів.

Усі дії, що пов'язані зі спостереженням і реєстрацією, повинні бути формально дозволені керівництвом.

**10. Синхронізація системних годинників.** Для забезпечення точності контрольних журналів важливо правильно встановити системний годинник і вчасно коригувати його у випадку значного відхилення.

**2.6. Аналіз захищеності інформації в СЗІ**

При створенні більшості АС виникає необхідність розв'язувати задачу розробки АС з мінімальною вартістю. Вартість створення подібних систем практично найчастіше пропорційна ступеню використання колективних ресурсів. Це означає, що з метою мінімізації вартості АС доцільно створювати колективний ресурс для всіх її користувачів - юридичних і фізичних осіб, 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 й експлуатації АС при реалізації заданих вимог до її функціонування [1,2].

Проте зберігання і обробка інформації з використанням можливостей колективного ресурсу не означає, що кожному користувачу АС доступні ці можливості. Доступність визначається правилами, що формулюються при створенні АС.

Однак першим все ж є питання: потрібен захист інформації в системі взагалі чи ні. Тільки потім виникає друга задача - визначити величину витрат на захист. Звичайно, для вирішення цих питань розроблено чимало методів, методик і навіть програмних продуктів. Нижче розглядається один з можливих підходів.

Отже, рішення про необхідність захисту приймається на основі оцінок за двома напрямками:

1. наявність конфіденційної інформації і небезпека її витоку;
2. економічна необхідність (доцільність) захисту конфіденційної інформації.

Розглянемо метод, призначений для проведення загальної і часткової оцінок, що дозволяють керівникові організації (фірми) прийняти обґрунтоване рішення про необхідність захисту конфіденційної інформації, що циркулює усередині організації (фірми), від конкурентів з

оцінкою майбутніх витрат на захист. Цей підхід допомагає швидко і досить об'єктивно провести експрес-оцінку необхідності захисту конфіденційної інформації і на її основі оперативно прийняти відповідне рішення, тобто він дозволяє керівнику уникнути великих комерційних невдач і втрат прибутку через доступність інформації конкурентам без тривалого шляху навчання на власних помилках і втратах.

Рішення про необхідність захисту конфіденційної інформації, що циркулює усередині фірми, повинно прийматися керівництвом організації (фірми), й у першу чергу її засновником. Ніхто не зацікавлений такою мірою в захисті секретів фірми і ніхто так не знає усієї сукупності циркулюючої на фірмі інформації, її ступеня таємності, внутрішньої і зовнішньої обстановки, як її засновник.

Отже, перша частина методу дає змогу на основі обробки результатів анкетного опитування принципово відповісти на запитання, потрібно чи не потрібно захищати інформацію, що циркулює на фірмі, а друга частина, у випадку позитивного вирішення першого питання, допомагає приблизно оцінити витрати на майбутній ЗІ.

З огляду на зацікавленість, компетентність і кругозір засновника фірми, запропонований метод максимально враховує знання, досвід і думку самого засновника фірми. В основу першої частини методу покладено анкетне опитування з наступною обробкою його результатів.

Для реалізації даного методу розроблено перелік анкетних питань для засновника фірми, що охоплює всі сторони діяльності фірми, пов'язані з циркулюючої на ній інформацією.

Питання анкети сформульовано таким чином, що вони не вимагають великих відповідей, а зводяться до односкладових відповідей «так», «ні». Заповнення анкети не вимагає спеціальної підготовки у сфері ЗІ і не викликає труднощів та великих часових витрат. Спеціальні знання щодо ЗІ враховані при розробці анкетних питань і при наступній обробці результатів опитування за участю фахівців із ЗІ.

Кількісна оцінка про стан і необхідність додаткового захисту отримується шляхом математичної обробки відповідей на анкетні питання. З цією метою кожному питанню анкети поставлена у відповідність вагова величина, що чисельно виражає частковий внесок змісту питання в загальну систему захисту конфіденційної інформації. Значення вагових коефіцієнтів отримані експертним методом заздалегідь.

При обробці результатів анкетного опитування можна одержати як загальну оцінку стану захисту на фірмі, так і ряд часткових оцінок за напрямками захисту. Сукупність усіх оцінок допомагає керівнику в кінцевому рахунку прийняти рішення про необхідність організації захисту шляхом проведення режимних, організаційних і технічних заходів.

На основі аналізу оцінок кожної складової захисту виявляються ті її ланки, де ЗІ не забезпечений й імовірність її перехоплення конкурентом (витік) неприпустимо висока. Провівши такий аналіз, керівник

фірми може цілеспрямовано проводити роботи з усунення витоку інформації за виявленими напрямками.

Як приклад розглянемо анкету, що використовувалася для вирішення питання необхідності захисту інформації у вищих навчальних закладах.

Порядок проведення оцінок першої частини методики є таким. На першому етапі зацікавлена в ЗІ сторона в особі засновника (керівника) фірми заповнює анкету, відповідаючи на її питання, наведені в табл. 5. Відповіді на питання анкети у формі «так» чи «ні» заносяться у графу 3 проти відповідних питань.

*Таблиця 5*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№** | **Питання анкети** | **Часткові коефіцієнти** | | **Відповіді**  **«так» або «ні»** | **Часткові суми**  **коефіцієнтів** | **Загальна сума коефіцієнтів** |
| **для загальних оцінок** | **для часткових оцінок** |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** |
| ***Рівень конкуренції*** | | | | | | |
| **1** | **1) чи конкурентоспроможне Ваше навчання на внутрішньому ринку?** | **3,5** | **35** |  |  |  |
| **2) чи конкурентоспроможне Ваше навчання на зовнішньому ринку?** | **5,0** | **50** |  |  |  |
| **3) чи є монопольним Ваше навчання на внутрішньому ринку?** | **1,5** | **15** |  |  |  |
| ***Ступінь конфіденційності інформації, яка циркулює в закладі*** | | | | | | |
| **2** | **1) чи є інформація, призначена тільки особам верхньої ланки управління?** | **11,0** | **55** |  |  |  |
| **2) чи є інформація, призначена обмеженому колу осіб, які виконують конкретні операції та завдання?** | **5,0** | **25** |  |  |  |
| **3) чи є інформація обмеженої доступності тільки працівникам закладу?** | **4,0** | **20** |  |  |  |
| **4) чи є інформація, призначена тільки замовникам та студентам?** | **2,0** | **10** |  |  |  |
| **Час "*старіння" конфіденційної інформації*** | | | | | | |
| **3** | **1) чи має конфіденційність довготривалий характер (рік та більше)?** | **5,0** | **50** |  |  |  |
| **2) чи має конфіденційність короткотривалий характер (місяць та більше)?** | **4,0** | **40** |  |  |  |
| **3) чи має конфіденційність оперативний характер (до місяця)?** | **1,0** | **10** |  |  |  |
| ***Режимні та організаційні заходи*** | | | | | | |
| **4** | **1) чи враховуються інтереси збереження таємниці закладу при кадровому відборі верхньої ланки управління?** | **5,8** | **15** |  |  |  |
| **2) те саме при підборі осіб, допущених до конфіденційної інформації?** | **4,7** | **20** |  |  |  |
| **3) те саме при кадровому відборі штатного персоналу закладу в цілому?** | **3,5** | **15** |  |  |  |
| **4) чи налагоджений контроль за зберіганням працівниками закладу комерційної таємниці?** | **3,8** | **15** |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **5) чи забезпечена охорона закладу і конфіденційної документації, яка містить комерційну таємницю?** | **4,2** | **15** |  |  |  |
| **6) чи є можливим доступ «недопу-щених» осіб до засобів розмноження та обробки інформації?** | **4,3** | **10** |  |  |  |
| **7) чи виділене спеціальне приміщення для нарад та переговорів з діловими партнерами?** | **4,2** | **10** |  |  |  |
| ***Устаткування службових приміщень технічними засобами*** | | | | | | |
| **5** | **1) телефонними апаратами?** | **2,5** | **8,5** |  |  |  |
| **2) переговорними пристроями?** | **1,5** | **5** |  |  |  |
| **3) датчиками пожежної та охоронної сигналізації?** | **0,6** | **3** |  |  |  |
| **4) електричними та електронними годинниками?** | **0,8** | **2,5** |  |  |  |
| **5) абонентськими гучномовцями?** | **0,9** | **3** |  |  |  |
| **6) телефонними апаратами з авто-набором і концентраторами, які використовуються в системах зв'язку?** | **1.5** | **5** |  |  |  |
| **7) установками прямого телефонного зв'язку?** | **1,3** | **4,5** |  |  |  |
| **8) радіоприймачами?** | **1,5** | **5** |  |  |  |
| **9) телевізорами?** | **1,5** | **5** |  |  |  |
| **10) магнітофонами?** | **0,5** | **1,5** |  |  |  |
| **11) диктофонами?** | **0,5** | **1,5** |  |  |  |
| **12) установкою оперативного зв'язку?** | **1,5** | **5** |  |  |  |
| **13) телефаксами?** | **2,2** | **7,5** |  |  |  |
| **14) персональними ЕОМ?** | **3,0** | **10** |  |  |  |
| **15) відеомагнітофонами?** | **0,9** | **3** |  |  |  |
| **16) автоматичною телефонною станцією?** | **3,0** | **10** |  |  |  |
| **17) радіотелефоном?** | **1,5** | **5** |  |  |  |
| **18) чи організовано технічний захист у закладі?** | **4,5** | **15** |  |  |  |

На другому етапі із залученням консультанта проводиться аналіз результатів опитування. Якщо відповідь на питання відповідає збільшенню небезпеки витоку інформації, то в графі 4 табл. 5 проставляється знак «+», в іншому разі проставляється знак «-».

На третьому етапі проводиться підсумовування часткових коефіцієнтів графи 5, що відповідають знаку «+», із усіх питань анкети. Результат підсумовування є загальною оцінкою *(G)* для ухвалення рішення про необхідність захисту конфіденційної інформації на фірмі в цілому. При цьому, якщо загальна оцінка *G* дорівнює чи більша 50 *(G >* 50), то захист необхідно проводити в усіх напрямках.

Якщо загальна оцінка *G* більша 20, але менша 50 (50 > *G >* 20), то ймовірність витоку інформації досить велика, необхідно провести часткові оцінки, захист необхідний за окремими напрямками. Якщо загальна оцінка менша 20 (G < 20), то ймовірність витоку інформації мала і додатковий захист інформації можна не проводити. На четвертому етапі проводиться аналіз за допомогою часткових оцінок по всіх 5 пунктах опитувальної анкети. Для одержання часткових оцінок проводять підсумовування часткових коефіцієнтів графи 6 табл. 5, позначених знаком «+», для кожного пункту окремо. При цьому вийде п'ять часткових оцінок:

1. по пункту 1 - оцінка конкурентоспроможності продукції (послуг)- G,;
2. по пункту 2 - оцінка ступеня конфіденційності інформації - *G2;*
3. по пункту 3 - оцінка тимчасових характеристик конфіденційності інформації - G3;
4. по пункту 4 - оцінка ЗІ режимними й організаційними методами - *G4*;
5. по пункту 5 - оцінка можливості витоку інформації через технічні засоби- *Gs.*

Якщо часткова оцінка по кожному з пунктів 1-3 дорівнює чи більша *20 (G1,G2,G3 >* 20), то це підтверджує необхідність ЗІ.

Якщо часткова оцінка по кожному з пунктів 4,5 дорівнює чи більша 20 (G4 , *G5 >* 20), то це вказує на необхідність проведення ЗІ режимними й організаційними методами або за допомогою технічних засобів захисту відповідно. У тому випадку, якщо часткова оцінка по одному з пунктів 1-3 менша 20 ( *G1, G2, G3 <* 20), то ЗІ можна не проводити.

Таким чином, на основі проведених оцінок, керівник фірми приймає рішення про необхідність робіт з організації ЗІ.

Цілком природно, що перед керівником фірми постає інше дуже важливе питання про майбутні витрати на організацію ЗІ. Це питання вирішується за допомогою другої частини методу.

Друга частина методу призначається для визначення орієнтовної оцінки очікуваних витрат, пов'язаних із захистом конфіденційної інформації. У загальному випадку витрати на ЗІ складаються з витрат на проведення організаційно-режимних і технічних заходів. У свою чергу, витрати на технічний захист складаються з витрат на проведення захисту мовної інформації і на захист інших видів інформації, зокрема, дискретної, оброблюваної на ЕОМ, телеграфного, факсимільного й інших видів, використовуваних у діяльності фірми.

Витрати на режимні й організаційні заходи ЗІ визначаються головним чином заробітною платою працівників режимних підрозділів (груп), що забезпечують організацію і контроль режимних заходів, які підвищують безпеку інформації. Розрахунок цих витрат цілком перебуває у віданні керівника фірми й труднощів не викликає.

Витрати на технічну ЗІ складаються з витрат на проведення досліджень, що дають змогу виявити канали витоку інформації, визначити способи її захисту, і з очікуваних витрат на реалізацію технічних рішень захисту.

Розрахунок вартості захисних заходів кожного з видів інформації має деякі особливості, але на етапі орієнтовних розрахунків можна використовувати методику захисту мовної інформації як найбільш просту і загальну. Така методика, що є другою складовою загальної методики оцінки, розроблена і представлена нижче. З огляду на те, що методика призначена для проведення експрес-оцінки вартості ЗІ, що дає змогу керівнику фірми грубо оцінити майбутні витрати, вона максимально спрощена і передбачає проведення елементарних розрахунків. З цією метою все технічне устаткування, що може бути встановлене на об'єкті (фірмі) і через яке можливий витік інформації, умовно розділено на три групи. Критерієм такого розподілу обрана частка (відсоток) витрат на захист устаткування від вартості самого устаткування (техніки). Часткові коефіцієнти *(К1, К2, К3),* визначені експертним шляхом, та перелік технічного устаткування по групах із зазначенням значень часткових коефіцієнтів витрат на захисні заходи наведено в табл. 6.

У таблиці позначено: *С1, С2, С3* - сумарна вартість технічного устаткування відповідної групи, встановленого на об'єкті (фірмі). Значення вартості зразків техніки, які знаходяться в приміщеннях фірми, визначаються за каталогами діючих цін виробника даної

*Таблиця 6*

|  |  |  |  |
| --- | --- | --- | --- |
| **Група** | **Перелік обладнання** | **Частка (відсоток)**  **витрат на ЗІ від**  **витоку інформації** | **Частка (відсоток) витрат на профілактичний контроль ефективності ЗІ** |
| 1 | Телефонні апарати;  переговорні пристрої;  датчики пожежної та охоронної  сигналізації;  електричні та електронні годинники;  абонентські гучномовці | *К*1=0,7*С*1 |  |
| 2 | Автонабори і концентратори, які  використовуються в системах зв'язку;  установки прямого телефонного  зв'язку;  радіоприймачі;  телевізори;  магнітофони;  диктофони | К2=0,ЗС2 | ***К***проф =(0,03-0,1)від (*С*1+*С*2+*С*3) |
| 3 | Пульти оперативного зв'язку до 100  номерів;  персональна комп'ютерна техніка;  відеомагнітофони;  АТС на 100- 1000 номерів | *К3* =0,13С3 |  |

техніки. Вартість технічного захисту всього устаткування (Стз), що складається з техніки різних груп, визначається за формулою:

Стз = *С1К1 + С2К2 + С3К3.*

Зазначимо, що у табл. 6 подано вартість захисту устаткування, не призначеного для передачі, обробки і збереження конфіденційної інформації. Вартість захисту устаткування, призначеного для обробки конфіденційної інформації, визначається індивідуально і може істотно перевищувати зазначену в табл. 6.

Вартість щорічного профілактичного контролю визначається за формулою:

***С*** проф**=*К***проф ***С***тз

де ***С*** проф =(0,03-0,1) - коефіцієнт витрат на щорічний профілактичний контроль ефективності ЗІ, визначений дослідним шляхом.

Таким чином, знаючи перелік і кількість встановленого на фірмі технічного устаткування і його вартість, можна легко розрахувати очікувані витрати на ЗІ технічними засобами. Додавши витрати на режимні й організаційні заходи ( Сроз) і на профілактичний контроль

у перший рік функціонування, одержимо загальні витрати на ЗІ ( Сзаг ): Сзаг *=*Стз *+С* роз *+С*проф.

Отже, на основі отриманої величини, а також маючи на увазі прибуткові можливості організації, керівництво приймає рішення щодо певних заходів із захисту інформації в організації.

Не менш важливою є проблема оцінки рівня захищеності уже створеної і навіть функціонуючої СЗІ.

З урахуванням моделей порушника для систем різного призначення і різних вимог повинні існувати різні критерії оцінки достатності захисних заходів. Порушник-професіонал може перебувати поза об'єктом захисту, і йому спочатку необхідно подолати контрольовану межу об'єкта. Порушник-користувач уже має певні повноваження щодо санкціонованого доступу до інформації відповідно до своїх функціональних обов'язків і завдань.

Аналіз об'єктів АС починається з визначення можливих каналів НСД (МКНСД). Найбільш об'єктивним процесом оцінки доцільно розглянути МКНСД, що очікуються від кваліфікованого порушника-професіонала, який знаходиться на початковій позиції поза об'єктом захисту. У такому разі оцінка буде відрізнятися меншою кількістю МКНСД, ніж у порушника більш низького класу, а також імовірністю подолання порушником захисних бар'єрів, кількістю шляхів, імовірностями їх обходу.

Після того як для обраної моделі порушника визначено всі МКНСД і на них встановлено засоби захисту, вважається, що віртуальний контур

захисту замкнуто. Тоді для контрольованого МКНСД визначається його вразливість, величина якої буде дорівнювати вразливості найбільш слабкої ланки захисного контуру, для чого використовуємо формулу

 (7.1)

де *РВбл -* імовірність виявлення і блокування несанкціонованих дій порушника, Рвідм - імовірність відмови системи, *Робхj-* імовірність обходу порушником *j-i* перешкоди. Ця формула виражає вразливість захисту *К-і* ланки захисту шляхом порівняння імовірностей і вибору однієї з них. При цьому для МКНСД, які закриті двома або більше засобами захисту, розрахунок вразливості ланки здійснює за формулою

 **(7.2)**

де *т* - кількість дублюючих перешкод, *Pt* - вразливість і-ї перешкоди. Для неконтрольованих МКНСД розрахунок здійснюється за формулою

 **(7.3)**

де *j* - кількість шляхів обходу.

Оцінка вразливості системи ідентифікації та автентифікації (СІА) здійснюється за формулою (7.1) з урахуванням таких параметрів.

* Імовірність подолання перешкоди порушником з боку законного введення в систему.
* Імовірність виявлення і блокування НСД в системі СІА. Вона визначається можливістю відповідної програми до відпрацювання даної функції у випадку розбіжності.
* Оцінка вразливості системи розмежування і контролю доступу у приміщення об'єкта захисту *Рпр,* визначається виходячи з технічних даних вхідного замка на дверях приміщення, режиму роботи КСА, наявності охоронної сигналізації і значення її параметрів. При цілодобовому режимі роботи, як правило, обмежуються кодовим замком на дверях. При перервах у роботі, коли у приміщенні нікого не повинно бути, апаратура вимикається, приміщення ставиться на дистанційний централізований контроль охоронної сигналізації (про оцінку її вразливості йтиметься нижче).
* Імовірність обходу перешкоди порушником *Робх* слід оцінювати безпосередньо на місці, тобто шляхом огляду приміщення на предмет вразливості стін і відсутності сторонніх люків, пошкоджень стін, стелі, вікон. Особливу увагу необхідно звернути на розміщення вікон і конструкцію їх рам, кватирок, замків, поверховість приміщення, вентиляцію. Якщо приміщення знаходиться на першому поверсі, на вікнах необхідно перевірити установку датчиків охоронної сигналізації.

• При оцінці вразливості системи контролю виведення апаратури з робочого контуру обміну інформацією під час ремонту і профілактики технічних засобів вважається, що спроба порушника, який знаходиться в зоні об'єктів АС, що відрізняється від зони робочого місця функціонального контролю (РМФК), ввести його знову в робочий контур АС малоймовірна. Значить, можна прийняти *Рпр =* 0. Але можливість обходу цього заходу в порушника існує.

Як показує практика, найбільш вразливим місцем для НСД є носії ПЗ і носії інформації. Цьому сприяє уніфікована конструкція носіїв, відносно невеликі габаритні розміри і маса, великі обсяги інформації, яка зберігається на них, збереження і транспортування на них ОС і прикладних програм.

Особливістю засобів захисту інформації на носіях є необхідність враховувати (залежно від технічного завдання) імовірність потрапляння носія з інформацією за межі об'єкта захисту, в зону, де відсутні засоби виявлення і блокування НСД. Вразливість захисту в таких випадках повинна збільшуватись і досягати такої величини, коли час подолання захисту порушником буде більшим, ніж час життя інформації, яка розміщена на носіях. Тому оцінка повинна проводитися за окремим показником.

Для захисту інформації і ПЗ на носіях використовуються організаційні, апаратні, програмні і криптографічні засоби.

Вразливість засобів захисту від ПЕВМН оцінюється ймовірністю перехоплення інформації порушником, який знаходиться за межами території об'єкта захисту, оскільки критерієм можливого перехоплення є відношення «сигнал-шум» на межі об'єкта захисту. Величини ймовірності визначають досвідчені спеціалісти шляхом аналізу засобів захисту, вимірювання сигналу і спеціальних досліджень.

Засоби реєстрації звертань до інформації, яку необхідно захищати, є достатньо ефективним заходом, який також потребує оцінки якості: виконання програми реєстрації (чи всі звертання реєструються, з якими атрибутами), імовірності її обходу користувачем-порушником, можливості прихованого відключення, часу роботи, безвідмовності.

Однак реєстрація подій з відкладеним виявленням більше служить для профілактичних цілей і подальшого аналізу конкретної ситуації, у зв'язку з чим цей захід слід вважати хоча й обов'язковим, але все ж резервним, тобто тим, що дублює інші заходи захисту.

Засоби управління захистом інформації в АС виконують функції захисту і є важливою складовою засобів захисту. Управління забезпечує функції контролю, виявлення і блокування НСД, а також безперебійне функціонування апаратних, програмних і організаційних засобів захисту, ведення статистики і прогнозування подій. Усі ці параметри враховуються при оцінці вразливості окремих засобів захисту АС. У результаті оцінка ефективності засобів управління

захистом може проводитися лише з якісного боку на предмет реалізації захисту як єдиного механізму - СЗІ в технічному сенсі розв'язання задачі: технології управління, складу апаратних і програмних засобів управління і організаційних заходів, наявності централізації контролю і управління захистом.

Така оцінка необхідна для визначення ступеня наближення отриманих значень вразливості захисту до дійсних. Чим більше автоматизованих засобів захисту, тим менше експертних оцінок, достовірніші оцінки і вищі гарантії ефективності захисту.

Складність і масштаби сучасних систем захисту не дають змоги проводити експерименти з ними, а експерименти з окремими елементами не дозволяють отримати уявлення про цілісні властивості систем. Розв'язання задач оцінки ефективності захисту ускладнюється тим, що в будь-якій системі захисту основною ланкою є людина. Крім того, великі проблеми при створенні точних аналітичних методів розрахунку й оцінки ефективності роботи систем захисту полягають у визначенні складних залежностей між середовищем функціонування АС, станом джерел інформації та системою захисту.

Залежно від співвідношення ресурсів, що виділяються на захист, та очікуваних результатів від її розв'язання задача синтезу оптимальних СЗІ може формулюватися в таких формах:

1. При фіксованому рівні витрат ресурсів забезпечити максимально можливий рівень захищеності.
2. При фіксованому рівні захищеності мінімізувати витрати на захист.

Однак сьогодні техніко-економічна оптимізація систем захисту -дуже складна і далека від вирішення проблема. Незважаючи на це, вона все ж має переваги, а саме:

* можливість отримання коректного математичного розв'язку задачі за обраним критерієм якості;
* можливість за допомогою сформульованих обмежень зрозуміти суть реальних процесів захисту;
* виявити в процесі оптимізації протиріччя у вимогах до системи захисту;
* можливість давати прогнозні оцінки у разі зміни умов функціонування;

• підвищити ефективність управління системою захисту.  
До недоліків оптимізації систем захисту слід віднести:

* складність математичної постановки задач проектування оптимальної системи захисту;
* суттєву залежність якості оптимальної системи захисту від точності вихідних припущень та характеру змін в об'єктах АС.

**2.17) Питання безпеки та брандмауери**

**Брандмауер**

**Міжмережевий екран**, **Мережевий екран**, **Фаєрво́л**, **файрво́л** [англ.](http://uk.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0_%D0%BC%D0%BE%D0%B2%D0%B0) *Firewall*, бук­ва­ль­­но «вогняна стіна» — [пристрій](http://uk.wikipedia.org/wiki/%D0%9F%D1%80%D0%B8%D1%81%D1%82%D1%80%D1%96%D0%B9) або набір пристроїв, сконфігурованих, щоб допускати, від­мов­ляти, шифрувати, пропускати через [проксі](http://uk.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%BA%D1%81%D1%96) весь комп'ютерний [трафік](http://uk.wikipedia.org/wiki/%D0%A2%D1%80%D0%B0%D1%84%D1%96%D0%BA) між областями різ­ної [безпеки](http://uk.wikipedia.org/wiki/%D0%91%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0)згідно з набором правил та інших критеріїв.

Функції

Фаєрвол може бути у вигляді окремого приладу (так звани­й­ [*маршрутиза­тор*](http://uk.wikipedia.org/wiki/%D0%9C%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%82%D0%BE%D1%80)*­* або­ *роу­тер*),­ або програмного забезпечення, що встановлюється на персональний комп'ютер чи [проксі-сервер](http://uk.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%BA%D1%81%D1%96-%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80). Простий та дешевий фаєрвол може не мати такої гнучкої системи нала­шту­вань правил фільтрації пакетів та *трансляції* адрес вхідного та вихідного трафіку (функція *редиректу*).

В залежності від активних з'єднань, що відслідковуються, фаєрволи розділяють на:

* *stateless* (проста фільтрація), які не відслідковують поточні з'єднання (наприклад [TCP](http://uk.wikipedia.org/wiki/TCP)), а фільтрують потік даних виключно на основі статичних правил;
* *stateful* (фільтрація з урахуванням контексту), з відслідковуванням поточних з'єднань та пропуском тільки таких пакетів, що задовольняють логіці й алгоритмам роботи відповідних протоколів та програм. Такі типи фаєрволів дозволяють ефективніше боротися з різноманітними DoS-атаками та вразливістю деяких протоколів мереж.

Типи фаєрволів

Для того щоб задовольнити вимогам широкого кола користувачів, існує три типи фаєрволів: мережного рівня, прикладного рівня і рівня з'єднання. Кожен з цих трьох типів використовує свій, відмінний від інших підхід до захисту мережі.

* **Фаєрвол мережного рівня** представлений [екрануючим маршрутизатором](http://uk.wikipedia.org/wiki/%D0%9C%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%82%D0%BE%D1%80). Він контролює лише дані мережевого і транспортного рівнів (див.[Модель OSI](http://uk.wikipedia.org/wiki/%D0%9C%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C_OSI)) службової інформації пакетів. Мінусом таких маршрутизаторів є те, що ще п'ять рівнів залишаються некон­трольованими. Нарешті, адміністратори, які працюють з екрануючими мар­шру­ти­за­то­рами, повинні пам'ятати, що у більшості приладів, що здійснюють фільтрацію пакетів, від­сутні механізми аудиту та подачі сигналу тривоги. Іншими словами, маршрутизатори мо­жуть піддаватися атакам і відбивати велику їх кількість, а адміністратори навіть не бу­дуть проінформовані.
* **Фаєрвол прикладного рівня** також відомий як [проксі-сервер](http://uk.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%BA%D1%81%D1%96-%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80) (сервер-посеред­ник).Фаєрволи прикладного рівня встановлюють певний фізичний поділ між локальною мере­жею і Internet, тому вони відповідають найвищим вимогам безпеки. Проте, оскільки прог­рама повинна аналізувати пакети і приймати рішення щодо контролю доступу до них, фаєрволи прикладного рівня неминуче зменшують продуктивність мережі, тому в якості сервера-посередника використовуються більш швидкі комп'ютери.
* **Фаєрвол рівня з'єднання** схожий на фаєрвол прикладного рівня тим, що обидва вони є серве­рами-посередниками. Відмінність полягає в тому, що фаєрволи прикладного рівня вима­гають спеціального програмного забезпечення для кожної мережевої служби на зра­зок FTP або HTTP. Натомість, фаєрволи рівня з'єднання обслуговують велику кількість про­токолів.

Спеціалізовані пристрої

* [.vantronix | Firewall ZL1](http://vantronix.com/products/vtfw/zl1/)(англ.)
* [Cisco PIX](http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/index.html)(англ.) та [Cisco ASA](http://www.cisco.com/en/US/products/ps6120/index.html)(англ.)
* [Checkpoint FireWall-1](http://www.checkpoint.com/products/firewall-1/index.html)(англ.)
* [Juniper Netscreen](http://www.juniper.net/products/integrated/)(англ.)
* [Nokia Firewalls](http://www.nokia.com/nokia/0,,76737,00.html)(англ.)
* [WatchGuard Firebox](http://www.watchguard.com/products/appliances.asp)(англ.)

Персональні фаєрволи

* [Zillya Internet Security](http://uk.wikipedia.org/w/index.php?title=Zillya_Internet_Security&action=edit&redlink=1) — [zillya.ua](http://zillya.ua/)
* [Outpost Firewall](http://uk.wikipedia.org/wiki/Outpost_Firewall) — [Agnitum Outpost](http://www.agnitum.ru/)
* [KIS](http://uk.wikipedia.org/w/index.php?title=KIS&action=edit&redlink=1) -[Kaspersky Internet Security 6.0](http://kaspersky.ru/kaspersky_internet_security)
* [Jetico Personal Firewall](http://www.jetico.com/jpfirewall.htm)(англ.)
* [Norton Personal Firewall 2006](http://www.symantec.com/home_homeoffice/products/overview.jsp?pcid=is&pvid=npf2006)
* [McAfee Firewall](http://www.mcafee.ru/products/homepc/firewall.html)
* [Zone Alarm](http://www.zonelabs.com/store/application?namespace=zls_catalog&origin=global.jsp&event=link.catalogHome&dc=12bms&ctry=US&lang=en&lid=nav_ho)
* [Kerio WinRoute Firewall](http://www.kerio.com/kwf_home.html)
* [Comodo Personal Firewall](http://personalfirewall.comodo.com/)
* [CA Personal Firewall](http://shop.ca.com/firewall/personal_firewall.aspx)(англ.)
* [SoftPerfect Personal Firewall](http://www.softperfect.com/products/firewall/)(англ.)

Програмне забезпечення

* [WIPFW](http://wipfw.sourceforge.net/)(англ.)
* [netfilter](http://uk.wikipedia.org/w/index.php?title=Netfilter&action=edit&redlink=1)

Як вибрати та налаштувати браузер, антивірус, брандмауер, ОС комп'ютера, щоб забезпечити максимальну безпеку роботи в інтернеті

Безпека комп'ютера під час роботи в інтернеті залежить від багатьох факторів, і в першу чергу — від дотримання користувачем усього комплексу правил та його обережності. Крім того, важливі налаштування (як ті, що здійснені користувачем, так і ті, що встановлені за замовчуванням), встановлені патчі та антивіруси, засоби захисту на інтернет-шлюзі та багато іншого. Крім того, враховуйте:

1. Браузери [Opera 11](http://opera.yandex.ru/) і [Firefox 7](http://fx.yandex.ua/?ncrnd=3660) безпечніші, ніж Opera та Firefox попередніх версій. [Microsoft Internet Explorer 9.0](http://windows.microsoft.com/uk-UA/internet-explorer/products/ie/home) значно безпечніший за попередні версії Microsoft Internet Explorer.
2. Якщо в ОС встановлено та ввімкнено антивірус — працювати в ній безпечніше, ніж без антивіруса:
   * високі оцінки [AV Comparatives](http://www.av-comparatives.org/) у лютому 2011 отримали [AVIRA AntiVir Personal 10](http://www.avira.com/), [BitDefender AV Pro 14](http://www.bitdefender.ru/), [MicroWorld eScan AntiVirus 11](http://www.avescan.ru/), [F-Secure AntiVirus 10](http://www.f-secure.com/), [Kaspersky AV 11](http://www.kaspersky.ru/), [McAfee AntiVirus+ 14](http://www.mcafee.com/), [Trustport Antivirus 11](http://www.trustport.com/), [Sophos AntiVirus 9](http://www.sophos.com/), [avast! Free Antivirus 5](http://www.avast.com/), [G Data Antivirus 21](http://www.gdatasoftware.com/), [ESET NOD32 Antivirus 4](http://www.esetnod32.ru/), [Symantec Norton Anti-Virus 18](http://www.symantec.com/),[Panda Anti-Virus Pro 10](http://www.pandasecurity.com/ukraine/), [Microsoft Security Essentials 2](http://www.microsoft.com/uk-ua/security_essentials/default.aspx);
   * при цьому [AVIRA AntiVir Personal 10](http://www.avira.com/), [avast! Free Antivirus 5](http://www.avast.com/) і [Microsoft Security Essentials 2](http://www.microsoft.com/uk-ua/security_essentials/default.aspx) безкоштовні;
   * оновлення та доступ до інтернету є для більшості сучасних антивірусів критично важливими, без цього ефективність їх захисту швидко знижується.
3. Якщо в ОС увімкнений і правильно налаштований файрвол, вона безпечніша; правильне налаштування полягає в тому, щоб у брандмауері була дозволена лише та мережева активність, яка є необхідною. Брандмауер можна ввімкнути так:
   * в Microsoft Windows 7:

Запустити —> Панель керування (переглянути за категоріями) —> Система й безпека —> Брандмауер Windows —> Увімкнення або вимкнення брандмауера Windows —> обрати «Увімкнути брандмауер Windows» в домашній або робочій (приватній) мережі, у мережі спільного використання.

1. Працювати під обліковим записом з обмеженими повноваженнями істотно безпечніше, ніж під обліковим записом із правами локального, а тим більше доменного системного адміністратора. Крім того, рекомендується, щоб:
   * повноваження облікового запису відповідали комп'ютерній грамотності та відповідальності тих, хто під ним працює;
   * вхід під обліковим записом системного адміністратора був можливий лише після введення пароля, до того ж не формального «qwerty» або «111», а повноцінного — мінімум 11 літер у різних регістрах, цифр і спеціальних символів.
2. Microsoft Windows 7 безпечніше попередніх ОС компанії Microsoft для робочих станцій, у тому числі Microsoft Windows XP. UNIX-подібні ОС (зокрема Linux, BSD, «промислові» UNIX) безпечніші за інші розповсюджені ОС.
3. Якщо програмне забезпечення, у тому числі операційна система, оновлюються, вони безпечніші. Оновлення можна ввімкнути так:
   * Microsoft Windows 7:

Запустити —> Панель керування (переглянути за категоріями) —> Система й безпека —> Увімкнення та вимкнення автоматичного оновлення —> обрати «Важливі оновлення: Інсталювати оновлення автоматично».

1. Неофіційні збірки, а також образи програмних продуктів, що поширюються неофіційно (в тому числі на контрафактних дисках, за допомогою торентів і «неофіційних» дзеркал сайтів) часто менш безпечні, ніж офіційні.
2. Безпека межує з надійністю — робіть резервні копії найцінніших для вас даних, тому що шкідливі програми можуть блокувати доступ до системи, шифрувати дані на дисках, а іноді й остаточно їх псувати. При цьому платити гроші зловмисникам за відновлення доступу до власних даних значить фінансувати розробку та розповсюдження нових, ще розвиненіших шкідливих програм.

Зручність майже завжди суперечить безпеці. Система з повністю вимкненою безпекою «не заважає» користувачу обмеженнями, питаннями, необхідністю додаткових підтверджень і дій. Робота антивірусу часто знижує продуктивність системи, авторизація та зміна облікових записів — дратує.

Але втрата даних часто коштує дорожче, адже серед них можуть бути результати роботи та хобі, фотографії, архіви, колекції, дані для авторизації в платіжних системах, системах обміну повідомленнями, соціальних мережах, онлайн-іграх. Навіть якщо враховувати лише втрату часу, то на одноразове відновлення даних і працездатності системи його зазвичай витрачається більше, ніж на дотримання правил техніки безпеки роботи з інтернетом протягом кількох років.