МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА

В. Л. Бурячок, Р. В. Киричок, П. М. Складанний

ОСНОВИ ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Навчальний посібник

Київ 2019

УДК 004.056
ББК 32/973-018.2я.73

Затверджено на засіданні Вченої Ради Київського університету імені Бориса Грінченка.
25.04.2019 р.

Автори:
В.Л. Бурячок, доктор технічних наук, професор
Р.В. Киричок
П.М. Складанний

Рецензенти:
доктор технічних наук, професор Ю.Я.Самохвалов
доктор технічних наук, доцент С.В.Казмірчук

Бурячок В. Л. Основи інформаційної та кібернетичної безпеки. [Навчальний посібник]. / В. Л. Бурячок , Р. В. Киричок, П. М. Складанний – К. , 2018. – 320 с.

У посібнику подано теоретичний і практичний матеріал із сучасних проблем інформаційної безпеки, який містить методичні, наукові та практичні рішення з підвищення рівня знань студентів у сфері інформаційної та кібернетичної безпеки. Також представлено низку лабораторних робіт розбитих за такими трьома розділами: кібернетичний простір, мережа Internet та система WWW; теорія інформаційної безпеки; методологія захисту інформації. Їх засвоєння дозволить більш глибоко та детально розглянути основні положення, поняття й визначення щодо базових аспектів захисту інформації, створення та експлуатації захищених інформаційних та комунікаційних систем.

Посібник буде корисний науковим та науково-педагогічним працівникам, аспірантам, магістрантам і студентам вищих навчальних закладів, що навчаються за спеціальністю 125 «Кібербезпека».

ISBN 978-966-676-281-1 **УДК 32.973я73 р.**
ISBN 978-966-676-323-8 **ББК 004.056(075.8)**

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АІС – автоматизована інформаційна система
АРМ – автоматизоване робоче місце
ЕЦП – електронний цифровий підпис
ЗІ – захист інформації
ЗК – загальні критерії
ІКТ – інформаційно-комунікаційна технологія
ІБ – інформаційна безпека
ІТ – інформаційна технологія
ІТС – інформаційно-телекомунікаційна система
КЗЗ – комплекс засобів захисту
КС – комп'ютерна система
КСЗІ – комплексна система захисту інформації
МЕ – міжмережевий екран
НСД – несанкціонований доступ
ОО – об'єкт оцінки
ОС – операційна система
ПБ – політика безпеки
ПЕМВН – побічні електромагнітні випромінювання та наведення
ПЗ – програмне забезпечення
ПК – персональний комп'ютер
СЗІ – система захисту інформації
СУБД – системи управління базами даних
СУІБ – система управління інформаційною безпекою
ТЗІ – технічний захист інформації
ФС – файлова система
ARP – Address Resolution Protocol
DAC – Discretionary Access Control
DHCP – Dynamic Host Configuration Protocol
DNS – Domain Name Service
MAC – Mandatory Access Control
PGP – Pretty Good Privacy
SD – Security Descriptor
SID – Security Identifiers
URL – Uniform Resource Locator
WWW – World Wide Web

ВСТУП

Глобальна інформатизація останнім час активно управляє існуванням і життєдіяльністю держав світового співтовариства, а інформаційні технології все частіше застосовуються при рішенні завдань забезпечення національної безпеки. Одним з фундаментальних наслідків цих процесів стало виникнення принципово нового середовища – кіберпростору.

Стрімко наростаючий у світі інтерес до проблематики кіберпростору багато в чому пов'язаний з активністю найбільш розвинених країн світу в питаннях тактики і стратегії ведення збройної боротьби, а також забезпечення безпеки критично важливих об'єктів їхньої економіки від внутрішніх і зовнішніх інформаційних та кібернетичних загроз. І якщо сьогодні між провідними у військовому і економічному відношенні світовими державами зложився певний паритет в області застосування звичайних озброєнь і зброї масового ураження, у міжнародному праві зафіксовані основні принципи взаємин цих держав у рамках таких просторів, як наземне, морське, повітряне та космічне, то питання про міждержавний паритет і взаємини в кіберпросторі на теперішній час продовжують залишатися відкритими. Це пояснюється насамперед наявністю факторів невизначеності вихідної інформації про розвиток науково-технічного прогресу, переходом від екстенсивних до інтенсивних шляхів підвищення ефективності розвитку інформаційного суспільства, а також доволі справедливим твердженням про те, що війни XXI століття будуть кібернетичними за своєю основною суттю.

У процесі формування глобального кіберпростору відбувається конвергенція військових і цивільних комп'ютерних технологій, у провідних закордонних державах інтенсивно розробляються нові засоби й методи активного впливу на інформаційну інфраструктуру потенційних супротивників, створюються різні спеціалізовані кібернетичні центри і підрозділи керування (командування), основним завданням яких є підготовка й проведення активних деструктивних дій в інформаційних системах супротивника, а також захист власних систем від подібного впливу. Терміни й визначення із приставкою «кібер...» останнім часом широко використовуються як у міжнародних, так і у внутрішньодержавних дискусіях і документах. Останнім часом вони знайшли своє відбиття в стратегічних доктринах окремих держав і міжнародних організацій, включаючи НАТО. Так, наприклад, Пентагон офіційно визнав кіберпростір новим полем можливих бойових дій, НАТО дорівнює кібератаки на країну-члена альянсу до збройного нападу, а їх фахівці в області інформаційних технологій одностайно відзначають той факт, що «держава, яка контролює кіберпростір, буде контролювати війну й мир».

Як наслідок, для будь-якої держави безпека в кіберпросторі й насамперед кібернетична безпека (кібербезпека) стають гострою й специфічною проблемою в забезпеченні своєї національної безпеки й захисті своїх інтересів. Це приводить до того, що кібербезпека все частіше розглядається, як стратегічна проблема, яка комплексно зачіпає економіку країни, у тому числі взаємодію національних розроблювачів програмного забезпечення й систем керування, виробників устаткування й компонентів для забезпечення інформаційно-комунікаційної інфраструктури, низька ринкова конкурентоспроможність яких приводить до необхідності використання рішень від іноземних виробників. На практиці дане явище приводить до стрімкого зростання залежності від ринку іноземних товарів і послуг, а також до зниження рівня інформаційного захисту у виді змушеного використання «закритого» програмного й апаратного забезпечення у всіх сегментах інфраструктури як для спеціальних державних відомств, так і цивільного сектора. З погляду економіки дане явище, позитивно впливаючи на розвиток електронної промисловості й реального сектора, створює реальну загрозу для національної безпеки, переводячи її під контроль іноземних спеціальних служб.

Для того щоб національна безпека України могла відповідати рівню провідних економічних держав, необхідні як послідовні дії з боку держави, спрямовані на підвищення ефективності й розвиток системи взаємодії учасників ІКТ-галузі та забезпечення безпеки критично важливих об’єктів інформаційної та кіберінфраструктур, так й приділення підприємствами та організаціями нашої держави більшої уваги до питань власної інформаційної і кібербезпеки.

РОЗДІЛ 1 КІБЕРНЕТИЧНИЙ ПРОСТІР, МЕРЕЖА INTERNET ТА СИСТЕМА WWW

Лабораторна робота №1
«Кібернетичний простір та доступ до системи WWW за допомогою веб-браузера»

Мета роботи:

1. Поглиблення та закріплення теоретичних знань з наступних питань:
   - кібернетичний простір: термінологія, структура;
   - поява та розвиток Інтернет;
   - основні поняття системи WWW;
   - структура верхнього рівня веб-браузера.
2. Набуття практичних навичок роботи з веб-браузерами.

Стислі теоретичні відомості:

> «Ми створюємо світ, в який можуть вступати всі, без привілеїв та упереджень, породжених расовими відмінностями, економічною владою, воєнною силою чи місцем народження. Ми створюємо світ, де будь-хто будь-де може виражати свої переконання, незалежно від того, наскільки він незвичайний, без остраху бути змушеним мовчати або конформізму»
>
> A Declaration of the Independence of Cyberspace
> by Barlow J. P

1.1. Поняття кібернетичного простору

Однією із домінуючих тенденцій сучасного світу є інтенсивний розвиток та удосконалення науки і техніки, зокрема інформаційно-комунікаційних технологій (ІКТ). Проголошена Резолюцією 3384(XXX) ГА ООН від 10 грудня 1975 р. Декларація про використання науково-технічного прогресу в інтересах світу та на благо людства, підкреслює, що науково-технічний прогрес став одним із найважливіших факторів розвитку суспільства. Безсумнівно, саме науково-технічний прогрес створює все більш широкі можливості для покращення умов життя людей та народів.

Виходячи з цього, у XX столітті, завдяки бурхливому розвитку інформаційних технологій, та їх використання в суспільстві, викликало появу так званого ***віртуального простору***. Його поступове і доволі умовне поєднання з реальним простором («*real place*») за допомогою інформаційно-телекомунікаційних систем і мережевих технологій різного функціонального призначення, які в процесах обробки, передачі та зберігання інформації використовують електромагнітний спектр і діють як єдине ціле, а також відповідного програмного забезпечення (ПЗ) призвело, як наслідок, до формування так званого ***кіберпростору*** («*cyberspace*»).

Нині під ***кіберпростором*** розуміють *високорозвинену модель об'єктивної реальності, у якій відомості про особи, предмети, факти, події, явища і процеси:*

подані у деякому математичному, символьному (у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень) або будь-якому іншому виді;

розміщуються в пам'яті будь-якого фізичного пристрою, спеціально призначеного для її зберігання, обробки й передачі;

перебувають у постійному русі по сукупності IT систем і мереж.

Графічне співвідношення реального і кібернетичного просторів подано на рис.1.1.

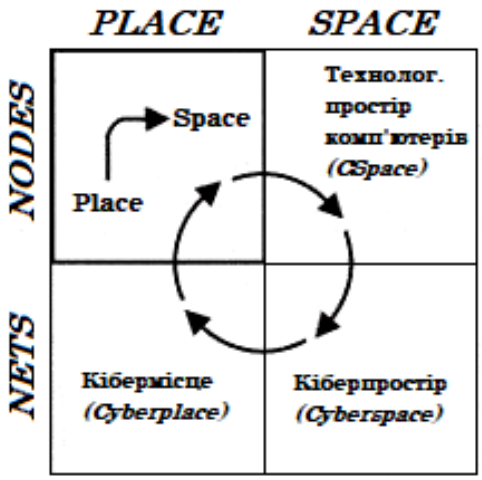


Рис.1.1. Матриця співвідношення реального і кібернетичного просторів А. Батті

Згідно матриці А. Батті співвідношення кіберпростору («cyberspace») з реальністю («Cspace») може бути представлене візуально у «мікросхемах комп'ютерів та проводах, що їх з'єднують». При цьому, якщо технологічними протоколами (наприклад, *TCP/IP – для передачі інтернет-трафіка від одного комп'ютера до іншого; DNS – для забезпечення адресації в Інтернеті тощо*) Cspace можна об'єднати в єдину технологічну основу кіберпростору – «***техносферу***», то власне *cyberspace* – представлятиме собою сукупність

інформаційних об’єктів, тобто загальне ***інформаційне поле***, яке включатиме усі IP-адреса мережі ***Інтернет***.

Інтернет – всесвітня система об’єднаних комп’ютерних мереж, побудована на використанні протоколу IP і маршрутизації пакетів даних (скорочення офіційного визначення). Інтернет являє собою фізичну основу значної частини кіберпростору. Тому у вузькому сенсі кіберпростір часто розуміється як сукупність інформаційних ресурсів, доступних за допомогою глобальної комп’ютерної мережі Інтернет.

Сам термін «***кіберпростір***» походить від двох коренів: *кібернетика* і *простір*. *Кібернетика* – це наука про загальні закономірності управління і передачі інформації в різних системах. *Простір* – це арена дій, контейнер для об’єктів, які розглядаються, сутність деякої системи. Таким чином, можна говорити, що кіберпростір – це простір для інформаційних об’єктів і подій.

Як *приклад* можна навести об’єкти кіберпростору: сайт, веб-сторінка, аккаунт на форумі, електронний лист, відеоролик та інше; та події в кіберпросторі: діалог в чаті, поява статті, дискусії на форумах і в блогах, поява і зникнення нових сайтів, хакерська атака на сайт та інше.

Для всіх цих подій і об’єктів не можна вказати, до якої країни вони належать, і навіть на якому сервері відбуваються (знаходяться). Наприклад, один веб-сайт може знаходитися на декількох серверах, хоча в кіберпросторі буде сприйматися як єдиний об’єкт. Крім того, деякі об’єкти кіберпростору можуть не існувати фізично на серверах, а генеруватися «на льоту» при запиті користувача. Найчастіше фізична структура сайту на сервері принципово відрізняється від логічної структури, яка доступна відвідувачеві сайту через кіберпростір.

Взагалі, термін кіберпростір (cyber space), був вперше застосованим американським письменником-фантастом Уільямом Гібсоном, який використав його в новелі «Burning Chrome», опублікованій у 1982 році. Два роки поспіль автор розвивав цю тему й у своєму кіберпанковому романі 1984 року під назвою «Neuromancer» описав кіберпростір як «*загальну, всеохоплюючу галюцинацію», яка не створена природою, а є штучною конструкцією із компонент, здатних змінюватися протягом часу і яку щодня бачать мільярди звичайних операторів у всьому світі.*

В офіційних джерелах термін кіберпростір вперше був використаним в Окінавській хартії глобального інформаційного суспільства та в Конвенції про злочинність у сфері комп’ютерної інформації від 23 листопада 2001 року. Сфера його регулювання в той час обмежувалась загальними межами правового регулювання суспільних відносин, специфічними об’єктами та інтересами

суб'єктів правовідносин, а також комп'ютерними мережами, за допомогою яких можна брати участь у відповідних правовідносинах.

Нині ж кіберпростір має досить багато визначень. Так, наприклад, відповідно до:

1) міжнародного стандарту ISO/IEC 27032: 2012 (Information technology – Security techniques Guidelines for cybersecurity) – це *середовище існування, отримане у результаті взаємодії людей, програмного забезпечення, інтернет сервісів і послуг в Інтернет за допомогою технологічних пристроїв і мережевих зв'язків, підключених до них, яке не існує у будь-якій фізичній формі;*

2) нормативної бази США – це *сфера, що характеризується можливістю використання електронних та електромагнітних засобів для запам'ятовування, модифікування та обміну даними через мережеві системи та пов'язану з ними фізичну інфраструктуру;*

3) офіційних документів Євросоюзу – це *віртуальний простір, в якому циркулюють електронні дані світових персональних комп'ютерів (ПК);*

4) офіційних документів Великобританії – це *всі форми мережевої, цифрової активності, що включають у себе контент та дії, які здійснюються через цифрові мережі;*

5) офіційних документів Німеччини – це *вся інформаційна інфраструктура, що доступна через Інтернет поза будь-якими територіальними кордонами;*

6) «Стратегії забезпечення кібернетичної безпеки України» це *середовище, яке виникає в результаті функціонування на основі єдиних принципів і за загальними правилами інформаційних (автоматизованих), телекомунікаційних та інформаційно-телекомунікаційних систем*.

При всьому різноманітті цих визначень можна відзначити, що при чіткому зазначенні на зв'язаність кіберпростору з ІКТ інфраструктурою, основна увага звернена не на технології, а на діяльність людей, які використовують ці технології. І таким чином, кіберпростір необхідно розглядати як тріаду, яка включає в себе три основні складові:

- інформація в її цифровому поданні: статичному (файли, записані на носії даних) і динамічному (пакети, потоки, команди, запити, і т.д. які передаються по різних мережах, оброблюються в автоматизованих системах (АС) і подаються на засоби відображення в графічному або текстовому вигляді);
- технічна інфраструктура, ІТ, програмне забезпечення, за допомогою яких здійснюється реалізація основних дій з інформацією: збір, обробка, зберігання та передача. До таких засобів відносяться інфраструктура Інтернет і мережевих взаємозв'язків, комп'ютери, всілякі гаджети і т.п.;

- інформаційна взаємодія суб'єктів з використанням інформації одержуваної (переданої) і оброблюваної за допомогою технічної інфраструктури. Тут маються на увазі всі види діяльності користувачів або учасників кіберпростору, які вони проводять з використанням інформаційних ресурсів, потоки і сховища яких розташовуються на технічній інфраструктурі.

Всі ці складові в сукупності і утворюють сутність, яку можна назвати *кіберпростором*.

1.2. Структура кіберпростору

Як відомо, фізична структура Інтернет в значній мірі визначає стан кіберпростору і динаміку його розвитку. Тому, розглянемо деякі приклади такого впливу.

Що таке для вас кіберпростір – зовсім недавно це визначалося швидкістю підключення до інтернету. Найважливішим фактором у формуванні кіберпростору є наявність високошвидкісних інформаційних комунікацій. Успіх того чи іншого проекту в кіберпросторі у величезній мірі визначається таким показником, як швидкість завантаження сторінок.

Чи стане певний сайт частиною кіберпростору залежить від того, чи доступний він через пошукові системи. Що, в свою чергу, визначається технічними особливостями пошукової машини і вмінням автора сайту використовувати ці особливості в своїх цілях. Дивовижне значення набули в кіберпросторі ***ключові слова***. За них розгортається справжня боротьба.

Яке доменне ім'я має сайт? Здавалося б, мало хто дивиться в рядок адреси. Разом з тим, прості доменні імена легко запам'ятати, і їх можна рекламувати поза кіберпростором.

Які технології використовуються на сайті? Можливо, користувачі одного або декількох з браузерів не зможуть працювати з сайтами через специфіку використовуваних інструментів (наприклад, технологія silverlight, не дивлячись на всю свою гнучкість, вимагає установки спеціальних програм).

Наскільки безпечні системи Інтернет? Над об'єктами в кіберпросторі досить легко втратити контроль: зламана електронна поштова скринька або сторінка в соціальній мережі – не рідкість. Сучасні сайти представляють собою віртуальні фортеці з декількома лініями оборони. Користувачі інтернету також змушені надягати на свої комп'ютери віртуальні «обладунки»: антивіруси, мережеві фільтри, proxy-сервери.

Таким чином, ***кіберпростір*** – це складна структура зі своїми законами функціонування, при цьому в істотній мірі залежить від своєї фізичної основи – *мережі Інтернет*.

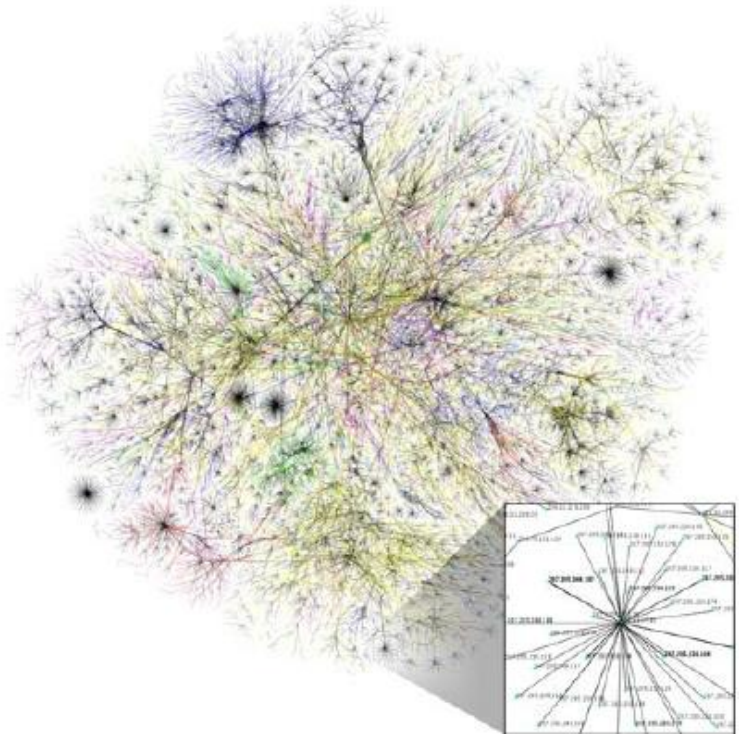
Можна виділити три рівні, що складають кіберпростір:

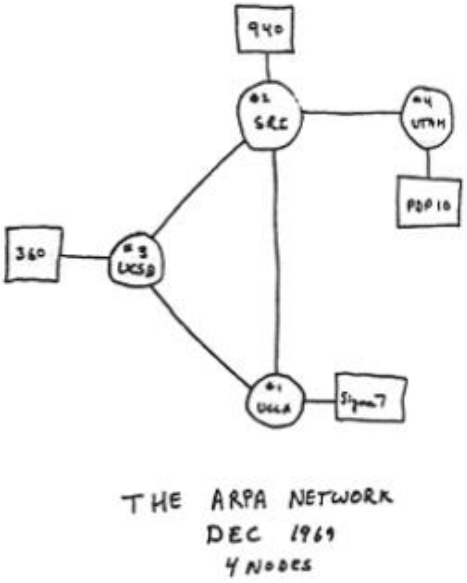
- фізична структура;
- межа;
- соціальна структура.

Нижче наведено приклади об’єктів, що відносяться до того чи іншого шару.

Фізична структура	Межа	Соціальна структура
мережева інфраструктура	доменне ім’я	блог-сфера
сервери	URL	електронна комерція
бази даних	пошукові системи	інтернет-меми
комутація та маршрутизація	управління контентом	інтернет-залежність
DNS-сервера	безпека в мережі Інтернет	Online-ігри
оптоволокно та вита пара	реклама	психологія сприйняття
протоколи передачі даних	мульти-медіа контент	мережеві спільноти
IP-адреса	гіпертекст	Інтернет-субкультури

1.3. Поява та розвиток Інтернет





Інтернет утворює всесвітнє (єдине) інформаційне середовище – сховище оцифрованої інформації, а також служить фізичною основою для Всесвітньої павутини.

Після запуску Радянським Союзом штучного супутника Землі в 1957 році, Міністерство оборони США вирішило, що на випадок війни Америці потрібна надійна система передачі інформації. Агентство передових дослідницьких проектів США (ARPA) запропонувало розробити для цього

комп’ютерну мережу. Розробка такої мережі була поручена чотирьом національним організаціям:

- Каліфорнійському університету в Лос-Анджелесі;
- Стенфордському дослідницькому центру;
- Університету штату Юта;
- Університету штату Каліфорнія в Санта-Барбарі.

Комп’ютерна мережа була названа ARPANET (англ. Advanced Research Projects Agency Network), і в 1969 році в рамках проекту мережа об’єднала чотири зазначених наукових установ, всі роботи фінансувалися за рахунок Міністерства оборони США.

1969 рік прийнято вважати роком заснування інтернету.

Потім мережа ARPANET почала активно рости і розвиватися, її почали використовувати вчені з різних областей науки. Перший сервер ARPANET був встановлений 1 вересня 1969 року в Каліфорнійському університеті в Лос-Анджелесі. Комп’ютер «Honeywell 516» мав 12 КБ оперативної пам’яті. До 1971 року була розроблена перша програма для відправки електронної пошти по мережі, котра відразу стала дуже популярною. У 1973 році до мережі були підключені через трансатлантичний телефонний кабель перші іноземні організації з Великобританії та Норвегії, мережа стала міжнародною.

У 1970-х роках мережа в основному використовувалася для пересилки електронної пошти, тоді ж з’явилися перші списки поштової розсилки, групи новин та дошки оголошень. Однак у той час мережа ще не могла легко взаємодіяти з іншими мережами, побудованими на інших технічних стандартах. До кінця 1970-х років почали бурхливо розвиватися протоколи передачі даних, що були стандартизовані в 1982-83 роках. 1 січня 1983 року мережа ARPANET перейшла з протоколу NCP на TCP/IP, який успішно застосовується до цих пір для об’єднання (або, як ще кажуть, *«нашарування»*) мереж. Саме в 1983 році термін «Інтернет» закріпився за мережею ARPANET.

IP-адреса. Кожен комп’ютер в Інтернет має унікальну 32-х бітову IP-адресу, яку прийнято записувати у вигляді чотирьох чисел від 0 до 255, що розділяються точками. Зазвичай перша частина адреси – число від 1 до 223.

Приклади:

192.13.77.190

182.182.10.1

195.130.12.47:210 (нестандартний порт)

У 1984 році у мережі ARPANET з’явився серйозний суперник, Національний науковий фонд США (NSF) заснував міжуніверситетську мережу NSFNet (скор. від англ. National Science Foundation Network), яка була сформована з дрібніших мереж (включаючи відомі на той час Usenet та Bitnet) і

мала набагато більшу пропускну здатність, аніж ARPANET. До цієї мережі за рік підключилися близько 10 тис. комп'ютерів, звання «Інтернет» почало плавно переходити до NSFNet. Мережа NSFNet була спочатку створена для зв'язку суперкомп'ютерів в основних дослідницьких організаціях, але вона швидко виросла і включила в себе більшість найбільших університетів і дослідницьких лабораторій.

У 1988 році був винайдений протокол Internet Relay Chat (IRC), завдяки чому в Інтернеті стало можливе спілкування в реальному часі (чат).

Протокол в даному випадку – це, образно кажучи, «мова», яка використовується комп'ютерами для обміну даними при роботі в мережі. Щоб різні комп'ютери мережі могли взаємодіяти, вони повинні «розмовляти» однією «мовою», тобто використовувати один і той же протокол. Простіше кажучи, ***протокол*** – це правила передачі даних між вузлами комп'ютерної мережі.

У 1995 році NSFNet повернулася до ролі дослідницької мережі, маршрутизацією всього трафіку Інтернету тепер займались мережеві провайдери, а не суперкомп'ютери Національного наукового фонду.

24 жовтня 1995 Федеральна рада по мережах (Federal Networking Council) одноголосно схвалив резолюцію, що визначає термін Інтернет (Internet):

Термін ***«Internet»*** (Інтернет) відноситься до глобальної інформаційної системи, яка – (I) логічно пов'язана глобально унікальним адресним простором на основі Протоколу Інтернет (IP) або його подальшими розширеннями/удосконаленнями; (II) здатна підтримувати комунікацію за допомогою пакета протоколів TCP/IP або його подальшими розширеннями/удосконаленнями, і/або іншими, сумісними з IP протоколами; і (III) надає, використовує або робить доступними, публічно або в приватному порядку, високорівневі служби, які спираються на комунікацію і описану тут інфраструктуру.

У 1990-х років Інтернет об'єднав у собі більшість існуючих на той час мереж (хоча деякі, як Фідонет, залишились відособленими). Об'єднання виглядало привабливим завдяки відсутності єдиного керівництва, а також завдяки відкритості технічних стандартів Інтернету, що робило мережі незалежними від бізнесу і конкретних компаній. До 1997 року в Інтернеті налічувалося вже близько 10 млн комп'ютерів, було зареєстровано понад 1 млн доменних імен. Інтернет став дуже популярним засобом для обміну інформацією.

І таким чином, на сьогоднішній день, Інтернет пов'язує в єдине ціле мільйони обчислювальних пристроїв, розміщених у різних точках землі. Цими пристроями можуть бути не лише настільні персональні комп'ютери, але й

сервери і навіть такі нетрадиційні кінцеві системи як телевізори, мобільні комп'ютери, смартфони, автомобілі, «розумній дім» та інші. (рис. 1.2).

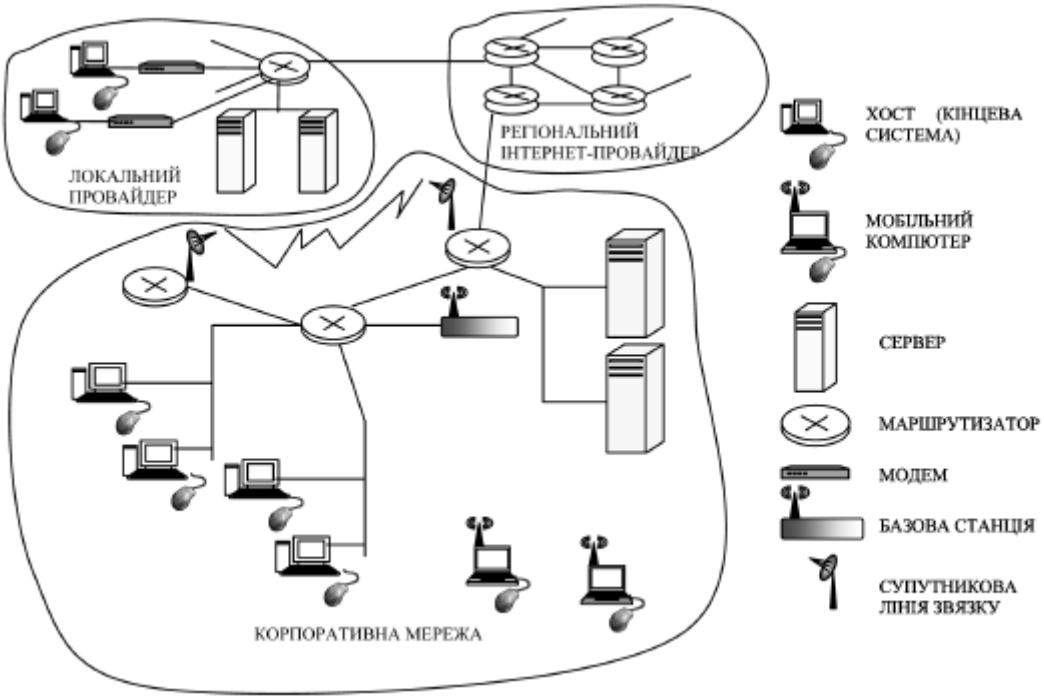


Рис. 1.2. Основні складові Інтернету

Всі ці пристрої за термінологією Інтернету називають ***хостами***, або кінцевими системами. За оцінкою фахівців кількість хостів у світі зростає майже експоненціально (рис. 1.3), лише в 2010 році за різними підрахунками, кількість хостів складала майже 500 мільйонів.

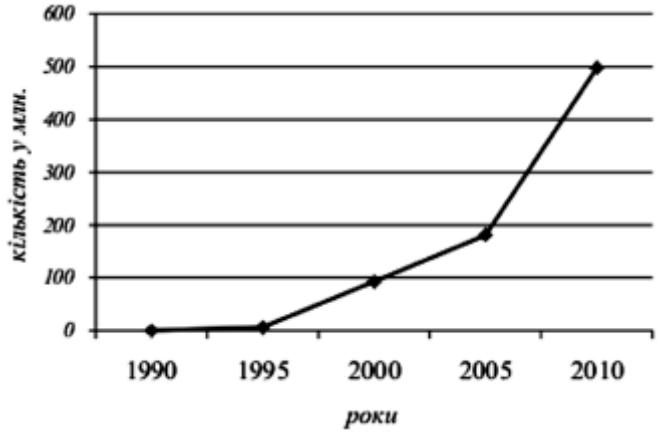


Рис. 1.3. Динаміка росту кількості хостів у світі

Кінцеві пристрої зв'язані величезною кількістю різноманітних ліній зв'язку, що використовують різні типи фізичних носіїв: коаксильних, мідних, оптично-волоконних кабелів а також ліній радіозв'язку і тому подібних. Саме лінія зв'язку визначає швидкість передачі даних, максимальне значення якої називають *пропускною здатністю*. Типовою схемою пов'язання кінцевих пристроїв являється поєднання множини послідовних ліній за допомогою

спеціальних комутаційних пристроїв *маршрутизаторів*. Маршрутизатор здійснює прийом деякої порції даних (пакетів) та перенаправления на один із своїх вихідних каналів зв'язку. Послідовність каналів зв'язку та маршрутизаторів при проходженні пакета є маршрутом чи шляхом пакету в мережі, причому, він заздалегідь не відомий й визначається безпосередньо в процесі передачі.

1.4. Всесвітня павутина

У 1989 році в Європі, в стінах Європейської ради з ядерних досліджень народилася концепція Всесвітньої павутини. Її запропонував знаменитий британський вчений *Тім Бернерс-Лі*, він же протягом двох років розробляв протокол ***HTTP***, мову ***HTML*** та ідентифікатори ***URI***.

Тімоті Джон Бернерс-Лі народився 8 червня 1955 року. Крім уже перерахованих винаходів він розробив перший браузер (перша назва – *WWW*, пізніше перейменований в *Nexus*), а пізніше – концепцію семантичної павутини. Тім Бернерс-Лі – діючий глава Консорціуму Всесвітньої павутини (W3 Consorcium), організації, що займається питаннями стандартизації у всесвітній павутині (сайт www.w3.org).

У 1990 році мережа ARPANET припинила своє існування, повністю програвши конкуренцію NSFNet. У тому ж році було зафіксовано перше підключення до Інтернету по телефонній лінії (т. зв. «Дозвон» англ. Dialup access).

У 1991 році Всесвітня павутина стала загальнодоступною в Інтернеті.

Всесвітня павутина (*World Wide Web*) – розподілена система, що надає доступ до пов'язаних між собою документів, розташованих на різних комп'ютерах, підключених до Інтернету. Більшість ресурсів всесвітньої павутини є ***гіпертекстом***.

У 1995 році Всесвітня павутина стала основним постачальником інформації в Інтернеті, обігнавши по об'єму трафіку протокол пересилки файлів FTP, тоді ж був створений Консорціум всесвітньої павутини (W3C). Можна сказати, що Всесвітня павутина перетворила Інтернет і створили його сучасний вигляд. З 1996 року Всесвітня павутина майже повністю підміняє собою поняття «Інтернет».

Середовище WWW не має централізованої структури. Воно поповнюється тими, хто бажає розмістити в Інтернеті свої матеріали, і може розглядатися як інформаційний простір. Як правило, документи WWW зберігаються на постійно підключених до Інтернету комп'ютерах Web-серверах. Зазвичай на Web-сервері розміщують не окремий документ, а групу

взаємопов'язаних документів. Така група є ***Web-вузлом*** (жаргонний термін Web-сайт). Розміщення підготовлених матеріалів на Web-вузлі називається Web-виданням або Web-публікацією.

Звичайний Web-вузол видає інформацію (запрошений документ) тільки у відповідь на звернення клієнта. Щоб стежити за оновленням опублікованих матеріалів, користувач змушений регулярно звертатися до даного вузла. Сучасна модель Web-вузла дозволяє автоматично в заданий час передати оновлену інформацію на комп'ютер зареєстрованого клієнта. Web-вузли, які здатні самостійно ініціювати поставку інформації, називають *каналами***.**

Окремий документ World Wide Web називають *Web-сторінкою*. Зазвичай це комбінований документ, який може містити текст, графічні ілюстрації, мультимедійні та інші вставні об'єкти. Для створення Web-сторінок використовується мова HTML (HyperText Markup Language – мова розмітки гіпертексту), який за допомогою вставлених в документ тегів описує логічну структуру документа, керує форматуванням тексту і розміщенням вставних об'єктів. Інтерактивні Web-вузли отримують інформацію від користувача через форми і генерують запитану Web-сторінку за допомогою спеціальних програм (сценаріїв CGI), динамічного HTML і інших засобів.

Відмінною особливістю середовища World Wide Web є наявність засобів переходу від одного документа до іншого, тематично з ним пов'язаного, без явної вказівки адреси. Зв'язок між документами здійснюється за допомогою гіпертекстових посилань (або просто гіперпосилань). ***Гіперпосилання*** це виділений фрагмент документа (текст або ілюстрація), з яким асоційований адрес іншого Web-документа. При використанні гіперпосилання відбувається перехід за гіперпосиланням – відкриття Web-сторінки, на яку вказує посилання. Механізм гіперпосилань дозволяє організувати тематичну подорож по World Wide Web без використання (і навіть знання) адрес конкретних сторінок.

Для запису адрес документів Інтернету (Web-сторінок) використовується форма, яка називається ***адресою URL***. Адреса URL містить вказівки на прикладний протокол передачі, адресу комп'ютера і шлях пошуку документа на цьому комп'ютері. Адреса комп'ютера складається з декількох частин, між якими ставлять крапку, наприклад www.intel.ua. Частини адреси, що розташовані праворуч, визначають мережну належність комп'ютера, а ліві елементи вказують на конкретний комп'ютер даної мережі. Перетворення адреси URL у цифрову форму IP-адреси здійснює ***служба доменних імен*** (*англ. Domain Name Service,* ***DNS***). Як роздільник в шляху пошуку документа Інтернету завжди використовується символ косої риски.

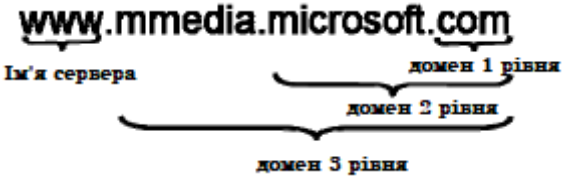
Як відомо документи Інтернету призначені для відображення в електронній формі, причому автор документа не знає, які можливості

комп’ютера, на якому документ буде відображатися. Тому мова HTML забезпечує не стільки форматування документа, скільки опис його логічної структури. Форматування і відображення документа на конкретному комп’ютері проводиться спеціальною програмою ***браузером*** (від англійського слова browser). До основних функцій браузерів можна віднести: встановлення зв’язку з Web-сервером, на якому зберігається документ, і завантаження всіх компонентів комбінованого документа; інтерпретація тегів мови HTML, форматування і відображення Web-сторінки відповідно до можливостей комп’ютера, на якому браузер працює; надання ресурсів для відображення мультимедійних та інших об’єктів, що входять до складу Web-сторінок, а також механізму розширення, що дозволяє налаштовувати програму на роботу з новими типами об’єктів; забезпечення автоматизації пошуку Web-сторінок і спрощення доступу до Web-сторінок, що відвідували раніше, надання доступу до вбудованих або автономних засобів для роботи з іншими службами Інтернета, а також забезпечення безпечної роботи в системі WWW.

1.5. Система доменних імен

Система доменних імен була розроблена ще у 1984 році.

Доменне ім’я – символьне ім’я, що служить для ідентифікації областей – одиниць адміністративної автономії в кіберпросторі – в складі вище стоячої по ієрархії такої області.



Загальні домени верхнього рівня (Generic TLDs – gTLDs) створені для всього інтернет-співтовариства. Спочатку було створено всього вісім gTLD: COM, NET, ORG, INT, EDU, GOV, MIL і ARPA (домен ARPA створювався на час, необхідний для впровадження системи доменних імен, але виявився зовсім не тимчасовим явищем, він використовується для технічних цілей). У 1984 р при затвердженні доменів, в документах було записано, що такої кількості «буде досить, і поява нових доменів малоймовірна». Однак зростання мережі інтернет перевершив очікування, у зв’язку з чим потреба світової інтернет-спільноти в числі доменів верхнього рівня збільшилася. Коли мережа переступила національні кордони США з’явилися національні домени першого рівня типу: uk, jp, au, ch, і т.п. Для СРСР також був виділений домен su. Після 1991 року, коли республіки Союзу стали суверенними, багато хто з них отримали свої власні домени: ua, ru, la, li, і т.п. У 2001 році було прийнято рішення про введення ще семи нових gTLD: INFO, BIZ, NAME, COOP,

MUSEUM, AERO і PRO. В даний час зазначені домени функціонують в повному обсязі.

Приклади: com – компанії, edu – освіту, org - організації, net – мережеві, gov – урядові, mil – військові, ua – Україна, ca – Канада, uk – Великобританія, au – Австралія і т.д.

З розвитком інтернету особливу цінність набули «красиві» адреси сайтів, інакше кажучи домени. Загальна кількість зареєстрованих доменів наближається до 200 мільйонів і підібрати вільне, красиве і коротке доменне ім'я стало дуже важко. Утворився ринок перепродажу доменних імен. Сюди входять компанії, які реєструють домени, купують і продають домени на вторинному ринку, займаються розміщенням реклами на зареєстрованих доменах, хостингові сервіси, юридичні та правові організації і т. п. Близько 30% сайтів не містять ніякої інформації і існують тільки для продажу рекламних посилань.

Передбачається, що тисячі компаній хотіли б мати свій офіційний сайт на домені *business.com.* Ось чому цей домен був проданий за 360 мільйонів доларів США (бюджет невеликої держави). На сьогоднішній день комерційну цінність мають будь-які домени, співзвучні з поширеними англійськими іменниками в однині, і домени, що складаються не більше, ніж з трьох букв або цифр. У зоні .com, після того як закінчилися у вільній реєстрації домени з трьох букв, цінність мають також будь-які чотирибуквені доменні імена.

Комп'ютери, які здійснюють перетворення імен комп'ютерів в адреси і навпаки, називаються ***DNS-серверами***. При посилці даних комп'ютеру із зазначенням його адреси, дані відразу направляються до пункту призначення. Якщо ж вказується ім'я, то спочатку хост-відправник робить запит у свого DNS-сервера, щоб дізнатися адресу за відомим іменем, і тільки потім відправляє дані.

Документ RFC 2606 (Reserved Top Level DNS Names – Зарезервовані імена доменів верхнього рівня) визначає назви доменів, які слід використовувати в якості прикладів (наприклад, в документації), а також для тестування. Крім example.com, example.org і example.net, в цю групу також входять test, invalid та ін.

URL (*Uniform Resource Locator*), як вже зазначалося раніше, це адреса об'єкта (зазвичай файлу) в Інтернеті. Загальна структура якої наведена нижче:

протокол: // адреса_сервера / ім'я_каталога / ім'я_файла

Приклади: http://www.fio.ua/about/index.htm
ftp://ftp.asu.ua/pub/music/mp3/alsu.mp3
mailto: //sergei@asu.ua

У травні 2010 року вперше в інтернеті з'явилися нелатинські домени верхнього рівня (.امارات - ОАЕ, .قيع دوع سلا - Саудівська Аравія, .مصر - Єгипет, .рф – Росія).

1.6. Браузери

Як вже зазначалося раніше, перший браузер був випущений в 1990 році і отримав назву *WorldWideWeb*. Пізніше, щоб не плутати «всесвітню павутину» з назвою програми, Бернерс-Лі перейменував браузер в Nexus.

Цей браузер текстовий, і картинки він не відображав.

У 1993 році з'явився перший браузер з графічним інтерфейсом NCSA Mosaic.

Це перший веб-браузер під операційну систему Microsoft Windows (тоді ще MS-DOS з графічною оболонкою MS Windows 3) з графічним інтерфейсом користувача і розвиненими можливостями, на якому засновані і Netscape Navigator, і Microsoft Internet Explorer. Однак, незважаючи на те, що NCSA (National Center for Supercomputing Applications) є піонером в області Web-браузерів, робота з розвитку програми Mosaic припинена в 1997 році. Остання версія Mosaic 3.0, хоча і володіє приємним інтерфейсом, але не підтримує такі сучасні технології, як Java, модулі розширення і навіть анімовані GIF-файли. Однак цей браузер все-таки має вбудовані e-mail і ftp-клієнти. Основними розробниками Mosaic були Марк Андерісен і Ерік Біна.

Нині ***браузер*** – комплексний додаток для обробки і виведення різних складових веб-сторінки, а також, для надання інтерфейсу між веб-сайтом і його відвідувачем. Для цього на сервер відправляється запит, а результат виводиться у вікні браузера.

Те, яким чином браузер обробляє і відображає HTML-файли, визначено специфікаціями HTML і CSS. Вони розробляються Консорціумом W3C, який впроваджує стандарти для Інтернету. Однак, як не дивно, специфікації, яка б визначала стандарти для користувача інтерфейсу браузера, не існує. Сучасні інтерфейси є результатом багаторічної еволюції, а також того, що розробники частково копіюють один одного. У специфікації HTML5 не вказано, що саме повинен містити інтерфейс браузера, однак перераховані деякі основні елементи. До них відноситься адресний рядок, рядок стану і панель інструментів.

Практично всі популярні браузери поширюються безкоштовно або «в комплекті» з іншим додатками:

- Internet Explorer та Microsoft Edge (як невід'ємна частина Microsoft Windows);
- Mozilla Firefox (безкоштовно, вільне ПЗ);

- Opera (безкоштовно, починаючи з версії 8.50);
- Safari (спільно з Mac OS або безкоштовно для Windows);
- Google Chrome (браузер з відкритим вихідним кодом).

1.6.1. Структура верхнього рівня веб-браузера

Нижче перераховані основні компоненти браузера (рис. 1.4).

Інтерфейс (User Interface) – включає адресний рядок, кнопки «Назад» і «Вперед», меню закладок і т. д. До нього відносяться всі елементи, крім вікна, в якому відображається запитувана сторінка.

Движок браузера (Browser engine) – управляє взаємодією інтерфейсу і модуля відображення.

Модуль відображення (Rendering engine) – відповідає за виведення запитаного вмісту на екран. Наприклад, якщо запитується HTML-документ, модуль відображення виконує синтаксичний аналіз коду HTML і CSS і виводить результат на екран.

Мережеві компоненти (Networking) – призначені для виконання Інтернет-викликів, таких як HTTP-запити. Їх інтерфейс не залежить від типу платформи, для кожного з яких є власні реалізації.

Виконавча частина користувацького інтерфейсу (UI Backend) – використовується для відтворення основних віджетів, таких як вікна і поля зі списками. Її універсальний інтерфейс також не залежить від типу платформи. Виконавча частина завжди застосовує методи користувацького інтерфейсу конкретної операційної системи.

Інтерпретатор JavaScript (JavaScript Interpreter) – використовується для синтаксичного аналізу і виконання коду *JavaScript*.

Сховище даних (Date Persistence) – необхідне для зберігання процесів. Браузер зберігає на жорсткий диск дані різних типів, наприклад файли *cookie*. У новій специфікації HTML (HTML5) є визначення терміну «веб-база даних»: це повноцінна (хоча і полегшена) браузерна база даних.

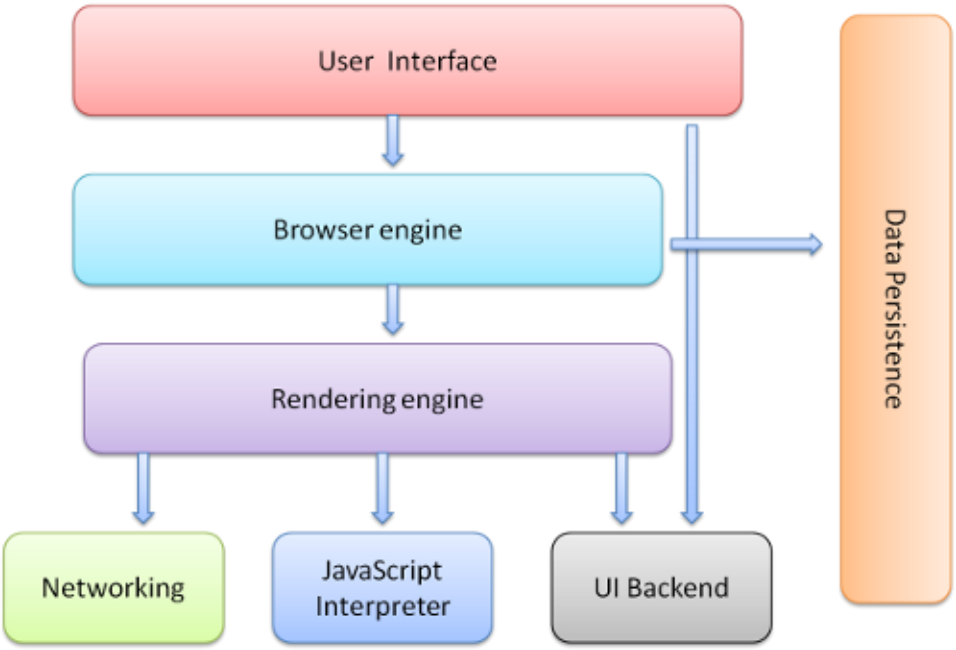


Рис.1.4. Основні компоненти веб-браузера

Слід зазначити, що Chrome, на відміну від більшості браузерів, використовує кілька модулів відображення, по одному в кожній вкладці, які представляють собою окремі процеси.

Порядок виконання лабораторної роботи №1:

1. Включити ПК.
2. Ознайомитися з короткими теоретичними відомостями.
3. Виконати теоретичне завдання згідно з номером бригади, який приведено в табл. 1.1, особливо звернути увагу на механізми забезпечення інформаційної безпеки в веб-браузерах.
4. Знайти і обробити інформацію відповідно до завдання та підготувати коротку доповідь (міні-презентацію).
5. Завантажити та встановити не менше 3-х веб-браузерів, здійснити їх налаштування, розібратися в їх функціоналі, та проаналізувати додаткові можливості.
6. Провести порівняльний аналіз обраних браузерів та сформувати відповідну порівняльну таблицю.
7. Оформити звіт згідно до вимог (додаток 1).
8. Зробити висновки, відповісти на контрольні питання та підготуватися до усного опитування.

Зміст звіту:

1. Титульний лист.
2. Постановка завдання.

3. Протокол виконання лабораторної роботи, що містить доповідь та порівняльну таблицю за результатами проведеного аналізу.

4. Висновки та відповіді на контрольні питання.

Завдання на виконання лабораторної роботи №1

Таблиця № 1.1 (розбитися на бригади по 2 чоловіки)

Номер варіанта	Завдання
1	Знайти загальнодоступні матеріали щодо веб-браузера Internet Explorer, проаналізувати його функціонал, оцінити переваги та недоліки.
2	Знайти загальнодоступні матеріали щодо веб-браузера Microsoft Edge, проаналізувати його функціонал, оцінити переваги та недоліки.
3	Знайти загальнодоступні матеріали щодо веб-браузера Google Chrome, проаналізувати його функціонал, оцінити переваги та недоліки.
4	Знайти загальнодоступні матеріали щодо веб-браузера Mozilla Firefox, проаналізувати його функціонал, оцінити переваги та недоліки.
5	Знайти загальнодоступні матеріали щодо веб-браузера Opera, проаналізувати його функціонал, оцінити переваги та недоліки.
6	Знайти загальнодоступні матеріали щодо веб-браузера Yandex, проаналізувати його функціонал, оцінити переваги та недоліки.
7	Знайти загальнодоступні матеріали щодо веб-браузера Safari, проаналізувати його функціонал, оцінити переваги та недоліки.
8	Знайти загальнодоступні матеріали щодо веб-браузера Tor, проаналізувати його функціонал, оцінити переваги та недоліки.
9	Знайти загальнодоступні матеріали щодо веб-браузера Vivaldi, проаналізувати його функціонал, оцінити переваги та недоліки.
10	Знайти загальнодоступні матеріали щодо веб-браузера Maxthon, проаналізувати його функціонал, оцінити переваги та недоліки.
11	Знайти загальнодоступні матеріали щодо веб-браузера UC Browser, проаналізувати його функціонал, оцінити переваги та недоліки.
12	Знайти загальнодоступні матеріали щодо веб-браузера SRWare Iron, проаналізувати його функціонал, оцінити переваги та недоліки.
13	Знайти загальнодоступні матеріали щодо веб-браузера Arora, проаналізувати його функціонал, оцінити переваги та недоліки.
14	Знайти загальнодоступні матеріали щодо веб-браузера Midori, проаналізувати його функціонал, оцінити переваги та недоліки.

Контрольні питання:

1. Надайте визначення наступним поняттям: «кібернетичний простір», «Інтернет», «Всесвітня павутина», «веб-браузер».
2. Опишіть основні складові кіберпростору.
3. Виділіть три рівні кібернетичного простору.
4. Що виконує служба доменних імен?
5. Назвіть основні функції веб-браузерів.
6. Перерахуйте та опишіть основні компоненти веб-браезера.

Лабораторна робота №2
«Фізична основа кіберпростору – Інтернет. Мережеві утиліти та їх використання для моніторингу та діагностики мережі»

Мета роботи:

1. Вивчення основ адресації в комп'ютерних мережах.
2. Набуття практичних навичок роботи з мережевими утилітами, а саме:
   - визначення налаштувань для підключення до локальної мережі і до мережі Internet з використанням утиліти ipconfig;
   - дослідження ймовірносно-часових характеристик фрагментів мережі Internet з використанням утиліти ping;
   - дослідження топології фрагментів мережі Internet з використанням утиліти tracert.

Стислі теоретичні відомості:

Одним із проявів наявності шкідливої програми може бути збільшена мережева активність. Шкідлива програма може відправляти листи, завантажувати інформацію з Інтернету, передавати комусь по мережі конфіденційну інформацію та багато іншого. При цьому необхідно пам'ятати, що легальні додатки також можуть використовувати Інтернет без дій користувача – наприклад, антивірусна програма може завантажувати оновлення бази сигнатур. Ось чому так важливо здійснювати контроль роботи мережі, а саме моніторинг і аналіз мережі. Незважаючи на те, що дані питання будуть розглядатися більш детально на наступних курсах, уже на даній лабораторній роботі розглядаються основи адресації в комп'ютерних мережах та використання декількох базових мережевих утиліт.

2.1. Основи адресації в комп'ютерних мережах

Кожен комп'ютер в мережі TCP/IP має адреси трьох рівнів:

1. На канальному рівні, локальну адресу вузла, яка визначається технологією, за допомогою якої побудована окрема мережа (в яку входить даний вузол). Для вузлів, що входять в локальні мережі, це MAC-адреса мережного адаптера або порту маршрутизатора, наприклад, 00-0C-29-7B-E6-3A.

2. IP-адреса, яка виражається одним 32-розрядним числом (4 байти), наприклад, 160.81.5.131 і використовується на мережному рівні. Вона призначається адміністратором під час конфігурування комп'ютерів і маршрутизаторів. IP-адреса складається з двох частин: адреси мережі і номера вузла (комп'ютера) в мережі. Адреса мережі може бути обрана адміністратором довільно, або призначена за рекомендацією спеціального підрозділу (Network Information Center, NIC), якщо мережа повинна працювати як складова частина мережі Інтернет. Зазвичай інтернет-провайдери отримують діапазони адрес у підрозділів NIC, а потім розподіляють їх між своїми абонентами. Номер вузла в протоколі IP призначається незалежно від локальної адреси вузла. Розподіл IP-адреси на поле адреси мережі і номера вузла – гнучке, і межа між цими полями може встановлюватися досить таки довільно. Комп'ютер може входити в кілька IP-мереж. В цьому випадку вузол повинен мати кілька IP-адрес, по числу мережевих зв'язків. Таким чином, IP-адреса характеризує не окремий комп'ютер або маршрутизатор, а одне мережеве з'єднання.

3. Символьний ідентифікатор – ім'я, наприклад, SERV1.IBM.COM. Ця електронна адреса призначається адміністратором і складається з декількох частин, наприклад, імені машини, імені організації, імені домену. Така адреса, так зване DNS-ім'я, використовується на прикладному рівні, наприклад, в протоколах FTP або telnet.

2.1.1. Адресація комп'ютерів на канальному рівні

Кожен комп'ютер, підключений до мережі, має мережевий адаптер (мережеву карту) з присвоєним йому унікальним адресом, так званим ***MAC-адресом***, який задається при виготовленні мережевого адаптера (виробниками устаткування) і в подальшому не змінюється. Довжина і інші особливості MAC-адреси залежать від використовуваної в локальній мережі технології. У мережах Ethernet MAC-адреса має довжину 6 байт, записаних в шістнадцятковому форматі і розділених дефісами (рис. 2.1): старші три байти – ідентифікатор фірми виробника, а молодші три байти призначаються унікальним чином самим виробником.

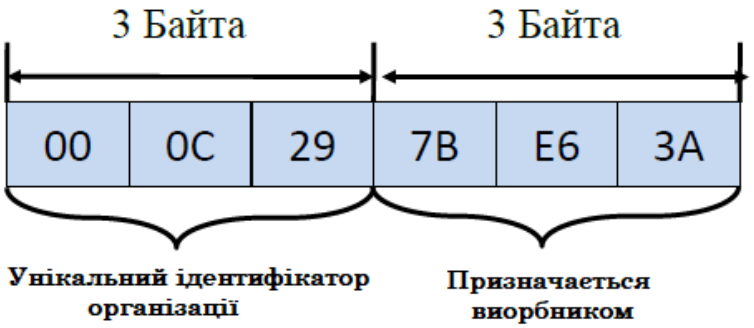


Рис. 2.1. Структура MAC-адреси

Для визначення локальної адреси за IP-адресою використовується протокол визначення адреси ***ARP*** *(Address Resolution Protocol).* Існує також протокол, що вирішує зворотну задачу – знаходження IP-адреси за відомим локальним адресом, так званий ***RARP*** – *реверсивний ARP*. Він використовується при старті бездискових станцій, які в початковий момент не знають свого IP-адресу, але знають адресу свого мережного адаптера.

Необхідність у зверненні до протоколу ARP виникає кожен раз, коли модуль IP передає пакет на рівень мережевих інтерфейсів, наприклад драйверу Ethernet. IP-адреса вузла призначення відома модулю IP. Потрібно на його основі знайти MAC-адресу вузла призначення. Робота протоколу ARP починається з перегляду так званої АКР-таблиці. Кожен рядок таблиці встановлює відповідність між IP-адресом і MAC-адресом. Поле «Тип запису» може містити одне з двох значень – «динамічний» або «статичний». Статичні записи створюються вручну за допомогою утиліти ARP і не мають строку дії, точніше, вони діють до тих пір, поки комп'ютер або маршрутизатор не будуть вимкнені. Динамічні ж записи створюються модулем протоколу ARP, що використовує широкомовні можливості локальних мережевих технологій. Динамічні записи повинні підлягати періодичному оновленню. Якщо запис не оновлювався протягом певного часу (порядку декількох хвилин), то він виключається з таблиці. Таким чином, в ARP -таблиці містяться записи не про всі вузли мережі, а тільки про ті, які активно беруть участь в мережевих операціях. Оскільки такий спосіб зберігання інформації називають *кешуванням*, ARP-таблиці іноді називають ***ARP-кеш***. Після того як модуль IP звернувся до модуля ARP із запитом на дозвіл адреси, відбувається пошук в ARP-таблиці зазначеної в запиті IP-адреси. Якщо така адреса в ARP-таблиці відсутня, то вихідний IP-пакет, для якого потрібно було визначити локальну адресу, ставиться в чергу. Далі протокол ARP формує свій запит (ARP-запит), вкладає його в кадр протоколу канального рівня і розсилає запит широкомовно. Всі вузли локальної мережі отримують ARP-запит і порівнюють зазначений там IP-адрес з власним. У разі їх збігу вузол формує ARP-відповідь, в якому вказує

свою IP-адресу і свою локальну адресу, а потім відправляє його вже за адресом комп'ютера, що сформував запит, так як адресу відправника вказано в самому запиті.

2.1.2. Адресація в IP-мережах та основні класи IP-адрес

Так як оперувати довгими двійковими числами досить складно, число, яке визначає IP-адресу версії 4 (IPv4), розбивають на 4 октети – восьмирозрядних двійкових числа, а кожне з цих чисел представляють в десятковому вигляді. Октети відокремлюють один від одного крапками. Таким чином, 32-розрядна IP-адреса представляється у вигляді: 255.255.255.255 (десяткове число може змінюватися від 0 до 255 – максимального значення восьмирозрядного двійкового числа). Наприклад: 160.81.5.131 – десяткова форма представлення IP-адреси, 10100000.01010001.00000101.10000011 – двійкова форма представлення цієї ж адреси.

Далі показана структура IP-адреси в залежності від класу мережі.

Рис 2.2. Структура IP-адреси в залежності від класу мережі

Як вже зазначалося раніше, адреса складається з двох логічних частин – номера мережі і номера вузла в мережі. Яка частина адреси відноситься до номера мережі, а яка до номера вузла, визначається значеннями перших бітів адреси:

- Якщо адреса починається з 0, то мережу відносять до ***класу А*** (великі мережі загального користування), і номер мережі займає один байт, інші три байти інтерпретуються як номер вузла в мережі. Мережі класу А мають номери в діапазоні від 1 до 126. (номер 0 не використовується, а номер 127 зарезервований для спеціальних цілей).
- Якщо перші два біти адреси рівні 10, то мережа відноситься до ***класу В*** і є мережею середніх розмірів з числом вузлів 28 – 216. У мережах класу В під адресу мережі і під адресу вузла відводиться по 16 біт, тобто по 2 байти.
- Якщо адреса починається з послідовності 110, то це мережа ***класу С*** з числом вузлів не більше 28. Під адресу мережі відводиться 24 біти, а під адресу вузла – 8 біт.
- Якщо адреса починається з послідовності 1110, то вона є адресою ***класу D*** і позначає особливу, групову адресу – ***multicast***. Якщо в пакеті, як адреса призначення, вказано адресу класу D, то такий пакет повинні отримати всі вузли, яким присвоєно цю адресу.
- Якщо адреса починається з послідовності 11110, то це адреса ***класу Е,*** вона зарезервована для майбутнього використання.

Таблиця 2.1. Список діапазонів адрес, відповідних кожному класу мереж

Клас	**Найменша адреса**	**Найбільша адреса**
A	0.0.0.0	127.255.255.255
B	128.0.0.0	191.255.255.255
C	192.0.0.0	223.255.255.255
D	224.0.0.0	239.255.255.255
E	240.0.0.0	255.255.255.255

Деякі IP-адреси мають спеціальне призначення, наприклад, адреса:

- 0.0.0.0 представляє адресу шлюза, тобто адресу комп’ютера, на яку повинні надсилатися інформаційні пакети, якщо вони не знайшли адресата в локальній мережі;
- 127.будь-яке число (часто 127.0.0.1) – адреса *«петлі»*. Дані, передані за цією адресою, надходять на вхід комп’ютера, як отримані по мережі. Така адреса необхідна при налагодженні мережевих програм;
- 255.255.255.255 – широкомовна адреса. Повідомлення, передані за цією адресою, отримують всі вузли локальної мережі, в яку входить комп’ютер-джерело повідомлення (в інші локальні мережі воно не передається);
- номер мережі. всі нулі – адреса мережі;
- всі нулі. номер вузла – вузол в даній мережі. Може використовуватися для передачі повідомлень конкретному вузлу всередині локальної мережі;

- номер мережі. всі одиниці (двійкові) – всі вузли зазначеної мережі.

У локальних мережах використовуються спеціальні, так звані «сірі» IP-адреси. Вони визначені документом RFC 1918 (RFC – Requests For Comments, запропонований проект стандарту, більшість документів, що регламентують Інтернет, описано в RFC) і приведені в табл. 2.2:

Таблиця 2.2.

Діапазони IP-адрес, що використовуються в локальних мережах
10.0.0.0 – 10.255.255.255
172.16.0.0 – 172.31.255.255
192.168.0.0 – 192.168.255.255

У невеликих за розміром локальних мережах зазвичай застосовується останній діапазон адрес. Мережеві маршрутизатори не передають інформацію для вузлів з цими адресами, тому вона виявляється «замкненою» всередині локальної мережі. Така схема дозволяє в різних локальних мережах використовувати одні й ті ж IP-адреси і не призводить до конфліктів.

Для підвищення гнучкості використання IP-адрес розподіл адреси на частини з використанням класів доповнюється технологією ***CIDR*** (Classless Inter-Domain Routing) – безкласової міждоменної маршрутизації. На відміну від класової (довжина маски фіксована по октетам), тут можна заощадити IP-адреси використовуючи маски змінної довжини (*VLSM* – variable length subnet mask). У цьому випадку адреса мережі формується за допомогою двох чисел: адреси і маски. Маска це теж 32-розрядне двійкове число, за допомогою якого з IP-адреси виділяється адреса мережі. Схема формування адреси мережі з використанням маски проста, її можна пояснити на прикладі, припустимо, адреса представлена двійковим числом 110101, маска числом 111100. Маска накладається на адресу, як трафарет, в якому одиниці відповідають прорізам, в яких ми «побачимо» адресу мережі, в нашому прикладі адреса мережі відповідає числу 110100. Маска завжди містить таке двійкове число, старші розряди якого поспіль одиниці, а молодші – нулі, одиниці представляють «прозору» частину трафарету, а нулі – «непрозору». Маска так само, як і адреса, записується у вигляді чотирьох десяткових чисел, розділених точками.

Для компактного запису пари чисел: IP-адреса-маска, використовується також інша форма, наприклад: 10.0.0.8/30. Число до слеша є IP-адресою, а число після слеша – кількість розрядів в IP-адресі, що відводяться для адресації мережі. Число 30 після слеша відповідає масці 255.255.255.252. Після визначення адреси мережі, решта IP-адреси використовується для адресації вузлів в мережі.

Приклад розбиття однієї мережі класу «С» на підмережі за допомогою маски відображено в таблиці 2.3.

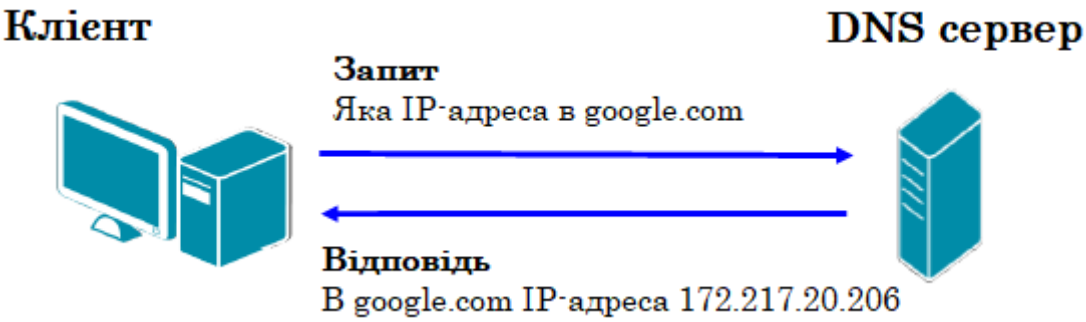
Таблиця 2.3.

Маска				Кількість хостів	Кількість підмереж	Префікс
1-й октет	2-й октет	3-й октет	4-й октет			
255	255	255	**252**	4(-2)	1/64	/30
255	255	255	**248**	8(-2)	1/32	/29
255	255	255	**240**	16(-2)	1/16	/28
255	255	255	**224**	32(-2)	1/8	/27
255	255	255	**192**	64(-2)	1/4	/26
255	255	255	**128**	128(-2)	1/2	/25
255	255	255	**0**	256(-2)	1	/24

2.1.3. Символьне відображення імені комп’ютера в мережі

Як нам вже відомо, кожен комп’ютер в мережі має унікальну адресу. При використанні IP-адресації це IP-адреса. Однак людині досить важко оперувати довгими наборами цифр, що не несуть смислового навантаження, тому завжди застосовуються системи перетворення імен, що ставлять у відповідність цифровій адресі комп’ютера його символьне ім’я. У глобальних мережах і мережі Інтернет це служба ***DNS* (*Domain Name System*)** – розподілена база даних, що підтримує ієрархічну систему імен для ідентифікації вузлів в мережі Інтернет. Служба DNS призначена для автоматичного пошуку IP-адреси за відомим символьним імені вузла. Специфікація DNS визначається стандартами RFC 1034 і 1035. DNS вимагає статичноїної конфігурації своїх таблиць, які відображають імена комп’ютерів в IP-адресу.

Протокол DNS є службовим протоколом прикладного рівня. Цей протокол несиметричний – в ньому визначені DNS-сервери і DNS-клієнти. DNS-сервери зберігають частину розподіленої бази даних про відповідність символьних імен і IP-адрес. Ця база даних розподілена по адміністративним доменам мережі Інтернет. Клієнти сервера DNS знають IP-адреса сервера DNS свого адміністративного домену і за протоколом IP передають запит, в якому повідомляють через відоме символьне ім’я і просять повернути відповідну йому IP-адресу.



Якщо дані щодо запиту відповідності зберігаються в базі даного DNS-сервера, то він відразу посилає відповідь клієнту, якщо ж ні – то він надсилає запит DNS-серверу іншого домену, який може сам обробити запит, або передати його іншому DNS-сервера. Всі DNS-сервери з'єднані ієрархічно, відповідно до ієрархії доменів мережі Інтернет. Клієнт опитує ці сервери імен, поки не знайде потрібні відображення. Цей процес прискорюється через те, що сервери імен постійно кешують інформацію, яка надається за запитами. Клієнтські комп'ютери можуть використовувати в своїй роботі IP-адреси декількох DNS-серверів, для підвищення надійності своєї роботи.

База даних DNS має структуру дерева, званого доменним простором імен, в якому кожен домен (вузол дерева) має ім'я і може містити піддомени. Ім'я домену ідентифікує його положення в цій базі даних по відношенню до батьківського домену, а точки в імені відділяють частини, відповідні вузлам домену, наприклад, www. ibm.ua.

Корінь бази даних DNS управляється центром Інтернет Network Information Center. Домени верхнього рівня призначаються для кожної країни, а також на організаційній основі. Імена цих доменів повинні слідувати міжнародним стандартом ISO 3166. Для позначення країн використовуються трьох буквенні та дво-літерні абревіатури, а для різних типів організацій використовуються наступні абревіатури:

- com – комерційні організації (наприклад, microsoft.com);
- edu – освітні (наприклад, mit.edu);
- gov – урядові організації (наприклад, nsf.gov);
- org – некомерційні організації (наприклад, pir.org);
- net – організації, що підтримують мережі (наприклад, nsf.net).

Кожен домен DNS адмініструється окремою організацією, яка зазвичай розбиває свій домен на піддомени і передає функції адміністрування цих піддоменів іншим організаціям. Кожен домен має унікальне ім'я, а кожен з піддоменів має унікальне ім'я усередині свого домену. Ім'я домена може містити до 63 символів. Кожен хост в мережі Інтернет однозначно визначається своїм повним доменним ім'ям (fully qualified domain name, FQDN), яке включає

імена всіх доменів у напрямку від хоста до кореня. Приклад повного DNS-імені:

server.aics.acs.cctpu.edu.ua

2.2. Автоматизація процесу призначення IP-адрес вузлам мережі – протокол DHCP

Протокол ***DHCP*** (*Dynamic Host Configuration Protocol*) був розроблений для того, щоб звільнити адміністратора від необхідності призначення комп'ютерам IP-адрес вручну. У локальній мережі, що містить DHCP-сервер, кожен комп'ютер при включенні надсилає запит до цього сервера на отримання IP-адреси. Таким чином, основним призначенням DHCP є динамічне призначення IP-адрес. Однак, крім динамічного, DHCP може підтримувати і більш прості способи призначення адрес: ручний і автоматичний статичний.

При ручному призначенні адрес активну участь приймає адміністратор, який надає DHCP-серверу інформацію про відповідність IP-адрес фізичним адресами або іншим ідентифікаторам клієнтів. Ці адреси повідомляються клієнтам у відповідь на їх запити до DHCP-сервера.

При автоматичному статичному способі DHCP-сервер привласнює IP-адресу (і, можливо, інші параметри конфігурації клієнта) з пулу (набору) наявних IP-адрес без втручання оператора. Межі пулу адрес, які призначаються задає адміністратор при конфігуруванні DHCP-сервера. Між ідентифікатором клієнта і його IP-адресою, як і при ручному призначенні, існує постійна відповідність. Вона встановлюється в момент первинного призначення сервером DHCP IP-адреси клієнта і таким чином при всіх наступних запитах сервер повертає той же самий IP-адрес.

При динамічному розподілі адрес DHCP-сервер видає адресу клієнту на обмежений час, що дає можливість згодом повторно використовувати IP-адреси іншими комп'ютерами. Динамічне розділення адрес дозволяє будувати IP-мережу, кількість вузлів в якій набагато перевищує кількість наявних у розпорядженні адміністратора IP-адрес.

2.3. Системні утиліти мережевої діагностики

Всі мережеві операційні системи мають в своєму складі утиліти для тестування мережі. А оскільки більшість користується ОС Windows, тому далі будуть розглянуті декілька мережевих утиліт саме ОС Windows, які запускаються з командного рядка.

2.3.1. Утиліта ipconfig

Утиліта ipconfig (IP configuration) призначена для настройки протоколу IP для операційної системи Windows. У даній лабораторній роботі ця утиліта буде використовуватися тільки для отримання інформації про з'єднання по локальній мережі. Для отримання цієї інформації введіть в командному рядку («Пуск» → «Виконати» → cmd):

ipconfig /all

У розділі «Адаптер Ethernet …» для даної лабораторної будуть необхідні поля «DHCP», «IP-адреса» і «DNS-сервери».

2.3.2. Утиліта ping

Утиліта ping (Packet Internet Groper) є одним з головних засобів, що використовуються для налагодження мереж, і служить для примусового виклику відповіді конкретної машини. Для цього використовується дейтаграмма ECHO_REQUEST протоколу ICMP.

Дана утиліта дозволяє перевіряти роботу програм TCP/IP на віддалених машинах, адреси пристроїв в локальній мережі, адресу і маршрут для віддаленого мережевого пристрою. У виконанні команди ping беруть участь система маршрутизації, схеми дозволу адрес і мережеві шлюзи. Це утиліта низького рівня, яка не вимагає наявності серверних процесів на машині, яка перевіряється, тому успішний результат при проходженні запиту зовсім не означає, що виконуються які-небудь сервісні програми високого рівня, а говорить про те, що мережа знаходиться в робочому стані, живлення машини, яка перевіряється, включено, і машина не відмовила («не зависла»).

У ОС Windows утиліта ping є в комплекті поставки і являє собою програму, що запускається з командного рядка.

Запити утиліти ping передаються по протоколу ***ICMP*** *(Internet Control Message Protocol)*. Отримавши такий запит, програмне забезпечення, що реалізує протокол IP у адресата, посилає відлуння-відповідь (ехо-відповідь). Якщо машина, яка перевіряється, в момент отримання запиту була завантажена більш пріоритетною роботою (наприклад, обробкою і перенаправленням великого обсягу трафіку), то відповідь буде відправлена не відразу, а як тільки закінчиться виконання більш пріоритетного завдання. Тому слід врахувати, що затримка, розрахована утилітою ping, викликана не тільки пропускною здатністю каналу передачі даних до машини, яка перевіряється, але і завантаженістю цієї машини.

Відлуння-запити надсилаються задану кількість разів (ключ -n). За замовчуванням передається чотири запити, після чого виводяться статистичні дані.

Зверніть увагу: *оскільки з утиліти ping можуть починатися більшість хакерських атак, деякі сервери з метою безпеки не посилають ехо-відповіді (наприклад, www.microsoft.com). Не чекайте марно, введіть команду переривання (CTRL + C).*

Таблиця 2.4. Параметри утиліти ping

Ключі	Функції
-t	Відправка пакетів на вказаний вузол до команди переривання
-a	Визначення імені вузла за IP-адресою
-n <число>	Число надісланих запитів (за замовчуванням – 4)
-l	Розмір буфера відправки – задає довжину (в байтах) поля даних в відправлених повідомленнях з ехо-запитами. За замовчуванням – 32 байта. Максимальний розмір – 65000.
-f	Установка флага, що забороняє фрагментацію пакету
-i TTL	Максимальна кількість переходів (поле «Time To Live» – час життя пакету)

На практиці більшість опцій в форматі команди можна опустити, тоді в командному рядку може бути прописано: ping ім’я вузла (для зациклення виведення інформації про з’єднання використовується опція -t; для виведення інформації n-раз використовується опція -n <кількість разів>).

Приклад:

```
ping –n 20 mountinn.net

Обмен пакетами с mountinn.net [184.168.221.20] с 32 байтами данных:
Превышен интервал ожидания для запроса.
Ответ от 184.168.221.20: число байт=32 время=734мс TTL=231
Ответ от 184.168.221.20: число байт=32 время=719мс TTL=231
Ответ от 184.168.221.20: число байт=32 время=688мс TTL=231
Ответ от 184.168.221.20: число байт=32 время=704мс TTL=231
Превышен интервал ожидания для запроса.
Ответ от 184.168.221.20: число байт=32 время=719мс TTL=231
Ответ от 184.168.221.20: число байт=32 время=1015мс TTL=231
Превышен интервал ожидания для запроса.
Ответ от 184.168.221.20: число байт=32 время=703мс TTL=231
Ответ от 184.168.221.20: число байт=32 время=688мс TTL=231
Ответ от 184.168.221.20: число байт=32 время=782мс TTL=231
Ответ от 184.168.221.20: число байт=32 время=688мс TTL=231
Ответ от 184.168.221.20: число байт=32 время=688мс TTL=231
Ответ от 184.168.221.20: число байт=32 время=688мс TTL=231
```

Превышен интервал ожидания для запроса.
Ответ от 184.168.221.20: число байт=32 время=687мс TTL=231
Ответ от 184.168.221.20: число байт=32 время=735мс TTL=231
Ответ от 184.168.221.20: число байт=32 время=672мс TTL=231
Ответ от 184.168.221.20: число байт=32 время=704мс TTL=231

Статистика Ping для 184.168.221.20:
    Пакетов: отправлено = 20, получено = 16, потеряно = 4 (20% потерь),
Приблизительное время приема-передачи в мс:
    Минимальное = 672мс, Максимальное = 1015мс, среднее = 580мс

Приклад визначення імені вузла за IP-адресою:

ping –a 212.42.76.253

Обмен пакетами с srv253.fwdcdn.com [212.42.76.253] с 32 байтами данных:
Ответ от 212.42.76.253: число байт=32 время=27мс TTL=60
Ответ от 212.42.76.253: число байт=32 время=26мс TTL=60
Ответ от 212.42.76.253: число байт=32 время=26мс TTL=60
Ответ от 212.42.76.253: число байт=32 время=26мс TTL=60

Статистика Ping для 212.42.76.253:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 26мсек, Максимальное = 27 мсек, Среднее = 26 мсек

2.3.3. Утиліта tracert

Ця команда подібна команді ping, обидві посилають в точку призначення ехо-пакети і потім чекають їх повернення. Відмінність пакетів команди traceroute від пакетів ping полягає в тому, що вони мають різний термін життя (Time to Live, TTL) і за допомогою цього, утиліта tracert дозволяє виявляти послідовність маршрутизаторів, через які проходить IP-пакет на шляху до пункту свого призначення.

Формат команди: *tracert імя_машини*

де *імя_машини* може бути ім’ям вузла або IP-адресою машини. Вихідна інформація являє собою список машин, починаючи з першого шлюзу і закінчуючи вузлом призначення.

Приклад:

tracert mountinn.net

Трассировка маршрута к mountinn.net [184.168.221.20] с максимальным числом прыжков 30:

№	Пакет 1	Пакет 2	Пакет 3	DNS-ім’я вузла та (або) його IP-адреса
1	<1 мс	<1 мс	<1 мс	router.asus.com [192.168.1.1]
2	<1 мс	<1 мс	<1 мс	91.197.186.1
3	1 ms	<1 мс	<1 мс	91.197.184.253
4	1 ms	1 ms	<1 мс	91.197.184.53
5	1 ms	1 ms	1 ms	ae8-347.RT1.NTL.KIV.UA.retn.net [87.245.237.38]
6	37 ms	37 ms	37 ms	ae3-8.RT.TC2.AMS.NL.retn.net [87.245.233.17]
7	*	*	*	Превышен интервал ожидания для запроса.
8	*	*	*	Превышен интервал ожидания для запроса.
9	167 ms	167 ms	167 ms	4.28.83.74
10	*	*	*	Превышен интервал ожидания для запроса.
11	167 ms	167 ms	167 ms	ip-184-168-0-86.ip.secureserver.net [184.168.0.86]
12	167 ms	167 ms	167 ms	te0-0-0-7.trmc0215-01.ars.mgmt.phx3.gdg [184.168.0.85]
13	167 ms	195 ms	167 ms	ip-184-168-0-94.ip.secureserver.net [184.168.0.94]
14	167 ms	167 ms	167 ms	ip-184-168-221-20.ip.secureserver.net [184.168.221.20]

Трассировка завершена.

Пакети надсилаються по три на кожен вузол. Для кожного пакету на екрані відображається величина інтервалу часу між відправленням пакета і отриманням відповіді. Символ * означає, що відповідь на даний пакет не була отримана. Якщо вузол не відповідає, то при перевищенні інтервалу очікування відповіді видається повідомлення «Перевищено інтервал очікування для запиту». Інтервал очікування відповіді може бути змінений за допомогою опції -w команди tracert.

Команда tracert працює шляхом установки поля часу життя (числа переходів) вихідного пакета таким чином, щоб цей час спливав до досягнення пакетом пункту призначення. Коли час життя закінчиться, поточний шлюз відправить повідомлення про помилку на машину-джерело. Кожне збільшення поля часу життя дозволяє пакету пройти на один маршрутизатор далі.

Примітка:

Для виведення інформації в файл використовуйте символ перенаправлення потоку виведення «>». Даний символ справедливий і для утиліт ping і tracert.

***Приклад*:**

```
tracert 91.197.186.1 > tracert.txt
```

Звіт про трасування маршруту до зазначеного вузла буде поміщений в файл tracert.txt.

2.3.4. Сервіс Whois

При реєстрації доменних імен другого рівня обов'язковою умовою є надання вірних відомостей про власника цього домену: для юридичних осіб – назва організації, для фізичних осіб – ПІБ і паспортні дані. Також обов'язковим є надання контактної інформації. Частина цієї інформації стає вільно доступною для будь-якого користувача мережі Інтернет через сервіс Whois. Отримати необхідну інформацію про власника домену можна через Whois-клієнт, наприклад, в Unix це консольна команда whois, в ОС Windows – це додаток SmartWhois. Але найпростіше відправити запит можна через веб-форму on-line сервісу Whois, наприклад через форму на сторінці https://www.whois.com

Порядок виконання лабораторної роботи №2:

1. Включити ПК.
2. Ознайомитися з короткими теоретичними відомостями.
3. Використовуючи утиліту ipconfig визначити IP адресу і фізичну адресу основного мережевого інтерфейсу свого комп'ютера, IP адресу шлюзу, IP адресу DNS-серверів і чи використовується DHCP. Результати представити у вигляді таблиці (табл. 2.5) і розмістити після таблиці зображення вікна (скріншот робочого столу).

Таблиця 2.5. Результати виконання завдання №3

IP-адреса (десятковий вигляд)	
IP-адреса (двійковий вигляд)	
Адреса мережі (десятковий вигляд)	
Довжина маски підмережі (кількість бітів)	
Фізична адреса	
IP-адреса шлюзу (десятковий вигляд)	
IP-адреси DNS-серверів (десятковий вигляд)	
Чи використовується DHCP (так чи ні)	

4. Перевірити стан зв'язку з будь-якими двома вузлами (працездатними) відповідно до варіанту завдання (табл. 2.9). Кількість відправлених запитів має становити не менше 20. Як результат відобразити для кожного з досліджуваних вузлів у вигляді таблиці (табл. 2.6) і розмістити після таблиці скріншот:

Таблиця 2.6. Результати виконання завдання №4

Ім'я вузла	
IP-адреса вузла	
Ім'я вузла, отримане за IP-адресою вузла	

Клас мережі, до якої належить даний вузол	
Відсоток втрачених пакетів	
Середній час прийому-передачі	
Кількість маршрутизаторів (з урахуванням шлюзу) до опитуваного вузла	

** У звіті необхідно пояснити, як були визначені значення.*

5. Провести трасування двох працездатних вузлів відповідно до варіанта завдання (табл. 2.9). Результати запротоколювати в таблиці (табл. 2.7).

Таблиця 2.7. Результати виконання завдання №5 (tracert)

№ вузла	Час проходження пакета №1	Час проходження пакета №2	Час проходження пакета №3	Середній час проходження пакета	DNS-ім'я маршрутизатора	IP-адрес маршрутизатора

Якщо значення часу проходження трьох пакетів відрізняються більш, ніж на 10 мс, або якщо є втрати пакетів, то для відповідних вузлів середній час проходження необхідно визначати за допомогою утиліти ping по 20 пакетам. За результатами таблиці 2.7 в звіті привести графік зміни середнього часу проходження пакета. Також, для кожного опитуваного вузла визначити ділянку мережі між двома сусідніми маршрутизаторами, яка характеризується найбільшою затримкою при пересиланні пакетів. За DNS-іменами маршрутизаторів спробуйте визначити їх географічне розташування і зробіть висновки про причини затримок. Для знайдених маршрутизаторів за допомогою сервісу Whois визначити назву організації та контактні дані (тел., Email) і представити у вигляді таблиці (табл. 2.8). Результати виконання завдання №5 необхідно супроводжувати скріншотами.

Таблиця 2.8. Результати виконання завдання №5 (Whois)

	DNS-ім'я вузла	DNS-ім'я вузла	DNS-ім'я вузла	DNS-ім'я вузла
Назва організації				
Контактний тел.				
Контактний email				
Ім'я адміністратора				

6. Оформити звіт згідно до вимог (додаток 1).
7. Зробити висновки, відповісти на контрольні питання та підготуватися до письмового опитування.

Зміст звіту:

1. Титульний лист.
2. Постановка завдання.

3. Протокол виконання лабораторної роботи, що містить результати використання утиліти ipconfig, перевірки стану зв’язку до вузлів та трасування працездатних вузлів.

4. Висновки.

Завдання на виконання лабораторної роботи №2

Таблиця № 2.9. (варіант відповідно до номера за списком у журналі)

Номер варіанта	Завдання
1	www.busytrade.com www.chinavasion.com www.imobile.com.cn
2	www.vancl.com www.happigo.com www.shop.com
3	www.alibaba.com www.tradekey.com www.made-in-china.com
4	www.paipai.com www.buynow.com.cn www.hktdc.com
5	www.aliexpress.com www.tias.com www.tradekey.com
6	www.china-direct-buy.com www.chinatronic.com www.ecvv.com
7	www.chinabuye.com www.amazon.cn www.importers.com
8	www.ecplaza.net www.made-in-china.com www.diytrade.com
9	www.dealextreme.com www.imobile.com.cn www.dhgate.com
10	www.diytrade.com www.lightinthebox.com www.modashop.net
11	www.busytrade.com www.webstorelist.com www.ecvv.com
12	www.tradekey.com www.importers.com www.diytrade.com
13	www.chinavasion.com www.ecplaza.net www.ecvv.com

14	www.dhgate.com www.diytrade.com www.made-in-china.com
15	www.importers.com www.busytrade.com www.dealextreme.com
16	www.modashop.net www.chinavasion.com www.lightinthebox.com
17	www.webstorelist.com www.vtcom.lv www.taobao.com
18	www.alibaba.com www.buynow.com.cn www.chinabuye.com
19	www.hktdc.com www.dhgate.com www.imobile.com.cn
20	www.tias.com www.lightinthebox.com www.dhgate.com
21	www.chinavasion.com www.dealextreme.com www.modashop.net
22	www.ecplaza.net www.webstorelist.com www.vancl.com
23	www.busytrade.com www.diytrade.com www.ecvv.com

Контрольні питання:

1. Назвіть три рівні адресації в комп'ютерних мережах, та наведіть приклади адрес до кожного з рівнів.
2. Поясніть, що таке MAC-адреса, та опишіть її структуру.
3. Опишіть структуру IP-адреси та поясніть що таке маска підмережі і для чого вона використовується?
4. Назвіть основні критерії віднесення IP-адреси до певного класу мережі.
5. Назвіть та опишіть IP-адреси спеціального призначення.
6. Поясніть, що таке служба DNS?
7. Поясніть, що таке протокол DHCP?
8. Для чого призначена утиліта ipconfig?
9. Назвіть основне призначення утиліти ping та опишіть алгоритм її роботи.

10. Пакетами якого мережевого протоколу є exo-пакети команди ping?
11. Назвіть основну відмінність утиліт ping та traceroute.
12. Поясніть, що таке сервіс Whois?

Лабораторна робота №3
«Гіпертекст як мова кіберпростору та психологія сприйняття інтернет-ресурсів»

Мета роботи:

1. Поглиблення та закріплення теоретичних знань з наступних питань:
   - поняття гіпертексту та його основні глобальні елементи;
   - процес розробки сайту;
   - структура інтернет-ресурсу, гіперпосилання та навігація по сайту;
   - макет сайту та сприйняття інтернет-ресурсу в кіберпросторі.
2. Набуття практичних навичок з розробки макета сайту.

Стислі теоретичні відомості:

3.1. Поняття гіпертексту

Вперше концепцію гіпертексту висунув Р. В. Буш в 1945 р в статті *«As we may think»*.

Сам термін «гіпертекст» введений Тедом Нельсоном в 1965 році, який визначав гіпертекст як текст що розгалужується або виконує дії за запитом.

Гіпертекст – це форма організації текстового матеріалу, при якій його одиниці представлені не в лінійній послідовності, а як система явно зазначених можливих переходів, зв'язків між ними.

Дотримуючись цих зв'язків, можна читати матеріал в будь-якому порядку, утворюючи різні лінійні тексти (М. М. Суботін).

Приклади паперової гіпертекстової літератури:

- Першою системою гіпертексту прийнято вважати тлумачення Книги псалмів Гільберта Порретанского з Пуатьє (близько 1150 року н. е.);
- Роман-лексикон «Хозарський словник» Мілорада Павича;
- Філософська повість «Нескінченний глухий кут» Дмитра Галковського;
- «Досконалий код», С. Макконнелл.

У сучасному розумінні *гіпертекст* – це набір текстів, що містять вузли переходу між ними, які дозволяють обирати відомості для читання або послідовність читання. Як правило, під гіпертекстом розуміється текст, сформований за допомогою ***мови HTML***.

Елементами сучасного гіпертексту є:

- невеликі фрагменти тексту;

- інфографіка та ілюстрації;
- відео та аудіо;
- інші мультимедіа-фрагменти (наприклад, інтерактивна flash-анімація, форми зворотного зв’язку і т. д.).

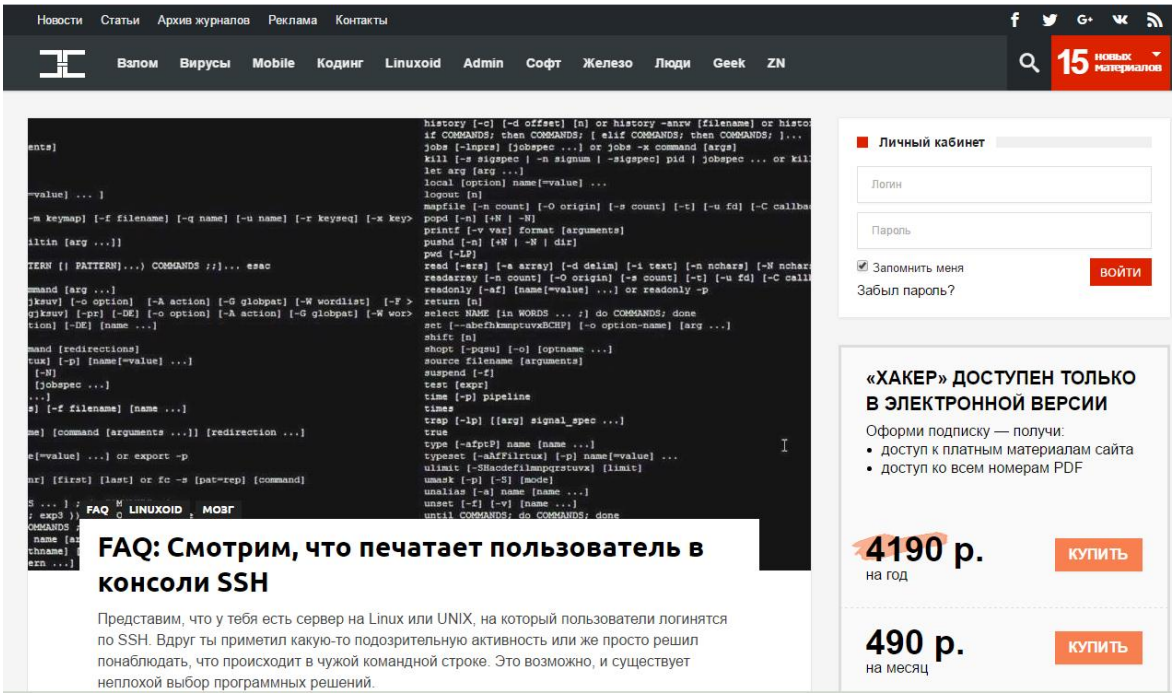


Рис. 3.1. Зразок веб-сторінки

3.2. Елементи глобального гіпертексту: сайти та веб-сторінки

Гіпертекст у всесвітній павутині сформований у логічно пов’язані компоненти – ***сайти***. Слово «сайт» походить від англійського «site» – місце. Таким чином, можна сказати, що сайти – це місця в кіберпросторі.

Сайт – набір web-сторінок, розміщених в одній або декількох папках сервера і мають схожі мережеві адреси – загальну частину URL.

Тут слід уточнити, що великі сайти рідко розташовуються на одному сервері. Крім того, у всіх ресурсів у всесвітній мережі є резервні копії – так звані ***дзеркала***. Сайт, як правило, має доменне ім’я другого або третього рівня. Крім того, один сайт може включати в себе інші сайти.

Приклади сайтів:

- сайт wikipedia.org (мережева енциклопедія) включає в себе, зокрема, українськомовний сегмент uk.wikipedia.org, англомовний сегмент en.wikipedia.org та інші. Ці частини одного сайту фізично розташовані на різних серверах.
- до сайту dut.edu.ua Державного університету телекомунікацій входять такі сайти як dl.dut.edu.ua – дистанційне навчання, e-rozklad.dut.edu.ua – розклад занять, та інші.
- сайт wikileaks Джуліана Ассанжа має 1426 дзеркал.

На логічному рівні сайти складаються з веб-сторінок.

Web-сторінка – документ, підготовлений у форматі гіпертексту і розміщений (або підготовлений для розміщення) в WWW.

Говорячи про веб-сторінки слід враховувати, що вони існують тільки в кіберпросторі. Тобто існування сторінки з URL «http://example.com/page.htm» зовсім не означає, що на одному з серверів Всесвітньої павутини лежить файл «page.htm». Більшість веб-сторінок генеруються безпосередньо при зверненні до них. Те ж стосується (правда, у меншій мірі) і інших ресурсів в мережі (зображень, документів негіпертекстових форматів).

Розглянемо основні види сайтів (табл. 3.1).

Таблиця 3.1. Види сайтів

Мережеві сервіси	
Сайти, орієнтовані на взаємодію в кіберпросторі	
Універсальний портал або портал пошукової системи	Дуже великий сайт, орієнтований на виключно мережеву взаємодію: пошук інформації, спілкування, обмін файлами, реєстрацію хостингу і т. д. Наприклад, google.com, yandex.ua, mail.ru
Соціальні мережі та спільноти, форуми	Сайти, орієнтовані на мережеве спілкування. Наприклад, facebook.com, vk.com.
Ігрові портали	Сайти, орієнтовані на підтримку on-line ігор. Наприклад, lioflash.com.ua
Технічні сайти (системи електронної оплати, хостинг та ін)	Сайти, що формують мереживу інфраструктуру. Наприклад, сайт електронної системи платежів easypay.ua, сайт хостинг-провайдера uh.ua, сайт для клієнтів інтернет-провайдера ukrtelecom-sales.com та ін.
Інформаційні сайти	
Сайти, основне призначення яких – надання інформації	
Тематичний сайт	Веб-сайт, що надає вичерпну інформацію по якій-небудь темі. Наприклад, сайт, присвячений татуюванням uniquetattoo.ru, сайт про кельтські орнаменти kelskornament.ru. Також до тематичних сайтів відносяться сайти державних органів управління (сайт адміністрації київської області koda.gov.ua, сайт міністерства освіти mon.gov.ua, і тематичні блоги, і живі журнали)
Тематичний портал	Дуже великий веб-ресурс, який надає вичерпну інформацію з певної тематики. Портали схожі на тематичні сайти, але додатково містять засоби взаємодії з користувачами і дозволяють користувачам спілкуватися в рамках порталу (форуми, чати) – це середовище існування користувача.
Мережева енциклопедія	Сайт, призначений для збору і систематизації знань у якій-небудь області. Наприклад, Wikipedia.org, lurkmore.ru та інші.
Сайти словників	Наприклад, synonymizer.ru, slovardalja.net
Комерційні сайти	
Сайти, основне призначення яких – реклама та залучення клієнтів	

Сайт-візитка	Такий сайт містить загальні дані про фірму (або будь-яку іншу організацію). Як правило, це інформація про організації, реквізити, план проїзду, тобто візитна картка організації. Наприклад, www.author.kiev.ua.
Каталог продукції	В каталозі присутній докладний опис товарів/послуг, сертифікати, технічні і споживчі дані, відгуки експертів і т. д. На таких сайтах розміщується інформація про товари/послуги, яку неможливо помістити в прайс-лист. Наприклад, mahno.com.ua
Інтернет-магазин	Веб-сайт з каталогом продукції, за допомогою якого клієнт може замовити потрібні йому товари. Використовуються різні системи розрахунків: від пересилання товарів післяплатою або автоматичною пересилання рахунку факсом до розрахунків за допомогою пластикових карток. Наприклад .rozetka.com.ua
Дошка оголошень	Вміст цих сайтів являє собою набір оголошень комерційного і/або некомерційного характеру і розміщується як на платній, так і на безоплатній основі, в залежності від конкретного сайту. Дошки оголошень бувають як тематичними, так і універсальними. Наприклад, olx.ua
Промо-сайт	Сайт про конкретну торгівельну марку або продукт, на таких сайтах розміщується вичерпна інформація про бренд, різних рекламних акціях (конкурси, вікторини, ігри тощо). Приклади: lenovo.com/ua.

3.3. Процес розробки сайту

Процес розробки сайту являє собою поєднання трьох видів діяльності: веб-дизайну, веб-мастерингу і контент-менеджменту.

Веб-дизайн – це вид діяльності, спрямований на вирішення двох завдань:

- розробка користувальницького інтерфейсу (побудову зручного для користувача способу подачі інформації і простої навігації по сайту);
- розробка зовнішнього вигляду сторінок сайту (підбір кольорів, шрифтів, створення зображень).

Веб-мастеринг – вид діяльності, що забезпечує функціонування і технічну підтримку веб-ресурсу (написання скриптів, адміністрування та налаштування веб-серверів та ін). *Веб-майстр* – це програміст або системний адміністратор з технічною освітою.

Контент-менеджмент – це вид діяльності з управління інформаційним вмістом сайту. Контент-менеджер (редактор сайту) підбирає статті та фотографії для сайту, веде розділ новин і підтримує актуальність інформації на сайті. Зазвичай професія контент-менеджера вимагає журналістської або філологічної освіти.

В залежності від розміру ресурсу створювати його може як одна людина, так і ціла команда. Усі три види діяльності в процесі створення сайту протікають паралельно, але починається розробка мережевого ресурсу з вирішення завдань контент-менеджменту.

Початковий (підготовчий) етап створення сайту:

1. Виділяється тема і мета створення сайту.
2. Проводиться аналіз інформаційної структури, вже утвореної навколо даної теми в кіберпросторі (виділяються великі портали, аналогічні сайти і сайти-конкуренти, статті в електронних ЗМІ та блогах, пошук додаткових ресурсів і сервісів (законодавство, об’єкти на картах та ін)).
3. Виділяються ключові слова для сайту, проводиться аналіз пошукової статистики.
4. Формується уявлення про цільову аудиторію сайту.
5. Підбирається інформація по темі сайту (тексти, ілюстрації та інфографіка), пишуться статті для сайту.

Далі розглянемо деякі аспекти детальніше.

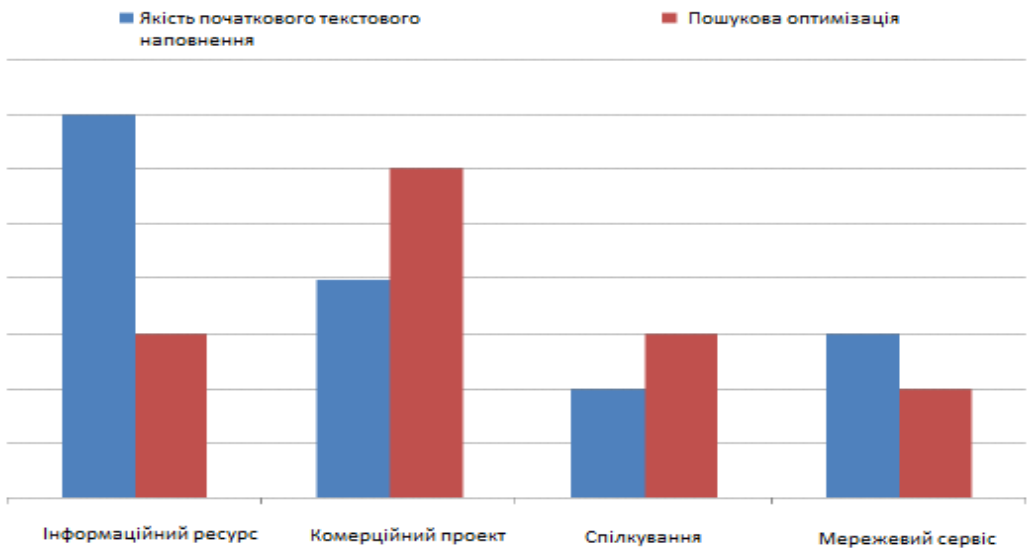
3.3.1. Мета створення сайту

Від мети створення сайту безпосередньо залежить співвідношення між якістю вмісту сайту і пошуковою оптимізацією під автоматизовані системи пошуку.

Можна виділити чотири основних мети створення сайту:

- *Інформаційний ресурс* (основне призначення – передача або розповсюдження інформації).
- *Комерційний проект* (основне призначення – реклама або отримання прибутку).
- *Спілкування* (формування мережевої спільноти навколо певної теми).
- *Мережевий сервіс* (надання мережних послуг, як платних, так і безкоштовних).

На малюнку показано, на що саме редактор сайту повинен звернути увагу в залежності від цілей сайту.



3.3.2. Ключові слова та анотація

Набір ключових слів – це пошуковий образ документа.

Ключові слова – це слова, використовувані для пошуку документа в мережі. Це ті слова, які, імовірно, буде використовувати людина, щоб знайти конкретний сайт. Ключові слова повинні міститися в достатній кількості (5-7%) у наступних елементах сторінки:

- заголовок;
- URL;
- ключові слова (спеціальний розділ) та анотація;
- основний текст;
- підписи до ілюстрацій;
- тексти посилань.

Анотація – це короткий виклад змісту статті.

На відміну від ключових слів, анотації орієнтовані на читача, а не на пошукову систему. Разом з тим, анотації враховуються пошуковими системами при виділенні ключових слів сторінки.

Анотація має три призначення:

- влучно і чітко описати, про що йдеться на сторінці;
- зробити презентацію відповідної сторінки сайту в результатах пошукової видачі;
- показати відповідність запиту користувача вмісту сторінки.

Анотації повинні бути дуже короткими.

3.3.3. Цільова аудиторія сайту

Цільова аудиторія – це відвідувачі, яким буде цікава інформація на вашому сайті (для інформаційних сайтів) або можливі покупці ваших товарів і послуг (для комерційного сайту). Щоб знайти ефективні способи залучення цільової аудиторії, потрібно скласти приблизний портрет цільового відвідувача. Він складається з декількох характеристик:

- вік та стать;
- сфера діяльності, освіта, галузь роботи та достаток;
- наскільки часто і звідки користувач виходить в мережу, які сайти найчастіше відвідує.

Щоб найбільш якісно проаналізувати цільову аудиторію необхідно скласти демографічний профіль її типового представника. Демографічний профіль враховує рід занять, вік, стать, частоту роботи та інтереси в Мережі (які сайти відвідують користувачі і чому, як часто вони здійснюють онлайнові покупки, наскільки добре вони орієнтуються в мережі). Більшість сайтів відвідує кілька чітко розділених категорій користувачів, тому може знадобитися створення кількох загальних профілів. Для цього необхідно описати типового користувача вашого сайту:

- Як часто він працює в режимі онлайн і для чого взагалі використовує Мережу?
- Який його вік і чим він заробляє собі на життя?
- Яка основна мета відвідування вашого сайту (зробити покупки, вступити в спільноти, знайти інформацію)?
- За яким головними причинами цільовий користувач вибирає продукцію і/або послуги вашої компанії (ціна, сервіс, якість)?

3.3.4. Інформаційне наповнення сайту

При формуванні інформаційного наповнення сайту переслідуються дві багато в чому протилежні цілі:

- зацікавити відвідувача, привернути його увагу, затримати відвідувача на сайті, зробити його постійним відвідувачем. Це означає, що вміст сайту має бути цікавим і корисним для людини;
- залучити на сайт як можна більше «корисних» відвідувачів. Більшість відвідувачів приходить на сайт з пошукових систем, тому необхідно, щоб на запити, відповідні цілям і тематиці сайту, цей сайт опинявся на першій-другій сторінці вибірки пошукової системи. Це означає, що сайт повинен бути зрозумілим автоматизованим систем пошуку, які орієнтовані на якість гіперпосилань і повторюваність ключових слів, а не на корисність ресурсу для користувача.

Детальніше про пошук інформації в кіберпросторі буде розглядатися на наступних практичних заняттях. На даному етапі важливо зрозуміти, що якість підбору ключових слів істотно впливає на успішність сайту.

Сам процес написання статей для сайту називається ***копірайтингом***.

Як вже зазначалося раніше, до інформаційного наповнення сайту, окрім тексту, відносяться також ілюстрації та інфографіка.

Ілюстрація – візуалізація, така як малюнок, фотографія, відео-фільм та інше, що використовується з ціллю виділення суб'єкта, а не форми і призначена для пояснення або декорування текстового змісту статті.

Інфографіка – це графічне візуальне подання інформації, даних або знань, призначених для швидкого та чіткого відображення комплексної інформації.

Інфографіка з'явилася дуже давно. Першою інфографікою вважається сцени-інструкції полювання в наскальному живопису. Сучасна інфографіка – це яркe, складне зображення, яке цікаво розглядувати.

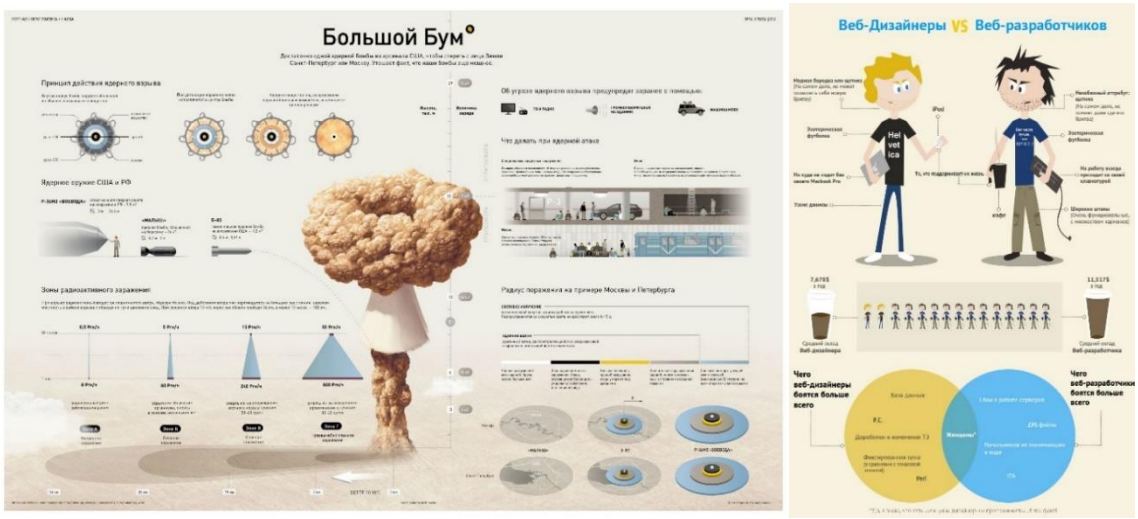


Рис. 3.2. Приклад сучасної інфографіки

3.4. Структура інтернет-ресурсу

Інформаційні розділи сайту:

- **Блок основного вмісту.** Основна інформація сайту, як правило, супроводжується заголовком.
- **Новинний блок.** У цьому блоці можуть відображатися новини як по тематиці сайту, так і технічні, наприклад «Виправлена помилка на форумі». Блок являє собою список новин, упорядкований за датами їх появи (починаючи з самої свіжої). Як правило, новина наводиться коротко, і супроводжується посиланням «Докладніше» на більш докладний текст. Разом з колонкою новин слід вести архів новин.

- **Блок поточної інформації.** Невеликі блоки, повідомляють, наприклад, дату і час, погоду, курси валют, рейтинг сайту. Такі блоки також називають інформерами.

Інформер – це заздалегідь підготовлений автоматично оновлюваний інформаційний елемент, який встановлюється на сайті користувача і служить для надання фінансової, політичної, спортивної та іншої інформації.

Однак, слід пам'ятати, що вміст блоків повинен бути корисним для відвідувача сайту, не варто вставляти блок про курс валют на сайті спортивного клубу.

- **Галерея зображень.** Поєднується з панеллю навігації по вибірці. При включенні цього блоку слід пам'ятати, що зображення повинні завантажуватися досить швидко. Можна організувати галерею в формі діафільму.
- **Каталог посилань.**

Допоміжні розділи сайту:

- *Головна сторінка*. Це вхід, «ворота» сайту. Тут може бути доречний більш витончений дизайн, наприклад, flash-анімація. Хоча, хибно вважати, що застосування головної сторінки-заставки, виконаної, наприклад, за допомогою flash анімації, дозволить залучити більшу увагу відвідувача сайту. На практиці виходить все навпаки. Тому головна сторінка повинна бути «яркою» і в той же час змістовною та інформаційно насиченою.
- *«Підвал»* – блок у кінці сторінки. Він може містити перелік основних розділів сайту або інформацію про web-майстра, web-дизайнера і авторські права.
- *Блок авторизації.* Багато сайтів вимагають від користувача зареєструватися або авторизуватися, щоб отримати доступ до закритої частини вмісту або до певних опцій сайту. Блок авторизації складається з полів вводу логіна і пароля користувача і кнопки «Вхід». Також блок може містити посилання «Зареєструватися» і «Нагадати пароль».
- *Блок вибору мови*.
- *Порожній блок.* Це пусте місце на сторінці, яке можна заповнити рекламою або банерами, наприклад, під вертикальним меню. Також даний блок може служити для відділення інших блоків.
- *Блок дизайнерського зображення*. Блок для оздоблення сайту.
- *Блок «Версія для друку».*
- *Рекламний блок.*
- *Блок авторських прав.*
- *Блоки зворотного зв'язку:*
  - координати;

- гостьова книга;
- форум.

3.5. Гіперпосилання та навігація по сайту

Гіперпосилання – об’єкт документа, що слугує вказівником на інший елемент, документ або файл.

Текст гіперпосилання є додатковим заголовком до того об’єкту, на який воно посилається. Однак потрібно пам’ятати, що це сприймається не лише користувачами сайту, але й пошуковими системами. Саме тому текст гіперпосилання повинен бути змістовним. Окрім цього, гіперпосилання повинно виділятися від іншого тексту, інакше користувач його не знайде (мається на увазі не лише зміна кольору але й сам зміст гіперпосилання).

Навігація – це переміщення по сайту. *Система навігації сайту* – одна із найважливіших складових поняття «дизайн сайту».

Окрім посилань в тексті використовуються наступні *елементи навігації*:

- **Горизонтальна панель навігації** і, можливо, спливаюче меню. Горизонтальне меню менш нав’язливе, чим вертикальне. Також горизонтальне меню зверху сторінки можна продублювати і внизу сторінки.
- **Вертикальна панель навігації.** Вертикальна панель приваблює більше уваги, чим горизонтальна, а також може вміщувати в себе більшу кількість пунктів меню.
- **Рядок «хлібні крихти».** Обов’язково розпочинається з головної сторінки і відображає ієрархію сайту. Саме «хлібні крихти» дозволяють користувачу, який перейшов на сайт не з головної сторінки, зорієнтуватися, де саме він знаходиться. Якщо ієрархія неглибока, то «хлібні крихти» не потрібні.
- **Меню переходів** – випадаючий список розділів і кнопка «перейти». Дозволяє користувачу знаходити необхідний йому розділ та швидко переміщуватися по сайту. Часто використовується на форумах для переміщення по розділам.
- **Блок пошуку.** Пошукові системи дозволяють реалізувати можливість пошуку на сайті.

Додаткові елементи навігації:

- **Перехід** «*На головну*» і «*До початку*»
- **Блок навігації по вибірці.** Якщо на вашому сайті є довгі списки, або об’ємні фотоальбоми, то для навігації по ним можна використовувати даний елемент, який складається із посилань на сторінки.

- **Карта сайту** – сторінка, що відображає структуру сайту. Наукові дослідження показали, що користувачам дійсно необхідна карта сайту, але вони не завжди можуть її знайти.

Необхідно завжди надавати можливість повернення до сторінки вищого рівня. Для достатньо довгих статей необхідне посилання «до початку». Більш того, якщо стаття розбита на декілька розділів, рекомендується ставити посилання «до початку» після кожного розділу.

3.6. Макет сайту

Дизайн-макет (або просто макет) – це малюнок, який представляє (презентує) передбачуваний майбутній зовнішній вигляд сторінок сайту. На макеті вказується, де які розділи сайту (інформаційні і технічні розміщуватимуться). Як правило, макет головної, «вхідної» сторінки сайту суттєво відрізняється від решти сторінок.

Макети сайтів можна розділити на *дві великі групи*: макети з фіксованою шириною і макети з плаваючою шириною.

Макети з фіксованою шириною використовують абсолютні розміри в пікселях для визначення ширини сторінки і застосовуються для сайтів з складним графічним дизайном (Приклад: dut.edu.ua).

Цей підхід не дозволяє елементам «розповзатися», дає більший контроль над подіями. Але такі сайти оптимізовані під певний розмір вікна браузера, і тому, якщо розрішення екрану менше задуманого дизайнером, сторінки виглядають стислими, з'являється горизонтальна смуга прокрутки. Якщо розрішення екрану більше передбачуваного, то залишається багато невикористаного місця. Щоб якось згладити цей недолік, необхідно обов'язково центрувати вміст сторінки у вікні браузера. Найбільш часто сайт з фіксованою шириною оптимізують під розширення 800px, 1024px або 1280px. При цьому ширина контейнерного елемента становить 760px і 954px відповідно.

В ***макетах з плаваючою шириною*** використовуються відносні розміри елементів, і вона масштабується під розміри вікна (Приклад: uk.wikipedia.org).

3.7. Сприйняття інтернет-ресурсу в кіберпросторі

Можна виділити 2 основних шаблони поведінки користувача в кіберпросторі: перегляд та пошук.

Перегляд (*browsing*) – поведінка, при якій користувач знайомиться з пропозицією (товарів, послуг, інформації) на сайті. У цьому разі користувача цікавить сайт цілком, але цей інтерес поверхневий, користувач не шукає щось

конкретне. При цьому шаблоні поведінки користувач приділяє більше уваги графічному контенту і рекламі.

Приклад:

- початкова фаза пошуку, коли користувач ще не визначився з конкретною метою;
- веб-серфінг;
- пошук нового інформаційного ресурсу або інтренет-магазину.

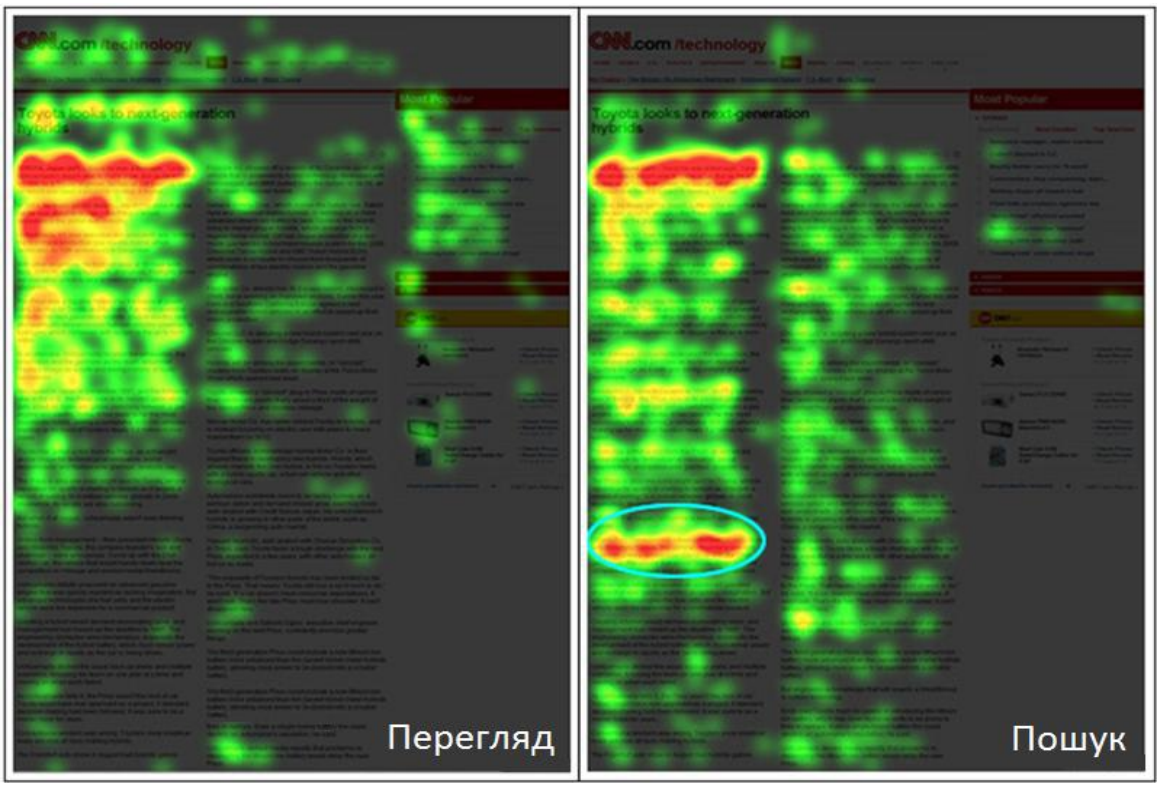
Пошук (*searching*) – поведінка, при якій користувач задовольняє свій попит на товари, послуги, інформацію на сайті. У користувача є цілком конкретна мета, з якою він відкрив веб-сторінку. У цьому випадку він приділяє більше уваги читанню тексту, ніж вивченню зображень.

Приклад:

- пошук конкретної інформації;
- пошук конкретного товару.

Для аналізу сприйняття інтернет-ресурсів використовується метод, що дозволяє по руху очей користувача визначити, на яких точках на сайті користувач фіксує погляд. Фіксувати погляд – значить зупиняти рух очей на 200-300 наносекунд. На малюнках зображені «теплові» карти, зеленим кольором позначені місця, де користувачі фіксували погляд, жовтим – місця, де це відбувалося частіше, червоним – найбільш часто.

На малюнку нижче представлена різниця в сприйнятті перегляду та пошуку. Блакитним овалом в правій частині малюнка обведена фраза, яку шукав користувач.

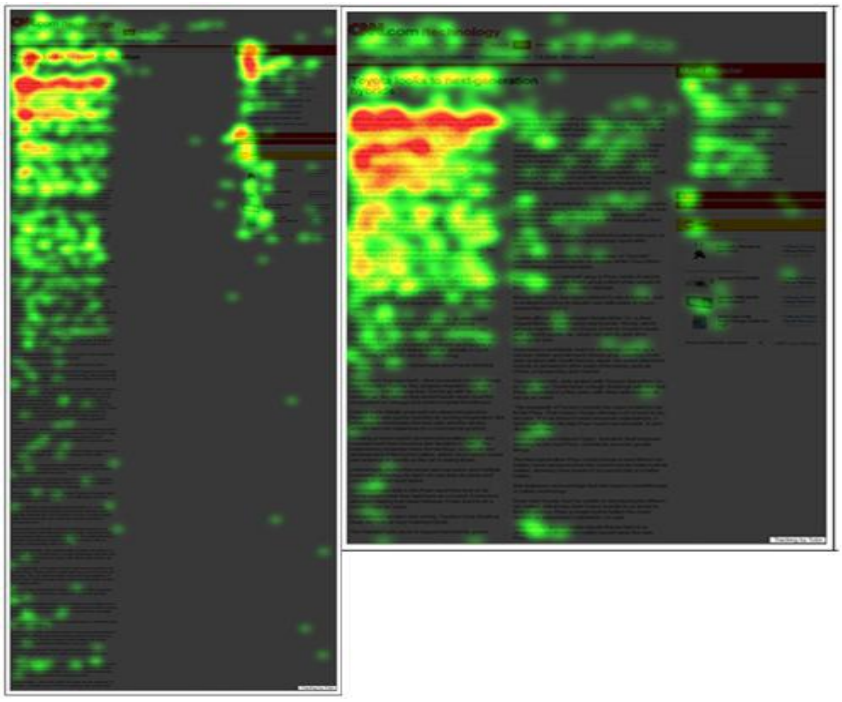


При перегляді користувач більше уваги приділяє банеру, меню навігації і картинкам.

3.7.1. F-патерн сприйняття веб- сторінок

Спеціальні дослідження на основі фіксації напрямку погляду користувача визначили, що на сторінці з текстом найбільше уваги зосереджено на верхній лівій частині веб-сторінки, потім увага фокусувалася на кількох фразах на початку кожного рядка, поступово зменшуючись, таким чином формуючи трикутник, схожий на букву F.

Таким чином, користувачі найбільше звертають увагу на цифри, графіки та зображення, а також на верхню частину сторінки незалежно від змісту. Саме тому при розробці сайтів необхідно всю найважливішу інформацію поміщати вгорі сторінки і (або) на початку рядків. Нижче розглянуто сприйняття дуже довгих веб-сторінок.



Користувачі приділяють середині довгої статті менше уваги, ніж початку та кінцю. Ця проблема може бути вирішена, якщо розміщувати текст у дві

колонки. Однак, довгі статті краще розділяти на частини, кожна з яких не довше трьох екранів.

Оптимальна довжина статті – не більше трьох екранів.

3.7.2. Графічний контент

Зображення на сайті можна розділити на п’ять видів:

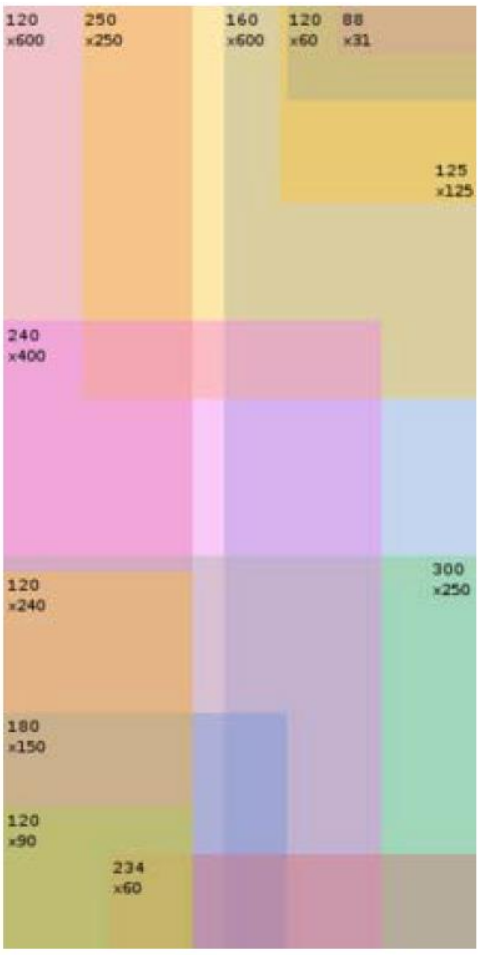
- зображення як основна інформація;
- зображення як допоміжний засіб передачі інформації;
- рекламне зображення, наприклад, банер;
- навігаційна графіка;
- дизайнерське зображення, що використовується для прикраси сайту.

Зображення як основна інформація – це зображення, які цінні самі по собі, наприклад: фотографії, картини в електронних галереях, набори іконок.

Зображення як засіб передачі інформації – це зображення, що ілюструють і доповнюють текст: схеми, ілюстрації, інфографіка.

Банер – один з переважаючих форматів інтернет-реклами. Являє собою графічне зображення, аналогічне рекламному модулю в пресі, але здатне містити анімовані (рідко відео-) елементи, а також є гіперпосиланням на сайт рекламодавця або сторінку з додатковою інформацією.

Дуже важливою характеристикою банера є його розмір у байтах, тобто місце, яке файл банера займає на сервері. Чим більший розмір банера, тим довше банер буде завантажуватися на сторінку і тим менша ймовірність, що користувач встигне подивитися на нього, перш ніж перейти на іншу сторінку; отже, розмір банера є одним з параметрів його ефективності. Сайти, що розміщують банери, зазвичай лімітують розмір файлів.



Розмір в пікселях	Найменування
300 x 250	прямокутник середньої довжини
250 x 250	спливаючий квадрат
240 x 400	вертикальний прямокутник
336 x 280	великий прямокутник
180 x 150	прямокутник
468 x 60	довгий банер
234 x 60	половина довгого банера
88 x 31	мікро смуга
120 x 90	кнопка 1
120 x 60	кнопка 2
120 x 240	вертикальний банер
125 x 125	квадратна кнопка

728 x 90	ведучий стенд
160 x 600	широкий хмарочос
120 x 600	хмарочос
600 x 90	горизонтальний середній
728 x 90	горизонтальний довгий
500 x 100	горизонтальний
100 x 100	квадратний маленький

Навігаційна графіка – графіка, яка підштовхує користувача, направляючи його до необхідної йому (шуканої) інформації.

Коли немає навігаційної графіки, користувач змушений покладатися лише на текст. Навігаційна графіка – це не завжди посилання. Якщо вона допомагає користувачеві вирішити куди клікнути – значить вона виконує свою задачу. Така графіка збагачує діалог, надаючи візуальний канал сприйняття, який не міг би бути отриманий за рахунок лише тексту. Коли дизайнер використовує правильні картинки – вони покращують взаємодію з користувачем.

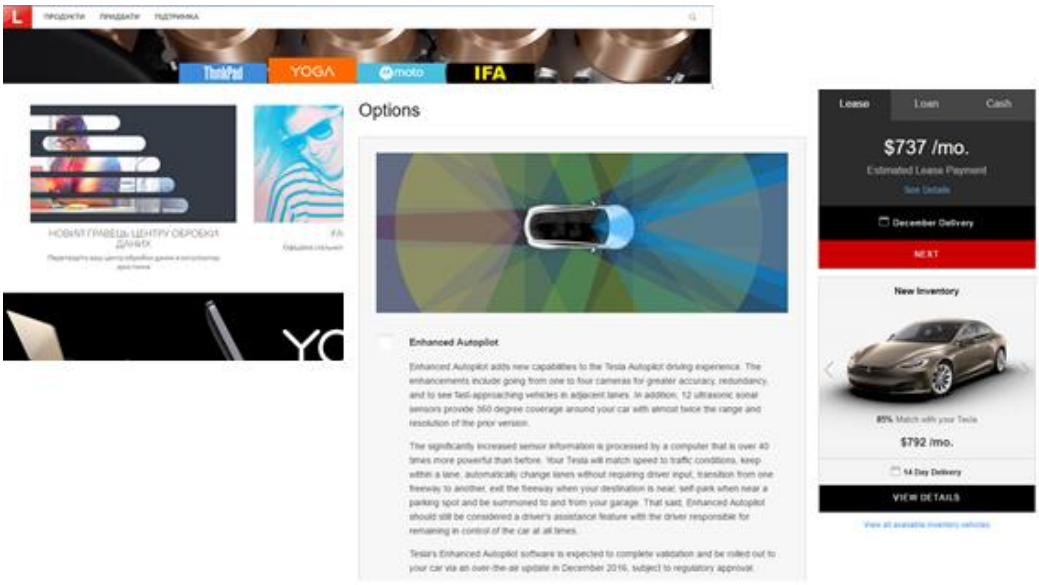


Рис. 3.3. Зразок навігаційної графіки

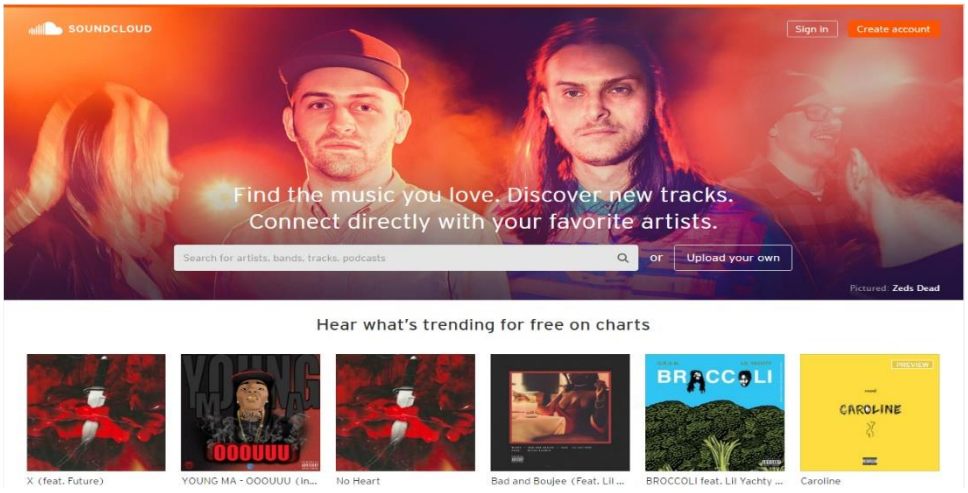
Дизайнерські зображення, які використовуються для прикраси сайту (або декоративна графіка) включають в себе:

- шапки сторінок;
- фон;
- елементи навігації та кнопки;
- заповнення пустого місця.

Шапка сторінки – це блок, розташований в самій верхній частині сторінки і шириною на весь макет. Це одне з найбільших дизайнерських зображень, тому стежте, щоб воно не важило дуже багато і не уповільнювало завантаження сторінки. При створенні шапки слід пам’ятати, що в мобільних пристроїв розширення екрану по вертикалі не перевершує 768px, тому занадто

широка шапка може призвести до того, що користувач не побачить основного вмісту. Крім того, рекомендується використовувати шапку як додатковий елемент навігації (наприклад, графічна карта посилань або посилання «На головну»).

Приклад:



Фонові зображення сторінок бувають найрізноманітнішими: світлими, темними, можуть містити водяні знаки. Світлі фони менш утомливі, ніж яскраві або темні, тому відвідувачі будуть залишатися на світлих сайтах довше.

Будь-який фон, відмінний від білого, часто викликає роздратування у відвідувачів сайту та відволікає їхню увагу від інформації, товарів і послуг, представлених на сайті.

Елементи навігації та кнопки теж часто доповнюються декоративною графікою.

Тут так само слід враховувати, що кожна додаткова картинка зменшує швидкість завантаження сторінки. Використання графічного меню погіршує подання інформації в пошуковій системі, тому застосування зображень в даному випадку має бути обґрунтованим.

Нерідко зображення використовуються на сайті, просто для заповнення порожнього місця. У більшості випадків вони нічого не дають сайту, лише відволікаючи від його вмісту. Єдиним винятком є асоціативна графіка. Часто для заповнення пустих місць використовуються фотографії людей. Це самий сильний відволікаючий фактор, тому застосовувати зображення осіб слід виключно акуратно.

3.7.3. Облік цільової аудиторії

Не можна створити сайт, який буде подобатися всім. Як вже зазначалося раніше, при замовленні виготовлення сайту необхідно орієнтуватися на цільову аудиторію сайту, тобто враховувати вік відвідувачів сайту, їх стать, соціальні, психологічні, фізіологічні та інші особливості, щоб дизайн сайту найбільш відповідав їхнім уподобанням.

Чим молодше передбачувана цільова аудиторія сайту, тим вище ймовірність, що їй сподобається яскравий і соковитий дизайн сайту, наповнений різними спецефектами, кумедними малюнками та іншими «наворотами».

Для сайту, який орієнтований на більш зрілу цільову аудиторію, спецефекти і яскраві (кричущі) кольори грають, радше, негативну роль.

Вважається, що чоловіки віддають перевагу синьому кольору над червоним, в той час як жінки навпаки – червоному над синім. Чоловіки віддають перевагу помаранчевому кольору, а жінки – жовтому.

При створенні сайту важливо враховувати і віросповідання цільових відвідувачів сайту. У представників різних релігійних конфесій (християнин, мусульманин, іудей і т. д.) реакція на той чи інший колір або поєднання кольорів можуть розрізнятися.

Нехтування цим фактором може негативно позначитися на прибутку власника сайту.

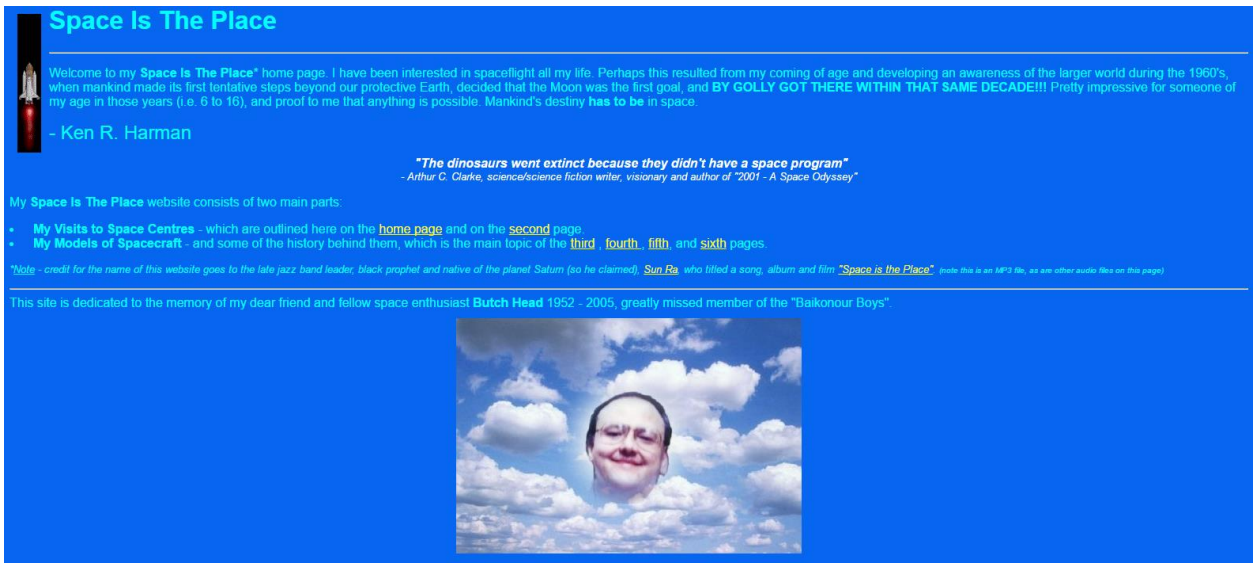
3.8. Приклади невдалого дизайну сайту

Нижче розглянуто декілька прикладів невдалого дизайну сайту.

Space is the Place (www.spaceistheplace.ca)

Першим ділом ви побачите набридливу GIFку, на якій кожну секунду злітає космічний корабель. На сліпучому яскраво-синьому тлі – текст небесно-блакитного кольору. Трохи нижче – голова автора сайту, літаюча в хмарах. Сайт містить розрізнену інформацію про космічні польоти і фотографії автора з ракетами і космонавтами.

Цей сайт не тільки неприємний для ока, але і може зацікавити хіба що знайомих автора сайту і тих, кому подобаються люди середнього віку, які захоплюються космонавтикою.



Ling's Cars (www.lingscars.com)

Сайт, присвячений продажу старих машин, весь наповнений яскравими банерами та стікерами всіх кольорів веселки, на ньому сотні посилань, які ведуть на такі ж сторінки з блискучими банерами. Скрізь, де можливо, ви побачите фотографії самого Ліна (власника сайту). Особливо дістає зображення Ліна з безперервно тремтячою головою. Все найгірше, що може бути в рекламі – на цьому сайті.

ARNGREN (www.arngren.net)

Це зразок того, як не потрібно робити сайти, призначені для торгівлі. Величезний асортимент товарів який ніби звалений в купу на стартовій сторінці в абсолютно безладній послідовності. Знайти товар, що цікавить дуже важко. У лівій частині сайту є меню, завдяки якому можна вибрати цікавий вид товару, але, пройшовши за посиланням, ви побачите той же хаотичний дизайн, а товари

часто не відповідають зазначеним категоріям. Також на сайті немає ніякої інформації про власників сайту, про те, що вони продають і чому у них варто що-небудь купувати.

Порядок виконання лабораторної роботи №3[1]:

1. Включити ПК.
2. Ознайомитися з короткими теоретичними відомостями.
3. На практиці пройти початковий (підготовчий) етап створення сайту, на основі чого, використовуючи будь-який графічний редактор (paint, adobe photoshop та інші), створити макет сайту.
4. Оформити звіт згідно до вимог (додаток 1).
5. Зробити висновки, відповісти на контрольні питання та підготуватися до усного опитування.

Зміст звіту:

1. Титульний лист.
2. Постановка завдання.
3. Протокол виконання лабораторної роботи, що містить повний опис проходження початкового етапу створення сайту та створений дизайн-макет вашого сайту (рисунки 3-4-х сторінок сайту).
4. Висновки та відповіді на контрольні питання.

Контрольні питання:

[1] *Примітка*: перед виконанням даної лабораторної роботи необхідно поділитися на бригади, в кожній з яких не більше трьох студентів.

1. Що таке гіпертекст у сучасному розумінні та назвіть основні його елементи?
2. Надайте визначення наступним поняттям: «сайт» та «web-сторінка».
3. Що таке копірайтинг та які основні цілі переслідуються при формуванні інформаційного наповнення сайту?
4. Опишіть структуру інтернет-ресурсу.
5. Назвіть основні шаблони поведінки користувача в кіберпросторі.

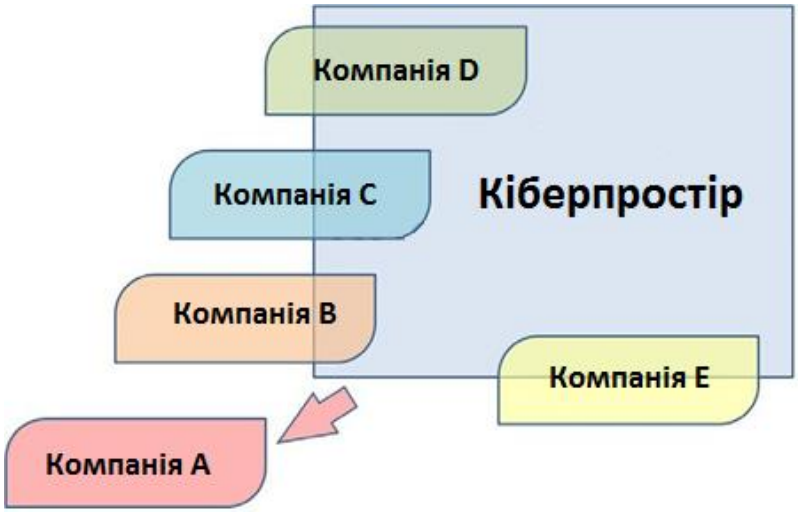
Лабораторна робота №4
«Інтернет-комерція та її вплив на соціум»

Мета роботи:

1. Поглиблення та закріплення теоретичних знань з наступних питань:
   - бізнес в кіберпросторі та основні напрямки інтернет- комерції;
   - організація роботи через інтернет та основні види реклами в інтернеті.
2. Набуття практичних навичок з представлення (презентування) свого власного інтернет-проекту.

Стислі теоретичні відомості:

4.1. Бізнес в кіберпросторі



За ступенем інтеграції комерційних фірм з кіберпростором можна виділити п’ять типів:

- ***Компанія A*** отримує інформацію для свого бізнесу з кіберпростору. При цьому компанія не має свого образу в кіберпросторі (тобто свого сайту), крім, можливо, оголошень і описів в каталогах фірм Приклад такої компанії – перукарня.
- ***Компанія B*** має в кіберпросторі свій образ – корпоративний сайт каталог продукції. Прикладами таких компаній є автоконцерни і будівельні компанії.

- ***Компанія C*** має свій інтернет-магазин. При цьому інтернет-магазин не є основною метою створення компанії. Прикладами таких компаній є косметичні фірми, виробники одягу.
- ***Компанія D*** працює в основному в кіберпросторі, у неї може не бути реального офісу для роботи з клієнтами. Прикладами таких компаній є хостинг-провайдери.
- ***Компанія E*** має в кіберпросторі свою інтрамережу. Приклади компаній – оператор стільникового зв'язку, банк.

Інтранет – внутрішньо-корпоративна мережа, що використовує стандарти, протоколи, технології, а часто – і фізичні канали зв'язку Інтернету.

4.1.1. Класифікація інтернет- комерції за цільовою аудиторією

- *Схема B2B або бізнес-бізнес* – взаємодія між підприємствами (наприклад, оптові інтернет-магазини, банківські послуги, оренда хостингу під корпоративні сайти).
- *Схема B2C або бізнес-споживач*. Приклад: інтернет-магазин.
- *Схема C2C або споживач-споживач*. Приклад: дошка приватних оголошень, біржа праці.

4.1.2. Переваги електронної комерції

1) Для організацій

- глобальний масштаб (можливість реклами і продажу по всьому світу, а не тільки в межах регіону);
- скорочення витрат (зниження потреби в особистих контактах);
- поліпшення ланцюгів постачань;
- бізнес завжди відкритий (24/7/365);
- персоналізація;
- швидке виведення товару на ринок (висока швидкість розповсюдження інформації);
- низька вартість розповсюдження цифрових продуктів.

2) Для споживачів

- повсюдність та великий вибір товарів і послуг;
- персоналізація;
- більш дешеві продукти і послуги;
- оперативна доставка;
- електронна соціалізація.

3) Для суспільства

- широкий перелік надаваних послуг;

- підвищення рівня життя;
- підвищення національної безпеки;
- зменшення «цифрового» розриву;
- зниження забруднення навколишнього середовища (зниження витрат на транспорт).

Однак існують і недоліки електронної комерції, основним з яких є ***цифровий бар'єр, цифрова нерівність*** – обмеження можливостей соціальної групи із-за відсутності у неї доступу до сучасних засобів комунікації.

4.2. Основні напрямки інтернет-комерції

- надання мережних ресурсів:
  - інтернет-провайдери;
  - хостинг-провайдери;
  - продаж доменних імен;
  - продаж процесорного часу Cloud Computing.
- розробка сайтів;
- організація роботи через Інтернет;
- продаж реальних товарів через інтернет;
- надання інформаційних послуг і віртуальні товари.

Далі розглянемо більш детально основні напрямки інтернет-комерції.

4.2.1. Інтернет-провайдери

Інтернет-провайдер – організація, що надає послуги доступу до Інтернету.

Провайдерів можна розділити на первинних (магістральних) – мають магістральні канали зв'язку у власності і вторинних (міських) – орендують канали зв'язку у первинних.

Провайдери займаються прокладанням кабелів, обслуговуванням супутникового зв'язку (тарілок і самих супутників), ADSL і Dial-up (як правило, телефонні компанії), проектуванням і налаштуванням Wi-Fi-мереж у межах підприємства, кафе та ін.

Товар провайдерів:

- можливість підключення до інтернету (стягується абонентська плата);
- підключення до інтернету (сплачується щохвилини або посекундно);
- кількість отриманого/переданого трафіку (оплачується кількість закачаних/відданих байтів);

- IP-адреси (через брак адрес IPv4 адреси комп'ютерів видаються динамічно, і можуть змінюватися при кожному з'єднанні; оплачується можливість мати постійну зовнішню IP-адресу (наприклад, для запуску веб-сервера)).

Ресурси:

- сервера зв'язку та proxy-сервера;
- комунікаційне обладнання та канали зв'язку.

4.2.2. Хостинг-провайдери

Хостинг-провайдер – компанія, що займається наданням послуг розміщення устаткування (серверів), даних і web-сайтів на своїх технічних майданчиках.

Товар:

- місце на серверах під сайти;
- ресурси для створення бази даних (MySQL, Postgre, Oracle та ін);
- інші ресурси для створення сайтів (підтримка різних мов програмування (php, perl, ruby, java) і ін.).

Ресурси:

- високопродуктивні сервера з можливістю віддзеркалення;
- комунікаційне обладнання;
- канали зв'язку.

Дзеркало – точна копія (понад 80 відсотків збігів) даних одного сервера на іншому. В Інтернеті **дзеркалом сайту** називають точну копію іншого сайту. Дзеркала підвищують надійність системи в разі виходу з ладу обладнання, дозволяють рівномірно розподіляти навантаження на сервера, що робить взаємодію через кіберпростір більш ефективною. Це технічна специфіка інтернету, і далеко не завжди видна користувачам. У більшості випадків кожен сайт має як мінімум одне дзеркало (це пов'язано з тим, що провайдери віддзеркалюють свої сервера).

4.2.3. Продаж доменних імен

Товар: доменні імена другого і третього рівня в різних зонах.

*Ресурси:*дозвіл на продаж доменних імен.

Загальне число зареєстрованих доменів наближається до 200 мільйонів і підібрати вільне, красиве і коротке доменне ім'я стало дуже важко. І саме тому з'явився ринок перепродажу доменних імен. Сюди входять компанії, які реєструють домени, купують і продають домени на вторинному ринку, займаються розміщенням реклами на зареєстрованих доменів, хостингові

сервіси, юридичні і правові організації і т. п. Близько 30% сайтів не містять ніякої інформації й існують тільки для продажу рекламних посилань.

Найдорожчі домени:

1.Business.com – більш 340 млн. доларів

2. Web.com – 129 млн. доларів

3. AllBusiness.com – 55 млн. доларів

4. Sex.com – понад 12 млн. доларів

5. CNN.com – 12 млн. доларів

Найпопулярнішою і дорогою доменною зоною є **.com**

Кіберсквотинг – придбання доменних імен, співзвучних з назвами відомих компаній, або просто з «дорогими» назвами з метою їх подальшого перепродажу або розміщення реклами.

Слово кіберсквотинг походить від слова *squatting*, що означає акт самовільного заселення покинутого або незайнятого місця.

Види кіберсквотинга:

- тайпсквотинг;
- брендовий та іменний кіберсквотинг;
- галузевий та географічний кіберсквотинг;
- захисний кіберсквотинг.

Тайпсквотинг – реєстрація доменних імен, близьких за написанням з адресами популярних сайтів в розрахунку на помилку частини користувачів.

Приклад: www.lenta.ru – wwwlenta.ru

Брендовий та іменний кіберсквотинг – реєстрація доменних імен, які містять товарні знаки, фірмові найменування, популярні власні імена, тобто засоби індивідуалізації, що охороняються законом. *Найчастіше незаконний.*

Галузевий і географічний кіберсквотинг – реєстрація доменних імен, географічних назв, назв сфер діяльності і популярних слів.

Приклад: kiev.karabas.com www.tourism-ua.net

Захисний кіберсквотинг – легальний власник популярного сайту (товарного знака) реєструє всі доменні імена, близькі, співзвучні, схожі, пов’язані за змістом з його власним доменним ім’ям.

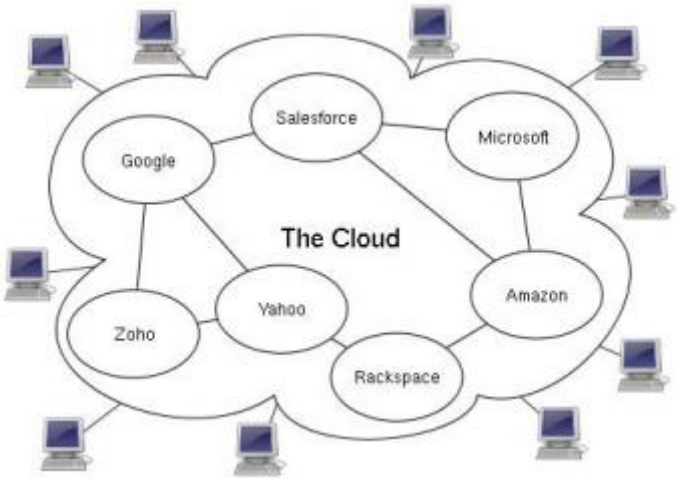
Приклад: Yandex.ua – Jandex.ua

4.2.4. Cloud Computing

Хмарні обчислення (англ. cloud computing) – технологія розподіленої обробки даних, в якій комп’ютерні ресурси і потужності надаються користувачеві як Інтернет-сервіс.

Назва «хмарні обчислення» пішла від того, що на схемах, що ілюструють структуру (топологію) локальних мереж Інтернет зображується у вигляді хмари. Як правило, компанії, що надають послуги Cloud Computing, володіють великими обчислювальними потужностями (суперкомп'ютерами або кластерами серверів).

Хмарні обчислення знижують вартість використання комп'ютерних технологій для кінцевого користувача, однак, хмарні обчислення менш безпечні, і не забезпечують необхідний рівень конфіденційності.



Види Cloud Computing:

- «все як послуга»;
- «інфраструктура як послуга» (замість покупки реальних серверів можна орендувати віртуальну машину, і платити за місце на дисках і за процесорний час);
- «платформа як послуга» (можливість користуватися налаштованим програмним забезпеченням на віддаленому сервері);
- «програмне забезпечення як послуга» (бізнес-модель продажу і використання програмного забезпечення, при якій постачальник розробляє веб-додаток і самостійно управляє ним, надаючи замовникам доступ до програмного забезпечення через Інтернет).
- «робоче місце як послуга» (клієнти отримують повністю готове до роботи («під ключ») стандартизоване віртуальне робоче місце, яке кожен користувач має можливість додатково налаштовувати під свої завдання; користувач отримує доступ не до окремої програми, а до необхідного для повноцінної роботи програмного комплексу);
- «дані як послуга» (користувач платить за доступ до даних через інтернет: бази різних об'єктів, напр., мобільних телефонних номерів, статистична інформація та ін).

4.3. Організація роботи через інтернет. Фріланс.

З появою кіберпростору поштовх до розвитку отримав ринок трудових ресурсів. З'явилися численні віртуальні біржі праці, що дозволяють встановлювати ефективні зв'язки між роботодавцями та шукачами.

Можна виділити *три основних види сайтів трудових ресурсів*:

- бази вакансій;
- бази резюме;
- фріланс-біржі.

Інтернет дозволяє кадровим відділам ефективно шукати працівників навіть у тих областях, де потрібно переглянути сотні резюме (наприклад бази непрофесійних акторів). Зникли географічні обмеження щодо пошуку персоналу. Став можливим ефективний хедхантинг.

Хедхантинг (полювання за головами) – це один з напрямків пошуку та підбору персоналу ключових і рідкісних, як за фахом, так і за рівнем професіоналізму фахівців. Головні бухгалтери, юристи, керівники підприємств та фахівці вузьких профілів найбільш часто стають об'єктом уваги хедхантерів.

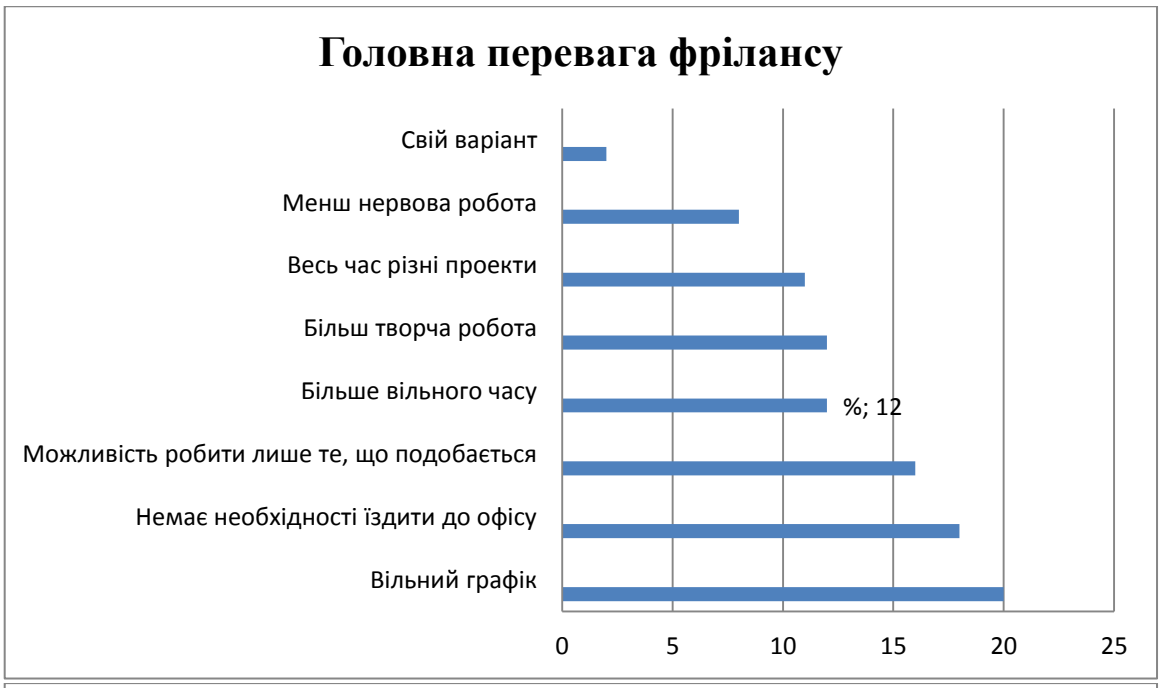
Нижче виділено основні аспекти впливу кіберпростору на ринок праці:

- спеціалізовані бази (можливість ефективного пошуку);
- активне використання соціальних мереж (цільова аудиторія вакансій);
- відео в рекрутингу: відеовакансії, відеорезюме і відеоінтерв'ю;
- Web-резюме у вигляді окремого сайту;
- віддалене інтерв'ювання кандидатів;
- корпоративні сайти як майданчик пошуку і залучення персоналу, створення іміджу фірми як роботодавця;
- бурхливий розвиток фрілансу.

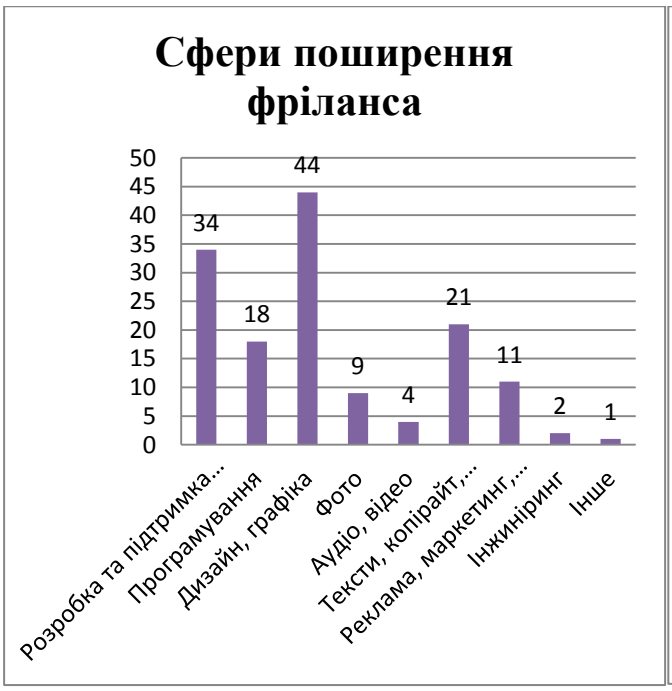
Фрілансер (freelancer – вільний списоносець, наймит) – людина, яка виконує роботу без укладання довгострокового договору з роботодавцем, тобто людина яку наймають лише для виконання певного переліку робіт.

Особливості фрілансу:

+ вільний графік та ефективне використання власного часу;
+ можливість займатися декількома видами діяльності;
+ ослаблення географічної прив'язки до місця роботи;
+ психологічний комфорт;
– нестабільність заробітку та недобросовісні замовники;
– необхідність самому шукати клієнтів;
– відсутність пільг, бонусів і офіційного стажу роботи;
– ненормований робочий день;
– організаційні витрати.



Середній дохід фрілансера більше ніж в два рази вищий, ніж середня заробітна плата в Україні. Однак, цей факт може зумовлюватися тим, що фріланс поширений в сферах, де потрібна висококваліфікована праця.



4.4. Продаж реальних товарів через інтернет

Основною формою продажу реальних товарів через кіберпростір є інтернет-магазини.

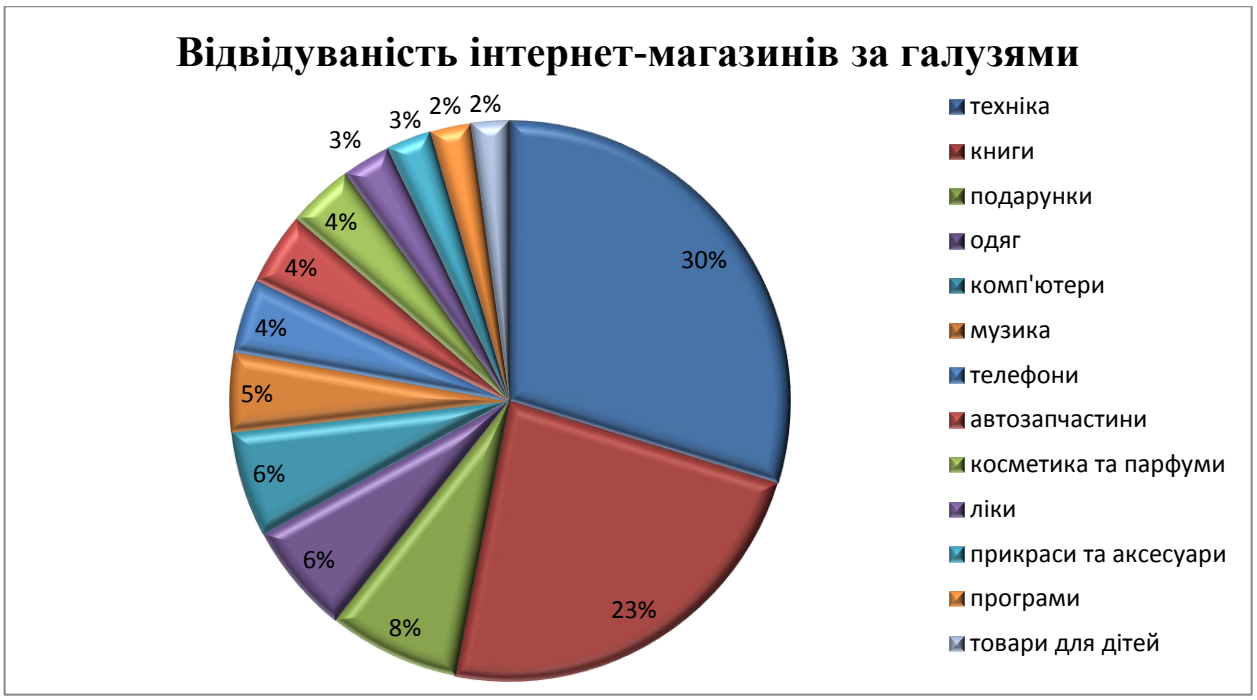
Інтернет-магазин – сайт з каталогом продукції і кошиком для формування замовлення по каталогу.

Основні елементи інтернет-магазину:

- каталог продукції;
- кошик покупця:
  - з попередньою реєстрацією та без попередньої реєстрації;
- система оплати:
  - банківський переказ (передоплата);
  - системи електронних платежів (передоплата);
  - післяплата на пошті або безпосередньо при доставці кур’єром;
- система доставки;
  - пошта або кур’єр;
  - самовивіз.

Умови ефективності інтернет-магазину:

- вдалий вибір товару;
- затребуваність товару;
- по опису легко зрозуміти, підходить товар чи ні;
- невеликий вибір у звичайних магазинах або унікальність;
- можливість ефективної доставки;
- якість «движка» інтернет-магазину;
- насиченість ринку;
- рівень довіри покупців. *Відвідувач не робить покупку, якщо він відчуває себе некомфортно і боїться бути ошуканим*;
- повна контактна інформація;
- подяки та відгуки;
- говорити правду;
- висока якість товару;
- реклама та пошукова оптимізація.



4.5. Надання інформаційних послуг та віртуальні товари

Види віртуальних товарів і послуг:

- Мережеві ігри:
  - купівля ресурсів у грі або платний доступ до самої гри;
  - реклама в грі.
- Реклама в мережі:
  - дошки оголошень;
  - реклама на сайтах та в блогах;
  - реклама в соціальних мережах.
- Платні послуги:
  - скачування контенту (плата за сам цифровий контент або за швидкість доступу до нього)
  - додаткові послуги в соціальних мережах, на сайтах знайомств та ін.
  - мережеві сервіси для сайтів (статистика)

4.5.1. Онлайн- ігри

Види онлайн-ігор:

- *ММО-ігри* (Масова багатокористувацька онлайн-гра – мережева комп'ютерна гра, в якій одночасно бере участь велика і практично не обмежена кількість гравців). ММО-ігри найбільш прибуткові для виробника, хоча і вимагають для свого виробництва дуже великих витрат. ММО-ігри створюють найбільше занурення в гру, викликаючи часто інтернет-залежність. Гравець

ММО готовий витрачати на гру більше грошей, ніж у казуальних і соціальних іграх. ММО-ігри формують своє соціальне середовище і є конкурентами соціальних мереж.

- *Казуальні ігри* (прості ігри, основне призначення яких – скрасити невеликі проміжки часу очікування). До казуальних ігор відносяться різноманітні головоломки, пазли, пасьянси.
- *Соціальні ігри* (ігри, що представляють собою оригінальний інструмент спілкування через Інтернет). Соціальні ігри сконцентровані не на ігровому процесі, а на спілкуванні гравців. Соціальні ігри як правило використовують інструменти соціальних мереж і є частиною цих мереж.

4.6. Реклама в Інтернет

Класифікація реклами за видом носія:

- банерна реклама;
- rich-media;
- текстова реклама;
- електронні розсилки.

Класифікація реклами за спрямованістю:

- медійна;
- контекстна;
- гео-контекстна;
- продакт-плейсмент.

4.6.1. Банерна, rich-media та текстова реклама

Банер – графічне зображення рекламного характеру, є гіперпосиланням на сайт рекламодавця або сторінку з додатковою інформацією.

Ефективність банерної реклами вимірюється за такими показниками:

- ***Кількість переглядів банера*** – це основний параметр для рекламної кампанії. Покази вимірюються тисячами і мільйонами.
- ***Кількість кліків*** (CTR, click through ratio) – це відношення кількості кліків до кількості переглядів, що вимірюється у відсотках. Зараз звичайним для банера вважається CTR в 0,3 - 0,5 %.

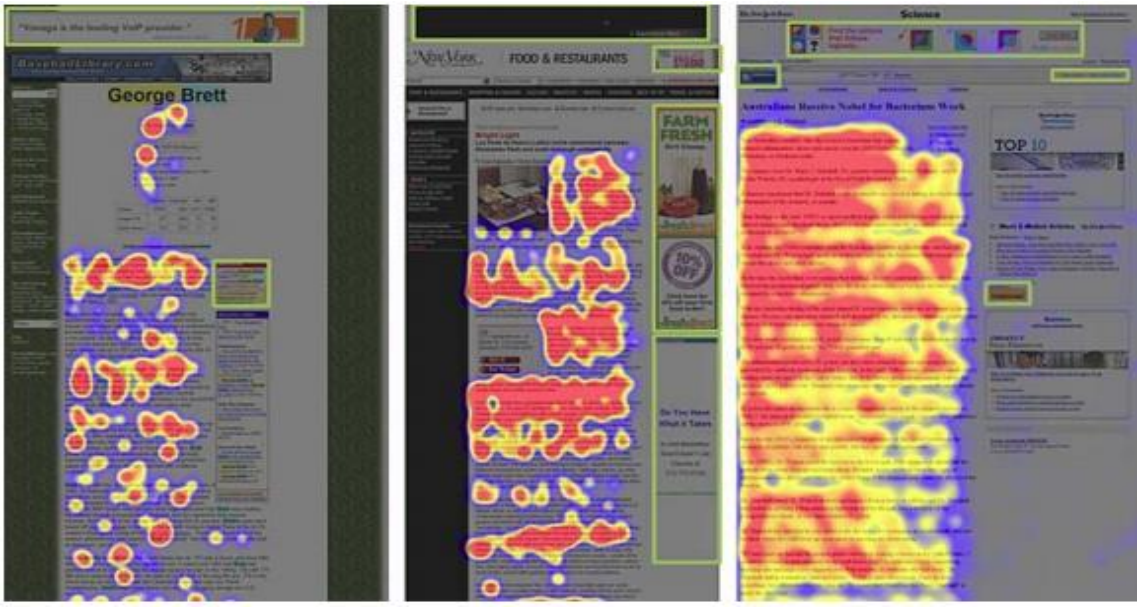
Банер можна отримати домовившись з рекламодавцем безпосередньо, або скориставшись банерною мережею.

Банерна мережа – система обміну рекламними графічними банерами або текстовими блоками, при якій за показ чужих банерів на своєму сайті учасник мережі отримує певний відсоток показів власного банера на сайтах інших

учасників проекту за вирахуванням відсотка комісії, який використовує власник мережі.

Надмірно активне використання банерної реклами призвело до того, що у більшості користувачів виробилося негативне ставлення до цього виду реклами, і навіть самий яскравий і красивий банер приваблює дуже мало уваги користувачів.

Банерна сліпота – психологічний ефект несприйнятливості до непотрібної банерної реклами на сайтах. На малюнку показано, що погляд користувача взагалі ніколи не потрапляє на банери (обведені світло-зеленими прямокутниками):



Rich media – технологія виготовлення рекламних інтерактивних матеріалів.

Для виготовлення такої реклами використовуються технології flash і javascript. До rich media відносяться рекламні банери, де користувача просять вчинити яку-небудь дію (прихлопнути комара, не чіпати гобліна, врятувати білку, т.п.) і так звані «спливаючі вікна». *Rich media* – дуже агресивний метод реклами, і часто викликає у користувача негативні враження. Крім того, rich media небезпечна і може бути розношиком вірусів і шпигунського програмного забезпечення.

Текстова реклама – вид інтернет-реклами, текстове рекламне оголошення, яке інтегровано в загальний текст на веб-сторінці і виглядає, як її складова частина.

Як правило, текстова реклама є контекстною. На відміну від графічної реклами, «імунітет» до текстової реклами не виробляється, так як користувач приходить на сторінку в першу чергу за текстовою інформацією. Текстова реклама – найефективніша в Інтернет. До текстової реклами відносяться:

- невеликі текстові оголошення рекламних бірж (google, begun та інші);
- рекламні статті в блогах.

4.6.2. Розсилка та спам

Існує три види розсилок:

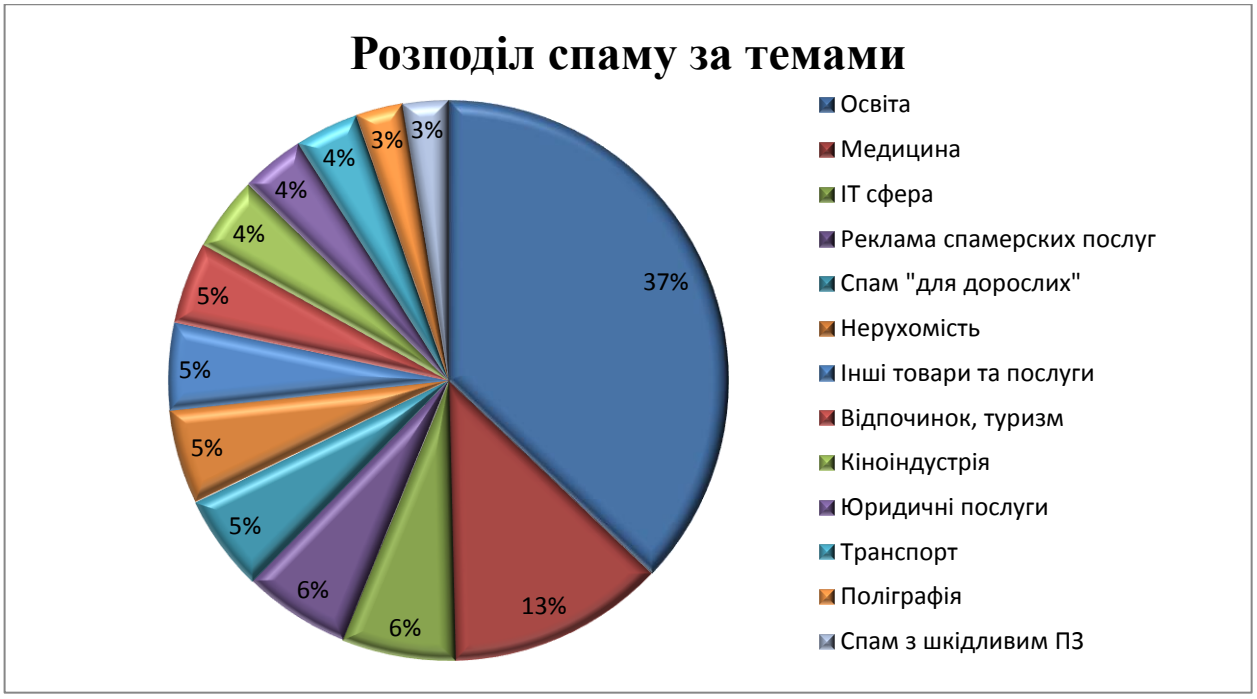
- розсилання передплатникам (користувач свідомо і добровільно підписався на отримання оновлень з сайту компанії, і має можливість у будь-який момент відмовитися від розсилки);
- розсилка зі стрічкою новин (реклама вкладається в розсилку rss новин);
- спам.

Розсилка є найбільш неефективним способом реклами в інтернет.

Вірусний маркетинг – загальна назва різних методів поширення реклами, де головним поширювачем інформації є самі одержувачі інформації шляхом формування змісту, здатного залучити одержувачів інформації за рахунок яскравої, креативної, незвичайної ідеї. Вірусна реклама розповсюджується на основі тих же механізмів, що і інтернет-меми.

Спам – масова розсилка рекламних оголошень електронною поштою без згоди одержувачів, основними цілями якої є:

- реклама (вкрай неефективна, швидше викликає відторгнення);
- анти-реклама або шахрайство.



Середовище розповсюдження спаму:

- електронна пошта;
- служби миттєвих повідомлень (ICQ, Jabber, Skype, Telegram, Viber, WhatsApp) або звичайні SMS;
- соціальні мережі, сайти знайомств та блоги.

Проблеми, пов’язані зі спамом:

- час, який користувач витрачає на розбір спаму;
- трафік (навантаження на мережі, як вже було раніше зазначено, спам становить від 70% всього поштового трафіку);
- віруси, фішинг та інші види шахрайства в інтернеті;
- помилкові спрацьовування спам-фільтра.

Фішинг – вид інтернет-шахрайства, метою якого є отримання доступу до конфіденційних даних користувачів – логінів і паролів.

На зародженні інтернету фішерів цікавили лише паролі від електронної пошти та форумів (з метою розсилки спаму під обліковими записами реальних користувачів). Сьогодні ж найбільш цікавими для фішерів є логіни і паролі від мережевих гаманців і номери банківських карт, а також паролі від акаунтів соціальних мереж і блогів.

4.6.3. Спрямованість реклами

Медійна реклама – традиційна реклама, не прив'язана до вмісту сайту.

Product placement – рекламний прийом, який полягає в тому, що реквізит у фільмах, телевізійних передачах, комп'ютерних іграх, музичних кліпах або книгах має реальний комерційний аналог.

Контекстна реклама – вид розміщення інтернет-реклами, в основі якої лежить принцип відповідності змісту рекламного матеріалу контексту (змісту) інтернет-сторінки, на якій розміщається даний матеріал.

Приклад:

- реклама VK, враховує вік, стать, освіту і уподобання користувачів;
- рекламні оголошення на пошукових порталах (в пошуковій вибірці, відповідні пошуковому запиту користувача);
- реклама автосалонів на форумах, присвячених автомобілям.

Геоконтекстна реклама – це вид реклами, заснованої на показі рекламних повідомлень в додатках для мобільних пристроїв і веб-сайтах, з урахуванням точного поточного місця розташування користувача або географії їх інтересів.

Приклад:

- реклама в google maps, 2gis; реклама, що визначає положення відвідувача сайту по пеленгу навігатора або мобільного телефону.

Порядок виконання лабораторної роботи №4:

1. Включити ПК.
2. Ознайомитися з короткими теоретичними відомостями.
3. На основі вже пройденого (підготовчого) етапу створення сайту, а також розробленого та створеного макета сайту, відтворити макет за допомогою одного з безкоштовних конструкторів, наприклад: wix.com, tilda.cc, ukit.com, LPgenerator, PlatformaLP, webnode.com.ua, і т. п.
4. Підготувати доповідь та презентацію свого інтернет-проекту.
5. Оформити звіт згідно до вимог (додаток 1).
6. Зробити висновки, відповісти на контрольні питання та підготуватися до усного опитування.

Зміст звіту:

1. Титульний лист.
2. Постановка завдання.
3. Протокол виконання лабораторної роботи, що містить доповідь щодо створеного вами інтернет-проекту та його скріншоти.
4. Висновки.

Контрольні питання:

1. Назвіть основні переваги електронної комерції для організації, споживачів та суспільства.

2. Назвіть та коротко охарактеризуйте основні напрямки інтернет-комерції.

3. Класифікуйте рекламу в Інтернеті та коротко охарактеризуйте кожен з видів.

Лабораторна робота №5
«Основи інформаційно-пошукових систем»

Мета роботи:

1. Поглиблення та закріплення теоретичних знань з наступних питань:
   - специфіка інформації в інтернеті;
   - структура та функціональні можливості інформаційно-пошукових систем інтернету;
   - мова запитів інформаційно-пошукових систем.
2. Опанування основних принципів роботи з пошуковими серверами та оволодіння методом пошуку інформації з використанням ключових слів.

Стислі теоретичні відомості:

5.1. Специфіка інформації в інтернеті

Інтернет зберігає величезні обсяги *слабоструктурованої інформації*. Щоб користувач міг отримати цю інформацію, потрібна організація спеціальних систем пошуку інформації. Такі системи діляться на жорстко структуровані (каталоги і бібліотеки) та неструктуровані (пошукові системи). Основним критерієм якості роботи системи доступу до інформації є ***релевантність*** (ступінь відповідності запиту і знайденого, тобто доречність результату). В жорстко структуровані системи інформація вноситься, як правило, вручну, і тому високорелевантна. Однак, інформації в таких системах набагато менше, так як процес внесення не автоматизований і займає багато часу. Неструктуровані системи доступу дозволяють отримувати інформацію з величезного числа ресурсів, однак автоматичні системи пошуку можна різними способами обманювати. Крім того, такі системи «не розуміють», що конкретно шукає користувач, і тому релевантність інформації тут нижча.

Основні протоколи, які використовуються в Інтернеті, не забезпечені достатніми вбудованими функціями пошуку, не кажучи вже про мільйони серверів, що знаходяться в ньому. Протокол HTTP, використовуваний в

Інтернеті, хороший лише щодо навігації, яка розглядається тільки як засіб перегляду сторінок, але не їх пошуку. Те ж саме відноситься і до протоколу передачі файлів FTP. Через швидке зростання інформації, доступної в Мережі, навігаційні методи перегляду швидко досягають межі їх функціональних можливостей, не кажучи вже про межі їх ефективності. Потрібну інформацію вже не представляється можливим отримати відразу, так як в Мережі зараз знаходяться мільярди документів і всі вони в розпорядженні користувачів Інтернет, до того ж сьогодні їх кількість дуже швидко зростає. Кількість змін, яким ця інформація піддається – величезна і, найголовніше, вони відбулися за дуже короткий період часу. Основна проблема полягає в тому, що єдиної повної функціональної системи оновлення і занесення такого обсягу інформації, одночасно доступного всім користувачам Інтернет в усьому світі, ніколи не було.

Виділимо основні аспекти, які обумовлюють складність пошуку інформації у Всесвітній Павутині:

- основні протоколи (http, ftp) не забезпечені достатніми вбудованими функціями пошуку;
- величезна кількість документів;
- кількість документів швидко зростає;
- вміст документів динамічно змінюється.

Для того, щоб структурувати інформацію, накопичену в мережі Інтернет, і забезпечити її користувачів зручними засобами пошуку необхідних їм даних, були створені пошукові системи. Пошукова система на сьогоднішній день найбільш ефективний і часто використовуваний спосіб доступу до інформації в Інтернет.

Наведемо декілька прикладів пошукових машин Інтернету (в індексі знаходяться сайти на англійській, німецькій та інших європейських мовах):

- Google – http://www.google.com
- Yahoo! – http://www.yahoo.com
- MSN Search – http://search.msn.com
- Bing – https://www.bing.com
- Yandex – http://www.yandex.com

Пошукова система – веб-сайт, що надає можливість пошуку інформації в Інтернеті.

Більшість інформаційно-пошукових систем світу – індексні пошукові системи, які ще називають пошуковими покажчиками, пошуковими серверами, словниковими пошуковими системами, автоматичними індексами, пошуковими машинами, Search Engines, Retrieval Systems – в англомовних джерелах тощо. В інтернеті їх функціонує декілька сотень. Перед ними ставиться завдання

якнайкраще охопити інформаційний Web-простір і подати його користувачам у зручному вигляді. Принцип роботи з індексними пошуковими системами ґрунтується на використанні ключових слів. Розшукуючи відомості з деякої теми, користувач повинен дібрати ключові слова, які описують цю тему, і задати їх індексній пошуковій системі як запит. Користувачам такої пошукової системи надається форма, або пульт управління пошуком, для введення ***ключового слова*** (слів) або фрази. Пошукова система знаходить у своїх базах даних, які називаються індексами або покажчиками, адреси Web-ресурсів, котрі містять ключові слова, і видає клієнту сторінку з посиланнями на ці ресурси. Така Web-сторінка називається звітом про результати пошуку.

Відомо, що переважна кількість пошукових систем шукають інформацію на сайтах Всесвітньої павутини, але існують також системи, здатні шукати файли на ftp-серверах, товари в інтернет-магазинах, а також інформацію в групах новин Usenet і навіть сервера, комп'ютери, роутери, вебкамери, принтери, системи відеоспостереження та інше. Як правило, основною частиною пошукової системи є пошукова машина (пошуковий движок) – комплекс програм, що забезпечує функціональність пошукової системи.

5.2. Внутрішня структура пошукової системи

Пошукова система складається з наступних основних компонентів:

- ***Spider*** *(павук)* – програма, яка завантажує веб-сторінки і переглядає HTML-код вибираючи з нього текстову інформацію: в метатегах, в підписах картинок і посилань, з основного тексту сторінки.
- ***Crawler*** *(краулер, «мандрівний» павук)* – програма, яка автоматично проходить по всіх посиланнях, знайдених на сторінці.
- ***Indexer*** *(індексатор)* – програма, яка аналізує веб-сторінки, завантажені павуками, і заносить інформацію в базу даних. Індексатор виокремлює на сторінці ключові слова, які потім використовуються для обчислення релевантності.
- ***Database*** *(база даних)* – сховище викачаних і оброблених сторінок. У базі, звичайно ж, не зберігається весь текст сторінок, тільки результат його обробки індексатором.
- ***Search engine, results engine*** *(система видачі результатів)* – витягує результати пошуку з бази даних і відранжовує їх (упорядковує знайдені сторінки за рівнем релевантності).

Фактори, що впливають на положення сторінки в вибірці:

- Внутрішні: наявність в статті, в заголовку статті, в підписах до зображень ключових слів із запиту користувача.

- Зовнішні: авторитетність сторінки на основі посилання ранжування (Google Page-Rank і Яндекс ВИЦ (зважений індекс цитування)).

Ранжування *(ranking)* – це процес вибудовування знайдених за запитом користувача сторінок в порядку найбільшої відповідності до шуканого запиту.

Основним методом для оцінки релевантності за ключовими словами є ***TF-IDF-метод***, який використовується в більшості пошукових систем. Його зміст зводиться до того, що чим більша локальна частота терміна (запиту) в документі (TF) і більша «рідкість» (тобто чим рідше він зустрічається в інших документах) терміну в колекції (IDF), тим вища вага даного документа по відношенню до терміну – тобто документ буде видаватися раніше в результатах пошуку за даним ключовим словом.

Крім цього пошукові системи можуть враховувати ще безліч факторів.

Наприклад, ***Google PageRank (PR)*** – алгоритм розрахунку авторитетності сторінки, використовуваний пошуковою системою Google. PR це чисельне значення, яке відображає, наскільки значима ця сторінка в інтернеті. Google вважає, що коли одна сторінка посилається на іншу, вона немов «віддає свій голос» за іншу сторінку. Тоді, чим більше голосів віддано за сторінку, тим важливіша повинна бути ця сторінка. Крім того, – і це важливо! – віддані голоси відрізняються за значимістю в залежності від того, хто голосує. Google підраховує важливість оцінюваної сторінки, виходячи з голосів, відданих за неї. При цьому в процесі розрахунків Google враховує, наскільки важливий (вагою) кожен з відданих голосів. PR є неєдиним фактор, який Google використовує для оцінки сторінок, але один з найважливіших.

5.2.1. Принцип роботи індексних пошукових систем

Індексні пошукові системи мережі інтернет дають змогу проводити досить глибокий пошук інформаційних ресурсів у рамках заданої теми. Робота індексної пошукової системи проводиться в три етапи.

На *першому етапі* пошукова система за допомогою спеціальних комп'ютерних програм обстежує інформаційний простір мережі інтернет (головним чином WWW); виявляє наявні, а особливо нові та оновлені, Web-ресурси; фіксує посилання на сайти та документи, які припинили своє існування. Тобто відбувається процес сканування інформаційного простору.

На *другому етапі* матеріал, зібраний у процесі сканування, із зазначенням посилань на те, де зберігається кожне слово, заноситься в індексну базу даних. Індексна база пошукової системи – це база даних слів, отриманих в результаті сканування. Далі відбувається перетворення бази даних так, щоб у ній можна було проводити прискорений пошук.

На *третьому етапі* індексна пошукова система приймає запит від користувача, проводить пошук у своїх базах даних і видає Web-сторінку оформлених результатів пошуку.

5.3. Мова запитів інформаційно-пошукових систем

Для пошуку інформації за одним ***ключовим словом*** необхідно набрати це слово в полі введення запитів і натиснути кнопку Знайти (Найти, Search). Пошук за одним словом доцільно проводити в тому випадку, якщо це слово є рідкісним, маловживаним, власним іменем, наприклад, конкорданс, Голомб, Джерард, Солтон.

Але, як правило, пошук за одним словом призводить до формування величезних списків Web-сторінок, на яких воно зустрічається. Знайти в такому списку потрібні ресурси не просто, і тому пошук за одним словом малоефективний. Набагато ефективнішим є пошук за кількома словами, але тут важливу роль відіграє правило, яке вказує пошуковій системі, як саме опрацьовувати групу слів. Наприклад, користувача можуть цікавити:

- документи, що містять І перше слово, І друге одночасно;
- документи, в яких ці слова зустрічаються поруч або недалеко одне від одного;
- документи, в яких зустрічається АБО перше слово, АБО друге, АБО обидва разом.

Таким чином, для ефективного пошуку за кількома ключовими словами потрібні спеціальні команди, які дають змогу пов’язати окремі слова між собою. Ці команди в пошукових системах утворюють спеціальну мову запитів. Відповідно, якщо користувач вводить запит:

Інформаційний пошук у мережі Інтернет

– фраза розбивається на слова, з яких видаляються загальні слова, інколи відбувається нормалізація лексики, потім всі слова пов’язуються між собою логічними операторами AND, OR або NOT, після чого запит буде перетворений у:

Інформаційний AND пошук AND мережі AND Інтернет

Що буде означати: «Знайти всі документи, у яких одночасно містяться слова Інформаційний, пошук, мережі, Інтернет».

Однак необхідно пам’ятати, що кожна індексна пошукова система використовує свою власну мову запитів, тому при використанні різних пошукових систем треба знати особливості кожної. Ретельний перелік правил написання запитів для конкретної пошукової системи можна знайти на її сервері за посиланнями Допомога, Як скласти запит, Поради з пошуку тощо.

Але є загальний принцип, згідно з яким усі команди можна поділити на три групи: команди простого пошуку, команди мови запитів і команди розширеного пошуку. У режимі простого пошуку запити створюються нескладними методами, але вони, як правило, призводять до численних результатів, з яких важко вибрати необхідні. Команди мови запитів дають змогу досить точно описати потрібний документ. Команди розширеного пошуку призначені для пошуку документів не за їх змістом, а, наприклад, для пошуку Web-вузлів за їх назвами, за фрагментами їх адрес, за адресами посилань, які зустрічаються на їх Web-сторінках і т.п.

5.3.1. Команди простого пошуку

Пошук за ключовими словами *– keyword search –* пошук документів, які містять вказані ключові слова.

Пошук групи слів. При роботі з будь-якою пошуковою системою слід з'ясувати, як вона сприймає групу слів у запиті, наприклад, *видатні фізики*. Україно- та російськомовні пошукові системи сприймають групу слів так, ніби між ними стоїть сполучник І, тобто шукають документи, в яких обидва ці слова зустрічаються одночасно. Так само працює пошукова система Google. Але більшість англомовних пошукових систем сприймають групу слів таким чином, ніби між ними стоїть сполучник АБО і шукають документи, які містять або перше, або друге слово, або обидва слова разом. Кількість слів у групі не обмежується.

Пошук за словосполученнями *(засоби контекстного пошуку).* Якщо ключові слова взяти в подвійні лапки «....», наприклад «To be or not to be», «Слово о полку Ігоревім», то пошукова система повинна знайти документи, в яких дана фраза присутня буквально, тобто саме так, як вона записана. Для пошуку фрази з абсолютно точним збігом пошуковій системі недостатньо індексного файлу, і вона звертається до копій раніше збережених у своїй базі Web-сторінок.

Пошук словоформ. У зв'язку з тим, що в українській та російській мовах слова змінюються за відмінками, важливою властивістю пошукової системи є пошук словоформ. У більшості випадків пошукові системи дозволяють знаходити різні словоформи, наприклад, раніше зазначений запит на пошук *видатні фізики* рівносильний запиту *видатний фізик*.

Роль великих літер. Загальне правило для більшості пошукових систем полягає в тому, що великі літери на початку слова сприймаються як додаткова умова, що обмежує область пошуку. Наприклад, за запитом Ліга Чемпіонів будуть знайдені лише ті документи, які містять слова Ліга Чемпіонів. Проте

пошук за запитом ліга чемпіонів поверне документи, в яких є слова Ліга чемпіонів, ліга Чемпіонів, Ліга Чемпіонів, ліга чемпіонів.

Пошук однокореневих слів. Більшість пошукових систем знаходить документи, які містять слова однокореневі з ключовими. Наприклад, пошук за запитом *модел* поверне документи, в яких є слова модель, моделей, модельний, моделізм, моделює, моделювання.

5.3.2. Команди мови запитів:

Пошук із зазначенням відстані – *proximity search* – пошук, при якому користувач вказує, на якій відстані одне від одного повинні розташовуватися ключові слова в документі. Під відстанню розуміють кількість слів між двома виділеними словами. В англомовних пошукових системах використовується оператор NEAR.

**Наприклад:*

- information NEAR resources – для англомовних систем (чим ближче розташовані ключові слова один до одного, тим вищою є релевантність документа. Якщо відстань між словами більше 50 слів, в такому разі релевантність вважається нульовою);
- [5, інформаційні ресурси] – для системи <META> (обидва ключові слова повинні належати одній групі довжиною не більше п’яти слів);
- информационные/ 3 ресурсы – для системи Yandex (відстань між ключовими словами не повинна перевищувати три слова).

Оператор title дозволяє здійснювати пошук за заголовком документа. Наприклад, за запитом title (дистанційна освіта) будуть знайдені документи, у заголовках яких міститься термін дистанційна освіта.

Оператор Heading дозволяє здійснювати пошук за назвами розділів документа. Так, за запитом Heading (інформаційна нерівність) будуть знайдені документи, які містять термін інформаційна нерівність у полі heading документа.

Булевий пошук – *Boolean search* – інформаційний пошук за запитом, побудованим з використанням операцій булевої алгебри (табл. 5.1): AND, OR і NOT. Використання булевих операцій істотно підвищує ефективність пошуку. Особливості конкретної мови запитів викладені у описах пошукових систем.

Таблиця 5.1. Логічні оператори

Оператор	Опис
AND	Логічне І дозволяє знайти документи, у яких присутні всі пошукові терміни, об’єднані цим оператором. Як було зазначено вище, в україно- та російськомовних пошукових системах списки

	слів і без такого оператора сприймаються так, ніби між ними стоїть оператор І. Але для більшості англомовних пошукових систем оператор І відіграє важливу роль, йому відповідають символи «&» та «+».
NOT	Логічне НЕ дозволяє виключити із результатів пошуку документи, які містять ключове слово, яке знаходиться після оператора. Необхідність у цьому виникає, коли треба уникнути двозначності або зменшити кількість посилань, що повертаються. Наприклад, у запиті освіта NOT вища із списку результатів будуть знайдені ті документи, у яких є слово освіта, але немає слова вища.
OR	Логічне АБО дозволяє знайти документи, які містять хоча б одне із слів запиту. Наприклад, у запиті університет АБО академія будуть знайдені документи, які містять або слово університет, або слово академія. У більшості пошукових систем оператор АБО записується у запиті як OR.

Логічні дужки. Порядок дії операторів можна задавати дужками (…). Наприклад, у запиті *(інформаційна система) OR технологія* будуть одержані документи, що містять фразу інформаційна система або слово технологія. Якщо необхідно знайти документи, у яких зустрічаються слова інформаційна система або інформаційна технологія, запит повинен бути таким: *інформаційна (система OR технологія*).

5.4. Параметри якості пошукових систем

У *релевантності* (адекватності) інформації не існує числового виразу. Тому пошукову систему оцінюють за кількома числовим характеристикам, близьким за змістом до релевантності.

Повнота – одна з основних характеристик пошукової системи, яка являє собою відношення кількості знайдених за запитом документів до загальної кількості документів в Інтернеті, які відповідають даному запиту.

Наприклад, якщо в мережі Інтернет є 100 сторінок, що містять словосполучення «Інформаційна технологія», а за відповідним запитом було знайдено всього 70 з них, то повнота пошуку буде 0,7. Чим повніше пошук, тим менше ймовірність, що користувач не зможе знайти потрібний йому документ, за умови, що він взагалі існує в Інтернеті. Повнота пошуку в великій мірі залежить від роботи системи збору та обробки інформації. У зв’язку з постійним зростанням кількості документів в мережі, ця система в першу чергу повинна бути масштабованою.

Масштабованість – це здатність системи розширюватися (збільшувати розмір бази даних, кількість оброблюваних даних і т. д.). Зазвичай масштабованість досягається за рахунок паралельного виконання завдання будь-якою кількістю комп'ютерів.

Точність – ще одна основна характеристика пошукової машини, яка визначається як ступінь відповідності знайдених документів запиту користувача.

Наприклад, якщо за запитом «Українська вишиванка» знаходить 150 документів, в 70 з них міститься словосполучення «Українська вишиванка», а в інших просто присутні ці слова («українська дівчина була вбрана в вишиванку»), то точність пошуку вважається рівною 70/150 (~0,5). Чим точніше пошук, тим швидше користувач знаходить потрібні йому документи, тим менше серед них зустрічається «сміття», тим рідше знайдені документи не відповідають запиту. Підвищення точності в пошукових машинах досягається за рахунок використання різних технологій на всіх етапах обробки і пошуку інформації. Величезну роль в підвищенні точності пошуку грає ранжування. Користувач дуже рідко переглядає більше трьох сторінок з результатами пошуку. Тому суб'єктивно він оцінює точність по «верхнім» документам. Навіть якщо потрібний документ знайдений пошуковою машиною, але розташований на двохсотій позиції, швидше за все, він ніколи не буде знайдений користувачем.

Актуальність – не менш важлива характеристика пошуку, яка визначається часом, який проходить з моменту публікації документів в мережі Інтернет до занесення їх в індексну базу.

З ростом обсягу інформації в мережі Інтернет зростає і індексна база пошукової машини. Поступово переіндексація та збирання бази починає займати все більше часу, а процес оновлення індексу стає більш громіздким. Надходження нових даних затягується, інформація починає втрачати свою актуальність.

Швидкість пошуку – кількість запитів в секунду яку може обробити пошукова система.

Швидкість пошуку тісно пов'язана зі стійкістю сервера до навантажень. Наприклад, на сьогоднішній день в робочі години до пошукової машини Google приходить близько 35 000 запитів в секунду. Така завантаженість вимагає скорочення часу обробки окремого запиту.

Крім кількісних показників оцінки пошукових машин є і якісні показники:

- наочність представлення результатів;
- цитата;

- можливість відновлення тексту.

Наочність представлення результатів є необхідним компонентом зручного пошуку. На поганий вітрині легко не помітити хороший товар. За більшістю запитів пошукова машина знаходить сотні, а то й тисячі документів. Внаслідок нечіткості запитів або неточності пошуку, навіть перші сторінки не завжди містять тільки потрібну інформацію. Це означає, що користувачеві часто доводиться проводити свій власний пошук усередині списку знайденого. Різні елементи відповідної сторінки допомагають орієнтуватися в результатах пошуку. Найбільш важливий такий елемент – *цитата*.

Цитата допомагає визначити, наскільки корисну інформацію містить знайдений документ. Дуже часто відвідувачеві не потрібно переходити по посиланню, щоб виявити, що текст не відповідає його інтересам і потребам. Іноді відповідь на питання користувача міститься безпосередньо в цитаті документа. Це економить час і підвищує ефективність роботи пошукової системи.

Відновлення тексту – іноді єдиний спосіб отримати доступ до вмісту знайденого документа. Ресурс може бути недоступним з різних причин. Документ може бути видалений, перенесений, змінений, але його текстовий зміст деякий час зберігається в індексній базі. Крім того, всередині самого документа часто відсутня навігація, що дозволяє швидко знайти фрагмент, релевантний запиту. У відновленому тексті всі слова запиту підсвічуються. Слід звернути увагу, що через цю функцію пошукової системи, можуть бути доступні закриті документи, що знаходяться в частині сайту з обмеженим доступом.

5.5. Порівняння пошукових систем

Дані взяті з сайту analyzethis, на якому можна знайти оцінки різних характеристик, таких як якість цитат і підказок, кількість пошукового спаму та інше.

Порівняння пошукових систем проводиться за двома основними видами пошуку:

- навігаційний пошук;
- тематичний пошук.

Навігаційний пошук. Навігаційним називається запит, за допомогою якого користувач шукає певний сайт. Такі, наприклад, запити як «ПриватБанк», «Українська правда», «Yahoo» і т. п. Кращим результатом у відповідь на навігаційний запит є шуканий сайт (маркер) на першій позиції пошукової видачі. Найбільш популярними пошуковими системами на сьогоднішній день є yandex та google.

Тематичний пошук. Людина краще машини може зрозуміти сенс пошукового запиту, припустити, яку інформацію хотів би отримати користувач, оцінити пропозицію інформації в Мережі і сформувати видачу у відповідь на запит. Тому видача, сформована експертом завжди краще алгоритмічної. Yandex, google володіють 20-30% ефективності експертів, інші пошукові системи – значно нижче.

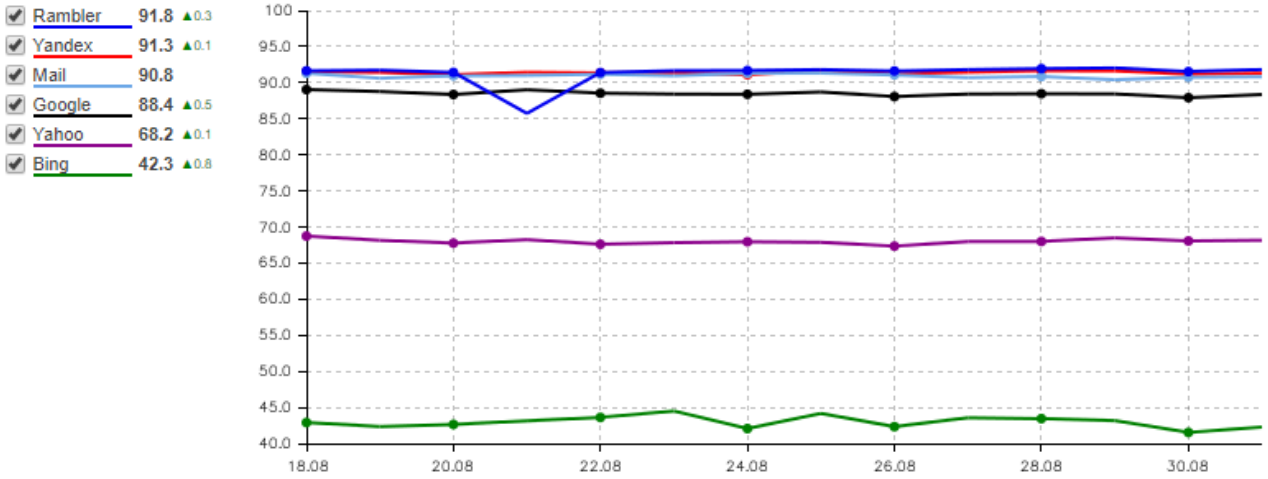


Рис. 5.1. Порівняльна діаграма інтегрального показника якості пошуку

Як можна бачити, пошукові системи, хоч і автоматизовані, але не дуже зручні інструменти пошуку інформації в Інтернет. У зв'язку з цим виник принципово інший підхід до організації інформації в мережі – ***Semantic Web.***

5.6. Технологія Semantic WEB

Семантична павутина *(англ. Semantic Web)* – частина глобальної концепції розвитку мережі Інтернет, метою якої є реалізація можливості машинної обробки інформації, доступної у Всесвітній павутині.

Основний акцент концепції робиться на роботі з метаданими, які однозначно характеризують властивості і зміст ресурсів Всесвітньої павутини, замість використовуваного в даний час текстового аналізу документів.

Термін вперше введений Тімом Бернерсом-Лі в травні 2001 року в журналі «Scientific American», і називається ним «наступним кроком в розвитку Всесвітньої павутини».

Метадані – це інформація про дані. Як приклад метаданих можна навести: структуру файлів, протокол передачі даних, структуру бази даних.

5.7. Електронні бібліотеки та каталоги

Каталог ресурсів в Інтернеті *(інтернет-каталог, англ. Web directory)* – структурований набір посилань на сайти з коротким їх описом. Сайти всередині

каталогу розбиваються за темами, а всередині тем можуть бути ранжовані або за індексом цитування (як в каталогах Yandex або Google), або за датою додавання, чи в алфавітному порядку, або по іншому критерію. Це один з найстаріших сервісів Інтернету. Переважна більшість рейтингів відвідуваності ресурсів мають класифікатор сайтів, але ранжування завжди засноване на відвідуваності сайтів. Залежно від широти тематики посилань каталоги можуть бути загальними і спеціалізованими (тематичними).

Білі каталоги – каталоги, які не потребують зворотнього посилання, і ставлять пряме посилання на ваш сайт.

Сірі каталоги – каталоги, що вимагають зворотне посилання, і ставлять пряме посилання на вас. Якщо ви зібралися ставити у себе зворотні посилання, то корисні тільки тематичні каталоги, інші будуть лише шкодити.

Чорні каталоги – каталоги, що вимагають зворотне посилання, і ставлять посилання на вас через редирект. Корисні тільки якщо у такого каталогу дуже хороша відвідуваність, і ваш сайт знаходиться вгорі каталогу.

Електронна бібліотека – впорядкована колекція різнорідних електронних документів, забезпечених засобами навігації та пошуку. Може бути веб-сайтом, де поступово накопичуються різні тексти (частіше літературні, але також і будь-які інші, аж до комп'ютерних програм) і медіа-файли, кожен з яких самодостатній і в будь-який момент може бути затребуваний читачем. Електронні бібліотеки можуть бути універсальними, які спрямовані до найбільш широкого вибору матеріалу, і більш спеціалізованими. Особливе місце в ряду електронних бібліотек займають інтернет-бібліотеки науково-освітньої тематики, в яких зібрані видання, необхідні для здійснення освітнього процесу.

5.8. Анонімні пошукові системи

В даному розділі будуть коротко розглянуті пошукові системи, які пропонують користувачеві більше анонімності та конфіденційності, ніж популярні і всім відомі інформаційно-пошукові системи.

В таких пошукових системах як Yandex та Google всі ваші запити аналізуються, зберігаються і обробляються, анонімні пошуковики, навпаки ж, не зберігають вашу активність. Однак перед тим як перейти безпосередньо до знайомства з конкретними анонімними пошуковими системами давайте розберемося з їхніми ключовими моментами.

1) Безпека пошукових систем

Безпечний пошук в інтернеті починається з зашифрованої передачі запиту, між користувачем і сервером. В такому разі пошуковик який позиціонує себе з

анонімним і безпечним пошуком в Інтернеті повинен в першу чергу примусовим чином автоматично встановлювати захищене SSL-з'єднання. Для перевірки шифрування можна використовувати такий інструмент як SSL Server Test.

Ще одним важливим критерієм є довжина ключа шифрування і чим він довше тим краще.

Також слід звернути увагу на *PFS (Perfect forward secrecy)* перекладається як досконала пряма секретність. Простими словами PFS – це захист від запису зашифрованої сесії спецслужбами і хакерами. Цей параметр навіть важливіше довжини ключа шифрування.

2) Анонімність пошукової системи

Окрім того, що анонімні пошуковики не зберігають вашу активність,також необхідно відзначити, що постійні cookie-файли в анонімних пошукових системах зберігаються лише в тому випадку, якщо змінюються стандартні настройки – наприклад, якщо встановлюється мова інтерфейсу DuckDuckGo або тема інтерфейсу Ixquick. Жодна з альтернативних анонімних пошукових систем не використовує в файлах Cookies ідентифікатор користувача. В той час як Google робить це при кожному запиті. Він для обробки IP-адреси динамічно використовує численні постійні Cookies з ID для точної ідентифікації користувача.

5.8.1. Анонімна пошукова система DuckDuckGo

DuckDuckGo був заснований Гебріелом Вайнбергом в 2006 році. Найбільшою перевагою даної пошукової системи, поряд з високим рівнем анонімності і безпеки, є релевантність пошукової видачі. Знаходить він інформацію добре, не ідеально як Yandex або Google, але добре. Крім цього із значущих плюсів необхідно відзначити швидкість роботи.

Також як і Google, пошукова система DuckDuckGo живе за рахунок реклами, але на відміну від першого працює за іншим принципом. Під час формування та показу рекламних блоків він враховує не історію пошукових запитів, а тільки використовувані користувачем ключові слова.

Крім свого основного пошукового індексу DuckDuckGo черпає інформацію у своїх великих братів: Yahoo, Google і Bing, і так до речі робить не лише він.

Пошукова система в роботі між клієнтом і сервером за замовчуванням використовує протокол HTTPS з алгоритмом шифрування AES і ключем довжиною 128 біт.

Ще одним цікавим фактом є те що розробники Tor вбудували його в браузер Firefox як пошукову систему за замовчуванням.

Основні можливості DuckDuckGo:

- стандарт шифрування SSL/PFS;
- сервери знаходяться в Америці;
- є версія для Android та iOS;
- не зберігає історію пошуку таку як: IP-адреса і конфіденційні дані;
- не передає конфіденційні дані третім особам;
- не зберігає ідентифікатор користувача в Cookies;
- не відстежує Cookies сторонніх осіб;
- є система розпізнавання друкарських помилок;
- можливість відключення показу реклами;
- локалізація інтерфейсу сайту.

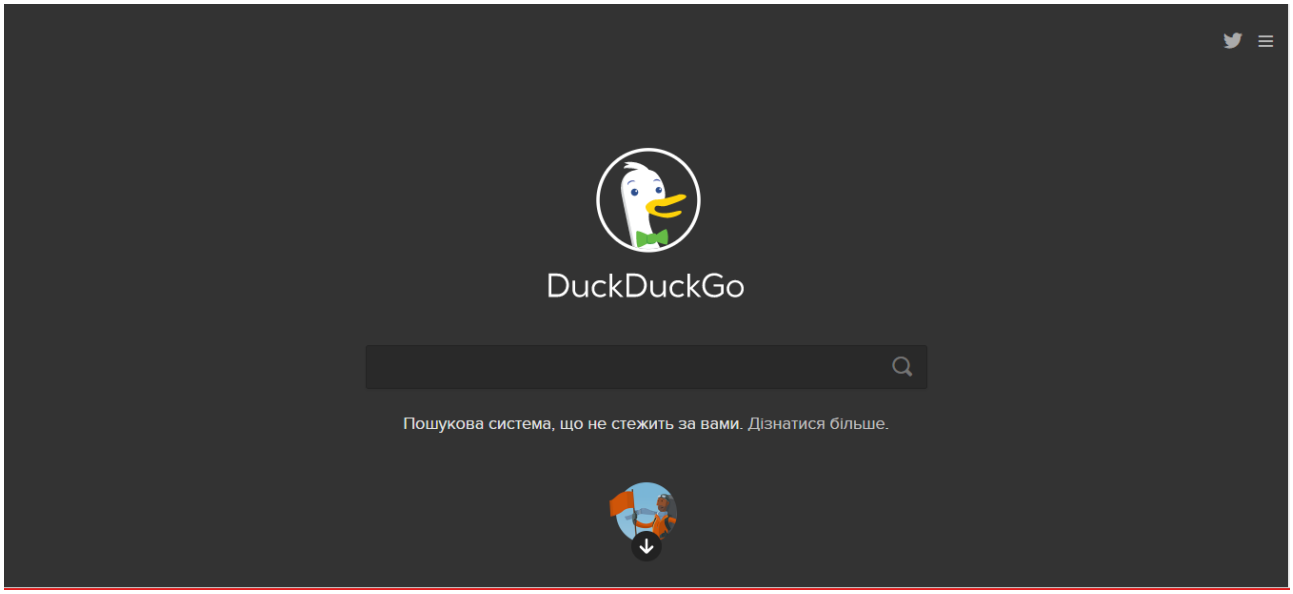


Рис. 5.2. Головна сторінка анонімної інформаційно-пошукової системи DuckDuckGo

5.8.2. Анонімна пошукова система Ixquick

Пошуковик Ixquick був заснований Девідом Боднікіном в 1998 році. З 2000 року належить голландській компанії Surfboard Holding BV.

Ixquick.com є першою пошуковою системою, яка видалила конфіденційні дані своїх користувачів. IP-адреси та інша персональна інформація користувачів видаляються через 48 годин після здійснення пошуку.

Також у даної пошукової системи є досить цікава фішка «Проксі режим». Працює дана функція наступним чином: поруч з кожним сайтом в пошуковій видачі є кнопка «Proxy», натиснувши на яку ви отримаєте інформацію з сайту анонімно – робот Startpage зайде на шукану сторінку, після чого завантажить її і відобразить вам.

Основні можливості Ixquick:

- стандарт шифрування SSL/PFS;

- сервери знаходяться в Нідерландах;
- є версії для Android та iOS;
- не зберігає історію пошуку/ IP-адресу/ конфіденційні дані;
- не передає конфіденційні дані третім особам;
- не зберігає ідентифікатор користувача в Cookies;
- не відстежує Cookies сторонніх осіб.

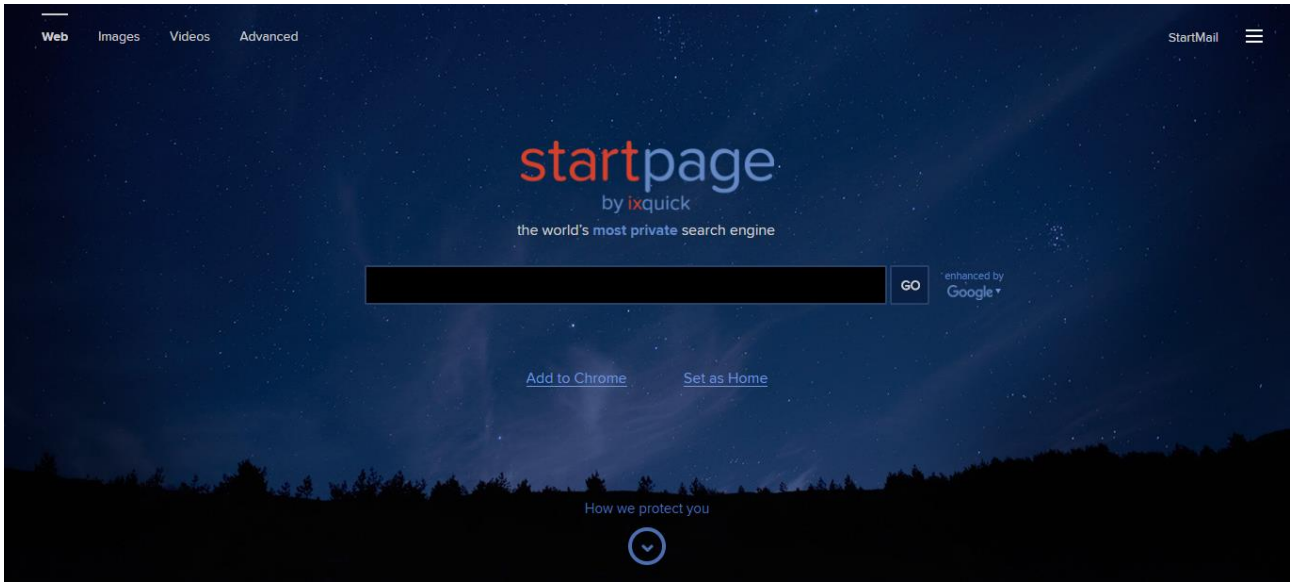


Рис. 5.3. Головна сторінка анонімної інформаційно-пошукової системи Ixquick

В яких же випадках виправдане використання таких анонімних пошукових систем?

У випадку, коли ви шукайте те, про що не хотіли б щоб знала всесвітня мережа!

У всіх інших краще використовувати звичайні пошукові машини, такі як Yandex і Google. На сьогоднішній день якість пошукової видачі цих пошукових гігантів набагато краще будь-якої анонімної пошукової системи.

Низька анонімність – це плата за використання провідних технологій пошукового ранжування, які намагаються всіма силами запобігти потраплянню шахрайських або неякісних сайтів в топ. У цьому світі за все треба платити, іноді грошима, а іноді і інформацією.

5.9. The Dark Side of Search[2]

Дивлячись на сьогодення, можна сказати що ми живемо в Інтернеті речей, вже зараз у повсякденному житті ми постійно стикаємося з підключеними речами, починаючи з домашніх Wi-Fi-роутерів і закінчуючи

[2] Розгляд даних пошукових систем здійснюється лише в навчальних цілях. Автор не несе відповідальності за особисті дії читачів!

вуличними камерами спостереження і системами управління світлофорами. І оскільки всі ці пристрої підключені до мережі, їх можна знайти відразу в двох світах – у реальному і в Інтернеті.

Інтернет часто ототожнюють з вебом, але, як вже зазначалось на першій практичній роботі, WWW – це всього лише вершина айсберга. Його глибинна частина куди різноманітніше, і хоч вона прихована від очей пересічних користувачів, ніщо не заважає вивчати її спеціалізованими засобами. І точно так само, як Google чи Yandex допомагає нам шукати інформацію в Інтернеті, інші пошукові системи дозволяють знайти ці підключені пристрої. А саме такі пошукові системи як, ***Shodan*** і ***Censys***.

5.9.1. Спеціалізована пошукова система Shodan

Shodan – це перша (і, мабуть, провідна) пошукова система яка дозволяє заглянути в прихований від очей світ Інтернету речей, тобто система яка дозволяє користувачам шукати пристрої підключені до мережі Інтернет. З його допомогою можна побачити маловивчену сторону глобальної мережі, зрозуміти її структуру, виявити вразливі місця і провести безліч інших практичних досліджень.

Тіньовий аналог Гугла допомагає оцінювати рівень поширення тих чи інших пристроїв, операційних систем і веб-інструментів, а також з'ясовувати поточний рівень проникнення інтернету в будь-які регіони – від кварталу до континенту. Можливості пошукової системи Shodan постійно розширюються, і деякі з них стають сюрпризом навіть для його творця.

Дана пошукова система була розроблена ще в 2009 році Джоном Матерлі і названа на честь головного лиходія (точніше, лиходійки) в серії комп'ютерних ігор System Shock – в грі це був вкрай злісний штучний інтелект. Звичайно, ця пошукова система не настільки безжальна, як її прототип, але і вона здатна заподіяти чимало шкоди. Саме тому багато людей описали Shodan як пошукову систему для хакерів, і навіть назвали її «найнебезпечнішою пошуковою системою в світі». Втім, перш, ніж перейти до розгляду всіляких страшних можливостей Shodan, давайте розберемося, як взагалі працює така пошукова система.

В основі Shodan лежить пошуковий робот (***crawler***), подібний «павукам» Google і Yandex. Він накопичує технічні відомості про всі вузли мережі обходячись без записів DNS і безпосередньо опитуючи мережні вузли, а саме порти пристроїв. Після чого пошукова система індексує інформацію на основі отриманих у відповідь банерів, тобто метаданих, які сервери відсилають назад хостинговим клієнтам та робить висновки про пристрої і сервіси.

Оскільки персональні комп'ютери та мобільні гаджети кінцевих користувачів зазвичай маскує *firewall*, тому набагато частіше в поле зору Shodan потрапляють всілякі мережеві пристрої, що формують так званий Інтернет речей. Таким чином, ще зовсім недавно його основну частку становили маршрутизатори, мережеві принтери і IP-камери, але тепер навіть деякі лампочки мають власну IP-адресу. До інтернету не замислюючись підключають практично всі – від розумної побутової техніки до різних датчиків і автоматизованих систем управління технологічними процесами. Багато з них розраховані на віддалене управління і мають великі проблеми з обмеженням доступу. До них можна підключитися по SSH, SNMP або навіть HTTP, причому кому завгодно. Паролі за умовчанням, стандартні логіни і пін-коди – це лише мала і очікувана частина проявів людського фактору. Набагато цікавіше, що практично всі ці пристрої відкрито передають свій мережевий ідентифікатор і відкликаються на запити настільки специфічно, що їх без зусиль можна виявити серед маси інших – особливо використовуючи інструменти розширеного пошуку в Shodan.

Потужні фільтри дозволяють відібрати результати по країні, місту або вручну заданому діапазону координат GPS. Тому сам Метерлі називає свій проект безневинним словом «*інтернет-картограф*». Це нагадує Інтернет-карту, яка дозволяє нам бачити, який пристрій підключено до якого порту або які порти відкрито на певному пристрої, чи яка операційна система там запущена, тощо.

Пошукова система є платною, річна підписка обійдеться в 20$, проте, спробувати його в дії можна і за так: після безкоштовної реєстрації доступні 50 результатів пошуку.

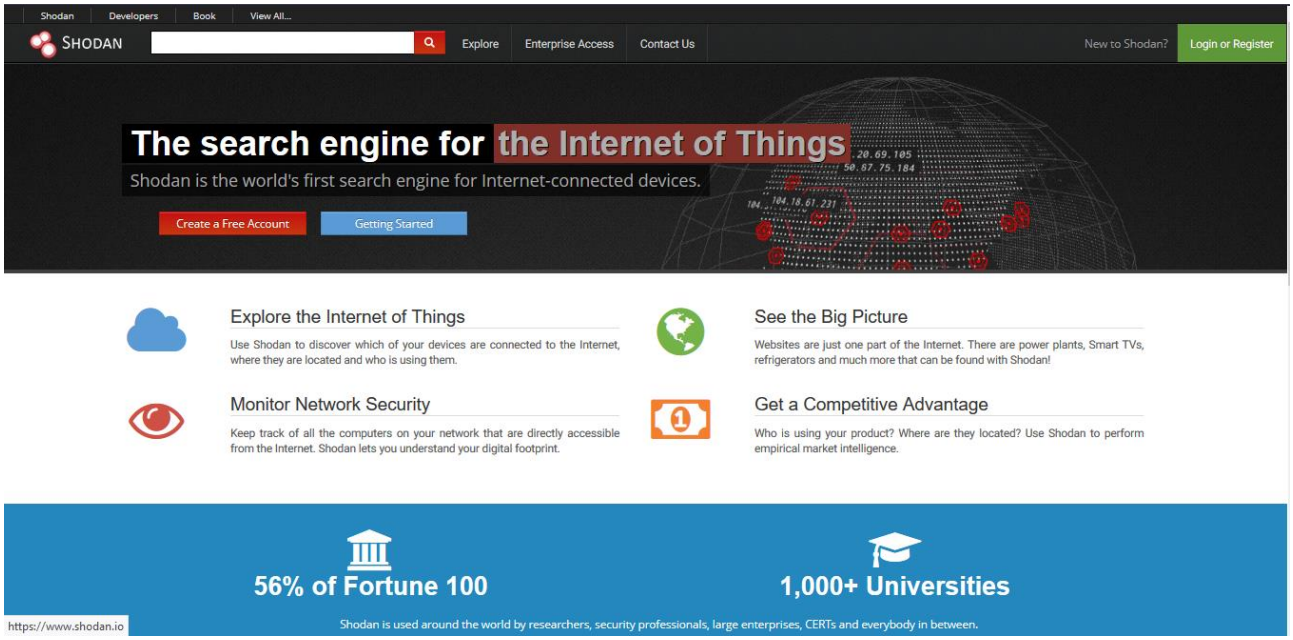


Рис. 5.4. Головна сторінка спеціалізованої інформаційно-пошукової системи Shodan

5.9.2. Спеціалізована пошукова система Censys

Довгий час Shodan був єдиним пошуковим движком по Інтернету речей. У 2013 році виник Censys – його безкоштовний конкурент. Нова система працює, спираючись на ті ж принципи, що і Shodan, однак її творці додатково зробили акцент на пошук вразливостей. Censys дійсно може видати вам список пристроїв, не захищених від якоїсь конкретної відомої загрози з числа найбільш поширених, наприклад від Heartbleed.

Пошукова система Censys була розроблена в Мічиганському університеті Закіром Дурумеріком (Zakir Durumeric) спершу як мережева утиліта, яку він зробив з ZMap для збору статистики поширеності відомих вразливостей в Мережі. Як відкритий проект Censys став доступний лише в жовтні 2015 роки після презентації на 22-й конференції з безпеки комп'ютерів і комунікацій (ACM CCS).

Відгуки мережевих вузлів на запити Censys допомагають ідентифікувати пристрої і багато чого довідатися про них. Серед цінної інформації: виробник, модель, тип, версія прошивки, відкриті порти, активні сервіси і деталі про програмне забезпечення. Наприклад, чи використовує воно шифрування і як саме налаштоване. Через Geo IP також можна дізнатися приблизно географічне розташування. Вся інформація оновлюється щодня в ході сканування загальнодоступного адресного простору IPv4 і першого мільйона доменів в рейтингу відвідуваності (його щодня поставляє Alexa Internet – дочірня компанія Amazon).

Порядок виконання лабораторної роботи №5:

1. Включити ПК.
2. Ознайомитися з короткими теоретичними відомостями.
3. Ознайомитися з заданою темою для пошуку, яка вказана в таблиці 5.3.
4. Визначити ключові слова, які найкраще відображають напрямок пошуку інформації, чи найповніше характеризують документ, який ви шукаєте.
5. Обрати декілька пошукових серверів (не менше трьох) та дослідити їх пошукові можливості.
6. Ознайомитися з їхньою системою команд та правилами складання запитів. Ця інформація є в системі допомоги (help), вказівник на яку, як правило, присутній на головній (титульній) сторінці цього серверу.
7. Зробити першу серію запитів українською, російською і англійською мовами до обраних вами серверів змінюючи кількість та послідовність ключових слів у запиті.

Приклади запитів: інформаційне суспільство, информационное общество, information society.

8. Переглядаючи список назв та зміст знайдених документів уточнити перелік ключових слів, які найбільш повно відповідають заданому вам напрямку пошуку та зробити другу сесію пошуку. Занести дані у таблицю (табл. 5.2). Порівняти одержані результати.

9. Знайти інформацію та різноманітні матеріали[3] (книги, статті, рисунки, графіки та інше) відповідно до зазначеної теми для пошуку.

10. Знайдену інформацію оформити у вигляді доповіді з прямими посиланнями на джерела, а всі знайдені матеріали додати в створений архів.

Таблиця 5.2. Результати пошукових запитів.

Пошукова система:	**?**	**?**	**?**
І серія пошукових запитів:	*Приблизна кількість результатів:*		
(укр. мовою)			
(укр. мовою)			
(укр. мовою)			
(рос. мовою)			
(рос. мовою)			
(рос. мовою)			
(англ. мовою)			
(англ. мовою)			
(англ. мовою)			
ІІ серія пошукових запитів:	*Приблизна кількість результатів:*		
(укр. мовою)			
(укр. мовою)			
(укр. мовою)			
(рос. мовою)			
(рос. мовою)			
(рос. мовою)			
(англ. мовою)			
(англ. мовою)			
(англ. мовою)			

11. Оформити звіт згідно до вимог (додаток 1).

12. Зробити висновки та підготуватися до усного опитування.

Зміст звіту:

[3] всі знайдені матеріали за темою пошуку повинні бути додані в архів і здані викладачу разом із звітом.

1. Титульний лист.
2. Постановка завдання.
3. Протокол виконання практичної роботи, що містить таблицю результатів пошукових запитів, порівняння отриманих результатів та повноцінну доповідь (15 сторінок) з прямими посиланнями на джерела.
4. Висновки.

Завдання на виконання лабораторної роботи №5

Таблиця № 5.3. (варіант відповідно до номера за списком у журналі)

Номер варіанта	Завдання
1	Інформаційна безпека в системі національної безпеки України.
2	Законодавчі методи забезпечення інформаційної безпеки.
3	Національні інтереси та загрози інформаційній безпеці України в інформаційній сфері.
4	Відомі сценарії комп'ютерних атак та їхня реалізація.
5	Комплексний підхід до побудови системи захисту інформації
6	Нормативно-правова база для організації і проведення заходів щодо захисту інформації в системах телекомунікацій.
7	Загрози, ризики та правопорушення у сфері інформаційної безпеки.
8	Методи захисту електронних платежів в мережі інтернет.
9	Загальна характеристика формальних моделей безпеки
10	Особливості захисту інформації у сучасних умовах.
11	Криптографічні та стенографічні методи забезпечення захисту інформації
12	Види захисту інформації від витоку технічними каналами.
13	Основні методи забезпечення захисту зовнішнього периметру.
14	Основні вектори атак на ІТС компанії.
15	Загальна характеристика і принципи функціонування DLP -системи
16	Основні теоретичні методи забезпечення інформаційної безпеки.
17	Загальна характеристика і принципи функціонування SIEM -системи
18	Шкідливе програмне забезпечення та засоби захисту від нього.
19	Методи та алгоритми оцінки рівня захищеності інформації.
20	Методи інженерно-технічного захисту інформації.
21	Критерії безпеки комп'ютерних систем «Помаранчева книга».
22	Поняття про модель загроз та модель порушника.
23	Інформаційна безпека в сучасному світі.
24	Стандарти в області оцінки захищеності інформаційних систем.
25	Кібератаки на корпоративні інформаційні системи з використанням різноманітних уразливостей.
26	Правові та інші засоби формування політики інформаційної безпеки

	України.
27	Способи реалізації комп’ютерних атак і загальноприйняті сценарії протидії.

Контрольні питання:

1. Охарактеризуйте призначення та основні можливості інформаційно-пошукових систем.
2. Опишіть внутрішню структуру пошукової системи та принцип її роботи.
3. Назвіть та охарактеризуйте команди мови запитів.
4. Охарактеризуйте поняття, які використовуються при оцінюванні ефективності та якості інформаційного пошуку.
5. Поясніть що таке навігаційний та тематичний пошук і в чому їх відмінність?
6. Поясніть що таке технологія Semantic Web?
7. Охарактеризуйте призначення та основні можливості електронних бібліотек та каталогів.

Лабораторна робота №6
«Основи віртуалізації в комп’ютерних системах»

Мета роботи:

1. Поглиблення та закріплення теоретичних знань з наступних питань:
   - поняття віртуалізації та основні технології віртуалізації;
   - гіпервізори та їх архітектура.
2. Ознайомлення з програмними продуктами віртуалізації та набуття практичних навичок роботи з ними: створення віртуальних машин і встановлення на них різних операційних систем (ОС) з подальшим налаштуванням мережі.

Стислі теоретичні відомості.

6.1. Поняття віртуалізації та основні технології віртуалізації

Сучасні комп’ютерні системи (КС) пройшли довгий шлях у тому, як вони оброблюють, зберігають та отримують доступ до інформації. Одним з таких досягнень є віртуалізація, яка протягом кількох останніх років набуває все більшої популярності. Те, що колись було новинкою і використовувалося в основному для тестових систем, на сьогоднішній день поширено використовується як на великих, так і на малих підприємствах для різних цілей. Але що ж таке віртуалізація і як насправді працює більшість систем віртуалізації?

Віртуалізація означає зрушення в мисленні від фізичного підходу до логічного (рис. 6.1), розглядаючи IT-ресурси як логічні, а не окремі фізичні ресурси. Це новий віртуальний погляд на ресурси складових частин, які не обмежені реалізацією, фізичною конфігурацією або географічним положенням.

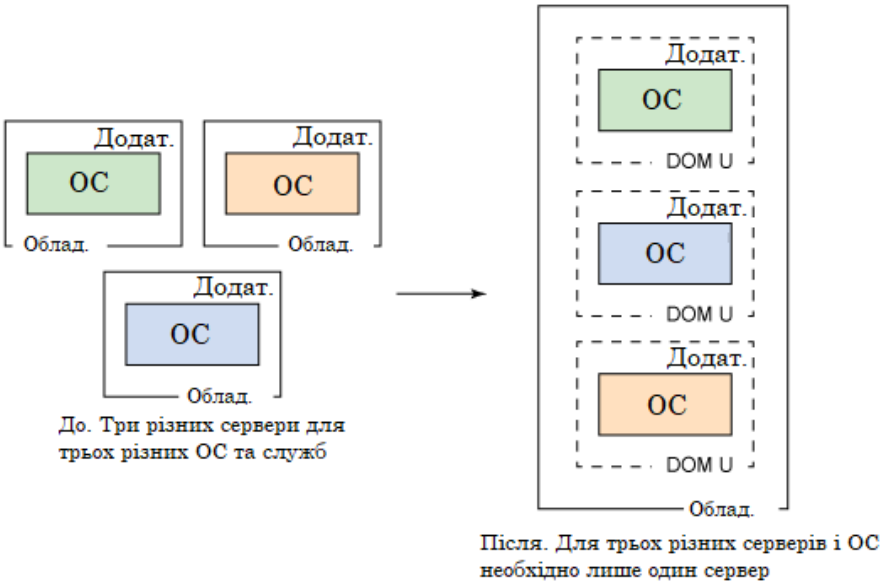


Рис. 6.1. Віртуалізація, перехід від фізичного підходу до логічного

У широкому сенсі, поняття віртуалізації являє собою приховування справжньої реалізації будь-якого процесу або об’єкта від істинного його уявлення для того, хто ним користується. У комп’ютерних технологіях під терміном *«віртуалізація»* зазвичай розуміється абстракція обчислювальних ресурсів і надання користувачеві системи, яка *«інкапсулює»* (приховує в собі) власну реалізацію. Простіше кажучи, користувач працює з зручним для себе поданням об’єкта, і для нього не має значення, як об’єкт влаштований в дійсності.

Таким чином, ***віртуалізація*** – це створення гнучкої заміни реальних ресурсів з ізоляцією обчислювальних процесів і ресурсів один від одного, залишаючи ті ж функції і зовнішні інтерфейси, що і у фізичних прототипів, але з різними атрибутами, такими як розмір, продуктивність і вартість. Така заміна називається *віртуальними ресурсами*, і користувачі, як правило, не знають про цю заміну.

З однієї сторони віртуалізація застосовується до фізичних апаратних ресурсів шляхом об’єднання кількох фізичних ресурсів в загальні пули (групи), з яких користувачі отримують віртуальні ресурси, а з іншої, за допомогою віртуалізації навпаки можна зробити декілька віртуальних ресурсів з одного фізичного. Більш того, віртуальні ресурси, за допомогою яких будуються віртуальні системи, можуть мати функції або особливості, які відсутні у вихідних фізичних ресурсів. Відповідно ***віртуальні системи*** – це незалежно функціонуючі середовища, які використовують віртуальні ресурси.

І саме тому, на основі вищесказаного, поняття віртуалізації умовно можна розділити на *дві фундаментально різні категорії*: віртуалізація ресурсів і віртуалізація платформ.

1. Віртуалізація ресурсів

Даний вид віртуалізації ставить за мету комбінування або спрощення подання апаратних ресурсів для користувача і отримання деяких користувальницьких абстракцій обладнання, просторів імен, мереж і т. п.

До даного виду віртуалізації відноситься:

1) об'єднання, агрегація і концентрація компонентів. Під таким видом віртуалізації ресурсів розуміється організація декількох фізичних або логічних об'єктів в пули ресурсів, що представляють зручні інтерфейси користувачеві. *Приклади* такого виду віртуалізації:

- багатопроцесорні системи, які представляються нам як одна потужна система;
- RAID-масиви та засоби управління томами, що комбінують декілька фізичних дисків в один логічний;
- віртуалізація систем зберігання, використовувана при побудові мереж зберігання даних SAN (Storage Area Network);
- віртуальні приватні мережі (VPN) і трансляція мережевих адрес (NAT), що дозволяють створювати віртуальні простори мережевих адрес та імен.

2) кластеризація комп'ютерів та розподілені обчислення (grid computing). Цей вид віртуалізації включає в себе техніки, застосовувані при об'єднанні безлічі окремих комп'ютерів у глобальні системи (метакомпьютери), які спільно вирішують загальну задачу.

3) поділ ресурсів (partitioning). Під час поділу ресурсів у процесі віртуалізації відбувається поділ якого-небудь одного великого ресурсу на кілька однотипних об'єктів, зручних для використання. У мережах зберігання даних це називається зонуванням ресурсів (***«zoning»***).

4) інкапсуляція – процес створення системи, що надає користувачеві зручний інтерфейс для роботи з нею і приховує подробиці складності своєї реалізації. *Наприклад*, використання центральним процесором кеша для прискорення обчислень ніяк не відображається на його зовнішніх інтерфейсах.

Віртуалізація ресурсів, на відміну від віртуалізації платформ, має більш широкий і розпливчастий сенс і являє собою масу різних підходів, спрямованих на підвищення зручності взаємодії користувачів з системами в цілому. Тому, далі ми будемо спиратися в основному на поняття віртуалізації платформ, оскільки технології, пов'язані саме з цим поняттям, в даний момент динамічно розвиваються і є найбільш ефективними.

2. Віртуалізація платформ

Під віртуалізацією платформ розуміють створення програмних систем на основі існуючих апаратно-програмних комплексів, залежних або незалежних від них. Система, що надає апаратні ресурси і програмне забезпечення, називається ***хостовою (host)***, а системи які її симулюють – ***гостьовими (guest) або цільовими (target)***. Щоб гостьові системи могли стабільно функціонувати на платформі хостової системи, необхідно, щоб програмне і апаратне забезпечення хоста було досить надійним і надавало необхідний набір інтерфейсів для доступу до його ресурсів.

Продуктом цього виду віртуалізації є віртуальні машини.

Віртуальна машина (virtual machine) – модель обчислювальної машини, створеної шляхом віртуалізації обчислювальних ресурсів: процесора, оперативної пам'яті, пристроїв зберігання та вводу/виводу інформації. Віртуальна машина, на відміну від програми емуляції конкретного пристрою, забезпечує повну емуляцію фізичної машини чи середовища виконання (для програми).

Також необхідно відзначити, що технології віртуалізації платформ в даний час активно розвиваються та прогресують, і мають безліч різних видів реалізації, які залежать від того, наскільки повно здійснюється симуляція апаратного забезпечення:

1) повна емуляція (симуляція) – вид віртуалізації при якому віртуальна машина повністю віртуалізує все апаратне забезпечення при збереженні гостьової операційної системи в незмінному вигляді. Такий підхід дозволяє емулювати різні апаратні архітектури. Наприклад, можна запускати віртуальні машини з гостьовими системами для x86-процесорів на платформах з іншою архітектурою. Довгий час такий вид віртуалізації використовувався, щоб розробляти програмне забезпечення для нових процесорів ще до того, як вони були фізично доступними. Такі емулятори також застосовують для низькорівневого налагодження операційних систем. Основний мінус даного підходу полягає в тому, що емульоване апаратне забезпечення достатньо сильно уповільнює швидкодію гостьової системи, що робить роботу з нею дуже незручною, тому, крім як для розробки системного програмного забезпечення, а також освітніх цілей, такий підхід мало де використовується.

Приклади продуктів для створення емуляторів: Bochs, PearPC, QEMU (без прискорення), Hercules Emulator.

2) часткова емуляція (нативна віртуалізація) – це технологія, що надає обчислювальні ресурси, абстраговані від апаратного рівня. У цьому випадку віртуальна машина віртуалізує лише необхідну кількість апаратного забезпечення, для того щоб вона могла бути запущена ізольовано. Якщо брати, наприклад, сегмент серверів, таке абстрагування дозволяє працювати декільком віртуальним системам на одній апаратній платформі, а також дає можливість

легко переносити віртуальні системи з одного апаратного сервера на інший – наприклад, при його виході з ладу або модернізації. Цей вид віртуалізації достатньо широко використовується в даний час і на відміну від повної емуляції дозволяє істотно збільшити швидкодію гостьових систем за рахунок використання спеціального «прошарку» (*«гіпервізору»*) між гостьовою операційною системою і устаткуванням, що дозволяє гостьовій системі безпосередньо звертатися до ресурсів апаратного забезпечення.

Гіпервізор *або* ***монітор віртуальної машини (Virtual Machine Monitor)*** – це комп'ютерне програмне забезпечення, компоненти прошивки або апаратні засоби, які можуть віртуалізувати системні ресурси, тобто створювати та запускати віртуальні машини.

Приклади продуктів для нативної віртуалізації: VMware Workstation, Virtual PC, VirtualBox та інші.

3) паравіртуалізація. На відміну від повної віртуалізації, гіпервізор паравіртуалізації не приховує себе від гостьових операційних систем. Але в цьому випадку вони повинні бути підготовлені до роботи з цією системою. В результаті, застосування паравіртуалізації вимагає модифікації коду гостьової ОС на рівні ядра, що дозволяє їй спілкуватися з гіпервізором на більш високому рівні, забезпечуючи більш високу швидкодію.

Гіпервізор надає гостьовій ОС спеціальний програмний інтерфейс (API), що виключає необхідність прямого звернення до таких ресурсів, як, наприклад, таблиці сторінок пам'яті. При застосуванні паравіртуалізації немає необхідності емулювати апаратне забезпечення, більш того, гостьова ОС і гіпервізор використовують загальний набір драйверів, що вигідно відрізняє цю технологію від емуляції пристроїв, коли гостьова ОС і гіпервізор використовують різні драйвери.

До недавнього часу основним недоліком паравіртуалізації була необхідність модифікації коду ОС, однак, з появою апаратної підтримки віртуалізації, такої як Intel VT і AMD-V, стало можливим виконання будь-яких ОС без модифікації ядра. А зняття обмежень по типу виконуваних ОС в поєднанні з високою продуктивністю і низькими накладними витратами дозволяє говорити про гарні перспективи цього методу віртуалізації.

Приклади платформ паравіртуалізації: XenSource, Virtual Iron, Microsoft Hyper-V, VMware vSphere.

4) віртуалізація рівня операційної системи. Суттю даного виду віртуалізації є віртуалізація фізичного сервера на рівні операційної системи з метою створення декількох захищених віртуалізованних серверів на одному фізичному. Гостьова система, в даному випадку, розділяє використання одного ядра хостової операційної системи з іншими гостьовими системами. В

результаті чого віртуальна машина являє собою оточення для додатків, що запускаються ізольовано. Даний тип віртуалізації застосовується при організації систем хостингу, коли в рамках одного екземпляру ядра потрібно підтримувати декілька віртуальних серверів клієнтів.

Приклади віртуалізації рівня ОС: Linux-VServer, Virtuozzo, OpenVZ, Solaris Containers і FreeBSD Jails.

5) віртуалізація рівня додатків. Цей вид віртуалізації не схожий на всі інші: якщо в попередніх випадках створюються віртуальні середовища або віртуальні машини, що використовуються для ізоляції додатків, то в даному випадку сам додаток поміщається в контейнер з необхідними елементами для своєї роботи: файлами реєстру, файлами налаштувань, користувацькими і системними об'єктами. У результаті виходить додаток, що не вимагає установки на аналогічній платформі. При переміщенні такого додатку на іншу машину та його запуску, віртуальне оточення, створене для програми, вирішує конфлікти між нею і операційною системою, а також іншими додатками. Такий спосіб віртуалізації схожий на поведінку інтерпретаторів різних мов програмування (недарма інтерпретатор, Віртуальна Машина Java (JVM), теж потрапляє в цю категорію).

Прикладом такого підходу служать: Thinstall, Altiris, Trigence, Softricity.

Таким чином, перспективність віртуалізації платформ визначається рядом її переваг, до числа яких входять такі її можливості, як: створення необхідних апаратних конфігурацій з необхідними параметрами; створення представлень пристроїв, неіснуючих в обчислювальній системі; проведення безпечних експериментів зі старими і новими операційними системами на одному фізичному комп'ютері в цілях перевірки на сумісність; безпечна робота з ізольованими сумнівними і підозрілими додатками і компонентами; створення віртуальної мережі з декількох систем на одному фізичному сервері; проведення безпечних експериментів і навчання в IT-сфері та сфері кібернетичної безпеки; забезпечення високої мобільності незалежно від платформ додатків, робочих столів і т. д.; економія апаратного забезпечення при віртуалізації серверів; краща керованість віртуальних машин в порівнянні з реальними.

Однак, незважаючи на переваги існують і недоліки технологій віртуалізації до яких (загальноприйнятих) відносяться: неможливість створення представлень пристроїв, які не враховані вендорами в системах віртуалізації; високі вимоги до апаратного забезпечення; висока вартість корпоративних платформ віртуалізації; більш низька швидкодія віртуальних машин в порівнянні з реальними; поява нових маловивчених і малодосліджених ризиків і загроз безпеці інформації.

6.2. Загальні відомості про гіпервізор

Як вже зазначалося раніше, віртуалізація системи найчастіше здійснюється за допомогою технології гіпервізора. Тому в даному підпункті розглянемо більш детально типи гіпервізорів та їх архітектуру.

Гіпервізор – це платформа віртуалізації, що дозволяє запускати на одному фізичному комп'ютері кілька операційних систем. Саме гіпервізор надає ізольоване оточення для кожної віртуальної машини, і саме він надає гостьовим ОС доступ до апаратного забезпечення комп'ютера.

По суті, гіпервізор створює контейнер для кожної гостьової операційної системи та визначає параметри для віртуального обладнання, пов'язаного з цим контейнером. Наприклад, контейнер, як правило, містить віртуальний жорсткий диск певного розміру, оперативну пам'ять, процесор (-и) та одну або декілька мережевих карт. Він також може включати в себе віртуальні дисководи, які вказують на фізичний диск або образ диска та навіть USB-пристрої. І вже після визначення контейнера на нього може бути встановлена гостьова операційна система. Рис 6.2. демонструє загальну архітектуру макета для більшості варіантів віртуалізації, однак ми повинні знати, що гіпервізор можна розділити на два типи за способом запуску (на «голому залізі» або всередині ОС) і на два типи за їхньою архітектурою (монолітна і мікроядерна).

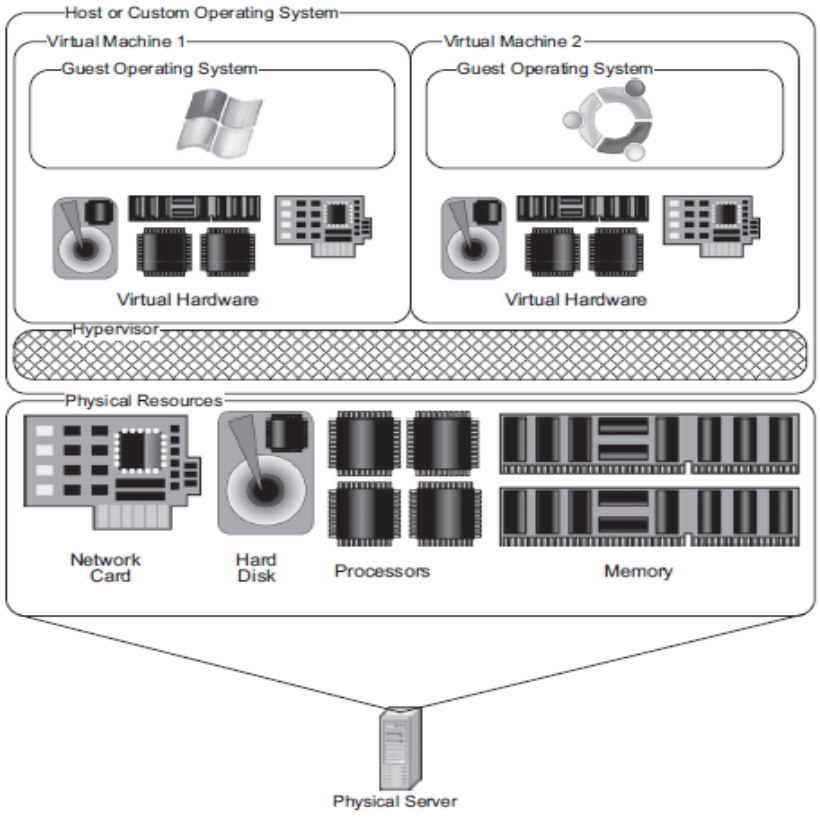


Рис. 6.2. Типова архітектура віртуалізації

Гіпервизор 1 типу запускається та працює безпосередньо з обладнанням (на фізичному «залізі») і керує ним самостійно, досягаючи більшої продуктивності, надійності та безпеки. Гостьові ОС, запущені всередині віртуальних машин, розташовуються рівнем вище, як це показано на рис. 6.3.

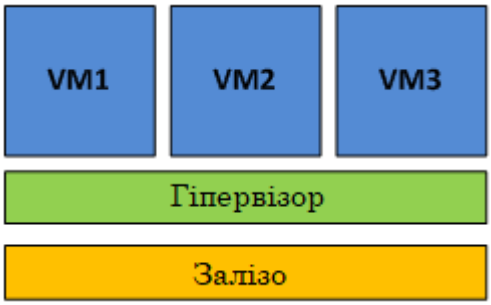


Рис. 6.3. Гіпервізор 1 типу, який запускається на «голому залізі»

Даний тип гіпервізора використовується в багатьох рішеннях Enterprise-класу: Microsoft Hyper-V, VMware vSphere, Citrix XenServer та інші.

Гіпервизор 2 типу, на відміну від 1 типу, запускається всередині (в просторі користувача) хостової ОС (рис. 6.4), що не найкращим чином позначається на продуктивності.

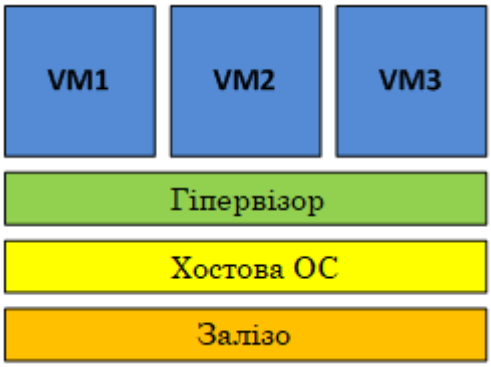


Рис. 6.4. Гіпервізор 2 типу, який запускається всередині хостових ОС

Прикладами гіпервізора 2 типу служать MS VirtualPC, VMware Workstation та інші.

Монолітна архітектура гіпервізора. Монолітний підхід розміщує гіпервізор на єдиному рівні (рис. 6.5), який також включає більшість необхідних компонентів, таких як ядро, драйвери пристроїв і стек введення/виведення.

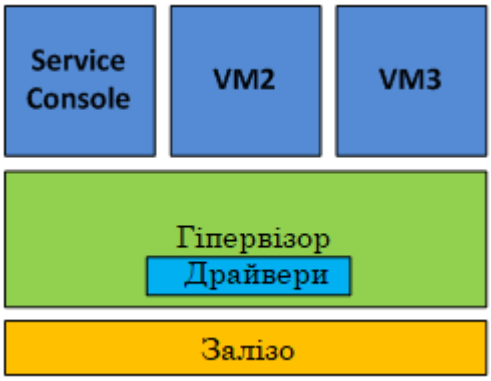


Рис. 6.5. Архітектура монолітного гіпервізора

Даний підхід передбачає, що всі драйвери апаратних пристроїв поміщені в код гіпервізора. У монолітної моделі – гіпервізор для доступу до обладнання використовує власні драйвери. Гостьові ОС працюють на віртуальних машинах поверх гіпервізора і коли гостьовій системі потрібен доступ до обладнання, вона повинна пройти через гіпервізор та його модель драйверів. Зазвичай одна з гостьових ОС грає роль адміністратора або консолі, в якій запускаються компоненти для надання ресурсів, управління і моніторингу всіх гостьових ОС, що працюють на сервері.

Монолітна архітектура має свої переваги і недоліки. Серед достоїнств можна відзначити:

- більш високу (теоретично) продуктивність через знаходження драйверів в просторі гіпервізора;
- більш високу надійність, так як збої в роботі керуючої ОС (в термінах VMware – «*Service Console*») не призведуть до збою всіх запущених віртуальних машин.

Недоліками ж у монолітної архітектурі можна вважати наступне:

- підтримка лише того обладнання, на яке у гіпервізора є драйвера. Через це вендор гіпервізора повинен тісно співпрацювати з вендорами обладнання, щоб драйвери для роботи всього нового обладнання з гіпервізором вчасно писалися і додавалися в код гіпервізора. З тієї ж причини при переході на нову апаратну платформу може знадобитися перехід на іншу версію гіпервізора, і навпаки – при переході на нову версію гіпервізора може знадобитися зміна апаратної платформи, оскільки старе обладнання вже не підтримується;
- потенційно нижча безпека – через включення в гіпервізор стороннього коду у вигляді драйверів пристроїв. Оскільки код драйверів реалізується в просторі гіпервізора, існує теоретична можливість скористатися вразливістю в коді і отримати контроль як над хостовою, так і над усіма гостьовими операційними системами.

Цей підхід використовується такими рішеннями, як VMware ESX і традиційними системами мейнфреймів.

Мікроядерна архітектура гіпервізора. При мікроядерному підході використовується дуже тонкий, спеціалізований гіпервізор, який виконує лише основні завдання забезпечення ізоляції розділів і управління пам'яттю. Цей рівень не включає стека введення/виведення або драйверів пристроїв. При використанні даної архітектури стек віртуалізації і драйвери конкретних пристроїв розташовані в спеціальному розділі ОС, іменованому батьківським розділом.

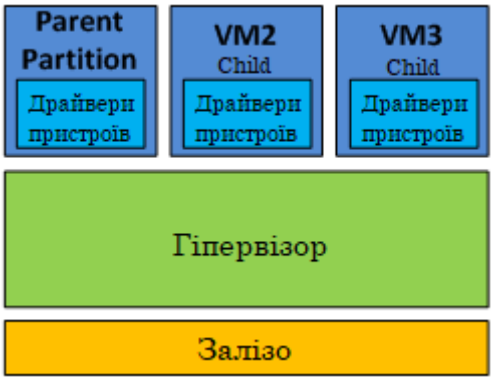


Рис. 6.6. Архітектура мікроядерного гіпервізора

У мікроядерній реалізації використовується таке поняття, як «тонкий гіпервізор», в цьому випадку в ньому зовсім немає драйверів. Замість цього драйвери працюють в кожному індивідуальному розділі, щоб будь-яка гостьова ОС мала можливість отримати через гіпервізор доступ до обладнання. При такій розстановці сил кожна віртуальна машина займає абсолютно окремий розділ, що позитивно позначається на захищеності і надійності. У мікроядерній моделі гіпервізора один розділ є батьківським (parent), де і розташована хостова ОС, решта – дочірніми (child). *Розділ* – це найменша ізольована одиниця, підтримувана гіпервізором.

Таким чином, кожному розділу призначаються конкретні апаратні ресурси – частку процесорного часу, обсяг пам'яті, пристрої та ін. Батьківський розділ створює дочірні розділи і керує ними, а також містить стек віртуалізації (virtualization stack), який використовується для управління дочірніми розділами. Батьківський розділ створюється першим і володіє всіма ресурсами, що не належать гіпервізору. Володіння всіма апаратними ресурсами означає, що саме кореневий (тобто, батьківський) розділ управляє живленням, підключенням самоналагоджувальних пристроїв, керує питаннями апаратних збоїв і навіть управляє завантаженням гіпервізора.

Переваги у такої архітектури наступні:

- не потрібні драйвери, «заточені» під гіпервізор. Гіпервізор мікроядерної архітектури сумісний з будь-яким обладнанням, яке має драйвери для ОС батьківського розділу;

- більш висока безпека за рахунок того, що гіпервізор не містить стороннього коду, відповідно і можливостей для атаки на нього стає менше.

Найяскравішим прикладом використання мікроядерної архітектури є Hyper-V.

6.3. Віртуальне середовище

На сьогоднішній день існує безліч програмних пакетів, як комерційних так і безкоштовних, з відкритим кодом, які дозволяють здійснювати віртуалізацію. Однак одними із найпопулярніших варіантів програмного забезпечення для віртуалізації залишаються: VMware та Oracle VM VirtualBox.

Oracle VM VirtualBox – кросплатформове вільне (GNU GPL) програмне забезпечення віртуалізації для операційних систем Microsoft Windows, Linux, FreeBSD, Mac OS X, Solaris/OpenSolaris, ReactOS, DOS та інших. Підтримуються як 32-бітові, так і 64-бітові версії ОС. Однак, незважаючи на те що VirtualBox – це безкоштовне рішення, віртуальна машина має свої *переваги* до яких відноситься:

- підтримка роботи через командний рядок;
- інтеграція екрану, загальний буфер обміну і обмін файлами між хостом і гостьової системою;
- підтримка необмеженої кількість знімків стану операційної системи;
- підтримка шифрування диска віртуальної машини через VBoxExtensions;
- підтримка запису відео з машини.

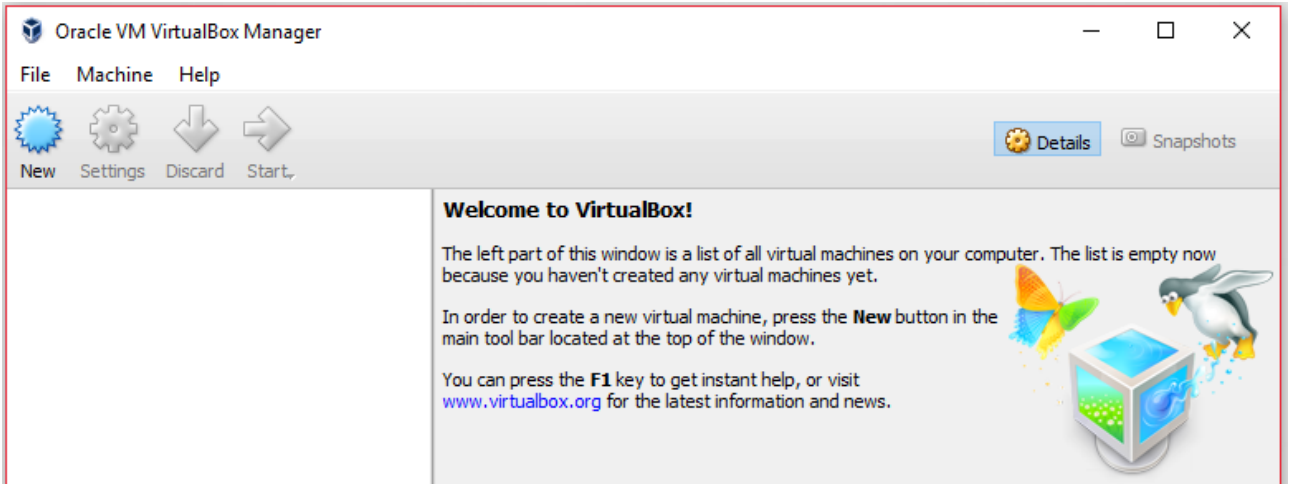


Рис. 6.7. Головне вікно програмного пакету Oracle VM VirtualBox

VMware Workstation Pro – комерційний програмний продукт віртуалізації, який дозволяє створювати і запускати одночасно кілька віртуальних машин (x86-архітектури), в кожній з яких працює своя гостьова операційна система. Підтримуються як 32-бітові, так і 64-бітові версії ОС.

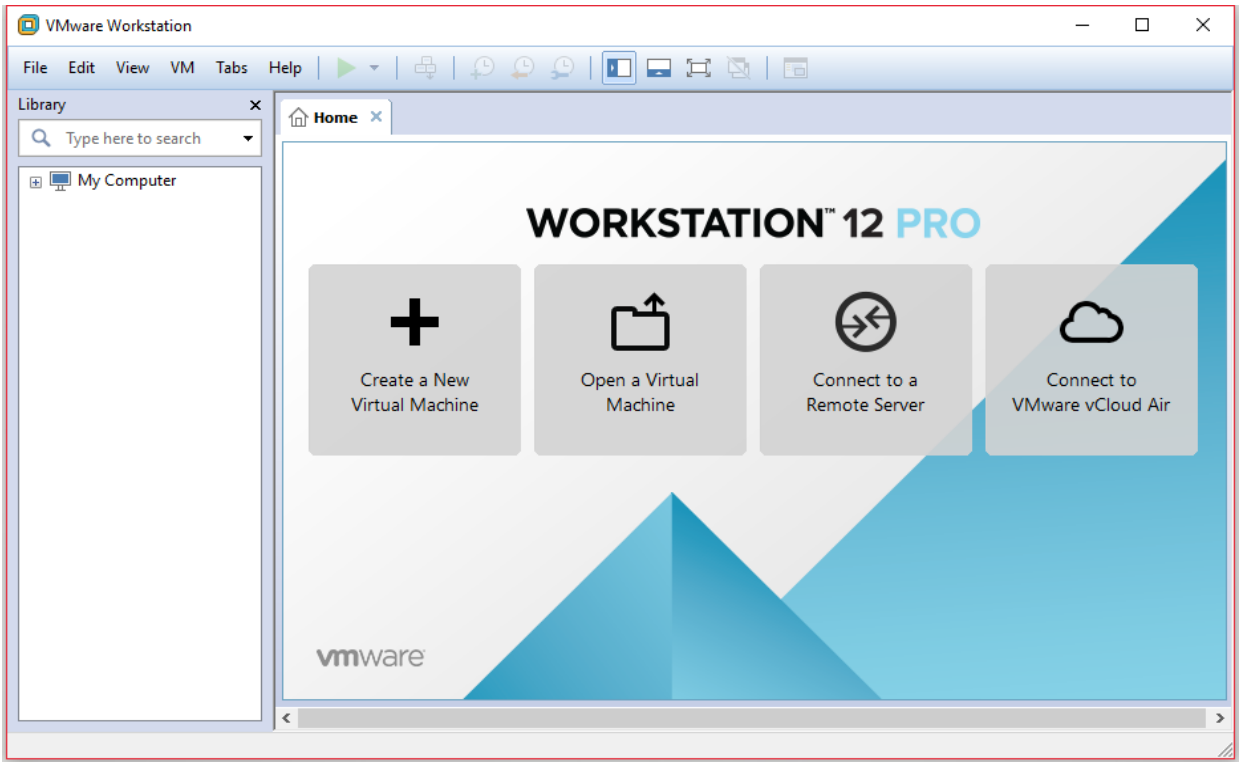


Рис. 6.8. Головне вікно програмного пакету VMware Workstation Pro

VMware Workstation Player – безкоштовний (для особистого некомерційного використання) програмний продукт, призначений для створення (починаючи з версії 3.0) і запуску готових віртуальних машин (створених в VMware Workstation, або VMware Server). Безкоштовне рішення з обмеженим, порівняно з VMware Workstation, функціоналом.

До основних можливостей VMware Workstation Player необхідно віднести:

- автоматичну установку систем за шаблоном;
- детальне налаштування обладнання, включаючи настройку ID процесора, довільної кількості відеопам'яті та інших параметрів;
- простоту налаштувань віртуальної мережі між машинами, яка зазвичай піднімається автоматично на відміну від VirtualBox;
- покращену підтримку графіки і DirectX 10, можна грати в ігри;
- повнішу реалізація BIOS і підтримку EFI.

Порядок виконання лабораторної роботи №6:

1. Включити ПК.
2. Ознайомитися з короткими теоретичними відомостями.

3. Виконати наступні завдання[4]:

1) Завантажити, встановити на хостову машину та ознайомитися з інтерфейсом і функціоналом програмного продукту VirtualBox або VMware (або іншого програмного забезпечення на вибір).

2) Завантажити по одному дистрибутиву Windows та Linux на вибір.

3) Створити віртуальну машину, використовуючи обране вами програмне забезпечення для віртуалізації, наприклад ***Test PC1 Win***, після чого встановити і запустити гостьову ОС Windows. Як ім'я користувача використовувати своє прізвище, пароль – ваше ім'я, ім'я комп'ютера – назва групи, робоча група – назва предмету.

4) Повністю вимкнути віртуальну машину ***Test PC1 Win*** та експортувати її в конфігураційний .OVA або .OVF образ.

5) На основі створеного .OVA (.OVF) образу необхідно створити ще одну віртуальну машину ***Test PC2 Win***.

6) Запустити обидві віртуальні машини ***Test PC1 Win*** і ***Test PC2 Win***, запустити на них та на хост-машині командний рядок і пропінгувати адресу 127.0.0.1.

7) За допомогою командного рядка дізнатися IP-адреси всіх машин (хостова та дві віртуальних) та налаштувати мережеві інтерфейси віртуальних машин і конфігуратора мереж обраного вами програмного забезпечення для віртуалізації таким чином, щоб хост-машина могла пінгувати віртуальні машини, а кожна з них могла пінгувати інші. Після чого перевірити здатність з'єднання між машинами по іменах вузлів, щоб все працювало.

8) Повністю видалити ***Test PC2 Win*** з хостової машини.

9) Створити ще одну віртуальну машину, на заміну видаленої, наприклад ***Test PC2 Lin***, після чого встановити і запустити гостьову ОС Linux. Як ім'я користувача використовувати своє прізвище, пароль – ваше ім'я, ім'я комп'ютера – назва групи.

10) Вивчити можливості мережевих утиліт ОС Linux *ifconfig*, *hostname*, *netstat*, *route* та *arp*, запустивши їх з ключем *-h*.

11) Підключити до мережі новостворену віртуальну машину та перевірити за допомогою мережевих утиліт можливість зв'язку між всіма машинами по IP-адресах.

12) Використовуючи мережеві утиліти ОС Linux заповнити наступні таблиці. Крім цього, необхідно визначити чи використовуються в локальній мережі сервери DNS, WINS, DHCP і якщо використовуються, вказати їх IP-адреси.

[4] Усі виконувані дії описувати в звіті та супроводжувати скріншотами.

Таблиця 6.1. Загальні відомості.

Символьне ім’я комп’ютера	Адреса локальної мережі	IP-адреса комп’ютера	MAC-адреса комп’ютера	Використовувана в локальній мережі технологія

Таблиця 6.2. Таблиця маршрутизації.

Активні маршрути:				
Мережева адреса	Маска підмережі	Адреса шлюзу	Інтерфейс	Метрика

Таблиця 6.3. Таблиця ARP-кешу.

IP-адреса	MAC-адреса	Тип

4. Оформити звіт згідно до вимог (додаток 1).
5. Зробити висновки, відповісти на контрольні питання та підготуватися до письмового опитування.

Зміст звіту:

1. Титульний лист.
2. Постановка завдання.
3. Протокол виконання лабораторної роботи, що містить скріншоти та опис всіх виконуваних дій.
4. Висновки.

Контрольні питання:

1. Надайте визначення поняттю віртуалізації.
2. Назвіть основні категорії віртуалізації та охарактеризуйте їх.
3. На які види поділяється віртуалізація ресурсів? Охарактеризуйте дані види.
4. На які види поділяється віртуалізація платформ? Охарактеризуйте дані види.
5. Що таке віртуальна машина?
6. Назвіть основну відмінність між хост-машиной та гостьовою.
7. Що таке гіпервізор?
8. Назвіть основні види гіпервізорів та опишіть їх архітектуру.

РОЗДІЛ 2 ТЕОРІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Лабораторна робота №7
«Основні положення теорії інформаційної та кібернетичної безпеки»

Мета роботи:

1. Закріплення основних понять інформаційної та кібернетичної безпеки.
2. Поглиблення теоретичних знання з наступних питань:
   - класифікація загроз інформаційної безпеки та їх джерела;
   - аналіз найбільш розповсюджених загроз.
3. Набуття практичних навичок щодо поверхневого аналізу інцидентів інформаційної безпеки, виявлення та аналізу реалізованих загроз інформаційної безпеки, а також проведення їх класифікації.

Стислі теоретичні відомості:

7.1. Основні поняття інформаційної та кібернетичної безпеки

Як відомо, поняття інформації, уже давно стало загальнолюдським, однак навіть на сьогоднішній день ще не існує загальнонаукового визначення даного терміну. Тому з точки зору різних галузей науки, це поняття визначається різноманітними специфічними ознаками. Так, наприклад, у філософії інформація розглядається як властивість матеріальних об’єктів і процесів зберігати і породжувати певний стан, який в різних матеріально-енергетичних формах може бути переданий від одного об’єкта до іншого. У кібернетиці інформацією прийнято називати міру усунення невизначеності. А в електронній енциклопедії «Вікіпедія», подається наступне визначення інформації:

Інформація – абстрактне поняття, яке має різні значення залежно від контексту. Походить від латинського слова «*informatio*», яке має декілька значень:

- роз’яснення, виклад фактів та подій, витлумачення;
- представлення, поняття;
- ознайомлення, просвіта.

В даному ж навчальному посібнику, буде використовуватися термін, який наведено в Законі України **«Про інформацію»:**

Інформація – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

Згідно з Статтею 10 та 20 цього Закону передбачено порядок класифікації інформації за змістом (інформація про фізичну особу; інформація довідково-енциклопедичного характеру; інформація про стан довкілля (екологічна інформація); інформація про товар (роботу, послугу); науково-технічна

інформація; податкова інформація; правова інформація; статистична інформація; соціологічна інформація; інші види інформації) і за порядком

доступу (відкрита інформація та інформація з обмеженим доступом).

Необхідно відзначити, що саме завдяки прийнятому порядку класифікації інформаційних ресурсів існує можливість їх відсортування за важливістю та встановлення конкретних (оптимальних) вимоги до їх захисту. У Законі України **«Про доступ до публічної інформації»** наводяться такі визначення:

Конфіденційна інформація – інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов.

Службова інформація – інформація, що:

- міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову;
- кореспонденція, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень;
- зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

Таємна інформація – інформація, доступ до якої обмежується в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання

авторитету і неупередженості правосуддя, розголошення якої може завдати шкоди особі, суспільству і державі.

Також необхідно зазначити що, ***інформація має певні властивості***, основні з яких наведені нижче:

- *цінність інформації* – визначається корисністю та здатністю забезпечити певного суб'єкта необхідними умовами для досягнення ним поставленої мети;
- *достовірність* – відповідність отриманої інформації реальності навколишнього світу*;*
- *актуальність* – відповідність цінності та достовірності отриманої інформації поточному часу;
- *конфіденційність* – властивість інформації бути захищеною від несанкціонованого ознайомлення;
- *цілісність* – властивість інформації бути захищеною від несанкціонованого спотворення, руйнування або знищення;
- *доступність* – властивість інформації бути захищеною від несанкціонованого блокування;
- *спостережність* – властивість інформації, що дозволяє фіксувати діяльність користувачів і процесів, а також встановлювати їх ідентифікатори;
- *автентичність* – властивість інформації, що дозволяє ідентифікувати джерело її походження (тобто встановлювати авторство).

Зрозуміло, що людям властиво захищати свої секрети (інформацію). А стрімкий розвиток інформаційних технологій (ІТ) та їхнє проникнення у всі сфери людської діяльності призводить до того, що проблеми інформаційної безпеки (ІБ) з кожним роком стають все більш і більш актуальними – і одночасно більш складними.

Під ***інформаційною безпекою*** розуміють стан захищеності інформації та інформаційного середовища від випадкових або навмисних впливів природного або штучного характеру, які можуть завдати неприйнятного збитку суб'єктам інформаційних відносин (у тому числі власникам і користувачам інформації).

Захист інформації (ЗІ) – комплекс заходів, спрямованих на забезпечення інформаційної безпеки.

На практиці, найпоширеніша модель інформаційної безпеки базується на забезпеченні трьох властивостей інформації: конфіденційність, цілісність і доступність.

Конфіденційність інформації, з точки зору захисту інформації означає, що з нею може ознайомитися лише обмежене коло осіб (легальні користувачі), визначене її власником. В разі отримання доступу до інформації неуповноваженою особою, відбувається втрата конфіденційності.

Для деяких видів інформації конфіденційність є одним з найбільш важливих атрибутів (це і медичні страхові записи, і відомості про грошові операції, про рахунки та вклади організацій; це і дані стратегічних досліджень, специфікації нових виробів; відомості про конкретних осіб: клієнти банку, кредитори, податкові дані; відомості медичних установ про стан здоров'я пацієнтів і т. д.).

Цілісність інформації забезпечується її здатністю зберігатися в неспотвореному вигляді, тобто редагувати дану інформацію має право лише законний користувач (зазвичай – власник) з відповідними повноваженнями. Неправомочні, і не передбачені власником зміни інформації (в результаті помилки оператора або навмисних дій неуповноваженої особи) призводять до втрати цілісності.

Потрібно відзначити, що особливо важливим є забезпечення цілісності даних, пов'язаних з функціонуванням об'єктів критичних інфраструктур (енерго-, водопостачання, управління повітряним рухом тощо).

Доступність інформації полягає в здатності системи надавати своєчасний безперешкодний доступ до інформації суб'єктам, наділеним відповідними повноваженнями. Блокування або знищення інформації (в результаті помилки або навмисних дій) призводить до втрати доступності.

Дана властивість є важливим атрибутом для функціонування ІС, орієнтованих на обслуговування клієнтів (це і системи продажу авіаційних та залізничних квитків, і розповсюдження оновлень програмного забезпечення тощо). Ситуацію, коли уповноважений користувач не може отримати доступу до певних послуг (частіше всього мережевих), називають ***відмовою в обслуговуванні***.

Відповідно до статті 1 Закону України **«Про інформацію»:**

захист інформації – сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї.

Отже, беручи до уваги все вище сказане, інформаційну безпеку можна умовно поділити на дві дисципліни (частини): навчально-наукову та прикладну. Навчально-наукова дисципліна досліджує природу перерахованих властивостей інформації, вивчає загрози цим властивостям, а також різноманітні методи, механізми і засоби протидії таким загрозам (захист інформації).

Прикладна ж дисципліна займається забезпеченням цих ключових властивостей, зокрема, шляхом розробки захищених інформаційних систем.

З плином часу з'являються нові загрози інформаційної безпеки, які все частіше характеризуються приставкою «кібер-»: «кіберзагроза», «кібербезпека»,

«кібертероризм» тощо. Для розуміння всіх цих терміни та інших з приставкою «кібер-» необхідно ввести понятійний апарат.

Відповідно до статті 1 Закону України *«Про основні засади забезпечення кібербезпеки України»*:

- *кіберпростір* – середовище, яке виникає в результаті функціонування на основі єдиних принципів і за загальними правилами інформаційних (автоматизованих), телекомунікаційних та інформаційно-телекомунікаційних систем;
- *кібербезпека* – стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі;
- *кіберзагроза* – наявні та потенційно можливі явища і чинники, що загрожують кібербезпеці;
- *кіберзахист* – сукупність заходів організаційного, нормативно-правового, воєнного, оперативного, технічного та іншого характеру, спрямованих на забезпечення кібербезпеки;
- *кібератака* – несанкціоновані дії, що здійснюються за допомогою інформаційно-комунікаційних технологій та спрямовані на порушення конфіденційності, цілісності і доступності інформації, яка обробляється в інформаційній (автоматизованій), телекомунікаційній, інформаційно-телекомунікаційній системі, або порушення сталого функціонування такої системи;
- *кіберінцидент* – надзвичайна подія, пов’язана з реалізацією або можливістю реалізації кібератаки;
- *кібероборона* – сукупність політичних, економічних, соціальних, воєнних, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, спрямованих на захист інформаційного суверенітету та забезпечення обороноздатності держави у кіберпросторі;
- *кібертероризм* – терористична діяльність, що провадиться у кіберпросторі або з його використанням.

7.2. Поняття захисту інформації в системах обробки та передавання інформації

Розібравшись з основними термінами інформаційної та кібернетичної безпеки необхідно виділити, в яких же системах повинен здійснюватися захист інформації, класифікувати загрози інформаційної безпеки та визначити їх джерела.

На сьогоднішній день спеціалісти часто використовують багато різноманітних понять для визначення захисту інформації в системах обробки та передавання інформації. Це і *захист інформації в інформаційних*

(автоматизованих) системах, і захист інформації в телекомунікаційних системах і захист в інформаційно-телекомунікаційних системах (ІТС) тощо. Однак, зараз в Україні загальноприйнятим є поняття ***захисту інформації в інформаційно-телекомунікаційних системах***, саме його найбільше використовують у законодавчих та нормативних документах.

Саме тому, далі буде розглянуто детальніше, що необхідно розуміти під визначенням тієї чи іншої інформаційної системи:

- *інформаційна (автоматизована) система* – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів;
- *телекомунікаційна система* – сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб;
- *інформаційно-телекомунікаційна система* – сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле.

Типовий склад інформаційно-телекомунікаціної системи:

- серверне обладнання (комп'ютери з підвищеною продуктивністю та технічними характеристиками; зазвичай призначені для надання одного або декількох специфічних сервісів, на кшталт електронного поштового обміну, баз даних, IP-телефонії, файлового сховища тощо);
- середовище передачі даних (телефонні кабелі, кабелі типу «вита пара», оптоволоконні лінії, бездротові канали передачі даних такі як Wi-Fi, Wi-Max, Bluetooth);
- активне мережеве обладнання (комутатори, маршрутизатори, модеми, бездротові точки доступу, телефонія);
- пристрої захисту (міжмережеві екрани, системи виявлення/попередження вторгнень тощо);
- автоматизовані робочі місця співробітників (скорочено – АРМ; стаціонарні комп'ютери, ноутбуки, мобільні пристрої та інші гаджети).

Тепер перейдемо безпосередньо до розгляду поняття загрози інформаційної безпеки.

7.3. Поняття загрози інформаційної безпеки

У загальному випадку, ***загроза*** – це потенційно можлива подія, дія, процес або явище, яке може привести до нанесення збитку чиїм-небудь інтересам.

Відповідно ***загрозою інформаційної безпеки*** називається потенційно можлива подія, процес або явище, яке за допомогою впливу на інформацію може прямо або опосередковано призвести до порушення конфіденційності, цілісності або доступності цієї інформації, а також має можливість впливу на компоненти ІТС (тобто нанесення шкоди активам організації), що призводить до їх втрати, знищення або збою функціонування, таким чином наносячи шкоду інтересам суб'єктів інформаційних відносин. А вже реалізована загроза є ***інцидентом інформаційної безпеки (або порушенням)***.

В літературі іноді зустрічається інше трактування терміну, яке є не зовсім коректним. Наприклад, іноді замість терміну «загроза» вживають термін «атака». Однак, враховуючи вищесказане, слід розрізняти атаку, яка є дією, спробою реалізувати певну загрозу, і загрозу, яка є потенційною можливістю здійснення несприятливого впливу. Також необхідно відзначити, що атака – це здебільшого цілеспрямований вплив, як правило, умисний, а загрози можуть бути випадковими, однак від цього збитки внаслідок їх реалізації не стають меншими. Тому захищати інформацію необхідно саме від загроз, а не лише від атак.

Найчастіше загроза є наслідком наявності слабких місць в ІТС або в системах їхнього захисту. Тобто ***уразливістю*** називається слабкість в інформаційних активах або в захисті інформаційних систем, що робить можливим реалізацію певної загрози.

Інформаційними активами можуть бути матеріальні (наприклад, дані та мережі) або нематеріальні об'єкти (наприклад, репутація та довіра), які:

- є інформацією або містять інформацію;
- є ключовими компонентами інфраструктури та служать для обробки, зберігання чи передавання інформації;
- мають певну цінність для організації.

Особи, які реалізують загрози називаються ***порушниками*** або ще зустрічається такий термін, як ***зловмисник***. Однак необхідно розрізняти дані терміни. А саме, у загальному випадку порушник може здійснювати порушення неумисно (наприклад, через необережність або недостатню обізнаність), а зловмисник це все ще порушник але який дії цілеспрямовано з певним умислом, тобто здійснює спробу реалізації атаки. Тобто таким чином термін «зловмисник» просто більш конкретизує «порушника» та підкреслює умисність порушення.

7.4. Класифікація загроз інформаційної безпеки та їх джерела

Історія розвитку інформаційних систем свідчить про те, що нові вразливості систем з'являються регулярно. З такою ж регулярністю, однак з

певним запізненням вони нейтралізуються. У проміжок часу між появою нової вразливості та до моменту її нейтралізації (ліквідації наявної діри) система є особливо вразливою і може бути скомпрометованою. Особливо небезпечним є випадок коли нова вразливість вперше виявляється потенційним порушником. Тому, такий «послідовний» підхід до забезпечення інформаційної безпеки є зовсім неефективним.

Більш ефективним є підхід упередженого захисту інформації, який базується на передбаченні всіх можливих, передбачуваних та потенційних загроз та розробці комплексної системи захисту інформації.

Комплексна система захисту інформації (КСЗІ) – взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації.

Виходячи з даного визначення можна сказати, що найбільш ефективний та економічний варіант комплексної системи захисту інформації базується на аналізі всіх можливих загроз інформаційної безпеки, які характеризуються джерелами загроз, факторами, що зумовлюють можливість реалізації загроз, способами (методами) їх реалізації і безпосередньо наслідками від реалізації загроз ІБ. Тому, розглянемо їх змістовніше.

В якості джерел загроз інформаційної безпеки можуть виступати суб'єкти (фізичні особи, організації, держави), об'єкти (технічні засоби, програмне забезпечення) або явища (техногенні аварії, стихійні лиха, інші природні явища).

Таким чином, джерела загроз ІБ можна розділити на три основних групи:

- антропогенні джерела (антропогенні загрози – загрози обумовлені діями суб'єкта);
- техногенні джерела (техногенні загрози – загрози обумовлені технічними засобами);
- стихійні джерела (загрози викликані стихійними лихами або іншими природними явищами).

В якості антропогенних джерел (порушників) загроз інформаційної безпеки можуть виступати:

- спеціальні служби іноземних держав (блоків держав);
- політичні супротивники (політичні партії);
- терористичні, екстремістські угрупування;
- злочинні групи (кримінальні структури);
- зовнішні суб'єкти (окремі фізичні особи);
- суб'єкти підприємницької діяльності та конкуруючі організації;
- розробники, виробники, постачальники програмних, технічних та програмно-технічних засобів;

- особи, які залучаються для установки, налагодження, монтажу, пусконалагоджувальних та інших видів робіт;
- технічний персонал – особи, які забезпечують функціонування інформаційних систем;
- допоміжний персонал (адміністрація, охорона, прибиральники і т. д.);
- користувачі інформаційної системи;
- адміністратори інформаційної системи і адміністратори безпеки;
- колишні працівники (користувачі).

В свою чергу до антропогенних джерел тобто порушників інформаційної безпеки можна віднести:

- осіб, які здійснюють навмисні дії з метою доступу до інформації (впливу на інформацію), що міститься в інформаційній системі, або порушення функціонування самої інформаційної системи чи її інфраструктури (навмисні загрози ІБ);
- осіб, які мають доступ до інформаційної системи, ненавмисні дії яких можуть призвести до порушення інформаційної безпеки (ненавмисні загрози ІБ).

А в залежності від наявних прав доступу і можливостей щодо доступу до інформації та (або) до компонентів інформаційної системи, джерела загроз ІБ (порушників) також можна поділити на два типи:

1) зовнішні джерела – особи, які не мають права доступу до інформаційної системи, її окремих компонентів і реалізують загрози безпеки інформації з-поза меж інформаційної системи;

2) внутрішні джерела – особи, які мають право постійного або разового доступу до інформаційної системи, її окремих компонентів.

Розглядаючи техногенні джерела загроз інформаційної безпеки, необхідно відзначити, що вони пов’язані безпосередньо з відмовами або збоями в роботі технічних засобів або програмного забезпечення і підлягають обов’язковому аналізу для інформаційних систем, в яких метою захисту є забезпечення цілісності та доступності оброблюваної інформації. Такі загрози можуть бути обумовлені:

- низькою якістю (надійністю) технічних, програмних або програмно-технічних засобів;
- низькою якістю (надійністю) мереж зв’язку і (або) послуг зв’язку;
- відсутністю або низькою ефективністю систем резервування або дублювання програмно-апаратних і технічних засобів;
- низькою якістю (надійністю) інженерних систем (кондиціонування, електропостачання, охоронних систем і т. п.);
- низькою якістю обслуговування з боку обслуговуючих організацій і осіб.

Таким чином, проаналізувавши можливі джерела загроз переходимо безпосередньо до класифікацій загроз інформаційної безпеки.

Сама ж класифікація загроз може бути проведена за безліччю критеріями, однак нижче буде наведено найпоширеніші з них.

1. За природою виникнення: природні (об'єктивні) і штучні (суб'єктивні).

Природними загрозами називають загрози, що виникли в результаті впливу на ІТС або її окремі елементи об'єктивних фізичних процесів чи стихійних природних явищ, незалежних від людини. Прикладами природних загроз можуть служити пожежі, повені, цунамі, землетруси і т. д., а особливістю таких загроз є надзвичайна складність або навіть неможливість їх прогнозування.

Щодо *штучних загроз*, то вони викликані діяльністю людини. Серед них, у свою чергу, виходячи з мотивації дій, можна виділити *ненавмисні* (випадкові) загрози, викликані помилками в проектуванні ІТС та її елементів, помилками в програмному забезпеченні, помилками в діях персоналу або їхньою халатністю та іншими причинами, і *навмисні* (умисні) загрози, пов'язані з цілеспрямованими діями зловмисників.

2. За розташуванням джерела загрози виділяють:

- загрози, джерело яких розташоване поза межами контрольованої зони. Прикладом можуть слугувати: перехоплення побічних електромагнітних, акустичних та інших випромінювань пристроїв та ліній зв'язку, а також наведень активних випромінювань на допоміжні технічні засоби, що безпосередньо не приймають участі в обробленні інформації (телефонні лінії, мережі живлення, опалення та ін.); перехоплення даних, що передаються каналами зв'язку, їх аналіз з метою вияснення протоколів обміну, правил входження у зв'язок та авторизацію користувача і наступних спроб їх імітації для проникнення в систему; дистанційна фото- і відеозйомка; перехоплення акустичної інформації з використанням спрямованих мікрофонів.
- загрози, джерело яких знаходиться в межах контрольованої зони (наприклад, інсайдери), території (приміщення), на якій знаходиться ІТС. Як приклад можна навести застосування підслуховуючих пристроїв; розкрадання носіїв, які містять конфіденційну інформацію; від'єднання або виведення з ладу підсистем забезпечення функціонування обчислювальних систем (електроживлення, охолодження та вентиляції, ліній зв'язку та ін.);

3. За ступенем впливу на ІТС виділяють пасивні і активні загрози.

Реалізація пасивних загроз не здійснює жодних шкідливих чи негативних змін у складі та структурі ІТС. Прикладом такої загрози є – несанкціоноване копіювання файлів з даними. При реалізації ж активних загроз, навпаки, порушується структура ІТС, к приклад можна навести: упровадження апаратних закладок, програмних закладок та комп'ютерних вірусів, які

дозволяють подолати систему захисту, при цьому мають можливість прихованого та незаконного здійснення доступ до системних ресурсів з метою реєстрації та передавання критичної інформації або дезорганізації функціонування системи; дії для дезорганізації функціонування системи (змінювання режимів роботи пристроїв або програм, страйк або саботаж персоналу, постановка потужних активних радіозавад на частотах роботи пристроїв системи і т. п.); загроза навмисної модифікації інформації.

4. Класифікація за видом використовуваної уразливості включає:

- загрози, які реалізуються з використанням уразливості системного ПЗ;
- загрози, які реалізуються з використанням уразливості прикладного ПЗ;
- загрози, що виникають в результаті використання уразливості в апаратних засобах;
- загрози, які реалізуються з використанням вразливостей протоколів мережевої взаємодії і каналів передачі даних;
- загрози, які реалізуються з використанням вразливостей, що обумовлюють наявність технічних каналів витоку інформації.

Можна й надалі продовжувати класифікувати загрози за різними критеріями, однак на практиці найчастіше використовується наступна основна класифікація загроз, яка базується на порушенні трьох раніше введених базових властивостей інформації, а саме: загрози порушення конфіденційності, цілісності та доступності інформації. Додатково можна виділити загрозу автентичності.

Однак, необхідно відзначити, що реальні загрози інформаційній безпеці далеко не завжди можна чітко віднести до якоїсь конкретної категорій. Так, наприклад, загроза розкрадання носіїв інформації може бути при певних умовах віднесена до всіх перерахованих категорій.

Для кращого розуміння, далі розглянемо перелік конкретних загроз:

I. Основні *ненавмисні штучні* загрози ІТС (без злого умислу):

1) ненавмисні дії, результатом яких є часткова або повна відмова системи в тому числі руйнування апаратних, програмних або інформаційних ресурсів ІТС (тобто ненавмисне пошкодження обладнання, видалення, спотворення файлів з важливою інформацією або прикладних чи системних програм тощо);

2) ненавмисне пошкодження носіїв інформації, апаратного устаткування або каналів зв’язку;

3) некомпетентне використання програмного забезпечення, що призводить до втрати працездатності системи (зависання або зациклення) або незворотних змін в системі (це і форматування носіїв інформації, і видалення даних, і спотворення системних файлів тощо);

4) неправомірне вимкнення обладнання або зміна режимів роботи пристроїв та ПЗ;

5) нелегальне встановлення і подальше використання неврахованого ПЗ (ігрове, навчальне, технологічне та ін., використання якого не являється необхідними для виконання порушником своїх службових обов'язків) з необґрунтованим витрачанням ресурсів (тобто завантаження процесора, використання оперативної пам'яті і пам'яті на твердих носіях);

6) некомпетентне використання, настроювання або взагалі відключення засобів захисту ІТС;

7) зараження всієї ІТС або окремих її компонентів шкідливим ПЗ;

8) втрата, передача або навіть ненавмисне розголошення атрибутів розмежування доступу (паролів, ключів шифрування, ідентифікаційних карток, перепусток тощо);

9) повне або часткове нехтування організаційними обмеженнями (встановленими правилами) при роботі в системі;

10) вхід в систему в обхід засобів захисту (наприклад завантаження сторонньої операційної системи з зовнішніх носіїв).

II. Основні *навмисні штучні* загрози ІТС (дезорганізація роботи системи):

1) навмисне фізичне руйнування ІТС (в результаті вибуху, підпалу тощо) або виведення з ладу всіх або окремих критичних компонентів ІТС;

2) відключення або виведення з ладу систем безперебійного живлення, охолодження або вентиляції, які забезпечують безперервне функціонування обчислювальних систем;

3) проникнення ворожих агентів у число персоналу ІТС, а також вербування (шляхом підкупу, шантажу тощо) персоналу або окремих користувачів, які мають певні повноваження;

4) використання підслуховуючих пристроїв, дистанційної фото- і відеозйомки тощо;

5) крадіжка або несанкціоноване копіювання носіїв інформації;

6) перегляд та аналіз виробничих відходів (документів, списаних носіїв інформації тощо);

7) зчитування залишкової інформації з оперативної пам'яті і зовнішніх носіїв інформації;

8) використання різноманітних уразливостей операційних систем або іншого ПЗ яке встановлено на компонентах ІТС;

9) злом шифрів криптозахисту інформації;

10) перехоплення побічних електромагнітних, акустичних та інших випромінювань пристроїв і ліній зв'язку, а також наведень активних

випромінювань на допоміжні технічні засоби, які безпосередньо не беруть участі в обробці інформації (телефонні лінії, мережі живлення, опалення тощо);

11) перехоплення даних, які передаються каналами зв'язку, і їх подальший аналіз з метою з'ясування протоколів обміну, правил входження в зв'язок і авторизації користувача;

12) «крадіжка особистості» – несанкціоноване заволодіння персональними даними особи або одержання паролів чи інших атрибутів розмежування доступу, з подальшим маскуванням під зареєстрованого користувача («маскарад»);

13) «фішинг» – спонукання користувача ввести свої ідентифікаційні та аутентифікаційні дані (логін, пароль) або іншу персональну інформацію шляхом запевнення користувачів щодо достовірності та справжності фальшивих (спеціально створених для цього) мережевих ресурсів, таких як пошта, веб-сайти, сторінки авторизації у соціальних мережах тощо;

14) «вішинг» – отримання у користувача під час телефонної розмови необхідної зловмиснику інформації, шляхом використання різних методів переконання;

15) розсилання спаму;

16) бот-мережі – сукупність комп'ютерів, уражених шкідливим ПЗ, ресурси яких через спеціальні командно-контрольні сервери (C&C) несанкціоновано використовуються зловмисниками;

17) DDoS-атака – розподілена мережева атака, яка за допомогою численної кількості джерел має на меті порушити доступність сервісу (автоматизованої системи) шляхом вичерпання його обчислювальних ресурсів;

18) несанкціонований доступ (НСД) до інформаційних ресурсів та інформаційно-телекомунікаційних систем з подальшим несанкціонованим використання терміналів користувачів (які мають унікальні фізичні характеристики, такі як номер робочої станції в мережі, фізична адреса, апаратний блок кодування тощо);

19) впровадження апаратних або програмних «закладок», шкідливого ПЗ (комп'ютерних вірусів, троянських коней і т. п.), з метою таємного, незаконного доступу до системних ресурсів, реєстрації та передачі критичної інформації або дезорганізації функціонування системи;

20) незаконне підключення до ліній зв'язку з метою роботи «між рядків», з використанням пауз в діях законного користувача від його імені з подальшим введенням неправдивих повідомлень або модифікацією переданих повідомлень;

21) незаконне підключення до ліній зв'язку з метою підміни законного користувача шляхом його фізичного відключення після входу в систему і

успішної аутентифікації з подальшим введенням дезінформації і нав’язування помилкових повідомлень.

Зауважимо, що для досягнення поставленої мети зловмисник буде використовувати не одну загрозу, а деяку їх сукупність, при цьому застосовуючи різноманітні напрями, методи та способи реалізації даних загроз.

До основних *напрямків реалізації загроз* зловмисником відносять:

- безпосереднє звернення до об’єктів доступу;
- створення програмних та технічних засобів, що виконують звернення до об’єктів доступу в обхід засобів захисту;
- модифікація засобів захисту, що дозволяє реалізовувати загрози інформаційній безпеці;
- упровадження в технічні засоби автоматизованої системи програмних або технічних механізмів, що порушують передбачувану структуру та функції автоматизованої системи.

До основних *методів реалізації загроз* інформаційній безпеці системи зазвичай відносять:

- визначення зловмисником типу та параметрів носіїв інформації;
- одержання зловмисником всієї необхідної інформації щодо програмно-апаратного середовища, типу та параметрів засобів обчислювальної техніки, типу та версії операційної системи, складу прикладного програмного забезпечення;
- одержання зловмисником детальної інформації щодо функцій, які виконуються автоматизованою системою;
- одержання зловмисником даних щодо системи захисту, яка застосовується в інформаційній системі;
- визначення способу подання інформації;
- визначення зловмисником змісту даних, що оброблюються в системі, на якісному рівні (застосовується для моніторингу автоматизованої системи і для дешифрування повідомлень);
- викрадення (копіювання) машинних носіїв інформації, які містять конфіденційні дані;
- використання спеціальних технічних засобів для перехоплення побічних електромагнітних випромінювань та наведень (ПЕМВН) – конфіденційні дані перехоплюються зловмисником шляхом виділення інформативних сигналів з електромагнітного випромінювання та наведень колами живлення засобів обчислювальної техніки, що входять до автоматизованої системи;
- знищення засобів обчислювальної техніки та носіїв інформації;
- викрадення (копіювання) носіїв інформації;

- несанкціонований доступ користувача до ресурсів автоматизованої системи в обхід, або шляхом подолання систем захисту з використанням спеціальних засобів, прийомів, методів;
- несанкціоноване перевищення користувачем своїх повноважень;
- несанкціоноване копіювання програмного забезпечення;
- перехоплення даних, що передаються каналами зв'язку;
- візуальне спостереження – конфіденційні дані зчитуються з екранів терміналів, роздруківок у процесі їх друку і т. п.;
- розкриття змісту інформації на семантичному рівні – доступ до смислової складової інформації, яка зберігається а автоматизованій системі;
- знищення машинних носіїв інформації;
- внесення користувачем несанкціонованих змін у програмно-апаратні компоненти автоматизовані системи та дані, які оброблюються;
- установка та використання нештатного апаратного і/або програмного забезпечення;
- зараження комп'ютерними вірусами;
- внесення спотворень в подання даних, знищення даних на рівні подання, спотворення інформації при передаванні лініями зв'язку;
- упровадження дезінформації;
- виведення з ладу машинних носіїв інформації без знищення інформації – виведення з ладу електронних блоків нагромаджувачів на жорстких дисках та інше;
- прояв помилок проектування та розробки апаратних і програмних компонентів автоматизованої системи;
- обхід (відключення) механізмів захисту – завантаження зловмисником нештатної операційної системи з флешки, використання налагоджувальних режимів програмно-апаратних компонент автоматизованої системи та інше;
- спотворення відповідності синтаксичних та семантичних конструкцій мови – встановлення нових значень слів, виразів і т. п.;
- заборона на використання інформації – наявна інформація за будь-яких причин не може бути використаною.

Однак, як вже зазначалось раніше, перед проведенням детального аналізу загроз інформаційної безпеки, спершу необхідно виділити їх та здійснити повний перелік.

Загалом, виділяють два основних методи перерахування загроз:

1) Побудова довільних списків загроз. При побудові таких списків можливі загрози виявляються експертним шляхом і фіксуються випадковим і неструктурованим способом. Для цього підходу характерні неповнота і суперечливість отриманих результатів.

2) Побудова дерев загроз. В цьому випадку, загрози описуються у вигляді одного або декількох дерев. Деталізація загроз здійснюється зверху вниз, і в кінцевому підсумку кожен лист дерева дає опис конкретної загрози.

В якості прикладу нижче розглянуто дерево загрози блокування доступу до мережного додатку (рис. 7.1).

Рис. 7.1. Приклад дерева загроз ІБ

З даної схеми можна побачити, що блокування доступу до мережевого додатку може відбутися або у результаті реалізації DoS-атаки на мережевий інтерфейс, або в результаті завершення роботи комп’ютера. У свою чергу, завершення роботи комп’ютера може статися внаслідок несанкціонованого фізичного доступу зловмисника до даного комп’ютера, або в результаті використання зловмисником уразливості, що реалізує атаку на переповнення буфера.

Таким чином, визначення, перелік, аналіз та класифікація можливих загроз інформаційної безпеки в ІТС є важливим етапом аналізу їх вразливостей і служать основою для подальшого проведення аналізу ризиків та формулюванню вимог до системи захисту.

Порядок виконання лабораторної роботи №7:

1. Включити ПК.
2. Ознайомитися з короткими теоретичними відомостями.
3. Розглянути та проаналізувати наведені нижче інциденти інформаційної безпеки, з ціллю виявлення загроз ІБ та подальшого їх аналізу:

1) За повідомленнями світових інформаційних агентств, невідомі хакери зламали сервер Hotmail.com, після чого в будь-яку з 40 млн. віртуальних поштових скриньок, розташованих на цьому сервері, можна було проникнути без пароля – просто ввівши ім’я

користувача. Протягом якого часу поштові адреси користувачів Hotmail.com були доступні будь-якому охочому, залишилося невідомим.

У понеділок вранці, компанія Microsoft (власниця Hotmail) на дві години відключила сервер і, за її заявою, повністю відновила систему безпеки Hotmail.

Незабаром після цього шведські ЗМІ повідомили, що відповідальність за здійснення атаки (а саме упровадження шкідливого коду) на сервер Hotmail, взяла на себе група хакерів під назвою Hackers Unite, до якої входить один швед і сім американців.

«Ми зробили це не для того, щоб щось зруйнувати, – заявив 21-річний шведський представник Hackers Unite. – Ми хотіли показати світові, наскільки погана система безпеки Microsoft».

2) В помсту за дуже маленьку премію 63-річний Рожер Дурон (колишній системний адміністратор компанії UBS Paine Webber) встановив на серверах компанії «логічну бомбу», яка знищила всі дані і паралізувала роботу компанії на тривалий час.

Впровадження «логічної бомби» Дурон здійснив з домашнього комп'ютера за кілька місяців до того, як отримав дуже маленьку, на його погляд, премію. «Логічна бомба» була встановлена приблизно на 1500 комп'ютерів в мережі філій по всій країні і налаштована на певний час – 9.30, якраз на початок банківського дня.

Звільнився Дурон з UBS Paine Webber 22 лютого 2002 року, а четвертого березня 2002 «логічна бомба» послідовно видалила всі файли на головному сервері центральної бази даних і 2000 серверів в 400 філіях банку, при цьому відключивши систему резервного копіювання.

3) Поверхом вище серверної прорвало трубу з гарячою водою, і системні блоки серверів виявилися заповненими окропом.

4) Співробітники компанії «Вимпелком» (колишні і діючі) організували в Інтернеті сайт www.sherlok.ru, про який в компанії «Вимпелком» дізналися в червні 2004 р. Організаторами даного сайту пропонувалася послуга – пошук людей за прізвищем, за номером телефону та іншими даними. У липні організатори сайту запропонували нову послугу – деталізацію телефонних переговорів стільникових операторів. В даному випадку під деталізацією розмов малося на увазі роздруківка номерів всіх вхідних і вихідних дзвінків з вказівкою тривалості розмов і їх вартості, яка використовується операторами, наприклад для виставлення рахунків абонентів. За цими даними можна зробити висновок про поточну діяльність абонента, його сферу інтересів і коло знайомств.

Співробітники компанії «Вимпелком», виявивши даний сайт, самостійно зібрали докази злочинної діяльності сайту і передали справу в МВС. Співробітники МВС порушили кримінальну справу і спільно з компанією «Вимпелком» встановили особи організаторів даного злочинного бізнесу. А 18 жовтня 2004 році було затримано на місці злочину головний підозрюваний.

Крім того, 26 листопада 2004 р були затримані інші шестеро підозрюваних, в числі яких були троє співробітників абонентської служби самої компанії «Вимпелком». В ході слідства з'ясувалося, що сайт був створений колишнім студентом Московського державного університету, який не працював в даній компанії.

5) Наприкінці 1999 року були виведені з ладу веб-сервери таких корпорацій, як Amazon, Yahoo, CNN, eBay, E-Trade і ряду інших, трохи менш відомих. Через рік, у грудні 2000-го «різдвяний сюрприз» повторився: сервери найбільших корпорацій були атаковані за технологією DDoS при повному безсиллі мережевих адміністраторів. З тих пір повідомлення

про DDoS-атаки вже не є сенсацією. Головною небезпекою тут є простота організації і те, що ресурси хакерів є практично необмеженими, так як атака є розподіленою.

6) Японська фірма Dai Nippon Printing, що спеціалізується на випуску поліграфічної продукції, допустила найбільший витік інформації в історії своєї країни. Хирофумі Йокояма, колишній співробітник одного з підрядників компанії, скопіював на мобільний вінчестер і вкрав персональні дані клієнтів фірми. В цілому під загрозу потрапили 8,64 млн. чоловік, так як викрадена інформація містила імена, адреси, телефони і номери кредитних карт. У викраденій інформації містилися відомості про клієнтів 43 різних компаній, наприклад про 1 504 857 клієнтів компанії American Home Assurance, 581 293 клієнтів компанії Aeon Co та 439 222 клієнтів NTT Finance.

7) Звільнившись, колишній системний адміністратор вирішив повернути у колишнього керівництва інтерес до своєї персони з використанням недосконалості системи «Банк-Клієнт», яка застосовується практично у всіх банках України. План системного адміністратора полягав у тому, що він вирішив розробити свою програму захисту і запропонувати її банку, повернувшись на своє колишнє місце роботи. Реалізація плану полягала в проникненні в систему «Банк-Клієнт» і внесенні в неї мінімальних змін. Весь розрахунок був зроблений на те, що в банку повинні були виявити злом системи.

Для проникнення в зазначену систему колишній системний адміністратор скористався паролями і кодами, які дізнався ще в процесі роботи з даною системою. Вся інша інформація, необхідна для злому, була отримана з різних хакерських сайтів, де в подробицях були розписані різні випадки зломів комп'ютерних мереж, методики злому і там же розміщувалося все необхідне для злому програмне забезпечення.

Створивши в системі лазівку, колишній системний адміністратор періодично проникав в комп'ютерну систему банку і залишав в ній різні знаки, намагаючись привернути увагу до фактів злому. Фахівці банку повинні були виявити злом і забити тривогу, але, на його подив, проникнення в систему ніхто навіть не помічав.

Тоді системний адміністратор вирішив змінити свій план, внісши в нього корективи, які б не змогли залишитися непоміченими. Він вирішив підробити платіжне доручення і перевести по ньому через комп'ютерну систему банку велику суму. За допомогою ноутбука і мобільного телефону з вбудованим модемом системний адміністратор близько 30 разів проникав в комп'ютерну систему банку: переглядав документи, рахунки клієнтів, рух грошових коштів – в пошуках відповідних клієнтів. В якості таких клієнтів ним були обрані регіональна митниця і дніпропетровська фірма-банкрут.

Отримавши в черговий раз доступ до системи банку, він створив платіжне доручення, в якому з особового рахунку регіональної митниці зняв і перерахував через банк на рахунок фірми-банкрута 5 млн. гривень. Крім того, ним цілеспрямовано було зроблено кілька помилок в «платіжці», що в свою чергу повинно було ще більше сприяти привернення уваги з боку фахівців банку. Однак навіть такі факти не були помічені фахівцями банку, які обслуговували систему «Банк-Клієнт», і вони спокійно перерахували 5 млн гривень на рахунок вже не існуючої фірми.

Насправді системний адміністратор розраховував на те, що грошові кошти не будуть переказані, що факт злому буде виявлений до переказу коштів, але на практиці все виявилося по-іншому і він став злочинцем і його липовий переказ переріс в крадіжку.

4. На основі проведеного аналізу заповнити таблицю аналізу інцидентів ІБ та виявлених загроз (для кожного з розглянутих інцидентів ІБ), яку наведено в додатку 2.

5. Доповнити таблицю трьома різнорідними інцидентами, які б охоплювали всі можливі варіанти реалізованих загроз.

6. На основі отриманих результатів (по можливості) сформувати та описати дерево загроз, а також провести класифікацію всіх виявлених (реалізованих) загроз інформаційної безпеки за наступними ознаками:

- за природою виникнення та способом здійснення (випадкові/навмисні, дії природного/штучного характеру);
- за розташуванням джерела загроз (всередині/поза межами контрольованої зони);
- за властивістю інформації, що порушується (доступність, цілісність, конфіденційність), проти якої загрози спрямовані в першу чергу.

7. Оформити звіт згідно до вимог (додаток 1).

8. Відповісти на контрольні питання та підготуватися до письмового опитування.

Зміст звіту:

1. Титульний лист.
2. Постановка завдання.
3. Опис усіх розглянутих інцидентів інформаційної безпеки.
4. Сформована таблиця аналізу інцидентів інформаційної безпеки та виявлених загроз.
5. Побудоване дерево загроз з коротким його описом.
6. Результати проведення класифікації виявлених загроз інформаційної безпеки.
7. Висновки.

Контрольні питання:

1. Надати визначення наступним поняттям: інформація, інформаційна безпека, захист інформації, кіберпростір, кібербезпека, загроза ІБ, інформаційний актив.
2. Коротко описати класифікацію інформації відповідно до порядку доступу до неї.
3. Назвати та коротко охарактеризувати основні властивості інформації.
4. Описати типовий склад інформаційно-телекомунікаційних систем.
5. Перелічити основні джерела загроз.
6. Навести відому вам класифікацію загроз.

7. Надати визначення поняттю «ненавмисні штучні загрози», та навести приклади даних загроз.
8. Надати визначення поняттю «навмисні штучні загрози», та навести приклади даних загроз.

Лабораторна робота №8
«Аналіз ризиків та основні принципи забезпечення інформаційної безпеки»

Мета роботи:

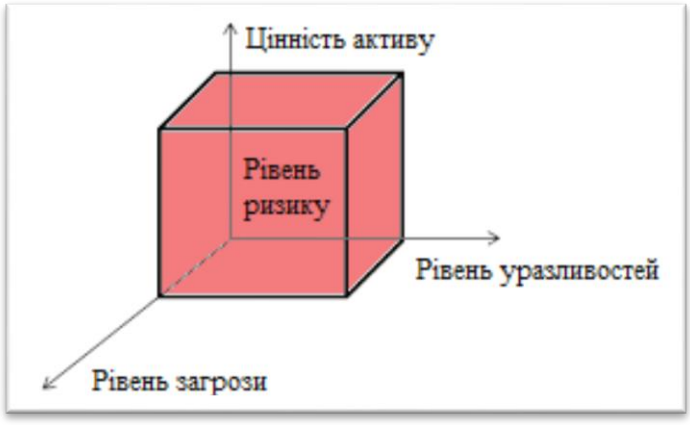
1. Поглиблення та закріплення теоретичних знання з наступних питань:
   - поняття ризиків інформаційної безпеки та їх аналіз;
   - основні принципи та методи забезпечення інформаційної безпеки.
2. Ознайомлення та дослідження алгоритму оцінки ризиків інформаційної безпеки організації.
3. Набуття практичних навичок щодо застосування методики матричного аналізу ризиків інформаційної безпеки та надання основних рекомендацій з забезпечення ІБ.

Стислі теоретичні відомості:

8.1. Поняття ризиків інформаційної безпеки

Порушення основних властивостей інформації може стати серйозною загрозою для організацій в даний час. Інформацію важче контролювати і вона піддається зростаючому числу загроз і вразливостей, в тому числі комп'ютерному шахрайству, шпигунству, саботажу, вандалізму, пожежі або повені. Інформаційні ресурси, як і матеріальні, володіють якістю та кількістю, мають собівартість і ціну. Оцінка ризиків є важливою частиною будь-якого процесу інформаційної безпеки. Її використовують для визначення масштабу загроз інформаційної безпеки та ймовірності реалізації цих загрози.

В зв'язку з цим, також необхідно володіти таким поняття як ***ризик інформаційної безпеки*** – потенційна можливість використання загрозою вразливостей інформаційного активу або групи активів для заподіяння шкоди об'єктам або інтересам суб'єктів інформаційних відносин.



Виходячи з визначення ризику, для проведення аналізу ризиків нам потрібні наступні дані про інформаційну систему:

перелік цінної інформації із зазначенням її рівня критичності, відомості про уразливість інформаційної системи і загрози, які на неї діють.

При цьому необхідно відзначити, що жоден найдосконаліший спосіб зниження ризиків інформаційної безпеки, будь це політика безпеки, що досконально опрацьована, або найсучасніший брандмауер, не може захистити від виникнення в інформаційному середовищі подій, що потенційно несуть загрозу діяльності організації. Складність і різноманітність середовища діяльності сучасного підприємства зумовлюють наявність залишкових ризиків незалежно від якості підготовки і впровадження заходів протидії. Також завжди існує вірогідність реалізації нових, невідомих до теперішнього часу, загроз інформаційній безпеці. Неготовність організації до обробки подібного роду ситуацій може істотно ускладнити відновлення бізнес-процесів та потенційно збільшити завдані збитки. Саме тому й проводиться аналіз та оцінка ризиків ІБ.

8.2. Аналіз ризиків інформаційної безпеки – матричний підхід

Розрізняють два методи аналізу та оцінки ризиків: ***кількісний*** та ***якісний***.

Для кількісної оцінки ризиків характерне використання об’єктивних чисельних, а саме фінансових характеристик. На відміну від кількісного, якісний аналіз ризиків не ставить своїм завданням отримання чисельних фінансових характеристик. Для оцінки активів і критичність загроз вводиться якісна неформальна або напівформальна шкала, і основною метою такого аналізу стає ранжування загроз відповідно з обраними критеріями.

Оскільки даний курс присвячений основам інформаційній та кібернетичній безпеці, а не менеджменту ІБ, в лабораторній роботі буде розглянуто один із якісних методів аналізу ризиків, а саме матричний підхід аналізу ризиків ІБ, який пов’язує активи, уразливості, загрози та засоби контролю (міри, які організація може прийняти для мінімізації дій загроз на один чи більше активів) і визначає важливість різних засобів контролю, відповідним активам організації.

Матричний підхід використовує три окремих матриці: матрицю уразливостей, матрицю загроз і матрицю засобів контролю, які дозволяють зібрати всі необхідні дані для аналізу ризиків ІБ.

Матриця уразливостей складається із взаємозв’язків між активами і уразливостями в організації, в свою чергу матриця загроз відображає взаємозв’язки між уразливостями і загрозами, а матриця засобів контролю містить взаємозв’язки між загрозами і засобами контролю. Таким чином, кожна клітинка в таблиці відображає значення взаємозв’язку між елементами рядків

та стовпців. В даному методі використовується наступна шкала взаємозв'язку (оцінки впливу): немає впливу, слабкий, помірний, сильний вплив.

При первинному аналізі ризиків формуються списки активів, уразливостей, загроз, засобів контролю, які в подальшому додаються до відповідних таблиць. Матриці заповнюються поступово шляхом додавання даних щодо взаємозв'язку елементів стовпця матриці з елементами рядка. Спершу заповнюється матриця уразливостей, дані якої обчислюються за допомогою формули (8.1), для визначення вагомості (значущість) уразливостей, після чого останні переносяться до наступної матриці – матриці загроз. Аналогічно, дані в матриці загроз обчислюються за допомогою формули (8.2), таким чином визначаючи потенційні ризики ІБ, а самі загрози переносяться до останньої таблиці. В результаті чого, формується матриця контролю, яка містить відносну важливість різних засобів контролю. Дана матриця визначає необхідність в застосуванні конкретних мір або засобів захисту для мінімізації впливу загроз на один або більше активів організації зменшуючи рівень ризиків (демонструючи «чистий ризик» – ризик з мінімізованою реалізацією загроз).

Матриця уразливостей Шкала взаємозв'язку немає 0 · слабкий 1 · помірний 3 · сильний 9 Ранг пріоритету (РП) 1 – незначний 2 – невеликий 3 – середній 4 – серйозний 5 – критичний $C_j \leftarrow$	**Активи:**	Секрети виробництва	Конфіденційна інформація	Репутація (довіра)	Апаратне забезпечення	Програмне забезпечення	Послуги	Комунікації	**Всього**	**Ранжування**
Уразливості:	РП								Σ	
Веб-сервер										
Обчислювальний сервер										
Міжмережевий екран										
Маршрутизатор										
Клієнтський вузол										
База даних										

Таблиця 8.1. Матриця уразливостей (взаємозв'язок між активами та уразливостями)

Припустимо, що є m активів, де відносна вартість активу a_j є $C_j\,(j=1,...,m)$. Також нехай v_{ij} – це відносний вплив уразливості v_i на актив a_j. Тоді потенційний вплив уразливості V_i на активи організації обчислюється за формулою:

$$V_i = \sum_{j=1}^{m} v_{ij} \cdot C_j \qquad 8.1$$

Матриця загроз Шкала взаємозв'язку немає 0 · слабкий 1 · помірний 3 · сильний 9 Ранг пріоритету (РП) 1 – незначний 2 – невеликий 3 – середній 4 – серйозний 5 – критичний $V_i \leftarrow$	**Уразливості:**	Веб-сервер	Обчислювальний сервер	Міжмережевий екран	Маршрутизатор	Клієнтський вузол	База даних	Передача даних	**Всього**	**Ранжування**
Загрози:	РП								∑	
Відмова в обслуговуванні (DoS)										
Шкідливе ПЗ										
Помилки користувача										
Спам										
«Фішинг»										
Ворожий агент										

Таблиця 8.2. Матриця загроз (взаємозв'язок між уразливостями та загрозами)

Давайте припустимо, що існує p загроз, які можуть бути реалізовані за допомогою n уразливостей і t_{ki} – відносна можливість використання загрозою t_k уразливості v_i. Тоді потенційна реалізація конкретної загрози T_k обчислюється за формулою:

$$T_k = \sum_{i=1}^{n} t_{ki} \cdot V_i \qquad 8.2$$

Матриця контролю Шкала взаємозв'язку немає 0 · слабкий 1 · помірний 3 · сильний 9 Ранг пріоритету (РП) 1 – незначний 2 – невеликий 3 – середній 4 – серйозний 5 – критичний $T_k \leftarrow$	**Загрози:**	Відмова в обслуговуванні (DoS)	Шкідливе ПЗ	Помилки користувача	Спам	«Фішинг»	Ворожий агент	Збій електроживлення	**Всього**	**Ранжування**
Засоби контролю:	РП								∑	
Система виявлення вторгнень (IDS)										
Навчання персоналу										
Міжмережевий екран										
Політика безпеки										

Конфігурація архітектури мережі										
Демілітаризована зона (DMZ)										

Таблиця 8.3. Матриця контролю (взаємозв'язок між загрозами та засобами захисту)

Припустимо, що є q засобів контролю (захисту), які можуть пом'якшити (мінімізувати) вплив p загроз, а z_{lk} – відносний вплив засобу контролю z_l на загрозу t_k. Тоді потенційне пом'якшення загроз за допомогою конкретного засобу контролю – Z_l, обчислюється за формулою:

$$Z_l = \sum_{l=1}^{p} z_{lk} \cdot T_k \qquad 8.3$$

Таким чином, за допомогою даної методики проводиться якісний аналіз ризиків: оцінюються активи організації, виділяються основні уразливості та критичні загрози, а також визначаються найвагоміші засоби контролю, в результаті чого ми одержуємо демонстрацію «чистого ризику», тобто ризику з мінімізованим впливом загроз на активи організації. І вже на основі даних результатів визначається доцільність використання тих чи інших механізмів забезпечення безпеки, надаються рекомендацій щодо побудови систем захисту інформації та плануються витрати на ІБ організації.

8.2.1. Приклад використання методики аналізу ризиків ІБ

Дослідження аналізу ризиків за допомогою запропонованої методики буде здійснюватися на прикладі компанії «Cyberstec», яка займається розробкою програмного забезпечення. На даний момент компанія займається розробкою проектів в основному зосереджених в таких областях як: безпека робочих станцій і мережева безпека, віртуалізація та віддалений доступ, управління поведінкою системи, обробка даних, робота з мобільними пристроями. Вона має фрагментовану організаційну структуру, працює у декількох містах України (Київ, Львів, Харків, Одеса), а також має бізнес-представництво у місті Мюнхен (Німеччина). Це достатньо конкурентний бізнес, де постійно розвиваються IT-технології і виробники постійно намагаються обійти один одного, таким чином, інформаційна безпека – є критичним фактором для захисту активів компанії і запобіганню зриву її діяльності.

Саме тому, для правильної організації системи безпеки, вибору конкретних методів захисту, та планування витрат на ІБ, в компанії проводиться аналіз інформаційних ризиків за допомогою запропонованої методики. Три матриці, які пов'язують активи та уразливості, уразливості та

загрози, загрози та засоби контролю, представлені в таблицях 8.4, 8.5 та 8.6 відповідно.

Таким чином, у таблиці 8.4 представлено матрицю уразливостей, яка пов’язує уразливості та активи компанії «Cyberstec». Для побудови матриці була визначена відносна цінність активів та проведено їхнє ранжування (з права на ліво). Наприклад, успішність компанії залежить від її здатності розвивати і захищати нові технології; тому вони високо оцінюються. Ґрунтуючись на активах, було визначено ключові уразливості, надано їм ранг пріоритету та встановлено відносний вплив уразливостей на активи компанії. Так як зовнішні порушники (хакери) спершу повинні обійти брандмауер, щоб отримати доступ до конфіденційної інформації, він займає перше місце у матриці уразливостей. Окрім того, як було зазначено раніше, філії компанії територіально розкидані, тому передача та синхронізація даних також оцінюються високо.

Матриця уразливостей Шкала взаємозв’язку немає 0 / слабкий 1 / помірний 3 / сильний 9 Ранг пріоритету (РП) 1 – незначний 2 – невеликий 3 – середній 4 – серйозний 5 – критичний $C_j \leftarrow$	**Активи:**	Новітні розробки (технології)	Конф. інф. (програмний код)	Репутація (довіра)	Доступність сервісів	Комунікації	Програмне забезпечення	Апаратне забезпечення	**Всього**	**Ранжування**
Уразливості:	РП	7	6	5	4	3	2	1	∑	
Брандмауер	5	9	9	3	9	9	9	9	222	9
Передача даних та лінії зв’язку	5	9	9	3	9	9	3	9	210	8
Фізична безпека	4	9	9	3	1	1	3	9	154	5
Помилки конфігурації серверів екстранет	4	9	9	1	9	3	9	1	186	7
ПК співробітників компанії	3	3	9	1	0	1	9	3	104	2
Бази даних	4	9	9	3	3	1	9	1	166	6
Стійкість паролів	3	9	9	1	1	3	9	1	154	4
Помилки конфігурації серверів інтернет	2	1	1	9	9	3	9	1	122	3
Ненадійне джерело живлення	1	0	0	3	9	9	0	1	79	1

Таблиця 8.4. Матриця уразливостей «Cyberstec»

В результаті, як бачимо, в матриці було проведено обчислення потенційного впливу уразливостей на активи «Cyberstec» за формулою (8.1) для того, щоб відранжувати уразливості і таким чином визначити їхню значущість. Після цього уразливості були перенесені до наступної матриці.

Беручи до уваги наявні уразливості в активах компанії, було визначено ключові загрози, надано їм ранг пріоритету та аналогічним чином, встановлено відносну можливість використання загрозою уразливості.

Матриця загроз Шкала взаємозв'язку немає 0 слабкий 1 помірний 3 сильний 9 Ранг пріоритету (РП) 1 – незначний 2 – невеликий 3 – середній 4 – серйозний 5 – критичний $V_i \leftarrow$	**Уразливості:**	Брандмауер	Передача даних та лінії зв'язку	Помилки конфігурації серверів екстранет	Бази даних	Фізична безпека	Стійкість паролів	Помилки конфігурації серверів інтернет	ПК співробітників компанії	Ненадійне джерело живлення	**Всього**	**Ранжування**
Загрози:	РП	9	8	7	6	5	4	3	2	1	∑	
Відмова в обслуговуванні (DoS/DDos)	5	9	9	9	0	1	1	9	1	1	255	5
Шкідливе ПЗ	4	1	1	9	1	1	1	3	9	1	123	2
Помилки працівника	2	1	1	3	3	3	3	3	9	1	111	1
Збої сервера	5	9	9	9	9	9	1	9	1	9	357	8
Вторгнення (атака на пароль)	3	9	3	9	9	1	9	3	3	1	279	6
Фізичне пошкодження ІТС	3	1	9	3	3	9	0	3	3	3	183	3
«Спуфінг» та «Маскарад»	2	1	9	9	3	1	1	9	9	1	217	4
НСД	5	9	3	9	9	9	9	9	9	1	349	7

Таблиця 8.5. Матриця загроз «Cyberstec»

В результаті обчислень за допомогою формули (8.2), було визначено потенційні ризики ІБ, а самі загрози переносяться до останньої таблиці.

Матриця контролю Шкала взаємозв'язку немає 0 слабкий 1 помірний 3 сильний 9 Ранг пріоритету (РП) 1 – незначний 2 – невеликий 3 – середній 4 – серйозний 5 – критичний $T_k \leftarrow$	**Загрози:**	Збої сервера	НСД	Вторгнення (атака на пароль)	Відмова в обслуговуванні	«Спуфінг» та «Маскарад»	Фізичне пошкодження ІТС	Шкідливе ПЗ	Помилки працівника	**Всього**	**Ранжування**
Засоби контролю:	РП	8	7	6	5	4	3	2	1	∑	
Система виявлення вторгнень (IDS)	5	9	9	3	9	9	1	3	3	246	6
Навчання персоналу	2	1	0	9	0	3	3	9	9	110	1
Міжмережеві екрани	5	9	9	9	9	9	1	3	1	280	7

Політика безпеки	4	1	9	9	3	9	1	9	3	200	4
Конфігурація архітектури мережі	5	9	3	1	9	1	0	0	1	149	2
Демілітаризована зона (DMZ)	3	9	9	3	9	3	0	0	3	213	5
Контроль території	4	3	9	9	1	1	9	3	1	184	3

Таблиця 8.6. Матриця контролю «Cyberstec»

Останньою формується матриця контролю, до якої, окрім загроз, були внесені запропоновані засоби контролю з відповідним рангом пріоритету. Після чого було встановлено відносний вплив засобу контролю на загрозу з використанням суб'єктивних суджень, і обчислено за формулою (8.3) потенційне пом'якшення загроз. Отримані дані були відранжовані з метою визначення пріоритетних засобів контролю. Ця інформація, в поєднанні з вартістю засобів контролю використовується для планування ІБ.

Таким чином, результати аналізу і узагальнення даних, що містяться в матрицях будуть використовуватися під час процесу інтеграції та вибору програмного забезпечення і апаратного устаткування в компанії «Cyberstec».

8.3. Основні принципи та методи забезпечення інформаційної безпеки

З метою протидії основним загрозам ІБ, система забезпечення інформаційної безпеки ІТС повинна вирішувати наступні завдання:

1) розмежування та контроль доступу користувачів до ресурсів ІТС;
2) захист всіх даних, що передаються по каналах зв'язку;
3) реєстрація, збір, зберігання, обробка і видача інформації про всі події, що відбуваються в системі і мають відношення до забезпечення її безпеки;
4) моніторинг роботи користувачів ІТС системою захисту інформації та оперативне сповіщення адміністратора безпеки про спроби несанкціонованого доступу до ресурсів системи;
5) забезпечення замкнутого середовища функціонування вже перевіреного ПЗ з метою захисту від неконтрольованого впровадження в систему потенційно небезпечних програм (які можуть містити «закладки» або критичні помилки) і засобів подолання системи захисту, а також від впровадження та поширення шкідливого ПЗ;
6) забезпечення доступності інформаційних ресурсів шляхом резервного копіювання даних;
7) забезпечення та контроль цілісності критичних ресурсів системи захисту ІТС.

Також необхідно відмітити, що розрізняють зовнішню та внутрішню безпеку ІТС. Зовнішня безпека полягає в захисті ІТС від загроз природного походження, а також від проникнення в систему зловмисників ззовні.

Внутрішня ж безпека повинна створювати надійний і зручний механізм регламентування діяльності усіх законних користувачів та обслуговуючого персоналу ІТС, а також забезпечувати цілісність даних.

Що стосується ***методів забезпечення інформаційної безпеки*** то вони достатньо різноманітні, однак їх можна розділити на наступні основні групи: теоретичні, законодавчі (правові), адміністративні (організаційні), інженерно-технічні (програмно-технічні) та криптографічні.

Теоретичні методи забезпечення інформаційної безпеки вирішують два основних завдання. Перше з яких – формалізація різного роду процесів, пов'язаних із забезпеченням інформаційної безпеки. Так, наприклад, формальні моделі управління доступом дозволяють строго описати всі можливі інформаційні потоки в системі – а значить, гарантувати виконання необхідних властивостей безпеки. Звідси безпосередньо випливає друге завдання – суворе обґрунтування коректності і адекватності функціонування систем забезпечення інформаційної безпеки при проведенні аналізу їх захищеності. Така задача виникає, наприклад, при проведенні сертифікації автоматизованих систем за вимогами безпеки інформації.

Законодавчі міри захисту визначаються діючими в країні нормативно-правовими актами, що регламентують правила поводження з інформацією, що закріплюють права та обов'язки учасників інформаційних відносин у процесі її обробки та використання, а також встановлюють відповідальність за порушення цих правил. Важливе значення мають стандарти в області захисту інформації (у першу чергу, міжнародні). Серед цих стандартів виділяються «Помаранчева книга», рекомендації X. 800 і «Загальні критерії оцінки безпеки інформаційних технологій».

Адміністративні методи захисту – методи організаційного характеру, які регламентують процеси функціонування ІТС, діяльність персоналу, а також порядок взаємодії користувачів із системою таким чином, щоб найбільшою мірою мінімізувати або виключити можливість реалізації загроз безпеки. Зазвичай вони включають:

- підбір та підготовку персоналу системи;
- організацію охорони та контрольно-пропускного режиму;
- організацію обліку, зберігання, використання та знищення документів та носіїв з інформацією;
- розподіл атрибутів розмежування доступу (паролів, ключів шифрування тощо).

Основою адміністративних методів захисту інформації є формування *політика безпеки* організації – сукупність вимог, правил, обмежень, рекомендацій, які регламентують порядок інформаційної діяльності в

організації і спрямовані на досягнення і підтримку стану інформаційної безпеки організації.

Криптографічні методи захисту інформації реалізується шляхом перетворення інформації (шифрування, кодування та інші перетворення) з використанням спеціальних (ключових) даних та алгоритму зворотного перетворення з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо. Можна стверджувати, що на теперішній час, криптографічний метод захисту є одним із найбільш надійніших методів захисту, оскільки захищається безпосередньо сама інформація, а не доступ до неї.

Інженерно-технічні методи захисту інформації засновані на використанні спеціальних інженерно-технічних заходів, апаратних засобів і програмного забезпечення, що входять до складу ІТС і унеможливлюють виток, знищення або блокування інформації, порушення цілісності та режиму доступу до неї.

Однак, необхідно відзначити, що універсальних методів захисту не існує, і тому під час вирішення питання щодо захисту інформації потрібно обов'язково враховувати критичність інформаційних активів, усі наявні ризики, а вже потім використовувати конкретні механізми забезпечення безпеки та планувати витрати на ІБ. Багато в чому успіх при побудові механізмів безпеки для реальної системи буде залежати від її індивідуальних особливостей, облік яких погано піддається формалізації. Тому часто інформаційну безпеку розглядають як певну сукупність неформальних рекомендацій щодо побудови систем захисту інформації того чи іншого типу.

Порядок виконання лабораторної роботи №8:

1. Включити ПК.
2. Ознайомитися з короткими теоретичними відомостями.
3. Провести якісний аналіз та оцінку ризиків інформаційної безпеки організації (згідно варіанту в табл. 8.7) за допомогою матричного підходу.
4. На основі отриманих результатів, надати основні рекомендації щодо забезпечення ІБ в даній організації.
5. Оформити звіт згідно до вимог (додаток 1).
6. Відповісти на контрольні питання та підготуватися до усного опитування.

Зміст звіту:

1. Титульний лист.
2. Постановка завдання.

3. Короткі відомості про організацію в якій буде проводитися аналіз та оцінка ризиків ІБ.

4. Сформовані списки та обґрунтування інформаційних активів організації, ймовірних уразливостей, загроз та засобів контролю.

5. Сформовані, заповнені та оброблені 3 матриці: матриця уразливостей, матриця загроз та матриця контролю.

6. Основні рекомендації щодо забезпечення інформаційної безпеки в даній організації.

7. Висновки та відповіді на контрольні питання.

Завдання на виконання лабораторної роботи №8

Таблиця № 8.7. (варіант відповідно до номера за списком у журналі)

Номер варіанта	Організація	Кількість інформаційних активів
1	Державний комерційний банк	8
2	Приватна поліклініка	9
3	Страхова компанія	7
4	Інтернет-магазин	9
5	Адвокатська контора	8
6	Агентство нерухомості	7
7	Рекламне агентство	7
8	Науково-проектне підприємство	9
9	Аудиторська компанія	8
10	Туристичне агентство	7
11	Консалтингова фірма	9
12	Фармакологічна компанія	8
13	Архітектурне агентство	7
14	Інтернет-провайдер	7
15	Будівельна компанія	8
16	Система електронних платежів	9
17	Видавництво	7
18	Благодійний фонд	8
19	Рекрутингове агентство	7
20	Міжнародний комерційний банк	9
21	Військове підприємство	6
22	Компанія-розробник ПЗ	9
23	Дизайнерська фірма	8

24	Організація з розробки електроніки	9
25	Державна поліклініка	8
26	Авіакомпанія	9
27	Редакція газети	7

Контрольні питання:

1. Надати визначення наступним поняттям: ризик ІБ.
2. Коротко описати алгоритм аналізу ризиків інформаційної безпеки організації.
3. Які повинна вирішувати завдання система забезпечення інформаційної безпеки ІТС?
4. Коротко охарактеризувати основні групи методів забезпечення ІБ.

РОЗДІЛ 3 МЕТОДОЛОГІЯ ЗАХИСТУ ІНФОРМАЦІЇ

Лабораторна робота №9
«Контроль доступу користувачів до інформаційно-телекомунікаційної системи. Парольна аутентифікація»

Мета роботи:

1. Поглиблення теоретичних знання з наступних питань:
   - контроль доступу користувачів до ІТС;
   - особливості парольних систем аутентифікації.
2. Вивчення технології аутентифікації користувача на основі пароля.
3. Проведення кількісної оцінки стійкості парольного захисту та реалізація найпростішого генератора паролів.

Стислі теоретичні відомості:

9.1. Контроль доступу користувачів до ІТС

Важливим елементом забезпечення цілісності та конфіденційної інформації є захист від несанкціонованого доступу до ресурсів інформаційних систем, що викликає необхідність створення надійних і зручних систем контролю доступу.

Контроль доступу – функція системи захисту інформації (СЗІ), яка дозволяє або забороняє доступ до певних типів даних.

Контроль доступу є одним із найбільш важливих елементів СЗІ в інформаційно-телекомунікаційних системах. Доступ до захищеної інформації повинен бути обмежений, щоб тільки люди, які мають право доступу, могли отримувати цю інформацію. Комп’ютерні програми і в багатьох випадках сторонні комп’ютери за допомогою локальної мережі, Інтернету, бездротової мережі можуть отримати секретну інформацію, яка не призначена їм. Це може завдати як фінансові, так і інформаційні втрати. У зв’язку з цим необхідний механізм контролю доступу до захищеної інформації. Складність механізмів контролю доступу, як зазначалось на попередньому занятті, має бути в паритеті з цінністю інформації, тобто чим більш важливою або цінною є інформація, тим більш складними повинні бути механізми контролю доступу. Основними механізмами контролю доступу є ***ідентифікація*** та ***аутентифікація***.

Кожний користувач сучасних інформаційно-телекомунікаційних систем декілька разів на день стикається з процедурами ідентифікації та аутентифікації. Ці процедури виконуються кожного разу, коли користувач вводить пароль для доступу до інформаційної системи, мережі, бази даних або

при запуску прикладної програми. Таким чином ідентифікація та аутентифікація це перша лінія оборони, «прохідна» інформаційного простору організації. В результаті їх виконання користувач або отримує допуск до роботи в інформаційній системі, або ні.

Під ***ідентифікацією*** (від лат. *Identifico* – ототожнювати) розуміють процедуру розпізнавання користувача в системі, як правило, за допомогою наперед визначеного імені (ідентифікатора) або іншої апріорної інформації про нього, яка сприймається системою. Ідентифікація використовується для отримання інформації про суб'єкт системи на основі наданого ним ідентифікатора. Є початковою процедурою надання доступу до системи. Після неї здійснюється аутентифікація та авторизація.

В свою чергу ***аутентифікація*** (з грец. αυθεντικός – реальний або істинний) особи в інформаційній системі – це перевірка приналежності суб'єкту доступу пред'явленого ним ідентифікатора та підтвердження його достовірності, за допомогою деякої унікальної інформації (паролю, відбитка пальця, голосу тощо). З позицій інформаційної безпеки аутентифікація є частиною процедури надання доступу до інформаційної системи, наступною після ідентифікації, та передує авторизації.

Таким чином, ідентифікація дозволяє суб'єкту (користувачеві, процесу, що діє від імені певного користувача, або іншого апаратно-програмного компоненту) назвати себе (повідомити своє ім'я). За допомогою аутентифікації друга сторона переконується, що суб'єкт дійсно той, за кого він себе видає. Як синонім слова «аутентифікація» іноді використовують словосполучення «перевірка справжності»[5].

Базову схему ідентифікації та аутентифікації відображено на рис. 9.1.

На представленій схемі враховуються можливі помилки оператора при проведенні процедури ідентифікації та аутентифікації: якщо процедури не були виконані, але допустиме число спроб не перевищено, користувачеві пропонується пройти їх ще раз.

Стійкість підсистеми ідентифікації та аутентифікації користувача в СЗІ багато в чому визначає стійкість до злому самої СЗІ. Дана стійкість визначається гарантією того, що зловмисник не зможе пройти аутентифікацію, привласнивши чужий ідентифікатор або вкравши його. В зв'язку з цим існують різні методи ідентифікації та аутентифікації користувачів інформаційної системи, які відрізняються своєю складністю, надійністю, вартістю та іншими показниками. Кожний з цих методів має як позитивні, так і негативні сторони, тому далі проведемо їх короткий аналіз.

---

[5] *Тим самим, завдання ідентифікації – відповісти на питання «хто це?», а аутентифікації – «а чи він це насправді?».*

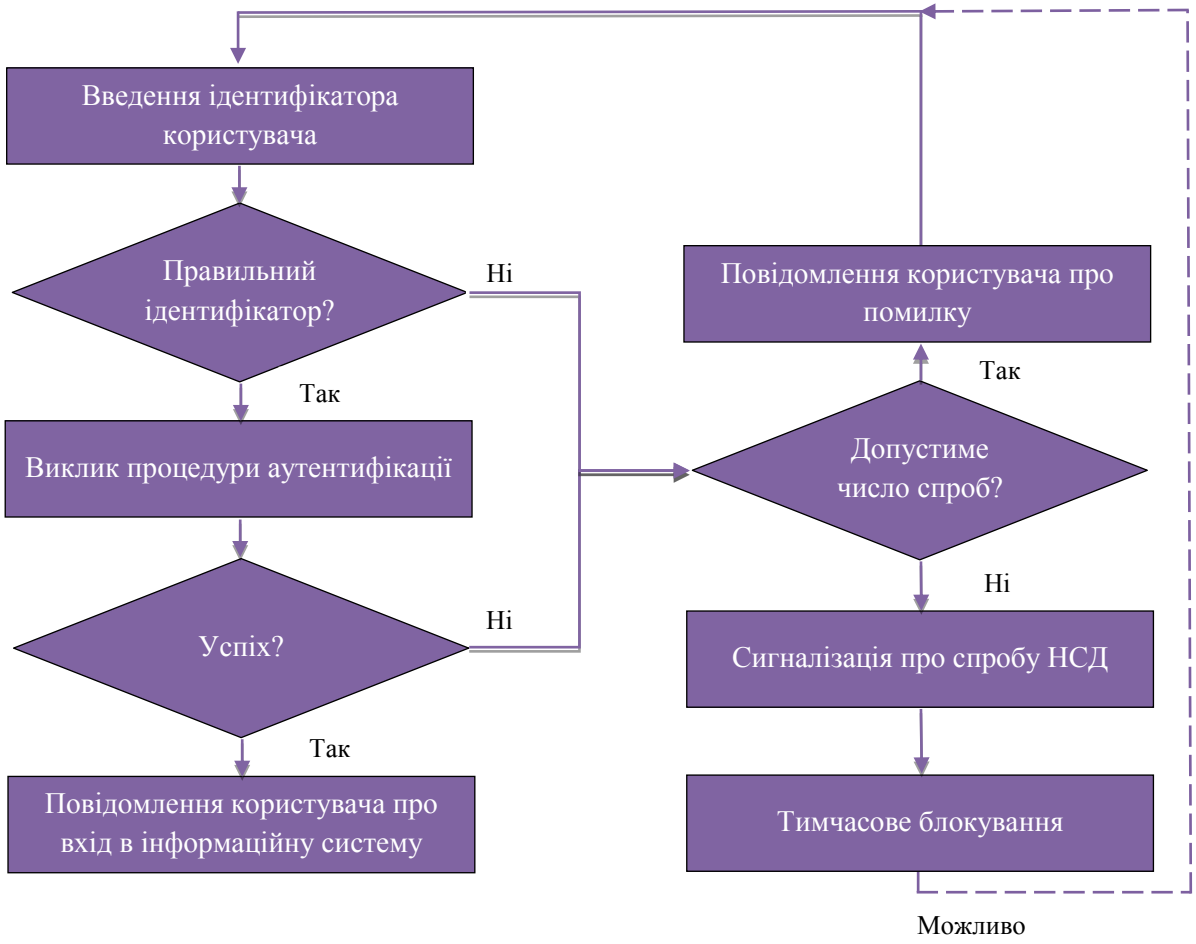


Рис. 9.1. Базова схема ідентифікації та аутентифікації

На сьогоднішній день, в інформаційних технологіях використовуються наступні види аутентифікації:

- однобічна аутентифікація – полягає в тому, що кожен клієнт системи для доступу до інформації обов'язково повинен доводити свою аутентичність;
- двобічна – полягає в тому, що окрім клієнта, свою аутентичність повинна підтверджувати і сама система;
- трибічна – полягає у використанні, так званої, нотаріальної служби аутентифікації для підтвердження достовірності кожного з партнерів при обміні інформацією.

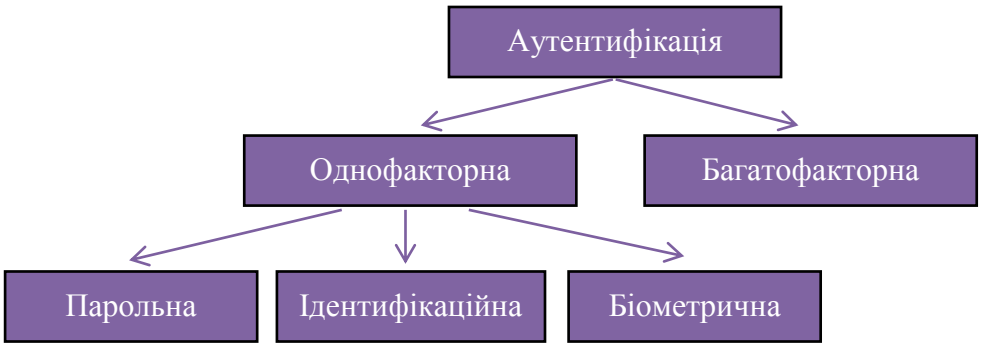


Рис. 9.2. Умовна класифікація методів аутентифікації

Методи аутентифікації умовно можна поділити (рис. 9.2) на однофакторні (слабкі, з точки зору безпеки) та багатофакторні (сильні)

Парольна система аутентифікації є одним із основних, простих та найбільш поширених методів. У цьому випадку при введенні суб'єктом свого пароля підсистема аутентифікації порівнює його з даними, які зберігаються в спеціальній захищеній базі еталонних даних в зашифрованому вигляді. У випадку успішної аутентифікації проводиться авторизація з подальшим отриманням певних повноважень і наданням доступ до конкретних ресурсів інформаційної системи.

Авторизація (*Authorization*) – процедура надання суб'єкту певних повноважень і ресурсів у даній системі, на основі введеного ним ідентифікатора та аутентифікатора (пароля). Іншими словами, авторизація встановлює сферу діяльності суб'єкта і доступні йому ресурси. Якщо система не може надійно відрізнити авторизовану особу від неавторизованої, в ній можуть бути порушені конфіденційність і цілісність інформації. Саме тому організації необхідно чітко визначити свої вимоги до безпеки та обрати відповідну модель безпеки, які будуть розглянуті на наступному занятті.

Парольні методи аутентифікації також можна розділити за ступенем змінності паролів:

- методи, що використовують постійні паролі (багаторазового використання);
- методи, що використовують одноразові паролі (динамічно змінюються).

Введення пароля, як правило, виконують з клавіатури або за допомогою сенсорного екрану.

Розглядаючи ідентифікаційну аутентифікацію потрібно відзначити, що у більшості випадків вона відбувається за допомогою унікальних предметів, які забезпечують більш надійний захист, ніж звична парольна аутентифікація. Ці предмети умовно поділяють на дві групи:

- *пасивні* предмети, які містять аутентифікаційну інформацію (наприклад, якийсь випадково згенерований пароль) і за вимогою передають її в модуль аутентифікації. При цьому, дана інформація може зберігатися як у захищеному вигляді (смарт-картки з захищеною пам'яттю, USB-токени) так і в відкритому (магнітні карти, смарт-карти з відкритою пам'яттю, електронні таблетки *Touch Memory*);
- *активні* предмети, які володіють достатніми обчислювальними ресурсами і беруть активну участь в процесі аутентифікації (мікропроцесорні смарт-карти і USB-токени).

Основний недолік вище зазначених методів ідентифікації та аутентифікації зумовлений неоднозначністю ідентифікованої особи. Передусім це пов’язано з тим, що для встановлення аутентичності особи застосовують атрибутивні й основані на певних відомостях розпізнавальні характеристики. Іншим важливим недоліком традиційних методів ідентифікації та аутентифікації, який випливає з вищезазначеного, є відсутність можливості виявлення підміни ідентифікованого користувача, що дає змогу зловмисникові отримати доступ до ресурсів системи, який обмежений тільки правами ідентифікованого користувача. Однак дані недоліки можна виправити, доповнивши систему захисту методами біометричної аутентифікації.

Біометричні методи аутентифікації працюють на основі використання устаткування для вимірювання і порівняння з еталоном заданих індивідуальних характеристик користувача. ***Біометрія*** – сукупність автоматизованих методів аутентифікації людей на основі їх фізіологічних (статичних), тобто унікальних, вроджених та невід’ємних від неї, і поведінкових характеристик (динамічних). До фізіологічних характеристик належать особливості відбитків пальців, сітківки та рогівки очей, геометрія руки й обличчя та ін. До поведінкових характеристик відносяться динаміка підпису, клавіатурний почерк, розпізнавання голосу. Такі засоби дозволяють з високою точністю розпізнати власника за конкретною біометричною ознакою, а підробити такі параметри практично неможливо.

І останніми методами аутентифікації які розглядаються на даній лабораторній роботі є багатофакторні методи, які отримують в результаті комбінації двох різних однофакторних методів, частіше всього ідентифікаційного та парольного. *Наприклад*: «пароль + USB-токен», «магнітна карта + PIN».

9.2. Особливості парольних систем аутентифікації

При всьому різноманітті існуючих механізмів аутентифікації, найбільш поширеним з них залишається парольний захист. Для цього є кілька причин, з яких ми відзначимо наступні:

- відносна простота реалізації, так як механізми захисту паролем зазвичай не вимагають залучення додаткових апаратних засобів;
- традиційність, оскільки механізми парольного захисту є звичними для більшості користувачів автоматизованих систем і не викликають психологічного відторгнення – на відміну, наприклад, від сканерів малюнка сітківки ока.

У той же час для парольних систем захисту характерний парадокс, що ускладнює їх ефективну реалізацію: стійкі паролі мало придатні для використання людиною. Дійсно, стійкість пароля виникає в міру його

ускладнення; але чим складніший пароль, тим важче його запам’ятати, і в користувача з’являється спокуса записати незручний пароль, що створює додаткові канали для його дискредитації.

Зупинимося більш детально на основних загроз безпеки парольних систем. У загальному випадку пароль може бути отриманий зловмисником одним з трьох основних способів:

1) *за рахунок використання слабкостей людського фактору*. В даному випадку методи отримання паролів можуть бути достатньо різноманітними: соціальна інженерія, підслуховування, підглядання, погрози, шантаж, і навіть, використання чужих облікових записів з дозволу їх законних власників;

2) *шляхом підбору*. Дана технологія народилася досить давно, але до цих пір використовується і дуже успішно. При цьому виділяють наступні методи:

- *повний перебір*. Даний метод дозволяє підібрати будь-який пароль в незалежності від його складності, проте для стійкого пароля час, необхідний для даної атаки, має значно перевищувати допустимі часові ресурси зловмисника;
- *підбір за словником*. Значна частина використовуваних на практиці паролів являє собою певні осмислені слова або вирази, на основі цього створюються словники найбільш поширених паролів, які в багатьох випадках дозволяють обійтися без повного перебору. Для того щоб досягти успіху в 60% випадків зазвичай досить словника розміром 50000 іменників. Величезне число інцидентів зі зломами систем змусило користувачів додавати до слів 1-2 цифри з кінця, записувати першу та/або останню букву у верхньому регістрі, використовувати «трансліт». Але як показали дослідження, навіть складання двох абсолютно не пов’язаних осмислених слів поспіль не дає достатньо реальної надійності пароля;
- *підбір з використанням відомостей про конкретного користувача*. Даний інтелектуальний метод підбору паролів ґрунтується на тому факті, що якщо політика безпеки системи передбачає самостійне призначення паролів користувачами, то в переважній більшості випадків в якості пароля буде обрана якась персональна інформація, пов’язана з користувачем АС. І хоча в якості такої інформації може бути вибрано що завгодно, від дня народження дружини і до прізвиська улюбленої домашньої тварини, наявність інформації про користувача дозволяє перевірити найбільш поширені варіанти (дні народження, імена дітей тощо);

3) *за рахунок використання недоліків реалізації самої парольної системи*. До таких недоліків реалізації відносяться критичні уразливості мережевих сервісів, які реалізуються в тих чи інших компонентах парольної системи захисту, несанкціонований доступ до носія інформації, на якому вони

містяться, або ж використання недокументованих можливостей відповідного програмного або апаратного забезпечення.

9.2.1. Рекомендації щодо практичної реалізації парольних систем

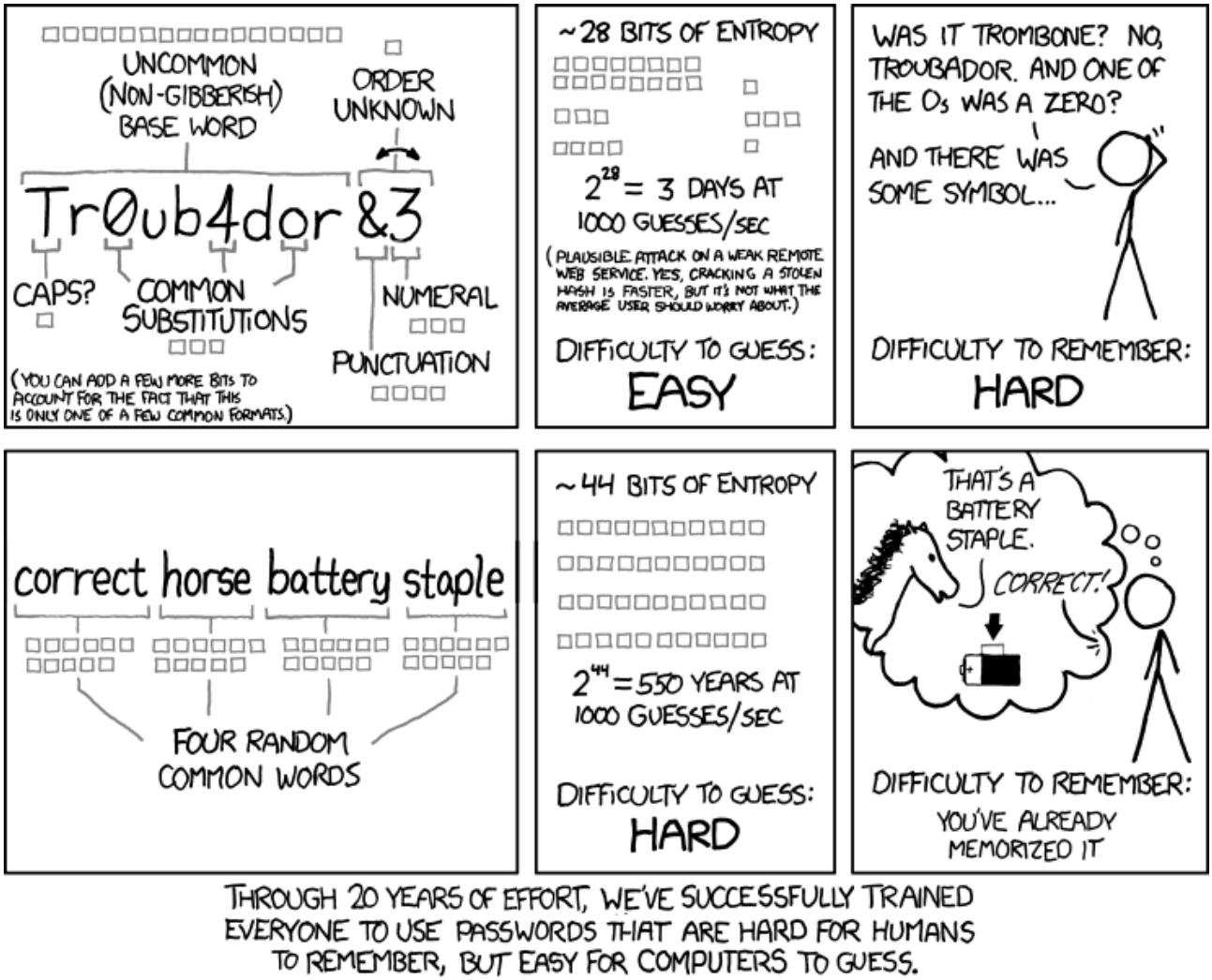
Як зазначалося раніше, парольна аутентифікація користувача, як правило, це передній край оборони СЗІ. У зв'язку з цим модуль такої аутентифікації найбільш часто піддається атакам з боку зловмисника, саме тому, при побудові системи парольного захисту необхідно враховувати специфіку ІТС і керуватися результатами проведеного аналізу ризиків. У той же час, до підсистеми парольної аутентифікації користувача можна привести наступні загальноприйняті **практичні рекомендації**:

- *чітке визначення мінімальної довжини пароля*. Очевидно, що регламентація мінімально допустимої довжини пароля ускладнює для зловмисника реалізацію підбору пароля шляхом повного перебору;
- *збільшення потужності алфавіту паролів*. За рахунок збільшення потужності (яке досягається, наприклад, шляхом обов'язкового використання спецсимволів) можна ускладнити повний перебір;
- *перевірка і заборона пароля за словником*. Даний механізм дозволяє ускладнити підбір пароля за словником за рахунок відбракування та заборони використання завідомо легких паролів;
- *встановлення максимального терміну дії пароля*. Логічно, що термін дії пароля обмежує проміжок часу, який зловмисник може затратити на підбір пароля. Тим самим, скорочення терміну дії пароля зменшує вірогідність його успішного підбору;
- *встановлення мінімального терміну дії пароля*. Даний механізм запобігає спробам користувача негайно змінити пароль на попередній;
- *відбраковування по журналу історії паролів*. Механізм запобігає повторному використанню паролів – можливо, раніше скомпрометованих;
- *встановлення обмежень числа спроб введення пароля*. Відповідний механізм ускладнює інтерактивний підбір паролів;
- *примусова зміна пароля при першому вході користувача в систему*. У разі, якщо первинну генерацію паролів для всіх користувач здійснює адміністратор, може бути запропоновано змінити початковий пароль при першому вході в систему – в цьому випадку новий пароль не буде відомий адміністратору;
- *тимчасове блокування при введенні неправильного пароля*. Механізм перешкоджає інтерактивному підбору паролів;

- *заборона створення пароля користувачем і автоматична генерація пароля*. Даний механізм дозволяє гарантувати стійкість згенерованих паролів – однак не варто забувати, що в цьому випадку у користувачів неминуче виникнуть проблеми із запам'ятовуванням паролів.

Що стосується вибору пароля, тут також встановлюються **основні мінімальні вимоги**:

- мінімальна довжина пароля повинна бути не менше 6-8 символів;
- пароль повинен складатися з різних груп символів (малі і великі літери латинського алфавіту або кирилиці, цифри, спеціальні символи '(', ')', '#' і т. д.);
- в якості пароля не повинні використовуватися реальні слова, імена, прізвища і т. д.



9.2.2. Оцінка стійкості парольних систем аутентифікації

При виконанні перерахованих вимог до паролів і до підсистеми парольної аутентифікації і за умови відсутності недоліків реалізації парольної системи аутентифікації, єдиним можливим методом злому даної підсистеми

зловмисником є прямий перебір паролів (*brute forcing*). В даному випадку, оцінка стійкості парольного захисту здійснюється наступним чином.

Нехай:

- A – потужність алфавіту паролів (кількість символів, які можуть бути використані при складанні паролю);
- L – довжина пароля;
- $S = A^L$ – потужність простору паролів (число всіляких паролів довжини L, які можна скласти з символів алфавіту A);
- V – швидкість підбору паролів зловмисником;
- T – максимальний термін дії пароля;
- P – ймовірність підбору пароля протягом його терміну дії.

Тоді, ймовірність підбору пароля зловмисником протягом строку його дії визначається за наступною формулою:

$$P = \frac{V \cdot T}{S} \qquad 9.1$$

Зазвичай швидкість підбору паролів V і максимальний термін дії пароля T можна вважати відомими. У цьому випадку, задавши допустиме значення ймовірності P підбору пароля протягом його терміну дії, можна визначити необхідну потужність простору паролів S.

Однак дана задача має неоднозначне рішення. При вихідних даних V, T, P однозначно можна визначити лише нижню межу S^* потужності простору паролів. Цілочислове значення нижньої межі обчислюється за формулою:

$$S^* = \left\lceil \frac{V \cdot T}{P} \right\rceil \qquad 9.2$$

де $\lceil \ \rceil$ – ціла частина числа, взята з округленням вгору.

Після визначення нижньої границі S^* необхідно вибрати такі A і L для формування $S = A^L$, щоб виконувалася наступна нерівність:

$$S^* \le S = A^L \qquad 9.3$$

При виборі S, що задовольняє нерівності (9.3), ймовірність підбору пароля зловмисника (при заданих V і T) буде менша, ніж задана P.

Слід зазначити, що при здійсненні обчислень за формулами (9.2) і (9.3), повинні бути узгоджені величини.

Приклад:

Вихідні дані: $P = 10^{-6}$, $T = 7$ днів = 1 тиждень, $V = 10$ (паролів/ хвилину) $= 10 \cdot 60 \cdot 24 \cdot 7 = 100800$ паролів в тиждень.

Тоді, значення нижньої межі потужності простору паролів:

$$S^* = \left[\frac{100800 \cdot 1}{10^{-6}} \right] = 1008 \cdot 10^8$$

Таким чином, умові $S^* \le A^L$ задовольняють, наприклад, такі комбінації A і L:

- $A = 26$, $L = 8$ (пароль складається з восьми лише малих/великих символів англійського алфавіту);
- $A = 52$, $L = 7$ (пароль складається з семи символів, серед яких повинні бути як малі так і великі латинські літери).

Порядок виконання лабораторної роботи №9:

1. Включити ПК.
2. Ознайомитися з короткими теоретичними відомостями.
3. Провести кількісну оцінку стійкості парольного захисту (згідно варіанту в табл. 9.1).
4. На основі отриманих результатів, реалізувати найпростіший генератор паролів, що володіє необхідною стійкістю до злому. Програма повинна формувати випадкову послідовність символів довжини L, при цьому повинен використовуватися алфавіт з A символів. Приклад вже реалізованого генератора паролів наведено в додатку 3.
5. Оформити звіт згідно до вимог (додаток 1) та прикріпити файл(-и) створеної програми.
6. Відповісти на контрольні питання та підготуватися до письмового опитування.

Зміст звіту:

1. Титульний лист.
2. Постановка завдання.
3. Опис та результати кількісної оцінки стійкості парольного захисту.
4. Програмний код, з описом та коментарями, створеного генератора паролів, який володіє необхідною стійкістю до злому.
5. Висновки.

Завдання на виконання лабораторної роботи №9

Таблиця № 9.1. (варіант відповідно до номера за списком у журналі)

Номер варіанта	P	V	T
1	10^{-6}	10 паролів/хв	5 днів
2	10^{-5}	10 паролів /день	1 місяць
3	10^{-4}	15 паролів /хв	2 тижні
4	10^{-7}	10 паролів /день	1 тиждень

5	10^{-4}	100 паролів /день	12 днів
6	10^{-7}	11 паролів /хв	6 днів
7	10^{-6}	100 паролів /день	15 днів
8	10^{-5}	100 паролів /день	1 місяць
9	10^{-6}	10 паролів /день	3 тижні
10	10^{-5}	3 паролів /хв	1 тиждень
11	10^{-7}	10 паролів /хв	6 днів
12	10^{-6}	3 паролів /хв	5 днів
13	10^{-7}	15 паролів /хв	20 днів
14	10^{-4}	20 паролів /хв	2 тижні
15	10^{-6}	15 паролів /хв	12 днів
16	10^{-5}	15 паролів /хв	10 днів
17	10^{-6}	20 паролів /хв	3 тижні
18	10^{-7}	3 паролів /хв	1 місяць
19	10^{-5}	11 паролів /хв	20 днів
20	10^{-5}	20 паролів /хв	6 днів
21	10^{-4}	10 паролів /день	5 днів
22	10^{-5}	3 паролів /хв	10 днів
23	10^{-4}	10 паролів /хв	3 тижні
24	10^{-7}	100 паролів /день	10 днів
25	10^{-4}	3 паролів /хв	15 днів
26	10^{-5}	10 паролів /хв	1 тиждень
27	10^{-6}	11 паролів /хв	2 тижні

Контрольні питання:

1. Надати визначення наступним поняттям: контроль доступу, ідентифікація, аутентифікація, авторизація.
2. Сформувати та коротко описати базову схему ідентифікації та аутентифікації.
3. Коротко описати класифікацію методів аутентифікації.
4. Назвати та коротко описати основні способи злому парольних систем аутентифікації.
5. Привести практичні рекомендації щодо підсистем парольної аутентифікації та формування пароля.
6. Вибір яких параметрів впливає на зменшення імовірності підбору пароля зловмисником при заданій швидкості підбору пароля зловмисником і заданому термін дії пароля?

Лабораторна робота №10
«Моделювання процедури надання доступу до автоматизованої інформаційної системи. Основні моделі безпеки»

Мета роботи:

1. Поглиблення теоретичних знання з наступних питань:
   - основні методи розмежування доступу та основані на них моделі безпеки.
2. Ознайомлення з проблемами реалізації моделі безпеки в автоматизованих інформаційних системах (АІС) на прикладі дискреційної моделі.

Стислі теоретичні відомості:

10.1. Моделі безпеки

Основну роль у методі формальної розробки інформаційної системи відіграє так звана ***модель безпеки*** (*модель управління доступом, модель політики безпеки*). Метою цієї моделі є вираження суті вимог до безпеки даної системи. Вона визначає потоки інформації, дозволені в системі та правила управління доступом до інформації.

Модель дозволяє провести аналіз властивостей системи, але не накладає ніяких обмежень на реалізацію тих чи інших механізмів захисту. Також необхідно відзначити, що хороша модель безпеки має властивості абстрактності, простоти і адекватності модельованої системи.

Перед тим як перейти до детального аналізу самих моделей безпеки, розглянемо основні поняття, які використовуються в моделях безпеки:

Доступ до інформації – ознайомлення з інформацією, її обробка, зокрема, копіювання, модифікація або знищення інформації.

Управління доступом (access control) звичайно розглядають як сукупність заходів з визначення повноважень і прав доступу, контролю за додержанням правил розмежування доступу.

Повноваження доступу (privilege) – право суб'єкта доступу на виконання певних дій, зокрема на одержання певного типу доступу до об'єктів.

Право доступу (access right) – право, надане суб'єктові на санкціоноване використання певного об'єкта (зокрема, програм та даних), який зберігається в системі.

Суб'єкт доступу – особа або процес, дії якого регламентуються правилами розмежування доступу.

Об'єкт доступу – одиниця інформаційного ресурсу (інформація) автоматизованої системи, доступ до якої регламентується правилами розмежування доступу.

Правила розмежування доступу – сукупність правил, які регламентують права доступу суб'єктів доступу до об'єктів доступу. Під самим же ***розмежуванням доступу*** прийнято розуміти встановлення повноважень суб'єктів для подальшого контролю санкціонованого використання ресурсів, доступних в системі.

> *******В різних джерелах також наводяться такі визначення поняття* ***розмежування доступу до інформації****, як:*
>
> - сукупність заходів, які здійснюють розділення інформації на частини і організацію доступу до неї посадових осіб у відповідності до їхніх функціональних обов'язків і повноважень;
> - сукупність процедур, що реалізують перевірку запитів на доступ і оцінку на підставі правил розмежування доступу можливості надання доступу.

На практиці прийнято виділяти два основних методи розмежування доступу – *дискреційний* і *мандатний*, відповідно два типи моделей безпеки, в основі яких лежить:

- дискреційне управління доступом (Discretionary Access Control – DAC);
- мандатне управління доступом (Mandatory Access Control – MAC).

В якості класичних прикладів моделей цих типів можна назвати дискреційну модель Харрісона-Руззо-Ульмана (модель HRU) і мандатну модель Белла-ЛаПадула (модель БЛ).

Однак існує також рольова модель, яка дуже близька до дискреційної, але при цьому містить ознаки мандатної моделі доступу.

10.1.1. Модель дискреційного доступу (DAC)

В межах дискреційної моделі забезпечується довільне управління доступом суб'єктів до об'єктів та контроль за розповсюдженням прав доступу. В рамках цієї моделі система обробки інформації представляється у вигляді сукупності активних елементів – суб'єктів (користувачів, додатків або процесів), які здійснюють доступ до інформації, пасивних сутностей – об'єктів (які представляють собою різні інформаційні ресурси: файли, програми, пристрої виведення і т. д.), що можуть містити секретну інформацію, та кінцевої множини прав доступу, які визначають повноваження на виконання відповідних дій (*read* – читання, *write* – запис та *execute* – виконання, лише для програм).

На практиці дискреційне розмежування доступу визначається двома правилами:

1) усі суб'єкти та об'єкти системи повинні бути ідентифіковані;

2) права доступу суб’єктів до об’єктів визначаються на основі деяких зовнішніх по відношенню до системи правилах.

Основним елементом систем з дискреційним розмежуванням доступу є матриця доступу (рис. 10.1).

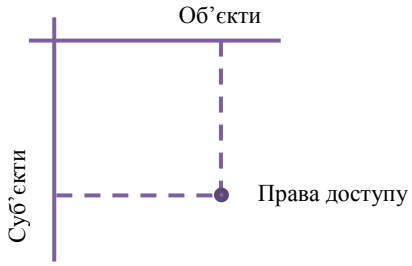


Рис. 10.1. Матриця доступу

Як видно з малюнка, матриця доступу визначає права доступу для кожного користувача по відношенню до кожного ресурсу.

Очевидно, що замість матриці доступу можна використовувати списки повноважень: наприклад, кожному користувачеві може бути зіставлений список доступних йому ресурсів з відповідними правами, або ж кожному ресурсу може бути зіставлений список осіб із зазначенням їх прав на доступ до цього ресурсу.

При запиті доступу до об’єкта, система шукає суб’єкта у списку прав доступу об’єкта, після чого дозволяє доступ якщо суб’єкт присутній у списку і надає повноваження на виконання відповідних (дозволених) дій. Інакше доступ не надається.

Класична система дискреційного контролю доступу є «закритою» в тому розумінні, що спочатку об’єкт не доступний нікому, і в списку прав доступу описується набір дозволів. Також існують «відкриті» системи, в яких за замовчуванням усі мають повний доступ до об’єктів, а в списку доступу описується набір обмежень.

Така модель реалізована в операційних системах Windows (див. рис. 10.2) і Linux.

Зокрема, в Linux для кожного файлу (всі ресурси в ОС Linux представлені у вигляді файлів, в тому числі пристрої введення-виведення) встановлюються права для трьох категорій суб’єктів: власник файлу, члени тієї ж групи, що і власник, і всі інші користувачі. Для кожної з цих категорій встановлюються права на читання (r), запис (w) і виконання (x). Набір прав доступу об’єкта може бути представлений у вигляді символьного рядка. *Наприклад*, запис «rwxr-xr--» означає, що власник файлу може робити з ним все, що завгодно; члени його групи можуть читати і виконувати файл, але не можуть записувати, а іншим користувачам доступно тільки для читання.

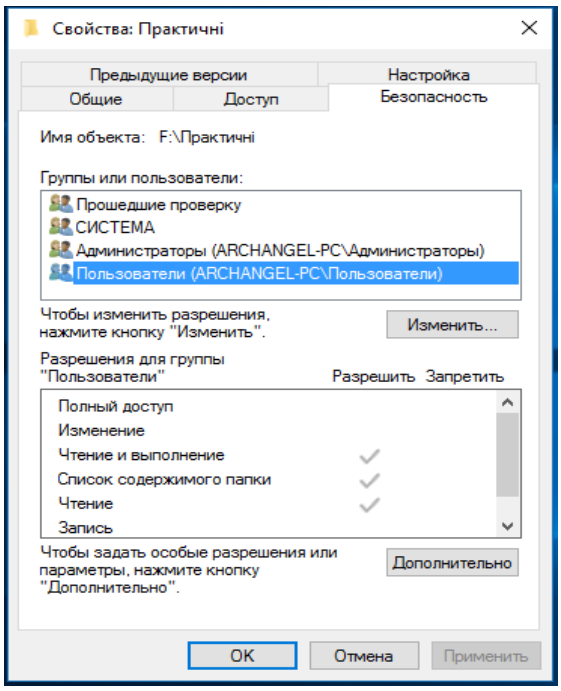


Рис. 10.2. Дискреційна модель доступу в Windows 10

До переваг дискреційної моделі доступу можна віднести відносно просту реалізацію системи розмежування доступу. Цим і зумовлений той факт, що більшість розповсюджених сьогодні AIC реалізують саме дискреційне розмежування доступу. Ще однією перевагою вважають високу деталізацію доступу.

Основний недолік моделі DAC полягає в тому, що суб'єкт, який має право на читання інформації може передати її іншим суб'єктам, які цього права не мають, без попередження власника об'єкта. Таким чином, немає гарантії, що інформація не буде доступна суб'єктам, які не мають до неї доступу. Крім того, не у всіх AIC кожному об'єкту можна призначити власника (у багатьох випадках дані належать не окремим суб'єктам, а всій системі).

У якості прикладу дискреційної моделі доступу розглянемо *модель Харрісона – Руззо – Ульмана*.

Нехай $\{S\}$ – множина суб'єктів;

$\{O\}$ – множина об'єктів системи;

$\{R\}=\{r,w,e\}$ – множина типів доступу (*r – read; w – write; e – execute*).

Тоді матриця доступу буде мати наступний вигляд:

	O_1	O_2	…	O_m
S_1	r	–	…	r,w
S_2	–	e	…	r
…	…	…	…	…

S_n	r, w	r, w, e	…	r, w, e

Приклад: Нехай маємо множину з трьох користувачів {Адміністратор, Гість, Користувач 1} і множину з чотирьох об'єктів {Папка 1, Файл 1, Файл 2, Змінні носії}. Множина можливих дій включає наступні: {Читання – *r*, Запис – *w*, Передача прав іншому користувачеві – *e*}. В даному випадку, матриця доступу, що описує дискреційну модель безпеки, може виглядати наступним чином.

Об'єкт / Суб'єкт	**Папка 1**	**Файл 1**	**Файл 2**	**Змінні носії**
Адміністратор	r, w, e	r, w, e	r, w, e	r, w, e
Гість	–	r	–	r
Користувач 1	r, w	r, e	r, w	–

10.1.2. Модель мандатного доступу (MAC)

Мандатне розмежування доступу зазвичай реалізується як розмежування доступу за рівнями таємності. Повноваження кожного користувача задаються у відповідності з максимальним рівнем секретності, до якого він допущений. При цьому всі ресурси АІС повинні бути класифіковані за рівнями таємності.

Обов'язково потрібно зазначити, що модель мандатного розмежування доступу повинна задовольняти чотири вимоги:

1) всі суб'єкти та об'єкти системи повинні бути однозначно ідентифікованими;

2) заданий лінійно упорядкований набір міток секретності – зіставлення кожному суб'єкту (користувачеві) і об'єкту системи класифікаційних міток, які можна умовно вважати рівнями секретності, крім того, всередині кожного рівня секретності містяться категорії (їх можна розуміти як відділи або підрозділи);

3) кожному об'єкту системи присвоєна мітка секретності, що визначає цінність інформації, яка міститься в ньому;

4) кожному суб'єкту системи присвоєна мітка секретності, що визначає рівень довіри до нього в АІС – максимальне значення мітки секретності об'єктів, до яких суб'єкт має доступ; мітка секретності суб'єкта називається його рівнем доступу.

Таким чином сформулюємо два основних правила МАС:

1) Суб'єкт може читати інформацію з об'єкта, якщо рівень доступу суб'єкта не нижче, ніж у об'єкта, а всі категорії, перераховані в мітці секретності об'єкта, повинні бути присутніми в мітці суб'єкта. В такому

випадку кажуть, що мітка суб'єкта *домінує* над міткою об'єкта. Зміст сформульованого правила – читати можна лише те, що дозволено.

2) Суб'єкт може записувати інформацію в об'єкт, якщо мітка секретності об'єкта домінує над міткою суб'єкта. Зокрема, наприклад, «конфіденційний» суб'єкт може писати в секретні файли, але не може – в несекретні (зрозуміло, що повинні також виконуватися обмеження на набір категорій). На перший погляд подібне обмеження може здатися дивним, проте воно є цілком розумним. Ні при яких операціях рівень секретності інформації не повинен знижуватися, хоча зворотний процес цілком можливий.

Ґрунтуючись на даних правилах можна сказати, що основною метою мандатної моделі доступу є перешкоджання витоку інформації від об'єктів з високим рівнем конфіденційності до об'єктів з низьким рівнем, тобто протидіяти виникненню небезпечних інформаційних потоків «з гори-вниз»; також цей механізм спрямований на захист від помилок користувачів, які можуть ненавмисно розголосити конфіденційні дані.

Також необхідно відзначити той факт, що мандатна модель безпеки стійка до атак «Троянським конем». На чому будується захист від таких атак пояснимо на прикладі.

Приклад : Нехай користувачі U_1 і U_2 знаходяться на різних рівнях, тобто $c(U_1) > c(U_2)$.

Тоді, якщо U_1 може помістити в об'єкт O_1 цінну інформацію, то він може писати туди і тоді справедливе співвідношення $c(U_2) < c(U_1) \le c(O_1)$, тобто $c(U_2) < c(U_1)$. Тоді будь-який «Троянський кінь» T, який вже міститься в об'єкті O_2, і може зчитати інформацію в O_1, повинен відображати співвідношення $c(O_2) \ge c(O_1)$.

Тоді $c(O_2) > c(U_2)$ і користувач U_2 не має право прочитати інформацію в O_2, що робить зчитування в O_1 і запис в O_2 безглуздим.

* Принципова відмінність між дискреційним і мандатним розмежуванням доступу полягає в наступному: якщо в разі дискреційного розмежування доступу права на доступ до ресурсу для користувачів визначає його власник, то в разі мандатного розмежування доступу рівні секретності задаються ззовні, і власник ресурсу не може чинити на них впливу. Сам термін «мандатний» є невдалим перекладом слова *mandatory* – «обов'язковий». Тим самим, мандатне розмежування доступу слід розуміти як примусове.

10.1.3. Модель безпеки Белла-ЛаПадула

Одна з найбільш відомих моделей безпеки – модель Белла-ЛаПадула (*модель мандатного управління доступом*). В ній визначено безліч понять, пов'язаних з контролем доступу; даються визначення суб'єкта, об'єкта та операції доступу, а також математичний апарат для їх опису. Ця модель в основному відома двома основними правилами безпеки: одне відноситься до читання, а інша – для запису даних, відповідно:

1) *No Read Up (NRU)* – заборона читання інформації вищого рівня конфіденційності;

2) *No Write Down (NWD)* – заборона запису інформації в об'єкти нижчого рівня конфіденційності. Це правило менш очевидне, але не менш важливе. Дійсно, якщо користувач з рівнем доступу до секретних даних скопіює ці дані у звичайний файл (помилково або зі злого умислу), вони стануть доступні кожному «несекретному» користувачеві. Крім того, у системі можуть бути встановлені обмеження на операції з секретними файлами (наприклад, заборона скопіювати ці файли на інший комп'ютер, відправляти їх по електронній пошті і т. д.). Друге правило безпеки гарантує, що ці файли (або навіть просто дані в них) ніколи не стануть несекретними і не «обійдуть» ці обмеження. Таким чином, наприклад, вірус, не зможе викрасти конфіденційні дані.

Для ілюстрації розглянемо дворівневу модель Белла-ЛаПадула (рис. 10.3). Нехай є два суб'єкти $S=\{S_1,S_2\}$ і два об'єкти $O=\{O_1,O_2\}$; список типів доступу налічує усього два види – читання та запис: $R=\{r,w\}$.

Рівні конфіденційності об'єктів та рівні доступу суб'єктів такі: $L_O=\{1,2\}$; $L_S=\{1,2\}$, причому рівень 1 вважається вищим за рівень 2.

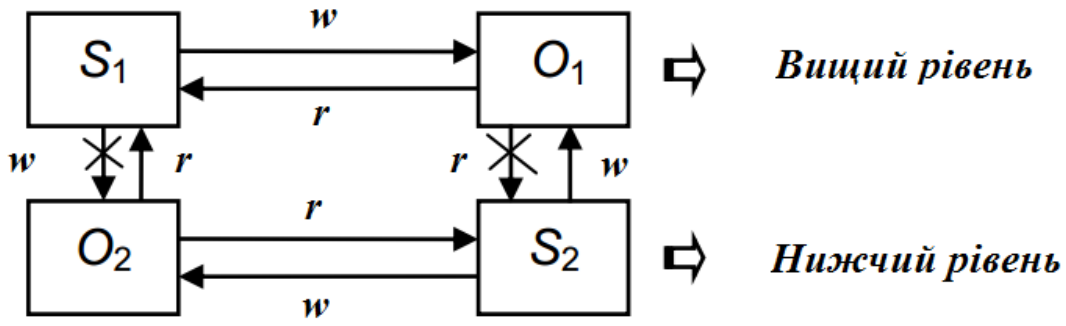


Рис. 10.3. Дворівнева модель Белла-ЛаПадула

Проаналізуємо отриману модель. Як можна спостерігати, всередині одного рівня доступ на запис та читання не забороняється. Однак, проблема тут полягає в іншому: як в межах моделі розмежувати права доступу до об'єктів різних користувачів, що мають один рівень доступу? В таких випадках всередині одного рівня конфіденційності використовують дискреційну модель доступу.

Що стосується різних рівнів конфіденційності, то, як бачимо, S_1 отримає доступ до об'єкта O_2 на читання, а от записати туди свою інформацію не зможе. Більш незвичним являється інший випадок: модель дозволяє суб'єкту S_2 записати свою інформацію в об'єкт O_1, а прочитати її система розмежування доступу потім не дозволить.

Модель Белла-ЛаПадула стала першою значною моделлю безпеки, придатною для АІС, і досі в зміненому вигляді застосовується у військовій галузі. Модель повністю формалізована математично. Основний акцент в моделі робиться на конфіденційність, але крім неї фактично нічого не представлено. Крім того, в моделі ігнорується проблема зміни класифікації: передбачається, що всі відомості відносяться до відповідного рівня секретності, який залишається незмінним. Нарешті, бувають випадки, коли користувачі повинні працювати з даними, які вони не мають права побачити. *Наприклад*: «Відомості про те, що літак несе вантаж з деякої кількості бомб, можливо, мають більш високий рівень секретності, ніж рівень доступу диспетчера, але диспетчеру тим не менш необхідно знати вагу вантажу».

10.1.4. Рольова модель контролю доступу (RBAC)

Рольову модель безпеки звичайно не відносять ні до мандатних, ні до дискреційних, тому що управління доступом у ній здійснюється як на основі матриці прав доступу для ролей, так і за допомогою правил, що регламентують призначення ролей користувачам та їх активацію під час сеансів. Тому рольова модель представляє цілком особливий тип розмежування доступу, заснований на компромісі між гнучкістю управління доступом, що є характерним дискреційним моделям, і жорсткістю правил контролю доступу, що властива мандатній моделі.

У ролевій моделі класичне поняття *суб'єкт* замінюється поняттями *користувач* і *роль*. *Користувач* – це особа, що працює з системою та виконує певні службові обов'язки. *Роль* – це абстрактна суттєвість, що активно діє в системі, з якою зв'язаний обмежений, логічно зв'язаний набір повноважень, необхідний для здійснення певної діяльності.

Основні переваги:

1) простота адміністрування. На відміну від моделі DAC немає необхідності прописувати дозвіл для кожної пари «об'єкт-користувач». Замість цього прописуються дозволи для пар «об'єкт-роль» і визначаються ролі кожного користувача. При зміні області відповідальності користувача, у нього просто змінюються ролі. Ієрархія ролей (коли роль нарівні зі своїми власними

привілеями може успадковувати привілеї інших ролей) також спрощує процес адміністрування;

2) принцип найменшого привілею. Рольова модель дозволяє користувачеві реєструватися в системі роллю, мінімально необхідною для виконання необхідних завдань. Заборона повноважень, не потрібних для виконання поточного завдання, не дозволяє обійти модель безпеки системи;

3) розподіл обов'язків.

Недоліки фактично ті ж самі, що і в дискреційній моделі.

RBAC широко використовується для управління користувацькими привілеями в межах єдиної системи або програми. Список таких систем включає в себе Microsoft Active Directory, SELinux, FreeBSD, Solaris, СУБД Oracle, PostgreSQL 8.1, SAP R/3 і безліч інших, ефективно застосовують RBAC.

Порядок виконання лабораторної роботи №10:

1. Включити ПК.
2. Ознайомитися з короткими теоретичними відомостями.
3. Сформувати та описати матрицю дискреційного доступу (згідно варіанту в табл. 10.1).
4. На основі отриманої матриці, змоделювати в MS Excel модель DAC[6], для реалізації в вашій компанії (розглянутої в лабораторній роботі № 8), використовуючи такі функції як: ЕСЛИ, И, ИЛИ, СОВПАД, в якій буде також задіяна система парольної аутентифікації та створений, на попередньому занятті, генератор паролів. Приклад вже реалізованої моделі DAC наведено в додатку 4.
5. Оформити звіт згідно до вимог та прикріпити файл MS Excel з готовою моделлю DAC.
6. Відповісти на контрольні питання та підготуватися до письмового опитування.

Зміст звіту:

1. Титульний лист.
2. Постановка завдання.
3. Сформована матриця дискреційного доступу та її опис.
4. Скріншоти та сутність роботи вже змодельованої в MS Excel моделі DAC.
5. Висновки.

Завдання на виконання лабораторної роботи №10

Таблиця № 10.1. (варіант відповідно до номера за списком у журналі)

[6] Модель DAC також може бути змодельована за допомогою *Visual Basic* або іншої мови програмування.

Номер варіанта	Кількість суб’єктів доступу	Кількість об’єктів доступу
1	5	4
2	3	3
3	7	4
4	3	6
5	3	5
6	4	4
7	3	6
8	3	4
9	3	5
10	6	5
11	7	3
12	9	4
13	4	6
14	5	3
15	8	3
16	6	4
17	8	5
18	7	4
19	5	5
20	8	4
21	3	7
22	6	3
23	5	4
24	4	6
25	6	3
26	5	8
27	4	7

Контрольні питання:

1. Надати визначення наступним поняттям: модель безпеки, доступ до інформації, управління доступом, повноваження доступу, право доступу, суб’єкт та об’єкт доступу, правила розмежування доступу.
2. Коротко охарактеризувати модель дискреційного доступу.
3. Коротко охарактеризувати модель мандатного доступу.
4. Коротко охарактеризувати модель безпеки Белла-ЛаПадула.

5. В чому полягає основна відмінність між дискреційним і мандатним розмежуванням доступу?
6. Коротко охарактеризувати рольову модель контролю доступу.

Лабораторна робота №11
«Нормативно-правовий підхід до забезпечення інформаційної безпеки України та провідних країн світу»

Мета роботи:

1. Ознайомлення з нормативно-правовими засадами системи забезпечення інформаційної безпеки України та відповідальністю за порушення у сфері захисту інформації і неправомірного використання автоматизованих систем.
2. Вивчення основних стандартів інформаційної безпеки.
3. Проведення аналізу основних державних стандартів України в сфері захисту інформації та нормативних документів системи технічного захисту інформації (ТЗІ).

Стислі теоретичні відомості:

Загальновизнано, що науково-технічний прогрес неможливий без широкомасштабного впровадження в суспільне життя та управлінську діяльність держави, у різні сфери науки, техніки і виробництва сучасних інформаційних технологій, електронно-обчислювальної техніки, інформаційних мереж і мереж електрозв'язку.

В сучасних умовах розвитку інформаційного суспільства активно розвивається інформаційна сфера, яка поєднує в собі інформацію, інформаційну інфраструктуру, зокрема інформаційні мережі, інформаційні відносини між суб'єктами цієї сфери, що складаються у процесі збирання, формування, розповсюдження і використання інформації. Інформаційні відносини займають чільне місце у формуванні інформаційної політики держави, в житті сучасного суспільства, а також в діловому та в особистому житті кожної людини. Це, в свою чергу, обумовлює необхідність розвитку й удосконалення правових засобів регулювання суспільних відносин у сфері інформаційної діяльності. Зрозуміло, що в демократичній правовій державі такі відносини мають базуватися на сучасній нормативно-правовій базі, що регулює діяльність в інформаційній сфері.

11.1. Нормативно-правове регулювання інформаційної безпеки в Україні

Традиційно правове забезпечення інформаційної безпеки розглядається в рамках інформаційного права. ***Інформаційне законодавство*** – одна з наймолодших галузей законодавства. З виникненням Інтернету і розвитком суспільних відносин з приводу інформації, у держав виникла необхідність правового регулювання даної сфери суспільних відносин, визначення інформаційної політики та її захисту.

Так, на зустрічі керівників країн «Великої вісімки» в Японії 22 липня 2000 року була прийнята Окінавська хартія глобального інформаційного суспільства, що містить положення, відповідно до якого інформаційні та телекомунікаційні технології є одним з пріоритетних факторів, що впливають на формування суспільства XXI століття.

Прийняттям хартії країни «Великої вісімки» проголосили основні положення, які будуть здійснювати при формуванні та поширенні інформаційного суспільства.

Зі зростанням ролі інформації, правове регулювання в інформаційній сфері також стає одним з пріоритетних напрямків законотворчого процесу і в Україні, мета якого – забезпечення інформаційної, кібернетичної безпеки держави та боротьби з кіберзлочинністю.

Під час створення сучасної та ефективної системи забезпечення інформаційної безпеки істотного значення набуває наявність відповідної нормативно-правової бази, без якої неможливо охопити усі сфери життєдіяльності суспільства в рамках єдиного правового поля, розробити загальнонаціональну концепцію розвитку держави й ефективно реалізовувати політику національної безпеки в інформаційній сфері. Це означає, що всі без винятку дії щодо захисту й реалізації національних інтересів України в будь-якій сфері й на будь-якому рівні мають передусім спиратися на чинне законодавство України, підтверджувати законність функціонування системи національної безпеки. Водночас у демократичному суспільстві такі дії суб'єктів забезпечення національної безпеки повинні відповідати національному законодавству, а також загальновизнаним міжнародно-правовим нормам та бути під контролем громадськості.

Таким чином, під ***нормативно-правовим регулюванням*** інформаційної безпеки України розуміється форма владного правового впливу на суспільні інформаційні відносини, що здійснюється державою з метою їх упорядкування, закріплення і забезпечення.

Нормативно-правову базу в області інформаційної безпеки в Україні складають:

- Конвенція Ради Європи про кіберзлочинність, ратифікована Законом України від 7.09.2005 року № 2824-IV;

- Конституція України та закони України: «Про інформацію», «Про основи національної безпеки України», «Про Державну службу спеціального зв'язку та захисту інформації України», «Про телекомунікації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про доступ до публічної інформації», «Про оборону України», «Про засади внутрішньої і зовнішньої політики», «Про об'єкти підвищеної небезпеки». Вказані нормативно-правові акти регулюють питання забезпечення інформаційної безпеки, питання захисту інформації, охорони державної таємниці, забезпечення захисту конфіденційної інформації, інформаційних ресурсів, спрямовані на реалізацію положень Доктрини безпеки особистості, держави і суспільства та ін.
- Укази Президента України, зокрема про: Доктрину інформаційної безпеки, Стратегію національної безпеки України та Воєнну доктрину України;
- окремі Постанови Кабінету Міністрів та Рішення РНБОУ;
- державні та міждержавні стандарти з інформаційної безпеки.

При цьому ключова роль у забезпеченні кібербезпеки покладається на:

1) Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», який регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та ІТ систем;

2) Закон України «Про Основні засади розвитку інформаційного суспільства України на 2007-2015 роки» у запропонованих змінах до якого указується на необхідність створення національної системи кібербезпеки;

3) запропонований Міністерством внутрішніх справ (МВС) законопроект «Про внесення змін до Закону України «Про основи національної безпеки України» щодо кібернетичної безпеки України», яким має бути запроваджено низку термінів, пов'язаних із кібербезпекою;

4) Указ президента України № 449/2014 від 01.05.2014 Про рішення Ради національної безпеки і оборони України від 28.04.2014 р. «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України»;

5) Указ президента України № 744/2014 від 24.09.2014 Про рішення Ради національної безпеки і оборони України від 28.08.2014 р. «Про невідкладні заходи щодо захисту України та зміцнення її обороноздатності».

Однак необхідно підкреслити, що особливим недоліком нормативно-правового регулювання інформаційної безпеки України є розпорошення його у численних нормативно-правових актах різної юридичної сили. Причому важливі проблеми нормативно закріплюються підзаконними нормативно-правовими актами. До того ж не менш важливою проблемою для ефективного

забезпечення інформаційної безпеки України є неузгодженість нормативно-правових актів як між собою, так і з чинною Конституцією.

11.2. Основні стандарти інформаційної безпеки

Як вже зазначалося раніше, особливу частину нормативно-правового забезпечення інформаційної безпеки становлять технічні нормативні правові акти – ***стандарти*** і *предстандарти*.

У загальному випадку ***стандартом*** прийнято називати документ, в якому з метою добровільного багаторазового використання встановлюються характеристики продукції, правила здійснення і характеристики процесів виробництва, експлуатації, зберігання, перевезення, реалізації та утилізації, виконання робіт або надання послуг. Стандарт може ставити й інші вимоги – наприклад, до символіки або термінології.

Формальною причиною ***необхідності використання*** стандартів є той факт, що необхідність дотримання деяких з них закріплена законодавчо. Реальні причини набагато глибше – зазвичай стандарт є результатом формалізації досвіду кращих фахівців в тій чи іншій області, і тому являє собою надійне джерело оптимальних і перевірених рішень. Стандарти є також одним з основних механізмів забезпечення сумісності продуктів і систем – зокрема, АС, що використовують рішення від різних виробників.

Зупинимося більш детально на стандартах в області інформаційної безпеки. Їх загальноприйнята класифікація з прикладами приведена на рис. 11.1.

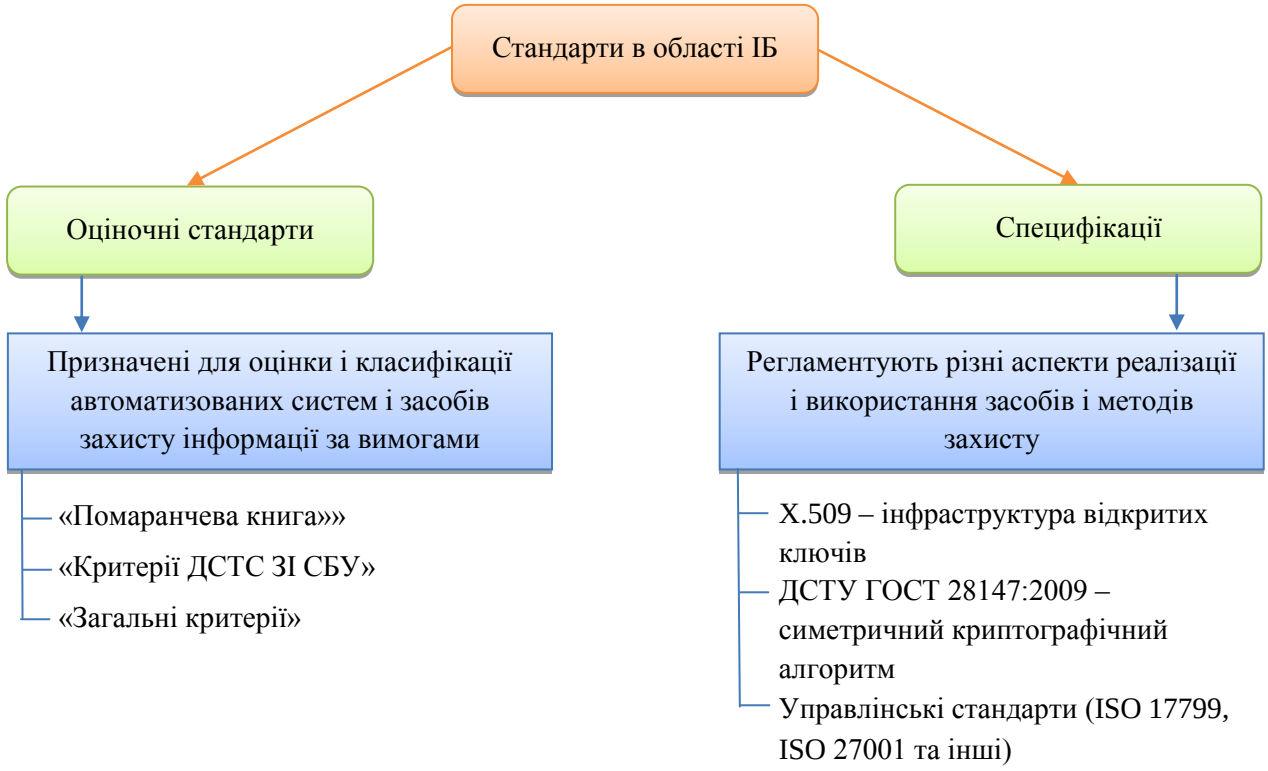


Рис. 11.1. Класифікація стандартів в області інформаційної безпеки

11.2.1. «Помаранчева книга»

Стандарт **«Критерії оцінки захищеності комп'ютерної системи»** (*Trusted Computer System Evaluation Criteria*), більш відомий як **«Помаранчева книга»**, був розроблений Міністерством Оборони США в 1983 р. і став першим в історії загальнодоступним оціночним стандартом в області інформаційної безпеки. Його прийняттю передували п'ятнадцятирічні дослідження, що проводилися спеціально створеною робочою групою і національним бюро стандартів США.

Стандартом передбачено шість фундаментальних вимог, яким повинні задовольняти ті обчислювальні системи, які використовуються для обробки конфіденційної інформації. Вимоги розділені на **три групи**: політика безпеки, підзвітність та гарантії – в кожній групі по дві вимоги наступного змісту.

1. Політика безпеки

Вимога 1. Система повинна підтримувати точно визначену політику безпеки. Можливість доступу суб'єктів до об'єктів повинна визначатися на підставі їх ідентифікації і набору правил управління доступом. У міру необхідності повинна використовуватися політика мандатного управління доступом.

Вимога 2. Маркування – з об'єктами повинні бути асоційовані мітки безпеки, що використовуються в якості вихідної інформації для процедур

контролю доступу. Для реалізації мандатного управління доступом система повинна забезпечувати кожному об'єкту набір атрибутів, що визначають ступінь конфіденційності об'єкта і режими доступу до цього об'єкта.

2. Підзвітність

Вимога 3. Ідентифікація – всі суб'єкти повинні мати унікальні ідентифікатори. Контроль доступу повинен здійснюватися на основі ідентифікації суб'єкта та об'єкта доступу, аутентифікації і правил розмежування доступу. Дані, використовувані для ідентифікації і аутентифікації, повинні бути захищені від несанкціонованого доступу, модифікації та знищення і повинні бути асоційовані з усіма активними компонентами комп'ютерної системи, функціонування яких критично з точки зору безпеки.

Вимога 4. Підзвітність – для визначення ступеня відповідальності користувача за дії в системі, всі події що відбуваються в ній, що мають значення з точки зору безпеки, повинні відслідковуватися і реєструватися в захищеному протоколі. Система реєстрації повинна здійснювати аналіз загального потоку подій і виділять з нього тільки ті події, які впливають на безпеку. Протокол подій повинен бути надійно захищений від несанкціонованого доступу, модифікації та знищення.

3. Гарантії

Вимога 5. Гарантії – засоби захисту повинні містити незалежні апаратні або програмні компоненти, що забезпечують працездатність функцій захисту. Це означає, що всі засоби захисту, що забезпечують політику безпеки, управління атрибутами і мітками безпеки, реєстрацію та облік, повинні перебувати під контролем засобів, що перевіряють коректність їх функціонування. Засоби контролю повинні бути повністю незалежні від засобів захисту.

Вимога 6. Постійний захист – всі засоби захисту повинні бути захищені від несанкціонованого втручання і відключення, причому цей захист повинен бути постійним і безперервним в будь-якому режимі функціонування системи захисту і автоматизованої системи в цілому. Ця вимога поширюється на весь життєвий цикл автоматизованої системи.

Нагадаємо, що «Помаранчева книга» є оціночним стандартом – а значить, призначена в першу чергу для проведення аналізу захищеності автоматизованих систем. За результатами такого аналізу АС повинна бути віднесена до одного з визначених у документі класів захищеності.

«Помаранчева книга» визначає **чотири групи класів** захищеності:

A – (верифікований захист) містить єдиний клас A1.

B – (мандатний захист) містить класи B1, B2 і B3.

C – (індивідуальний захист) містить класи C1 і C2.

D – (мінімальний захист) містить єдиний клас D1.

Необхідний рівень захищеності системи зростає від групи D до групи A, а в межах однієї групи – зі збільшенням номера класу. Кожен клас характеризується певним фіксованим набором вимог до підсистеми забезпечення інформаційної безпеки, реалізованої в АС.

Наведемо короткі характеристики кожного з класів захищеності.

I. Група D – мінімальний захист.

До даної категорії відносяться ті системи, які були представлені для сертифікації за вимогами одного з вищих класів захищеності, але не пройшли випробування.

II. Група C – дискреційний захист.

Дана група характеризується наявністю дискреційного управління доступом і реєстрації дій суб'єктів.

- ***Клас C1 – дискреційний захист***

Система включає в себе засоби контролю і управління доступом, що дозволяють задавати обмеження для окремих користувачів. Клас C1 розрахований на однокористувацькі системи, в яких здійснюється спільна обробка даних одного рівня конфіденційності.

- ***Клас C2 – управління доступом***

Система забезпечує більш виборче управління доступом шляхом застосування засобів індивідуального контролю за діями користувачів, реєстрації, обліку подій і виділення ресурсів.

III. Група B – мандатний захист

Система забезпечує мандатне управління доступом з використанням міток безпеки, підтримку моделі і політики безпеки. Передбачається наявність специфікацій на функції ядра безпеки. Реалізується концепція монітора безпеки звернень, який контролює всі події в системі.

- Клас B1 – захист із застосуванням міток безпеки

Крім виконання всіх вимог до класу C2, система повинна підтримувати маркування даних і мандатне управління доступом. При експорті із системи інформація повинна піддаватися маркуванню.

- Клас B2 – структурований захист

Ядро безпеки має підтримувати формально певну і чітко документовану модель безпеки, що передбачає дискреційне і мандатне управління доступом, яке поширюється на всі суб'єкти. Повинен здійснюватися контроль прихованих каналів передачі інформації. У структурі ядра безпеки повинні бути виділені елементи, критичні з точки зору безпеки. Інтерфейс ядра безпеки повинен бути чітко визначений, а його архітектура і реалізація повинні бути виконані з

урахуванням можливості проведення тестових випробувань. Управління безпекою має здійснюватися адміністратором безпеки.

- Клас В3 – домени безпеки

Ядро безпеки має підтримувати монітор безпеки звернень, який контролює всі типи доступу суб'єктів до об'єктів і який неможливо обійти. Ядро безпеки містить виключно підсистеми, що відповідають за реалізацію функцій захисту, і є досить компактним для забезпечення можливості ефективного тестування. Засоби аудиту повинні включати механізми оповіщення адміністратора про події, що мають значення для безпеки системи. Необхідна наявність засобів відновлення працездатності системи.

IV. Група А – верифікований захист

Група характеризується застосуванням формальних методів верифікації коректності функціонування механізмів управління доступом. Потрібна додаткова документація, що демонструє, що архітектура і реалізація ядра безпеки відповідає вимогам безпеки. Функціональні вимоги збігаються з класом В3, проте на всіх етапах розробки АС потрібне застосування формальних методів верифікації систем захисту.

Розробка і публікація «Помаранчевої книги» стали важливою віхою в становленні теорії інформаційної безпеки. Такі базові поняття, як «політика безпеки», «монітор безпеки звернень» або «адміністратор безпеки» вперше у відкритій літературі з'явилися саме в «Помаранчевій книзі».

У той же час з плином часу стали проявлятися численні недоліки «Помаранчевої книги» і запропонованого підходу до класифікації АС в цілому. Багато в чому її старіння було пов'язано з принциповими змінами апаратної бази засобів обчислювальної техніки, що відбулися з 1983 р – і перш за все, з поширенням розподілених обчислювальних систем і мереж, особливості яких в «Помаранчевій книзі» ніяк не враховуються. Чи не знайшли відображення в «Помаранчевої книзі» і питання забезпечення доступності інформації. Нарешті, з ускладненням АС все більше стала виявлятися принципова обмеженість «табличного» підходу до класифікації систем за вимогами безпеки інформації, коли автоматизована система повинна бути віднесена до одного з класів захищеності виходячи з виконання фіксованого набору вимог до функціональних характеристик – такий підхід принципово не дозволяє врахувати особливості системи і є недостатньо гнучким.

Намагаючись не відстати від інформаційних технологій, що постійно розвиваються, розробники «Помаранчевої книги» аж до1995 р випустили цілий ряд допоміжних документів, відомих як «Райдужна серія». Ці документи містили рекомендації щодо застосування положень «Помаранчевої книги» для різних категорій автоматизованих систем, а також вводили ряд додаткових

вимог. Найбільший інтерес в «Райдужній серії» представляють три документа: «Інтерпретація для захищених мереж», «Інтерпретація для захищених СУБД» і «Керівництво з управління паролями».

В даний час «Помаранчева книга» не використовується для оцінки автоматизованих систем і становить інтерес виключно з історичної точки зору.

11.2.2. «Критерії ДСТС ЗІ СБУ» (Держспецзв'язку)

НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу». Цей нормативний документ встановлює критерії оцінки захищеності інформації, оброблюваної в комп'ютерних системах, від несанкціонованого доступу і є методологічною базою для визначення вимог з захисту інформації в комп'ютерних системах від несанкціонованого доступу; створення захищених комп'ютерних систем і засобів захисту від несанкціонованого доступу; оцінки захищеності інформації в комп'ютерних системах і їх придатності для обробки критичної інформації (інформації, що вимагає захисту).

Функціональними критеріями за документом є: конфіденційність; цілісність; доступність; спостереженість.

У стандарті використовується поняття об'єкта інформаційного обміну, що відрізняється від інших. Сутність КС розглядається як сукупність об'єктів, а їх взаємодія описується наступною трійкою:

- об'єкт-користувач;
- об'єкт-процес, що діє від імені користувача;
- об'єкт як пасивний елемент.

Такий підхід дозволяє за ситуації, коли один користувач запускає багато процесів, використовувати для опису цієї ситуації один об'єкт-користувач і безліч асоційованих з ним об'єктів-процесів. При цьому політика безпеки (ПБ) розрахована на одного користувача, що здійснює доступ до об'єктів за допомогою декількох процесів.

Загальна оцінка рівня безпеки системи складається з потужності функціональних вимог комплексу засобів захисту (КЗЗ) і рівня вимог адекватності їх реалізації (рис. 11.2).

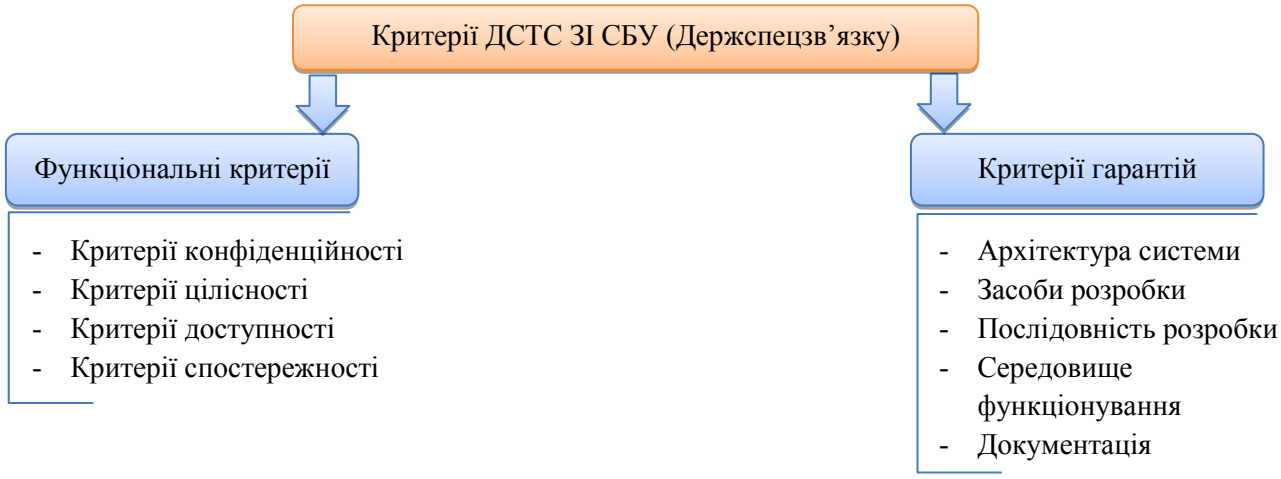


Рис. 11.2. Складові загальної оцінки рівня безпеки системи

Для забезпечення максимального ступеня абстрагованості та інваріантності щодо ПБ і методів її реалізації у стандарті використовується поняття ***«Атрибути доступу»***, що позначає сукупність атрибутів безпеки, які асоціюються з користувачем, процесом або об'єктом. Як атрибут доступу користувача, процесу або об'єкта можуть виступати відповідний унікальний ідентифікатор, мітка безпеки або цілісності, криптографічний ключ, таблиця прав доступу або інші атрибути відповідно до реалізованої в комп'ютерній системі ПБ.

Функціональні можливості використовуваних засобів захисту характеризуються окремими показниками забезпечуваного рівня безпеки стосовно однієї з чотирьох загроз. Рівень адекватності реалізації (гарантій) ПБ має один узагальнений параметр (Г-1…Г-7).

Стисло розглянемо ранжування вимог «Критеріїв ДСТС ЗІ СБУ» (Держспецзв'язку).

В таблиці 11.1 відображено окремі показники критеріїв конфіденційності.

Таблиця 11.1. Показники критеріїв конфіденційності

Критерії конфіденційності			
Рівень	Найменування	Пов'яз. рів.	Розділ
КД-1	Мінімальна довірча конфіденційність	НИ-1	Довірча конфіденційність
КД-2	Базова довірча конфіденційність		
КД-3	Повна довірча конфіденційність	КО-1, НИ-1	
КД-4	Абсолютна довірча конфіденційність		
КА-1	Мінімальна адміністративна конфіденційність	НО-1, НИ-1	Адміністративна конфіденційність
КА-2	Базова адміністративна конфіденційність		
КА-3	Повна адміністративна конфіденційність	КО-1, НО-1, НИ-1	
КА-4	Абсолютна адміністративна конфіденційність		
КК-1	Виявлення прихованих каналів	КО-1, Г-3	Аналіз прихованих каналів
КК-2	Контроль прихованих каналів	КО-1, НР-1,	

		Г-3	
КК-3	Перекриття прихованих каналів	КО-1, Г-3	
КВ-1	Мінімальна конфіденційність при обміні	-	Конфіденційність при обміні
КВ-2	Базова конфіденційність при обміні	НО-1	
КВ-3	Повна конфіденційність при обміні	НО-1, НВ-1	
КВ-4	Абсолютна конфіденційність при обміні	НО-1, НВ-1, НР-1, Г-3	
КО-1	Повторне використання об’єктів	-	Повторне використання об’єктів

Особливістю функціональних критеріїв є те, що деякі їх рівні залежать від інших, і для того, щоб задовольнити вимоги цих рівнів, необхідно дотримуватись не тільки наведених у них вимог, але й вимог, пов’язаних розділів інших функціональних критеріїв і критеріїв гарантій у рамках зазначених рівнів.

Критерії конфіденційності регламентують захист ресурсів КС від несанкціонованого доступу шляхом реалізації відповідних послуг. Більш детальна характеристик цих послуг буде розглядатися в рамках інших предметів.

Критерії цілісності визначають можливості комп’ютерної системи щодо забезпечення власної цілісності та цілісності оброблюваної інформації, що в ній зберігається. Критерії цілісності передбачають наступні послуги: довірча та адміністративна цілісність, відкат, цілісність при обміні. В таблиці 11.2 показані окремі показники критеріїв цілісності.

Таблиця 11.2. Показники критеріїв цілісності

Критерії цілісності			
Рівень	Найменування	Пов’яз. рів.	Розділ
ЦД-1	Мінімальна довірча цілісність	НИ-1	Довірча цілісність
ЦД-2	Базова довірча цілісність		
ЦД-3	Повна довірча цілісність	КО-1, НИ-1	
ЦД-4	Абсолютна довірча цілісність		
ЦА-1	Мінімальна адміністративна цілісність	НО-1, НИ-1	Адміністративна цілісність
ЦА-2	Базова адміністративна цілісність		
ЦА-3	Повна адміністративна цілісність	КО-1, НО-1, НИ-1	
ЦА-4	Абсолютна адміністративна цілісність		
ЦВ-1	Мінімальна цілісність при обміні	-	Цілісність при обміні
ЦВ-2	Базова цілісність при обміні	НО-1	
ЦВ-3	Повна цілісність при обміні	НО-1, НВ-1	
ЦО-1	Обмежений відкат	НИ-1	Відкат
ЦО-2	Повний відкат		

Критерії доступності регламентують роботу засобів, що забезпечують доступність комп'ютерної системи в цілому, окремих її функцій або ресурсів протягом певного інтервалу часу для авторизованих користувачів, а також гарантувати функціонування КС у разі відмови її окремих компонентів. Як заходи забезпечення доступності розглядаються контроль щодо використання ресурсів системи, забезпечення стійкості системи до відмов, забезпечення живучості й відновлення системи в умовах виходу з ладу її компонентів. В таблиці 11.3 показані окремі показники критеріїв доступності.

Таблиця 11.3. Показники критеріїв доступності

Критерії доступності			
Рівень	Найменування	Пов'яз. рів.	Розділ
ДР-1	Квоти	НО-1	Використання ресурсів
ДР-2	Припинення захоплення ресурсів		
ДР-3	Пріоритетність використання ресурсів		
ДС-1	Стійкість при обмежених відмовах	НО-1	Стійкість до відмов
ДС-2	Стійкість з погіршенням характеристик обслуговування		
ДС-3	Стійкість без погіршенням характеристик обслуговування		
ДЗ-1	Модернізація	НО-1	Гаряча заміна
ДЗ-2	Обмежена гаряча заміна	НО-1, ДС-1	
ДЗ-3	Гаряча заміна будь-якого компоненту		
ДВ-1	Ручне відновлення	НО-1	Відновлення після збоїв
ДВ-2	Автоматичне відновлення		
ДВ-3	Вибіркове відновлення		

Критерії спостереженості регламентують роботу засобів, що дозволяють встановити відповідальність користувачів за події в системі. Спостереженість забезпечується наступними засобами (послугами): реєстрація (аудит); ідентифікація й аутентифікація; достовірний канал; розмежування обов'язків; цілісність КЗЗ; самотестування; ідентифікація та аутентифікація при обміні; аутентифікація відправника; аутентифікація одержувача. В таблиці 11.4 відображені окремі показники критеріїв спостереженості.

Таблиця 11.4. Показники критеріїв спостереженості

Критерії спостережності			
Рівень	Найменування	Пов'яз. рів.	Розділ
НР-1	Зовнішній аналіз	НИ-1	Реєстрація
НР-2	Захищений журнал	НИ-1, НО-1	
НР-3	Сигналізація про небезпеку		
НР-4	Детальна реєстрація		

НР-5	Аналіз у реальному часі		
НИ-1	Зовнішня ідентифікація та аутентифікація	-	Ідентифікація та аутентифікація
НИ-2	Одиночна ідентифікація та аутентифікація	НК-1	
НИ-3	Множинна ідентифікація та аутентифікація		
НК-1	Однонаправлений достовірний канал	-	Достовірний канал
НК-2	Двонаправлений достовірний канал		
НО-1	Виділення адміністратора	НИ-1	Розмежування обов'язків
НО-2	Розмежування обов'язків адміністраторів		
НО-3	Розмежування обов'язків на підставі привілеїв		
НЦ-1	КСЗ з контролем цілісності	НР-1, НО-1	Цілісність КСЗ
НЦ-2	КСЗ з гарантованою цілісністю	-	
НЦ-3	КСЗ з функціями диспетчера доступу		
НТ-1	Самотестування за запитом	НО-1	Самотестування
НТ-2	Самотестування при старті		
НТ-3	Самотестування у реальному часі		
НВ-1	Аутентифікація за запитом	-	Ідентифікація та аутентифікація при обміні
НВ-2	Аутентифікація джерела даних		
НВ-3	Аутентифікація з підтвердженням		
НА-1	Базова аутентифікація відправника	НИ-1	Аутентифікація відправника
НА-2	Аутентифікація відправника з підтвердженням		
НП-1	Базова аутентифікація одержувача	НИ-1	Аутентифікація одержувача
НП-2	Аутентифікація одержувача з підтвердженням		

Критерії гарантій регламентують вимоги до процесу розробки та реалізації КЗЗ, що дозволяють визначити адекватність реалізації ПБ і відображають ступінь довіри до комплексу засобів захисту. Критерії гарантій охоплюють усі стадії та аспекти створення й експлуатації системи і включають розділи, що належать до:

1) архітектури КЗЗ;
2) середовища розробки:
   - процесу розробки;
   - управління конфігурацією;
3) послідовності розробки:
   - розробки функціональних специфікацій:
     - ПБ;
     - моделі ПБ;
     - проекту архітектури;
     - детального проекту;
     - його реалізації;
4) середовища функціонування;
5) документації:

- керівництва з безпеки для користувача;
- керівництва адміністратора безпеки;

6) випробування комплексу засобів захисту.

Передбачено сім рівнів гарантій (Г1...Г7). Із зростанням номера рівня відбувається конкретизація, доповнення й посилення вимог без зміни їх структури. Рівень гарантій (адекватності) реалізації ПБ характеризує якість усієї системи в цілому.

Порядок оцінки КС на предмет відповідності даним критеріям визначається відповідними нормативними документами Держспецзв'язку (ДСТС ЗІ СБУ). Експертна комісія, яка проводить оцінку КС, визначає кількість і рівень реалізованих у КС послуг безпеки і ступінь дотримання вимог гарантій.

Результатом оцінки є рейтинг (функціональний профіль захищеності), який складається з ряду (переліку) літерно-числових комбінацій, що позначають рівні реалізованих послуг, у поєднанні з рівнем гарантій.

Нормативні документи Держспецзв'язку (ДСТС ЗІ СБУ) вводять ***функціональні профілі захищеності***, що є переліком мінімально необхідних рівнів послуг, які повинен реалізовувати КЗЗ обчислювальної системи КС, щоб задовольняти певні вимоги до захищеності оброблюваної інформації. Стандартні функціональні профілі формуються на основі існуючих вимог до захисту певної інформації від певних загроз і відомих на сьогодні функціональних послуг, що дозволяють протистояти загрозам і забезпечити виконання цих вимог.

Опис профілю складається з трьох частин:

1) літерно-числового ідентифікатора;

2) знака рівності;

3) переліку рівнів послуг у фігурних дужках.

Ідентифікатор у свою чергу включає:

- позначення класу КС (1, 2 або 3);
- літерну частину, що характеризує види загроз, від яких забезпечується захист (К, і/або Ц, і/або Д);
- номер профілю;
- необов'язкове літерне позначення версії.

Усі частини ідентифікатора відокремлюються одна від одної крапкою.

Наприклад, 3.КЦД.1 = { КД-2, КО-1, КВ-1, ЦД-1, ЦО-1, ЦВ-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1 } – функціональний профіль номер один, що відображає вимоги до КС класу 3, основна вимога щодо захисту оброблюваної інформації – забезпечення конфіденційності, цілісності, доступності.

11.2.3. «Загальні критерії»

Стандарт ***ISO/IEC 15408-1999 «Common Criteria for Information Technology Security Evaluation»*** був розроблений спільними зусиллями фахівців із Канади, США, Великобританії, Німеччини, Нідерландів і Франції у період з 1990 по 1999 рік, розвиток якого безперервно триває й по сьогоднішній день. Історично за стандартом закріпилася розмовна назва *«Common Criteria»* – ***«Загальні критерії»*** (ЗК).

«Загальні критерії» як об'єкт безпеки розглядають не КС, а ІТ-систему і ІТ-продукт, які є похідними від поняття «інформаційна технологія». Під інформаційною технологією розуміють цілеспрямовану організовану сукупність інформаційних процесів, реалізованих з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розподіл даних, доступ до джерел інформації незалежно від місця їх розташування. Відповідно розглядають і безпеку інформаційних технологій (ІТ-безпека).

У «Загальних критеріях» ключовими поняттями є: *Protection Profile* – ***профіль захисту***, *Security Target* – мета безпеки (завдання з безпеки) або ***проект захисту*** і *Target of Evaluation* – об'єкт оцінки. Під ***об'єктом оцінки*** (ОО) розуміється довільний продукт інформаційних технологій або система з керівництвами адміністратора і користувача. ***Продукт*** розглядається як сукупність програмних, програмно-апаратних або апаратних засобів інформаційних технологій, що надає певні функціональні можливості і призначена для безпосереднього використання або включення до складу різних систем. У свою чергу, ***система*** – це специфічне втілення інформаційних технологій з конкретним призначенням і умовами експлуатації.

При підготовці до оцінки формалізуються наступні ***аспекти середовища об'єкта оцінки:***

1. Припущення безпеки

Припущення виділяють ОО із загального контексту і задають кордони його розгляду. Передбачається, що середовище ОО задовольняє даним припущенням. При проведенні оцінки припущення безпеки приймаються без доказів.

2. Загрози безпеці

Виділяються загрози, наявність яких в даному середовищі встановлено або передбачається. Загроза характеризується наступними параметрами:

- джерело загрози;
- передбачуваний спосіб реалізації загрози;

- уразливості, які є передумовою для реалізації загрози;
- активи, які є метою нападу;
- властивості безпеки активів, які порушуються;
- можливі наслідки реалізації загрози.

3. Політики безпеки

Викладаються положення політики безпеки, що застосовуються в організації, які мають безпосереднє відношення до ОО.

На підставі сформульованих припущень безпеки, при обліку загроз і політик формуються ***цілі безпеки*** для ОО, спрямовані на забезпечення протистояння загрозам і виконання положень політики безпеки.

Для досягнення поставлених цілей до ОО та його середовищу пред'являються вимоги безпеки. Друга і третя частини «Загальних критеріїв» є каталогами вимог безпеки наступних типів:

- ***Функціональні вимоги*** (Частина 2) – регламентують порядок функціонування забезпечувальних компонентів ОО (ІТ-продукту) і визначають можливості засобів захисту.
- ***Вимоги довіри*** (Частина 3) – пред'являються до технології та процесу розробки, експлуатації та оцінки ОО і покликані гарантувати *адекватність* реалізації механізмів безпеки. ***Адекватність*** є характеристикою ІТ-продукту, яка відображає ефективність підтримання заявленого рівня безпеки, а також ступінь коректності реалізації засобів захисту. Адекватність ґрунтується на інформації про процеси проектування, створення й експлуатації ІТ-продукту.

При формулюванні вимог до ОО можуть бути розроблені два документи:

1. Профіль захисту – це незалежна від конкретної реалізації структура для визначення й обґрунтування вимог безпеки, що є незмінним і повним набором завдань безпеки, функціональних вимог і вимог адекватності для певного класу продуктів або систем. Наприклад, може бути розроблений профіль захисту на міжмережевий екран корпоративного рівня або на білінгову систему.

2. Проект захисту[7] – це структура, що залежить від реалізації і є повним набором завдань безпеки, функціональних вимог і вимог адекватності, узагальнених специфікацій і обґрунтувань. Вимоги безпеки, що містяться у проекті захисту, визначаються за допомогою посилань на відповідні профілі захисту і вимоги «Загальних критеріїв». На основі проекту захисту здійснюється оцінка конкретного ІТ-продукту.

Проект захисту служить основою для проведення оцінки ОО з метою демонстрації відповідності його вимогам безпеки.

---

[7] Проект захисту можна розглядати як технічне завдання на підсистему забезпечення інформаційної безпеки для ОО.

Неважко зрозуміти, що в порівнянні з традиційними стандартами «Загальні критерії» представляють собою принципово більш гнучкий і універсальний інструмент. Однак стандарт не претендує на всеосяжну універсальність і, зокрема, має такі обмеження:

1. ЗК не містять критеріїв оцінки, які стосуються адміністрування механізмів безпеки, що не відносяться безпосередньо до заходів безпеки інформаційних технологій (управління персоналом, питання фізичної безпеки і т.д.). Відповідні аспекти в рамках «Загальних критеріїв» можуть розглядатися виключно у вигляді припущень безпеки. Передбачається, що оцінка відповідних механізмів повинна проводитися з використанням інших стандартів.
2. Питання захисту інформації від витоку технічними каналами, такі як контроль ПЕМВН, безпосередньо не зачіпаються, хоча чимало концепцій ЗК потенційно можуть бути застосовані і в даній області.
3. В ЗК не розглядаються ні методологія оцінки, ні адміністративно-правова структура, в рамках якої критерії можуть застосовуватися органами оцінки.
4. Процедури використання результатів оцінки при атестації продуктів і систем виходять за межі області дії ЗК.
5. В ЗК не входять критерії оцінки специфічних властивостей криптографічних алгоритмів. Незалежна оцінка математичних властивостей криптографічних компонентів, вбудованих в ОО, повинна проводитися як самостійна незалежна процедура.

11.2.4. Стандарти в галузі управління інформаційною безпекою

Найбільш поширеними управлінськими стандартами на сьогоднішній день є документи, розроблені Британським інститутом стандартів (BSI – British Standards Institution). Стандарти BS 7799-1, BS 7799-2 і BS 7799-3 вкрай популярні в усьому світі, перші два з них мають міжнародний статус стандартів ISO (останні версії цих стандартів мають позначення ISO/IEC 17799:2005 та ISO/IEC 27001:2005 відповідно).

У порівнянні з загальними критеріями, дані документи носять набагато більш неформальний характер і являють собою скоріше набір практичних рекомендацій з розгортання та підтримання системи управління інформаційною безпекою.

1) ISO/IEC 17799:2005

Стандарт ***ISO/IEC 17799:2005 «Information technology – Security techniques – Code of practice for information security management»***

(Інформаційні технології. Методи забезпечення безпеки. Практичний посібник з управління інформаційною безпекою) являє собою набір практичних рекомендацій з побудови комплексної корпоративної системи управління інформаційною безпекою.

Згідно з положеннями стандарту, інформаційна безпека розглядається як процес захисту інформаційних активів організації від різного роду загроз, який досягається шляхом реалізації тих чи інших ***сервісів безпеки***. ***Вимоги до системи безпеки*** визначаються за результатами попередньо проведеного аналізу ризиків, виходячи з вимог нормативних і законодавчих актів, а також шляхом аналізу специфічних потреб бізнесу. Сервіси вибираються таким чином, щоб мінімізувати ідентифіковані інформаційні ризики.

Саме каталог рекомендованих сервісів безпеки і становить основний зміст стандарту. Сервіси згруповані за такими ***тематичними розділами***:

1. Політика безпеки.
2. Організація інформаційної безпеки.
3. Управління активами.
4. Безпека людських ресурсів.
5. Фізична безпека і безпека навколишнього середовища.
6. Управління телекомунікаціями і операціями.
7. Управління доступом.
8. Придбання, розробка і впровадження інформаційних систем.
9. Управління інцидентами в сфері інформаційної безпеки.
10. Управління безперервністю бізнесу.
11. Відповідність.

Для кожного сервісу наведені його *визначення, керівництво по реалізації* та *додаткова інформація*.

Політика інформаційної безпеки розглядається як базовий високорівневий документ, затверджений вищим керівництвом організації і визначає загальний підхід до організації та управління інформаційної безпеки. Політика також містить посилання на низькорівневі стандарти, керівництва та процедури, що визначають практичні аспекти реалізації механізмів безпеки. Перегляд політики здійснюється через заплановані проміжки часу або в разі принципових змін в інформаційній системі.

Вимоги щодо ***організації інформаційної безпеки*** включають в себе питання поділу обов'язків і розподілу відповідальності між усіма учасниками інформаційної взаємодії, що існує в організації.

Управління активами передбачає проведення інвентаризації активів і забезпечення коректного їх використання. В якості одного з базових механізмів забезпечення інформаційної безпеки пропонується проведення категоріювання

інформації з точки зору її цінності, секретності, критичності для організації, або ж за вимогами законодавчих і нормативних актів.

Питання ***безпеки людських ресурсів*** покликані забезпечити дотримання встановленого режиму інформаційної безпеки співробітниками та контрагентами. У всіх випадках права і обов'язки сторін у сфері інформаційної безпеки повинні бути строго обумовлені в трудовому договорі. Регламентуються порядок найму та коректного звільнення співробітників, а також питання навчання і освітніх тренінгів в області інформаційної безпеки.

Фізична безпека та ***безпека навколишнього середовища*** досягаються шляхом застосування комплексу механізмів управління фізичним доступом до активів організації, використання протипожежних систем, систем кондиціонування, а також шляхом своєчасного та повноцінного технічного обслуговування споруд та інфраструктури. Розглядаються питання коректної утилізації активів і повторного використання обладнання.

Управління телекомунікаціями і операціями реалізується шляхом чіткої формалізації всіх процедур, пов'язаних з обробкою інформації в АС. Всі зміни в процедурах і самих засобах обробки інформації повинні строго документуватися. Визначаються механізми боротьби з шкідливим програмним забезпеченням і методи забезпечення безпеки мобільного коду. Пропонуються підходи до забезпечення безпеки специфічних мережевих сервісів, таких, наприклад, як механізми електронних платежів. Окремо розглядаються питання безпеки носіїв інформації.

При розгляді питань ***управління доступом*** особлива увага приділяється рекомендаціям щодо коректної реалізації механізмів парольного захисту. Визначається порядок організації віддаленого доступу користувачів до інформаційної системи, наводяться рекомендації по роботі з мобільними обчислювальними пристроями.

В ході ***придбання, розробки та впровадження інформаційних систем*** передбачається встановлювати акцент на забезпеченні цілісності інформаційних активів і програмних компонентів системи, що досягається, зокрема, з використанням *криптографічних механізмів*. Пропонуються також механізми захисту від витоку інформації на різних етапах життєвого циклу інформаційної системи.

Управління інцидентами в сфері інформаційної безпеки може здійснюватися силами фахівців організації або із залученням уповноважених органів безпеки. Дана діяльність в загальному випадку включає в себе збір доказів, проведення розслідування і аналіз результатів розслідування з метою недопущення повторних інцидентів і підвищення загальної захищеності інформаційної системи.

Забезпечення безперервності бізнесу є однією з основних задач системи управління інформаційною безпекою та має реалізувати захист критичних бізнес-процесів від збоїв або стихійних лих. Розроблені плани безперервності бізнесу повинні гарантувати доступність критичних інформаційних ресурсів і сервісів на необхідному рівні. Плани безперервності бізнесу повинні ретельно тестуватися і своєчасно оновлюватися при зміні структури інформаційної системи або бізнес-моделі організації.

Відповідність вимогам законодавчих актів, галузевих стандартів та інших нормативних документів є обов'язковим для всіх інформаційних систем. Вимоги безпеки також можуть бути визначені в договірних зобов'язаннях. Розглядаються також питання забезпечення захисту від зловживань користувачів різними сервісами і інформаційними ресурсами.

2) ISO/IEC 27001:2005

Міжнародний стандарт ***ISO/IEC 27001:2005 «Information technology – Security techniques – Information security management systems – Requirements»*** (Інформаційні технології. Методи забезпечення безпеки. Системи управління інформаційною безпекою. Вимоги.) Являє собою розширення ISO/IEC 17799:2005, встановлює вимоги щодо процесу створення, впровадження, експлуатації, моніторингу, аналізу, підтримки та вдосконалення корпоративних систем управління інформаційною безпекою (СУІБ).

Реалізація СУІБ здійснюється шляхом впровадження чотирьох етапної моделі PDCA (Plan-Do-Check-Act, Планування – Реалізація – Оцінка – Дія/Коригування). Структура моделі показана на рис. 11.3.

Рис. 11.3. Модель PDCA

Система управління інформаційною безпекою отримує в якості вихідних даних вимоги інформаційної безпеки та очікування зацікавлених сторін і шляхом застосування необхідних заходів і процесів реалізує необхідні механізми безпеки.

Попередньою умовою початку робіт з ***планування*** *СУІБ* є прийняття *політики безпеки*, яка встановлює загальні принципи забезпечення інформаційної безпеки в організації та задає область дії СУІБ. Планування здійснюється шляхом проведення оцінки ризиків та вибору сервісів безпеки, що відповідають вимогам, ідентифікованим за результатами аналізу ризиків. Каталог сервісів безпеки, які повністю відповідають наведеним в ISO/IEC 17799:2005, міститься в *додатку А* до стандарту ISO/IEC 27001:2005.

На етапі ***реалізації*** необхідно, вирішивши питання фінансування і розподілу обов'язків, реалізувати обрані на етапі планування сервіси безпеки і забезпечити коректну їх експлуатацію. Необхідно передбачити наявність механізмів оцінки ефективності сервісів безпеки і реалізувати програми навчання користувачів питань інформаційної безпеки. При здійсненні експлуатації СУІБ необхідно ретельно контролювати і коректно відпрацьовувати інциденти, пов'язані з інформаційною безпекою.

Проведення ***оцінки*** СУІБ передбачає проведення аналізу ефективності функціонування як окремих сервісів безпеки, так і СУІБ в цілому. Відстеження змін, що відбуваються в системі, має супроводжуватися переглядом результатів аналізу ризиків. Внутрішній аудит СУІБ повинен проводитися через заплановані інтервали часу.

Фаза ***коригування*** повинна забезпечити безперервне вдосконалення системи управління інформаційною безпекою з урахуванням ризиків і вимог, які постійно змінюються. У ряді випадків проведення коригування може потребувати повернення до попередніх фаз моделі – наприклад, до етапів планування і реалізації.

Реалізація СУІБ супроводжується розробкою системи документації, яка повинна включати наступні матеріали:

- положення політики безпеки організації;
- область дії СУІБ;
- процедури і сервіси безпеки, що підтримують СУІБ;
- опис застосовуваних методів оцінки ризиків;
- звіти, що містять результати оцінки ризиків;
- план управління ризиками;
- методики оцінки ефективності застосовуваних сервісів безпеки;
- декларація застосовності;
- записи, що підтверджують ефективність функціонування СУІБ і надають свідчення її відповідності положенням стандарту.

Своє відображення стандарт ISO/IEC 27001:2005 знаходить у постанові Правління Національного банку України від 28.10.2010 № 474 «Про набрання

чинності стандартами з управління інформаційною безпекою в банківській системі України»:

- СОУ Н НБУ 65.1 СУІБ 1.0:2010 – *Методи захисту в банківській діяльності. Система управління інформаційною безпекою. Вимоги;*
- СОУ Н НБУ 65.1 СУІБ 2.0:2010 – *Методи захисту в банківській діяльності. Звід правил для управління інформаційною безпекою.*

11.3. Відповідальність за порушення у сфері захисту інформації та неправомірного використання автоматизованих систем

Законом України «Про захист персональних даних», що поширюється на діяльність з обробки персональних даних, яка здійснюється повністю або частково із застосуванням автоматизованих систем, персональні дані віднесено до об'єкту захисту. Статтею 5 цього Закону персональні дані за режимом доступу віднесено до інформації з обмеженим доступом. При цьому, згідно з нормами статті 24 Закону України «Про захист персональних даних» власники, розпорядники персональних даних та треті особи зобов'язані забезпечити захист цих даних від випадкових втрати або знищення, від незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних.

Таким чином, оскільки законодавством персональні дані віднесено до інформації з обмеженим доступом, а також встановлено вимогу щодо їх захисту, то згідно до вимог статті 8 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» така інформація (інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом) повинна оброблятися в автоматизованій (інформаційній, телекомунікаційній та інформаційно-телекомунікаційній) системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством. Статтею 9 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» відповідальність за забезпечення захисту інформації в системі покладається на власника системи.

За порушення вимог законодавства передбачена відповідальність:

1. Кодекс України про адміністративні правопорушення:

Стаття 188-31. Невиконання законних вимог посадових осіб органів Державної служби спеціального зв'язку та захисту інформації України.

Невиконання законних вимог посадових осіб органів Державної служби спеціального зв'язку та захисту інформації України щодо усунення порушень законодавства про криптографічний та технічний захист інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо

захисту якої встановлена законом, та законодавства у сфері надання послуг електронного цифрового підпису, а також створення інших перешкод для виконання покладених на них обов'язків – тягнуть за собою накладення штрафу на посадових осіб від п'ятдесяти до ста неоподатковуваних мінімумів доходів громадян.

Ті самі дії, вчинені повторно протягом року після накладення адміністративного стягнення, – тягнуть за собою накладення штрафу на посадових осіб від ста до ста п'ятдесяти неоподатковуваних мінімумів доходів громадян. (Застосовується стосовно осіб, яким рекомендовано спеціально уповноваженим органом усунути виявлені порушення з питань ТЗІ, у тому числі стосовно обробки інформації в АС до завершення робіт зі створення комплексної системи захисту інформації та отримання за результатами державної експертизи атестату відповідності)

Стаття 188-39. Порушення законодавства у сфері захисту персональних даних.

Неповідомлення або несвоєчасне повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних або про зміну відомостей, які підлягають повідомленню згідно із законом, повідомлення неповних чи недостовірних відомостей – тягнуть за собою накладення штрафу на громадян від ста до двохсот неоподатковуваних мінімумів доходів громадян і на посадових осіб, громадян – суб'єктів підприємницької діяльності – від двохсот до чотирьохсот неоподатковуваних мінімумів доходів громадян.

Стаття 188-40. Невиконання законних вимог Уповноваженого Верховної Ради України з прав людини

Невиконання законних вимог Уповноваженого Верховної Ради України з прав людини або представників Уповноваженого Верховної Ради України з прав людини – тягне за собою накладення штрафу на посадових осіб, громадян – суб'єктів підприємницької діяльності від ста до двохсот неоподатковуваних мінімумів доходів громадян.

2. Кримінальний кодекс України:

Стаття 182. *Порушення недоторканності приватного життя:*

1. Незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконна зміна такої інформації, крім випадків, передбачених іншими статтями цього Кодексу, – караються штрафом від п'ятисот до однієї тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або арештом на строк до шести місяців, або обмеженням волі на строк до трьох років.

2. Ті самі дії, вчинені повторно, або якщо вони заподіяли істотну шкоду охоронюваним законом правам, свободам та інтересам особи, – караються арештом на строк від трьох до шести місяців або обмеженням волі на строк від трьох до п’яти років, або позбавленням волі на той самий строк.

Примітка. Істотною шкодою у цій статті, якщо вона полягає у заподіянні матеріальних збитків, вважається така шкода, яка в сто і більше разів перевищує неоподатковуваний мінімум доходів громадян.

Стаття 231. Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю.

Умисні дії, спрямовані на отримання відомостей, що становлять комерційну або банківську таємницю, з метою розголошення чи іншого використання цих відомостей, а також незаконне використання таких відомостей, якщо це спричинило істотну шкоду суб’єкту господарської діяльності, **караються штрафом** від **трьох тисяч до восьми тисяч** неоподатковуваних мінімумів доходів громадян.

Стаття 232. Розголошення комерційної або банківської таємниці.

Умисне розголошення комерційної або банківської таємниці без згоди її власника особою, якій ця таємниця відома у зв’язку з професійною або службовою діяльністю, якщо воно вчинене з корисливих чи інших особистих мотивів і завдало істотної шкоди суб’єкту господарської діяльності, **карається штрафом** від **однієї тисячі до трьох тисяч** неоподатковуваних мінімумів доходів громадян з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років.

Стаття 361. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку

1. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації, – карається штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк від двох до п’яти років, або позбавленням волі на строк до трьох років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до двох років або без такого та з конфіскацією програмних та технічних засобів, за допомогою яких було вчинено несанкціоноване втручання, які є власністю винної особи.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, – караються позбавленням волі на

строк від трьох до шести років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років та з конфіскацією програмних та технічних засобів, за допомогою яких було вчинено несанкціоноване втручання, які є власністю винної особи.

Примітка. Значною шкодою у статтях 361 – 363-1, якщо вона полягає у заподіянні матеріальних збитків, вважається така шкода, яка в сто і більше разів перевищує неоподатковуваний мінімум доходів громадян.

Стаття 361-2. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації

1. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства, – караються штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк до двох років з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані збут або розповсюдження інформації з обмеженим доступом, які є власністю винної особи.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, – караються позбавленням волі на строк від двох до п'яти років з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані збут або розповсюдження інформації з обмеженим доступом, які є власністю винної особи.

Стаття 362. Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї

1. Несанкціоновані зміна, знищення або блокування інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї, – караються штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років з конфіскацією програмних або технічних засобів, за допомогою яких було вчинено несанкціоновані зміна, знищення або блокування інформації, які є власністю винної особи.

2. Несанкціоновані перехоплення або копіювання інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинені особою, яка має право доступу до такої інформації, – караються позбавленням волі на строк до трьох років з позбавленням права обіймати певні посади або займатися певною діяльністю на той самий строк та з конфіскацією програмних чи технічних засобів, за допомогою яких було здійснено несанкціоновані перехоплення або копіювання інформації, які є власністю винної особи.

3. Дії, передбачені частиною першою або другою цієї статті, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, – караються позбавленням волі на строк від трьох до шести років з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років та з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані дії з інформацією, які є власністю винної особи.

Порядок виконання лабораторної роботи №11:

1. Включити ПК.
2. Ознайомитися з короткими теоретичними відомостями.
3. Розділитися на бригада по 2 чоловіки та провести аналіз державного стандарту або нормативного документу відповідно вашому варіанту (зазначеному в табл. 11.5).
4. На основі проведеного аналізу підготувати коротку доповідь.
5. Розкрити зміст функціонального профілю захищеності зазначеного в вашому варіанті завдання (згідно з НД ТЗІ 2.5-004-99) та провести його аналіз.
6. Оформити звіт згідно до вимог (додаток 1).
7. Зробити висновки, відповісти на контрольні питання та підготуватися до усного опитування.

Зміст звіту:

1. Титульний лист.
2. Постановка завдання.
3. Протокол виконання лабораторної роботи, що містить результати проведеного аналізу та опис заданого профілю захищеності.
4. Висновки та відповіді на контрольні питання.

Завдання на виконання лабораторної роботи №11

Таблиця № 11.5

Номер	Завдання

варіанта	
1	ДСТУ ISO/IEC TR 13335-1:2003 «Інформаційні технології. Керівництво з управління безпекою інформаційних технологій. Частина 1. Концепції та моделі безпеки інформаційних технологій»
	Функціональний профіль захищеності: 2.ЦД.4 = {КО-1, ЦД-4, ЦА-4, ЦО-2, ДР-3, ДС-3, ДЗ-3, ДВ-3, НР-4, НИ-2, НК-1, НО-3, НЦ-3, НТ-2}
2	НД ТЗІ 2.5-001-99 «Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації функціональних послуг захисту»
	Функціональний профіль захищеності: 3.КЦД.3 = {КД-2, КА-2, КО-1, КК-1, КВ-3, ЦД-1, ЦА-3, ЦО-2, ЦВ-2, ДР-2, ДС-1, ДЗ-1, ДВ-2, НР-3, НИ-2, НК-1, НО-2, НЦ-3, НТ-2, НВ-2}
3	ДСТУ ISO/IEC TR 13335-2:2003 «Інформаційні технології. Керівництво з управління безпекою інформаційних технологій. Частина 2. Управління та планування безпеки інформаційних технологій»
	Функціональний профіль захищеності: 1.КЦД.3 = {КА-1, КО-1, ЦА-1, ЦО-1, ДР-2, ДС-2, ДЗ-2, ДВ-2, НР-3, НИ-2, НК-1, НО-1, НЦ-2, НТ-2}
4	НД ТЗІ 2.5-002-99 «Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації гарантій захисту»
	Функціональний профіль захищеності: 3.КЦ.6 = {КД-4, КА-4, КО-1, КК-2, КВ-4, ЦД-4, ЦА-4, ЦО-2, ЦВ-3, НР-5, НИ-2, НК-2, НО-3, НЦ-3, НТ-2, НВ-2, НА-1, НП-1}
5	ДСТУ ISO/IEC TR 13335-3:2003 «Інформаційні технології. Керівництво з управління безпекою інформаційних технологій. Частина 3. Методи управління захистом інформаційних технологій»
	Функціональний профіль захищеності: 2.КД.4 = {КД-4, КА-4, КО-1, КК-2, ДР-3, ДС-3, ДЗ-3, ДВ-3, НР-5, НИ-2, НК-2, НО-3, НЦ-3, НТ-2}
6	НД ТЗІ 2.5-003-99 «Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації довірчих оцінок коректності реалізації захисту»
	Функціональний профіль захищеності: 3.КЦД.3 = {КД-4, КА-4,

	КО-1, КК-2, КВ-4, ЦД-4, ЦА-4, ЦО-2, ЦВ-3, ДР-3, ДС-3, ДЗ-3, ДВ-3, НР-5, НИ-2, НК-2, НО-3, НЦ-3, НТ-2, НА-1, НП-1, НВ-2, НА-1, НП-1}
7	ДСТУ ISO/IEC TR 13335-4:2003 «Інформаційні технології. Керівництво з управління безпекою інформаційних технологій. Частина 4. Вибір засобів захисту»
	Функціональний профіль захищеності: 1.КЦ.2 = {КА-1, КО-1, ЦА-2, ЦО-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-1}
8	НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» (зі зміною № 1).
	Функціональний профіль захищеності: 3.КЦД.4 = {КД-3, КА-3, КО-1, КК-1, КВ-3, ЦД-1, ЦА-3, ЦО-2, ЦВ-2, ДР-3, ДС-2, ДЗ-2, ДВ-2, НР-4, НИ-2, НК-1, НО-3, НЦ-3, НТ-2, НВ-2, НА-1, НП-1}
9	ДСТУ ISO/IEC TR 13335-5:2003 «Інформаційні технології. Керівництво з управління безпекою інформаційних технологій. Частина 5. Керівництво з управління мережевою безпекою»
	Функціональний профіль захищеності: 2.КЦ.2 = {КД-2, КО-1, ЦД-1, ЦО-1, НР-2, НИ-2, НК-1, НО-1, НЦ-2, НТ-1}
10	НД ТЗІ 2.5-008-02 «Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу «2»»
	Функціональний профіль захищеності: 3.КЦД.2 = {КД-2, КА-2, КО-1, КВ-2, ЦД-1, ЦА-2, ЦО-1, ЦВ-2, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1}
11	НД ТЗІ 2.5-010-03 «Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу»
	Функціональний профіль захищеності: 2.КЦД.2 = {КД-2, КА-2, КО-1, ЦД-1, ЦА-2, ЦО-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2}
12	ISO/IEC 27002:2005 «Information technology – Security techniques – Code of practice for information security management»
	Функціональний профіль захищеності: 3.КЦД.1 = {КД-2, КО-1, КВ-1, ЦД-1, ЦО-1, ЦВ-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1}

Контрольні питання:

1. Що ви розумієте під поняттями нормативно-правового забезпечення та нормативно-правового регулювання?
2. З чого складається нормативно-правова база в області інформаційної безпеки в Україні?
3. Опишіть всі фундаментальні вимоги що передбачено «Помаранчевою книгою».
4. Які групи класів захищеності визначає «Помаранчева книга»?
5. Назвіть основні складові загальної оцінки рівня безпеки системи згідно «Критеріїв ДСТС ЗІ СБУ».
6. Перерахуйте всі показники критеріїв конфіденційності згідно НД ТЗІ 2.5-004-99.
7. Що ви розумієте під Критеріями цілісності згідно «Критеріїв ДСТС ЗІ СБУ»?
8. Що регламентують критерії доступності та спостережності згідно НД ТЗІ 2.5-004-99?
9. Що таке критерії гарантій і для чого вони потрібні?
10. Назвіть та розкрийте ключові поняття «Загальних критеріїв».
11. Коротко опишіть стандарт ISO/IEC 17799:2005.
12. Опишіть модель PDCA.

Лабораторна робота №12
«Організаційний підхід до забезпечення інформаційної та кібернетичної безпеки провідних країн світу»

Мета роботи:

1. Ознайомлення з сучасними трендами кібербезпекової політики та з ситуацією із забезпеченням кібербезпеки в Україні.
2. Проведення аналізу основних принципів забезпечення інформаційної та кібернетичної безпеки в США, Китаї, РФ, Україні та країнах Євросоюзу.

Стислі теоретичні відомості:

12.1. Кібербезпекова політика провідних держав світу

Тенденції розвитку інформаційних технологій, які спостерігаються в останні роки, не лише дають змогу будувати більш ефективне та успішне суспільство, але й надають нових імпульсів традиційним загрозам безпеки держави, які можуть вже в недалекому майбутньому привести до появи якісно нових (інформаційних) форм боротьби, в тому числі і на міждержавному рівні, які можуть приймати форму інформаційної війни, а сама інформаційна війна

стане одним з основних інструментів зовнішньої політики, включаючи захист державних інтересів і реалізацію будь-яких форм агресії.

В таких умовах особливого значення набуває пошук нових можливостей забезпечення безпеки держави з огляду на формування нового поля протиборства – *кіберпростору*. На сьогоднішній день кіберпростір, через певну новизну, все ще не повністю нормативно врегульований на міжнародному рівні, тому спецоперації, що здійснюються в ньому військовими чи розвідувальними підрозділами, не підпадають під визначення «акту війни» і можуть бути віднесені до операцій «відмінних від війни». Фактично, йдеться про можливість забезпечити ефект військового втручання без подальших офіційних санкцій як з боку держави, що зазнала нападу, так і світового співтовариства. Це є однією з причин, чому корисно ознайомитися з основними принципами забезпечення ІБ в провідних зарубіжних країнах.

Інша причина полягає в тому, що більшість засобів і методів забезпечення ІБ, які застосовуються на території України засновані на імпортних методиках і будуються з імпортних компонентів, які були розроблені відповідно до норм і вимог щодо забезпечення ІБ країн-виробників. У зв’язку з цим, перш ніж приступити до вивчення безпосередньо технологій і засобів забезпечення ІБ, слід познайомитися з кібербезпековою політикою провідних зарубіжних країн.

На сьогоднішній день більшість потужних держав світу (США, Росія, ЄС, Китай, Індія та інші) знаходяться в процесі трансформації власних військових потенціалів з огляду на можливості використання мережі Інтернет. За даними керівника компанії McAfee, оприлюдненими на Всесвітньому економічному форумі в Давосі ще у 2010 р., на той час, більше 20 країн планували здійснювати або реально здійснювали різноманітні інформаційні операції. Також були сформовані спецпідрозділи, які мають на меті: ведення розвідувальної роботи в мережах, захист власних мереж, блокування і «обвал» структур супротивника. Згідно з офіційними заявами, такі підрозділи створено в США (U.S. Cyber Command), Великобританії (Cyber Security Operations Centre при уряді Великобританії), Німеччині (Internet Crime Unit та Federal Office for Information Security), Австралії (The Cyber security operations centre), Індії та інших державах. Активну позицію щодо протидії кіберзагрозам займає і провідна міжнародна міжурядова організація – НАТО (Cooperative Cyber Defence Centre of Excellence).

Про рівень занепокоєності провідних держав світу у сфері кібербезпеки свідчить і бажання врегулювати на міжнародному рівні можливість визнання кібератаки «актом війни». 30 січня 2010 р., під час Всесвітнього економічного форуму у Давосі, сенатор США від Республіканської партії С. Колінз зазначила, що США всерйоз розглядають питання щодо ставлення до кібератак як до

оголошення війни, а 12 травня 2010 р. помічник заступника міністра оборони США з політичних питань Дж. Мілер заявив, що США готові нанести військовий удар у відповідь на кібератаки на свої комп'ютерні мережі. Така позиція США щодо трактування кібератак та потенційних кібервійн набуває свого продовження і в межах НАТО: група експертів під керівництвом М. Олбрайт у червні 2010 р. запропонувала трактувати масштабні кібератаки як такі, що підпадають під п'яту статтю Північноатлантичного договору і вважаються атаками на всіх членів Альянсу.

На сьогоднішній день найбільш потужними та активними вважають військові кіберпідрозділи КНР та США, які були створені майже синхронно. Дані про потенціал, чисельність чи завдання китайських кібервійськ практично відсутні, однак відомо шифр відповідної структури – «61398», у складі якої приблизно 2 тисячі фахівців, готових атакувати комп'ютерні мережі противника. Додатково також використовуються і групи хакерів, найбільша з яких – так званий Альянс червоних хакерів із щонайменше 80 тис. фахівців цієї справи. Причому до гільдії «червоних» входять хакери не тільки з КНР, а й з китайської діаспори в усьому світі. Альянс тісно взаємодіє з 3-м і 4-м управліннями Генштабу Народно-визвольної армії Китаю.

За даними видання The Daily Beast, ФБР підготувало секретний звіт, який висвітлює рівень розвитку кібервійськ КНР та тих загроз, які цей розвиток несе для США. В цьому Звіті КНР названо «найбільшою цілісною загрозою США у сфері кібертероризму» та силою, що вже зараз може володіти потенціалом «знищувати життєво важливу інфраструктуру, отримувати доступ до банківських, комерційних, військових та оборонних баз даних». Лише за приблизними розрахунками, збиток американських компаній від китайського економічного шпіонажу оцінюють у понад 300 млрд доларів. У світі вже навіть придумали цьому феномену назву – *«холодна кібервійна»*. При цьому Китай і надалі продовжує розширювати свої можливості ведення кібервійни, купуючи іноземні системи космічного моніторингу і збору розвідданих, антирадари, інфрачервоні приманки й генератори хибних цілей, удосконалюючи військові інформаційні мережі.

Не менш активною політикою в сфері кібербезпеки у США була і за Адміністрації Б.Обами:

- 29 травня 2009 року було оприлюднено «Огляд кібербезпеки» (Cyber Security Review) – комплексний документ, що визначає основні пріоритети нової команди у сфері кібербезпеки;
- створено посаду Керівника Кібербезпеки Ради національної та внутрішньої безпеки;

- створено Кіберкомандування США (U.S. Cyber Command) під головуванням генерала К. Александера, що одночасно очолював і згаданий підрозділ і Агентство з національної безпеки. Приблизна чисельність структури – 30 000 військових;
- оприлюднено нову «Стратегію національної безпеки» (2010) в якій кіберзагрозам вперше відведено окреме місце в загальній структурі загроз США;
- збільшено держзамовлення на розробку нових засобів ведення війни і зокрема – кіберозброєнь та нових, більш захищених, військових мереж;
- створено проекти нормативних документів, що спрямовані на покращення взаємодії в сфері кібербезпеки союзниками США та убезпечення власного Інтернет простору в разі виникнення ситуацій, що загрожують національній безпеці.

Ще однією країною потенціал якої в сфері кіберзахисту вважається одним з найпотужніших є Великобританія, яка все ще продовжує розбудовувати власні сили безпеки у кіберпросторі. У 2010 році запустила у повноцінному режимі роботу Оперативного центру з кібербезпеки (20 співробітників) з метою координації вже існуючих різноманітних центрів із кібербезпеки різних відомств та створення майданчику для співпраці між урядом та приватним сектором із проблем кібербезпеки. Крім того у Великобританії ефективно працює Командування урядових комунікацій (Government Communications Headquarters), що забезпечує як захист критично важливої урядової інформації, так і отримання розвідувальних даних за допомогою новітніх комунікативних засобів.

Згідно з відкритими даними, активно створюються відповідні підрозділи у Південній та Північній Кореї, Російській Федерації, Франції.

Така увага до забезпечення кібербезпеки та створення засобів ведення кібервійн, змушує уряди держав переглядати і свою внутрішню політику в кіберсфері. Це обумовлено, в тому числі, і зростанням кількості випадків використання розвідувальними службами та спеціалізованими військовими підрозділами можливостей та технічних потужностей транснаціональних кримінальних груп, що спеціалізуються у сфері кіберзлочиності. Це логічним чином спричиняє зміни у політиці провідних держав світу до можливостей обмежувальної та, певною мірою, цензурної політики, як однієї із форм ведення внутрішньої інформаційної політики. Все активніше застосовується так званий «низько технологічний» (low-tech) рівень контролю, до якого відносять бюрократичні, організаційні та обмежувальні методи захисту власного інформаційного та кіберпростору від латентних загроз безпеці даних та постійного впровадження іноземних програмних продуктів.

Таким чином, політика країн Заходу в сфері внутрішнього інформаційного (кіберпростору) все частіше набуває окремих рис політики тих країн, що традиційно відносять до авторитарних, хоча і з певними суттєвими відмінностями. Якщо в країнах авторитарного типу спостерігається політики в першу чергу прямого обмеження доступу, то країни Заходу йдуть шляхом нарощування кількості даних про користувачів, моніторингу в першу чергу національного Інтернет-трафіку та отриманню можливостей цільового відключення окремих елементів Мережі чи її користувачів. Такий акцент на «моніторинговому дискурсі» обумовлений, в тому числі, зростанням кількості телекомунікаційних послуг та мереж, контроль за якими значною мірою ускладнено для державних правоохоронних служб. Зокрема це відноситься і до контролю за перемовинами власників смартфонів та VoIP-системи. Так наприклад смартфони Blackberry не лише підтримують систему шифрування даних, що передаються, але й сервери цих компаній знаходяться в США та Великобританії, що більшістю правоохоронних органів інших країн вважається джерелом небезпеки, оскільки унеможливлює контроль за спілкуванням користувачів Blackberry та потенційно робить доступним листування власників для американських та британських спецслужб. Саме це стало причиною введення обмежень на використання даних смартфонів (особливо в державному секторі) в таких країнах як Франція, Німеччина, Індія, Об'єднані Арабські Емірати та Російська Федерація. Крім того, керівництво ЄС також заборонило своїм службовцям користуватись смартфонами даної фірми.

Щодо VoIP-телефонії, то основні претензії виникають до програмного продукту Skype, оскільки він забезпечує ефективний криптографічний захист перемовин абонентів, що практично унеможливлює перехоплення їх з боку спецслужб. Це стало однією з причин конфлікту між авторами програми та спецслужбами деяких країн (Італія, Російська Федерація, Індія, Німеччина, Великобританія). Крім того, в 2010 році урядом США для ФБР було виділено додатково 234 млн дол. для спеціального проекту з прослуховування Інтернет (Advanced Electronic Surveillance - Going Dark), що спрямований, в першу чергу, на можливість прослуховування Інтернет-комунікаторів (наприклад того ж Skype).

Варто зазначити, що, частіше за все, такі заходи із більш інтенсивного моніторингу контенту Всесвітньої Мережі та окремих технологічних рішень, що забезпечують доступ до неї, пояснюються однією з трьох (або їх сукупністю) причин:

1. Зростанням терористичної загрози, використанням терористами та міжнародними кримінальними структурами новітніх інформаційних технологій та зростання загрози критичній інфраструктурі держави.

2. Боротьба із комп'ютерним піратством, протидія порушенню авторських прав на ті чи інші продукти (зокрема аудіо та відео контент) тощо.

3. Протидія розповсюдженню дитячої порнографії.

Також сталим залишається бажання держави більше знати про Інтернет-трафік громадян, а за можливості – і про контент їх персональних комп'ютерів. В контексті цього держави намагаються посилити контроль за точками доступу до мережі Інтернет (зокрема – Інтернет-кафе) та Інтернет-трафіком громадян. Так в КНР для Інтернет-кафе діють такі ж правила, як і для барів – розміщення не ближче ніж 200 ярдів від школи, обов'язковий віковий ценз для отримання доступу для певних послуг. В цілому, для того щоб отримати можливість попрацювати із Мережею обов'язково потрібен документ, що засвідчує особу. Однак, в деяких містах Китаю (наприклад Пекіні, де кількість Інтернет-кафе сягає 1500) застосовуються додаткові методи ідентифікації – встановлюються камери спостереження, а будь-який користувач має бути сфотографований. Схожі обмеження впроваджує і Білорусь. Однак практика контролю за діяльністю Інтернет-кафе притаманна і західним державам: поліція Великобританії також планує налагодити співробітництво із власниками Інтернет-кафе з метою контролю за контентом, що переглядається відвідувачами (для запобігання підготовки терактів).

Спостерігаються і активні спроби посилити контроль за Інтернет-трафіком громадян та збільшити можливості правоохоронних органів у боротьбі із шкідливим контентом. Так у Франції в серпні 2010 року урядовою агенцією HADOPI, що займається охороною авторського права в мережі Інтернет, з метою поліпшення практичного виконання закону про «Три попередження», було внесено пропозицію запропонувати французьким користувачам поки що добровільно встановити на свої комп'ютери спеціальне програмне забезпечення, що буде відслідковувати весь трафік користувача, шукати встановлене нелегальне на комп'ютері програмне забезпечення, надавати відомості правоохоронним органам щодо переглянутого користувачем відео в мережі Інтернет. На загальноєвропейському рівні дії Директива ЄС «Щодо охорони прав на інтелектуальну власність» (Directive 2004/48/EC, Intellectual Property Rights Enforcement Directive, IPRED), яка дозволяє правоохоронним органам збирати особисті дані користувачів, запідозрених у незаконному файлообміні. Водночас варто відзначити, що дана Директива поки що імплементована в законодавство лише декількох країн ЄС (Великобританія, Франція, Данія, Швеція). Особлива увага з боку правоохоронних органів приділяється контролю за контентом у соціальних мережах, блогах тощо.

В США, з метою контролю за соціальними мережами інвестиційний підрозділ ЦРУ In-Q-Tel фінансує компанію Visible Technologies, яка займається

моніторингом блогів та соціальних мереж. Розробка Visible Technologies дозволяє щоденно піддавати моніторингу більш ніж півмільйона різноманітних сайтів, перевіряючи пости у блогах, а також коментарі на форумах та сервісах Flickr, YouTube, Twitter та Amazon. Так наприклад за результатами схожого за суттю моніторингу у липні 2010 року було закрито блогхостинг Blogetery.com, на якому розміщувалось 73.000 блогів – фахівці ФБР знайшли на ньому посилання на матеріали Аль-Каіди. Така практика поступової актуалізації участі державних органів у функціонуванні мережі Інтернет та посилення їх моніторингових та контролюючих функцій вже практично не зустрічає опору навіть у тих країнах, де існує активний контроль за збереженням демократичних свобод. За результатами опитування компанії Sophos, більшість американців не бачать проблем із тим, що уряд використовує технології для моніторингу та фільтрації мереженого трафіку, а також має доступ до поштових серверів. Опитані стверджують, що не проти доступу спецслужб до їх пошти.

12.2. Ситуація із забезпеченням кібербезпеки в Україні

В Україні основними напрямами державної політики у сфері кібербезпеки є:

- створення захищеного національного сегмента кіберпростору, що сприятиме підтриманню відкритого суспільства і забезпечуватиме безпечне використання цього простору суспільством;
- запобігання втручанню у внутрішні справи України і нейтралізація посягань на її інформаційні ресурси з боку інших держав;
- посилення обороноздатності держави у кіберпросторі;
- боротьба з кіберзлочинністю та кібертероризмом;
- зниження рівня уразливості об’єктів кіберзахисту;
- забезпечення повноправної участі України в загальноєвропейській та регіональних системах забезпечення кібербезпеки;
- дотримання міжнародних зобов’язань щодо боротьби з кіберзлочинністю та кібертероризмом.

В самі ж системі забезпечення кібербезпеки держави задіяно низку військових та правоохоронних органів:

1. Міністерство оборони України (та його спеціальні підрозділи – зокрема Головне управління розвідки);
2. Генеральний штаб Збройних Сил України;
3. Службу безпеки України;
4. Державну службу спеціального зв’язку та захисту інформації;
5. Міністерство внутрішніх справ України (Кіберполіція);

6. Службу зовнішньої розвідки.

Водночас, діяльність цих відомств не завжди відповідним чином забезпечується. Так в системі Міністерства оборони України існують спеціальні підрозділи на які покладено задачі із забезпечення кібербезпеки військових інформаційних ресурсів та мереж. В цій діяльності, зокрема, задіяні сили Головного управління Військової служби правопорядку, Військової розвідки (Головне управління розвідки МО України) та підрозділи радіоелектронної боротьби. Водночас, матеріально-технічне та, частково, кадрове забезпечення даних служб залишається на незадовільному рівні, а значна частина матеріально-технічної бази практично не оновлювалась протягом тривало часу.

Окрім цього в Україні, досі, жодного разу не проводились комплексні навчання із проблем кібербезпеки (на кшталт навчань «Кіберштурм», що проводяться в США) із залученням всіх відомств, що задіяні в системі кібербезпеки держави. До того ж, незважаючи на зусилля спеціальних відомств, на думку деяких фахівців, Україна все ще залишається уразливою (особливо її телекомунікаційна складова), не в останню чергу через надмірно широке впровадження західних програмних продуктів (зокрема фірми Microsoft) та використання матеріально-технічної бази іноземного виробництва. Пошук можливих «закладок» у цій продукції практично унеможливлений, а залежність української держави від згаданих продуктів становить загрозливий рівень для національної безпеки (зокрема фінансової). Актуальною залишається проблема створення національної операційної системи (принаймні для використання в системі органів державної влади), відновлення вітчизняних потужностей із виробництва матеріально-технічної телекомунікаційної бази (особливо для потреб закритих відомчих інформаційних систем), стимулювання з боку держави створення національного антивірусу.

Порядок виконання лабораторної роботи №12:

1. Включити ПК.
2. Ознайомитися з короткими теоретичними відомостями.
3. Підготувати коротку доповідь з заданого питання (згідно варіанту в табл. 12.1).
4. Сформувати та заповнити порівняльну таблицю країн згідно з завданнями визначеними в таблиці 12.1 на основі підготовлених матеріалів та доповідей інших студентів[8].
5. Оформити звіт згідно до вимог (додаток 1).

[8] Пояснення: тобто, наприклад, якщо у вашому варіанті вказано завдання: «основні принципи забезпечення кібербезпеки», то необхідно сформувати порівняльну таблицю основних принципів забезпечення кібербезпеки всіх зазначених країн в таблиці.

6. Відповісти на контрольні питання та підготуватися до усного опитування.

Зміст звіту:

1. Титульний лист.
2. Постановка завдання.
3. Протокол виконання лабораторної роботи, що містить доповідь та порівняльну таблицю за результатами проведеного аналізу.
4. Висновки та відповіді на контрольні питання.

Завдання на виконання лабораторної роботи №12

Таблиця № 12.1. (варіант відповідно до номера за списком у журналі)

Номер варіанта	Завдання
1	Основні принципи забезпечення кібербезпеки в США
2	Державна система забезпечення інформаційної безпеки в Німеччині
3	Основні положення кіберстратегії Франції
4	Основні принципи забезпечення кібербезпеки в Швеції
5	Основні положення кіберстратегії України
6	Основні вимоги щодо забезпечення ІБ в Китаї
7	Основні принципи забезпечення кібербезпеки в Канаді
8	Основні вимоги щодо забезпечення ІБ в Німеччині
9	Державна система забезпечення інформаційної безпеки в Китаї
10	Основні принципи забезпечення кібербезпеки в Сінгапурі
11	Основні вимоги щодо забезпечення ІБ в Франції
12	Державна система забезпечення інформаційної безпеки в США
13	Основні принципи забезпечення кібербезпеки в Китаї
14	Основні положення кіберстратегії Німеччини
15	Основні принципи забезпечення кібербезпеки в Естонії
16	Основні вимоги щодо забезпечення ІБ в Канаді
17	Державна система забезпечення інформаційної безпеки в Сполученому Королівстві Великобританії та Північної Ірландії
18	Основні принципи забезпечення кібербезпеки в Швейцарії
19	Основні вимоги щодо забезпечення ІБ в США
20	Основні принципи забезпечення кібербезпеки в Німеччині
21	Основні положення кіберстратегії РФ
22	Державна система забезпечення інформаційної безпеки в Франції
23	Основні принципи забезпечення кібербезпеки в Франції
24	Державна система забезпечення інформаційної безпеки в Швеції

25	Основні положення кіберстратегії США

Контрольні питання:

1. В чому полягає необхідність ознайомлення з основними принципами забезпечення інформаційної та кібернетичної безпеки провідних країн світу?
2. Що означає вислів «холодна кібервійна»?
3. Назвати основні причини зростання інтенсивного моніторингу контенту Всесвітньої Мережі в Західних країнах.
4. Перерахувати основні військові та правоохоронні органи України, які задіяні в системі забезпечення кібербезпеки держави.
5. Назвати основні прогалини в забезпеченні кібербезпеки України.

Лабораторна робота №13
«Криптографічні методи забезпечення конфіденційності та цілісності інформації»

Мета роботи:

1. Закріплення основних понять криптографічних методів захисту інформації.
2. Поглиблення теоретичних знання з наступних питань:
   - симетричне та асиметричне шифрування;
   - функції хешування;
   - електронний цифровий підпис.
3. Ознайомлення та дослідження проблем реалізації симетричної криптосистеми обміну повідомленнями в ІТС з використанням шифрування методом перестановки.
4. Вивчення технології хешування на основі хеш-функції Adler-32.

Стислі теоретичні відомості:

13.1. Основні поняття і задачі криптографії

Проблема приховування інформації була актуальна для людства ще в стародавні часи, письмові свідчення про використання найпростіших методів шифрування зустрічаються ще у стародавніх греків у V-VI ст. до н. е. Розвиток цивілізації, поява нових засобів комунікації (спочатку письмових, потім електронних) пред'являли до методів шифрування все більш жорсткі вимоги, що вилилося в появу окремої науки, яка займається захистом інформації шляхом її перетворення – ***криптології*** (kryptos – таємний, logos – наука). У цієї науки є два напрямки: криптографія та криптоаналіз.

До 70-х років XX століття ***криптографією*** називали напрям науки і практичної діяльності, пов'язаний з вивченням і розробкою методів шифрування даних. В даний час це напрям науки, техніки і практичної діяльності, пов'язаний з розробкою, використанням і аналізом криптографічних систем захисту інформації.

Криптографічна система – це система забезпечення інформаційної безпеки мережі або ІТС, використовуючи криптографічні засоби. Може включати підсистеми шифрування, ідентифікації користувачів, електронного цифрового підпису та ін.

Криптографічні засоби – методи і засоби забезпечення інформаційної безпеки, що використовують криптографічні перетворення інформації. У вузькому сенсі під криптографічними засобами можуть розумітися окремі пристрої, документи і програми, що використовуються для виконання функцій криптосистеми.

Криптографічне перетворення інформації – перетворення інформації з використанням одного з криптографічних алгоритмів. До криптографічних алгоритмів відносяться алгоритми шифрування/розшифрування, хешування, формування та перевірки електронного цифрового підпису, розподілу ключів і безліч інших алгоритмів, кожен з яких призначений для протидії визначеним загрозам інформаційної безпеки з боку можливого порушника (противника, зловмисника) або небажаних впливів природного характеру. Більшість криптографічних алгоритмів будуються на математичній основі.

Таким чином, під ***криптографічним захистом інформації*** (КЗІ) прийнято розуміти вид захисту, що спрямований на унеможливлення реалізації загроз несанкціонованого доступу до інформації з обмеженим доступом, модифікації або нав'язування хибної інформації (тобто порушенню конфіденційності, цілісності та авторства на інформацію) шляхом використання математичних перетворень інформації з використанням секретних параметрів – ***ключових даних***.

До основних задач захисту інформації, які вирішуються шляхом застосування криптографічних перетворень, відносяться:

1) забезпечення конфіденційності інформації, захист від несанкціонованого ознайомлення з її змістом;

2) контроль цілісності інформації, уникнення несанкціонованих її змін шляхом вставки, видалення або зміни фрагментів;

3) аутентифікація суб'єктів і ідентифікація об'єктів інформаційного обміну, підтвердження істинності сторін, самої інформації, часу її створення;

4) підтвердження авторства, забезпечення неможливості відмови.

Друга частина криптології – ***криптоаналіз***. До 70-х років XX століття ця наука займалася оцінкою сильних і слабких сторін методів шифрування, а також розробкою методів злому шифрів. В даний час *криптоаналіз* – галузь науки, що займається вивченням криптографічних систем захисту в пошуку способів порушення інформаційної безпеки, яку забезпечує ця система. Таким чином, криптоаналіз вивчає інженерно-математичні методи відновлення первинного вигляду зашифрованої інформації без знання секретних параметрів перетворень (*методів дешифрування*). Криптографія та криптоаналіз – дві сильно взаємодіючі науки з протилежними цілями. За останні кілька десятиліть вони безперервно й інтенсивно розвиваються, причому досягнення однієї з них змушують іншу швидко реагувати вдосконаленням свого апарату.

Будь-який криптографічний метод характеризується двома основними характеристиками. Першою є ***криптостійкість*** – мінімальний обсяг зашифрованого тексту, статистичним аналізом якого можна розкрити вихідний текст. Таким чином, стійкість визначає допустимий обсяг інформації, зашифрованої з використанням одного ключа. Іншою важливою характеристикою є ***трудомісткість*** методу, яка визначається кількістю елементарних операцій, необхідних для шифрування одного символу вихідного тексту.

Основними криптографічними процедурами є *шифрування* і *розшифрування*, але також необхідно не забувати про можливість *дешифрування*.

Шифрування – це перетворення вихідного (інакше – відкритого) тексту T в *шифрований* текст S з використанням конфіденційних даних K відповідно до деякого алгоритму E (від англ. encryption – шифрування). Параметр K в криптографії називається ***ключем***. Ключ є тією інформацією, без якої неможливе відновлення початкового повідомлення. Рівняння шифрування записують у вигляді:

$$S = E(T, K) \text{ або } S = E_K(T). \qquad 13.1$$

Шифрування нерідко плутають з кодуванням, але між цими двома процесами є значна різниця. Кодування також являє собою перетворення вихідного повідомлення в іншу форму, але мета цього перетворення – зручність обробки або передачі повідомлення. Наприклад, символьний текст кодується в двійковий (кожний символ замінюється послідовністю нулів і одиниць) для того, щоб його можна було зберігати та обробляти в ЕОМ, а двійковий текст перетворюється в послідовність електричних імпульсів, для того, щоб стала можливою його передача по кабелю. Мета шифрування – протилежна. Текст зашифровується для того, щоб сторонні особи, що не володіють ключем, не змогли б ознайомитися з закладеною в ньому інформацією, навіть перехопивши

сам зашифрований текст. Таким чином, шифрування є засобом забезпечення конфіденційності інформації.

Розшифрування (не путати з *дешифруванням*) – обернена відносно шифрування процедура D (від англ. decryption – розшифрування), в результаті виконання якої шифрований текст з використанням ключа перетвориться у вихідний:

$$T = D(S, K) \text{ або } T = D_K(S). \qquad 13.2$$

Конкретну процедуру відновлення інформації або розкриття шифру без знання секретних параметрів перетворень, називають ***дешифруванням*** (або *криптоаналітичною атакою*).

Також необхідно відмітити, що сам процес криптографічного перетворення даних може здійснюватися як програмно, так і апаратно. Апаратна реалізація відрізняється суттєво більшою вартістю, однак їй властиві й переваги: висока продуктивність, простота, захищеність і т.д.. Програмна реалізація більш практична, допускає відому гнучкість у використанні.

Для сучасних криптографічних систем захисту інформації сформульовані наступні *загальноприйняті вимоги*:

- зашифроване повідомлення повинне піддаватися читанню тільки при наявності ключа;
- число операцій, необхідних для визначення використовуваного ключа шифрування по фрагменту шифрованого повідомлення й відповідного йому відкритого тексту, повинне бути не менше загального числа можливих ключів;
- число операцій, необхідних для розшифровування інформації шляхом перебору всіляких ключів, повинне мати строгу нижню оцінку й виходити за межі можливостей сучасних комп'ютерів (з урахуванням можливості використання мережних обчислень) або вимагати неприйнятно високих витрат на ці обчислення;
- знання алгоритму шифрування не повинне впливати на надійність захисту;
- незначна зміна ключа повинна приводити до істотної зміни виду зашифрованого повідомлення навіть при шифруванні того самого вихідного тексту;
- незначна зміна вихідного тексту повинна приводити до істотної зміни виду зашифрованого повідомлення навіть при використанні того самого ключа;
- структурні елементи алгоритму шифрування повинні бути незмінними;
- додаткові біти, що вводяться в повідомлення в процесі шифрування, повинні бути повністю й надійно сховані в шифрованому тексті;
- довжина шифрованого тексту не повинна перевищувати довжину вихідного тексту;

- не повинно бути простих і легко встановлюваних залежностей між ключами, послідовно використовуваними в процесі шифрування;
- будь-який ключ із множини можливих повинен забезпечувати надійний захист інформації;
- алгоритм повинен допускати як програмну, так і апаратну реалізацію, при цьому зміна довжини ключа не повинна призводити до якісного погіршення алгоритму шифрування.

Алгоритми шифрування поділяються на дві великі групи:

1. Симетричне (традиційне шифрування).
2. Асиметричне (шифрування з відкритим ключем).

13.2. Симетричне шифрування

Симетричні криптографічні алгоритми – це спосіб криптографічного захисту інформації, у якому для шифрування і розшифрування використовується один і той же криптографічний ключ. Ключ алгоритму повинен зберігатися в секреті обома сторонами (резидентом – одержувачем і респондентом – відправником).

Історично симетричне шифрування з'явилося першим. Більше того, до середини XX століття це було єдиним різновидом шифрування, воно широко застосовуються і в даний час.

Симетричні криптографічні алгоритми поділяються на ***блокові*** і ***потокові***. Блочні алгоритми обробляють інформацію блоками певної довжини (64, 128, 192, 256 біт), застосовуючи до блоку даних ключ в установленому порядку, як правило, декількома циклами перемішування і підстановки, які називаються *раундами*. Результатом повторення раундів є лавинний ефект – наростаюча втрата відповідності бітів між блоками відкритих і зашифрованих даних.

До переваг блокових алгоритмів відносять схожість процедур шифрування і розшифрування, які відрізняються тільки порядком дій. Це спрощує створення апаратури для реалізації цих алгоритмів. Найбільш поширені блочні алгоритми шифрування – це *метод перестановки* і *метод заміни* з різними варіаціями.

Шифрування методом заміни (підстановки) полягає в заміні символів одного алфавіту на символи іншого алфавіту, званого шифроалфавітом. Останній отримують перестановкою літер алфавіта у довільному порядку. Шифроалфавіт (таблиця відповідностей) і є ключем для шифрування і розшифрування. Заміна може бути заміною «символи на символи або символи на цифри». По стійкості та трудомісткості методи заміни поділяються на:

одноалфавітну підстановку, багатоалфавітну одноконтурну підстановку, багатоалфавітну одноконтурну монофонетичну підстановку, багатоалфавітну багатоконтурну підстановку. Шифрування методом перестановки, детально, буде розглянуто нижче.

В потокових алгоритмах, шифрування проводиться над кожним бітом або байтом вихідного тексту з використанням *гамування* (накладення на вихідний текст гамма-послідовності бітів з логічною операцією XOR – «Виключне АБО»).

Шифр може бути легко створений на основі блокового шифру, запущеного в спеціальному режимі (наприклад, по ГОСТ 28147-89 в режимі гамування). Потокові алгоритми шифрування також зручні для апаратурної реалізації і широко використовувалися задовго до появи комп'ютерів.

Початок широкого застосування потокових алгоритмів шифрування поклала робота *Клода Шеннона*, опублікована в 1949 році. В ній Шеннон довів абсолютну стійкість шифру *Вернама* (також відомого як одноразовий блокнот). У шифрі Вернама ключ має довжину, рівну довжині самого переданого повідомлення. Таким чином, відкритий текст складається з абсолютно випадковим ключем, який збігається з ним за розміром. Після цього ключ знищується (тобто не використовується для шифрування інших текстів). Стійкість даного шифру полягає в тому, що ключ використовується в якості гами і, якщо кожен біт ключа вибирається випадково, то розкрити шифр неможливо (оскільки всі можливі відкриті тексти будуть рівноймовірні).

На практиці одноразові блокноти застосовуються дуже рідко (лише для повідомлень найвищої секретності). По-перше, виготовлення такого блокнота є досить дорогим (так як абсолютно випадкова послідовність не може генеруватися алгоритмічно), а блокнот призначений лише для одноразового використання. По-друге, виникає проблема передачі ключа: єдиний надійний варіант – особиста зустріч. Дійсно, припустимо що у відправника і одержувача повідомлення є надійний канал обміну інформацією. Тоді чому б не передавати по цьому каналу незашифровані повідомлення. Якщо ж відправити ключ, зашифрувавши його іншим алгоритмом, вся система виявиться надійної не більше, ніж цей алгоритм.

До теперішнього часу створено чимало алгоритмів потокового шифрування. Найбільш відомі з них: A3, A5, A8, RC4, PIKE, SEAL, eSTREAM та ін.

Відомо і комбіноване застосування алгоритмів блокового і потокового шифрування. Наприклад, у відомому алгоритмі DES процедури CFB і OFB використовують алгоритми блочного шифрування в режимі потокового шифрування.

Перевагою потокових алгоритмів порівняно з блочними є висока швидкість шифрування, порівнянна зі швидкістю надходження вхідної інформації. Недоліком потокових алгоритмів шифрування є істотно більша кількість методів їх злому (криптоаналізу) порівняно з блочними алгоритмами.

Всі алгоритми симетричного шифрування мають загальну проблему, що випливає з тієї обставини, що і відправник і одержувач повідомлення повинні володіти одним і тим же ключем. При цьому передбачається, що у них немає абсолютно надійного каналу зв'язку, оскільки в іншому випадку в шифруванні б не було потреби.

Якщо століття тому ця проблема цілком вирішувалася, наприклад, шляхом особистої зустрічі, то в даний час, коли інтенсивність обміну інформацією зросла в сотні разів і автоматизовані практично всі сфери людської діяльності, це неможливо. Необхідність термінового конфіденційного листування може виникнути у ділових партнерів, які живуть у різних країнах (можливо навіть не знайомих особисто), або інтернет-банкінг, який дозволяє управляти своїм банківським рахунком, не виходячи з дому, але при цьому всі операції повинні бути конфіденційними, а отже, весь потік даних між банком і клієнтом повинен бути зашифрований. При цьому ключі шифрування повинні регулярно змінюватись, оскільки обмін навіть кількома повідомленнями з одним ключем зменшує надійність шифрування.

Таким чином, для симетричних алгоритмів характерна *проблема обміну ключами*.

13.2.1. Шифрування методом перестановки

Шифрування методом перестановки відноситься до симетричних криптографічних алгоритмів. Найпростіше шифрування перестановкою полягає в перестановці символів повідомлення відповідно до заданих порядкових номерів (ключа). Наприклад, слово «шифр» по ключу 3-1-4-2 зашифрується в «фшри». Якщо довжина повідомлення перевищує довжину ключа, ключ застосовують повторно.

На практиці застосовують більш складні алгоритми перестановки з двох і більше ключів. Наприклад, потрібно *зашифрувати* відкритий вихідний текст: «ШИФРУВАННЯ_ПЕРЕСТАНОВКОЙ». По ключу $k_1 = 5\text{-}3\text{-}1\text{-}2\text{-}4\text{-}6$ записуємо даний текст у таблицю рядками (табл. 13.1). Починаємо з рядка 5. Коли комірки цього рядка заповняться, продовжуємо записувати вихідний текст в рядок 3, потім – у рядок 1 і так далі у відповідності з ключем k_1.

Таблиця 13.1. Шифрування методом перестановки за ключами k_1 та k_2.

	1	2	3	4
1	Н	Я	_	П
2	Е	Р	Е	С
3	У	В	А	Н
4	Т	А	Н	О
5	Ш	И	Ф	Р
6	В	К	О	Й

По ключу $k_2 = 4\text{-}2\text{-}3\text{-}1$ зчитуємо текст за стовпцями в таблиці. Розпочинаючи з колонки 4, потім читаємо стовпець 2 і так далі у відповідності з ключем k_2. Після проведення всіх операцій отримаємо зашифрований текст: «ПСНОРЙЯРВАИК_ЕАНФОНЕУТШВ».

Розшифрування проводиться в зворотному порядку. Спочатку по ключу k_2 записуємо зашифрований текст у таблицю по стовпцях. Потім по ключу k_1 зчитуємо записаний текст з таблиці по рядках.

Вимоги до ключів:

- номери в ключі повинні бути цілими додатними числами більше 0;
- номери в ключі не повинні повторюватися;
- максимальне значення номера в ключі має не перевищувати кількості номерів в ключі.

Якщо повідомлення, яке підлягає шифруванню, не вміщується в таблиці, заданої ключами k_1 та k_2 (*шифротаблиці*), то його необхідно розділити на блоки, розмір кожного з яких відповідає розміру шифротаблиці. Тому цей метод називають ще блоковим шифруванням.

Існують і більш складні алгоритми шифрування методом перестановки, наприклад, засновані на алгоритмі кубика Рубіка, реалізовані у відомому пакеті програм для шифрування «Рубікон».

13.3. Асиметричне шифрування

Великим досягненням криптографії останньої чверті XX століття стало винайдення методу шифрування, заснованого на використанні пари ключів, один з яких призначений тільки для шифрування, а інший – для розшифрування. Таким чином, резидент генерує два ключі: закритий (*секретний*), який нікому не передає і зберігає тільки у себе, і відкритий (*публічний*), який передає респондентові, не побоюючись виявлення зловмисником, оскільки знаходження секретного ключа за відомим відкритим є складною щодо обчислення математичною задачею, яка, як правило не розв’язується за допомогою звичайної електронної обчислювальної техніки.

Якщо користувач А хоче надіслати зашифроване послання користувачеві В, він шифрує його за допомогою відкритого ключа В. Тепер текст не зможе прочитати ніхто, окрім В (навіть сам А), оскільки для розшифрування потрібен закритий ключ.

Математичною основою цього методу стала розробка так званих *хеш-функцій*, які володіють особливою характерною властивістю – високою складністю зворотного перетворення. Чим вища ця складність, тим вища і криптостійкість асиметричного алгоритму. Особливості хеш-функцій буде розглянуто пізніше.

Схему шифрування можна записати в наступному вигляді:

- шифрування: $S = E(T, K_{відк})$ або $S = E_{K_{відк}}(T)$, 13.3
- розшифрування: $T = D(S, K_{секр})$ або $T = D_{K_{секр}}(S)$, 13.4

де S – шифрований текст, T – відкритий текст, E – функція шифрування, D – функція розшифрування, а $K_{відк}$ і $K_{секр}$ відповідно відкритий і секретний ключі одержувача повідомлення.

Принциповий метод шифрування з відкритим ключем вперше був публічно запропонований в *1976 році Діффі* і *Хеллманом*. При цьому вони не змогли придумати конкретного алгоритму, але сформулювали принципові умови, яким такі алгоритми повинні відповідати:

1. Процес генерації пари ключів (відкритий і закритий) не повинен представляти обчислювальних труднощів.

2. Процес зашифрування тексту, тобто обчислення $E(T, K_{відк})$, а також процес розшифрування, тобто обчислення $D(S, K_{секр})$ також не повинні представляти обчислювальних труднощів.

3. Для супротивника повинно бути неможливим (з точки зору обчислювальних можливостей) обчислення закритого ключа $K_{секр}$ по наявному відкритому ключі $K_{відк}$.

4. Для супротивника повинно бути неможливим (з точки зору обчислювальних можливостей) обчислення відкритого тексту T по наявному зашифрованому тексті S і відкритого ключа $K_{відк}$.

Такі системи використовуються, наприклад, для захищеного обміну ключами по відкритих каналах зв'язку, при цьому вихідна інформація зашифровується за допомогою відкритого ключа, доступного всім користувачам деякої ІТС, а розшифровується тільки тим абонентом мережі, який має відповідний секретний ключ.

Основним недоліком алгоритмів з відкритим ключем є низька швидкість виконуваних операцій. Так, в алгоритмі RSA шифрування і розшифрування

полягає у піднесенні дуже великого числа до дуже великого степеня, а це досить ресурсномістка операція.

Тому на практиці найчастіше використовується комбінація двох алгоритмів. Повідомлення шифрується за допомогою симетричного алгоритму шифрування (наприклад, AES). При цьому кожен раз генерується новий випадковий ключ. Цей ключ шифрується відкритим ключем одержувача (наприклад, RSA) і відправляється разом з листом. Така гібридна схема забезпечує як швидкість операцій шифрування/розшифрування, так і надійність.

Можливий й інший варіанти використання асиметричних систем – створення математичного апарату ***електронного цифрового підпису*** (ЕЦП).

ЕЦП в криптографії – це результат криптографічного перетворення за допомогою секретного ключа функції відкритого тексту. Таким чином, з'єднаний текст з ЕЦП, посилається іншим користувачам ІТС, які за допомогою загальнодоступного відкритого ключа і криптографічного перетворення можуть перевірити авторство і автентичність повідомлення. Більш детально ЕЦП буде розглядатися пізніше.

13.4. Криптографічні методи забезпечення конфіденційності інформації

Початкове завдання криптографії полягає в розробленні методів, спрямованих на приховування змісту переданої або збереженої інформації. І хоча на сьогодні сфера застосування криптографічних механізмів значно розширилася, основні ідеї можна проілюструвати саме на прикладі забезпечення конфіденційності інформації. Очевидно, що властивість конфіденційності досягається тоді, коли з перетвореного відкритого тексту, тобто криптограми, не можна дізнатись про зміст цього тексту, а несанкціоновані користувачі не зможуть здійснити обернене перетворення з криптограми у відкритий текст.

В цілях забезпечення конфіденційності інформації загалом використовуються дві криптосистеми які базуються на раніше згаданих методах шифрування, а саме: симетричні (рис. 13.1) та асиметричні криптосистеми (рис. 13.2).

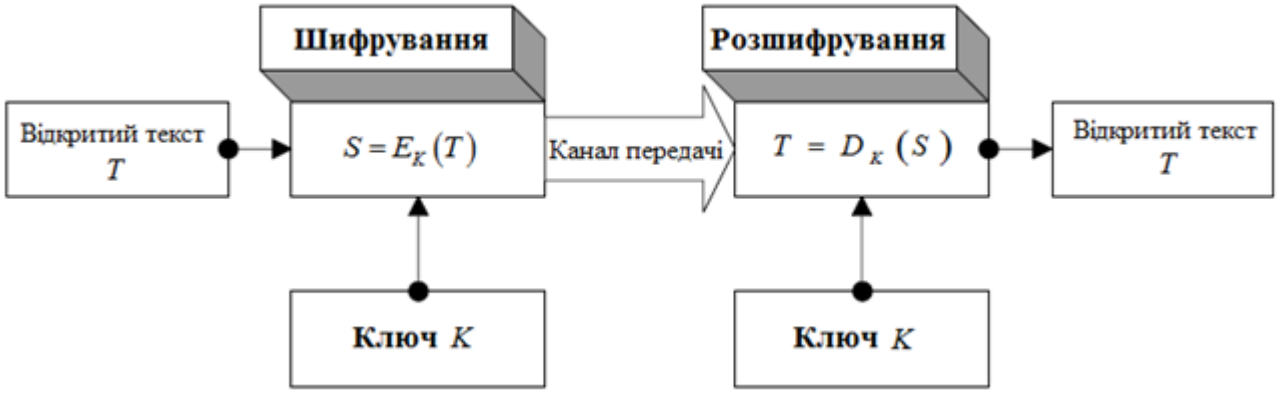


Рис. 13.1. Структура симетричної криптосистеми

В якості прикладів симетричних криптосистем можна привести російський алгоритм ГОСТ 28147-89, а також міжнародні стандарти DES і AES, який прийшов йому на зміну.

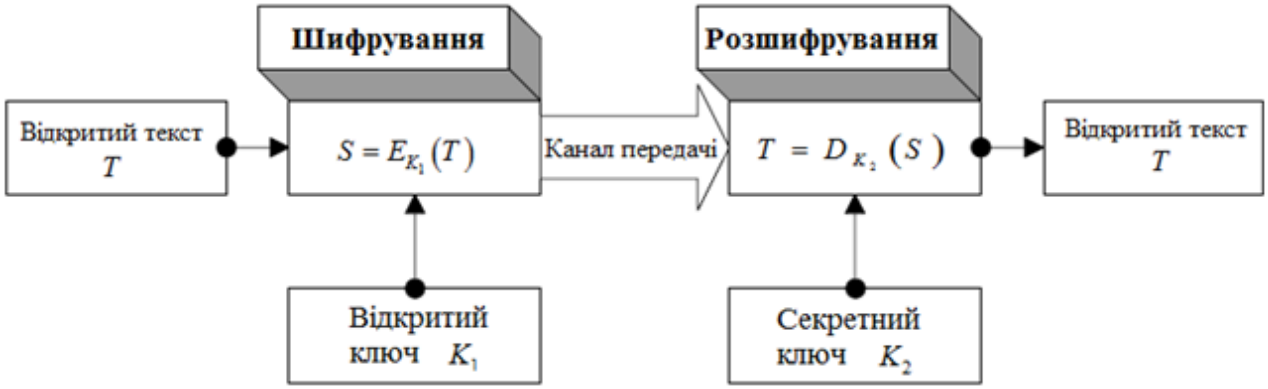


Рис. 13.2. Структура асиметричної криптосистеми

Незважаючи на досить велике число різних криптосистем з відкритим ключем, найбільш популярна – криптосистема RSA, що розроблена в 1977 році і отримала назву на честь її творців: Рівеста, Шаміра і Ейдельмана. Для застосування цього алгоритму буде потрібно кілька визначень.

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

Таким чином, проаналізувавши представлені схеми, необхідно відмітити, що симетричні і асиметричні криптосистеми, а також різні їх комбінації використовуються в АС насамперед для шифрування даних на різних носіях і для шифрування трафіку.

13.5. Криптографічні методи забезпечення цілісності інформації

При побудові систем захисту від загроз порушення цілісності інформації використовуються такі криптографічні примітиви:

- електронні цифрові підписи;
- криптографічні хеш-функції;
- коди автентифікації повідомлень.

13.5.1. Функції хешування

Невід'ємною частиною електронного цифрового підпису є використовування хеш-функцій. ***Хеш-функцією*** (англ. *hash* – подрібнювати, змішувати) $z = h(m)$ або *хешуванням,* називається перетворення бітового рядка довільної довжини в бітовий рядок (блок) фіксованої довжини (як правило, 128-512 біт - хеш-код, також називають хешем або *дайджестом* повідомлення), що має такі властивості:

- результат роботи хеш-функцій має залежати від усіх двійкових символів вихідного повідомлення, а також від їхнього взаємного розташування;
- хеш-функція має бути стійкою в розумінні обернення;
- хеш-функція має бути стійкою в розумінні виявлення колізій:
  1) стійкість до колізій першого роду: для заданого повідомлення m повинно бути обчислювально неможливо підібрати інше повідомлення n, для якого $h(n) = h(m)$;
  2) стійкість до колізій другого роду: повинно бути обчислювально неможливо підібрати пару повідомлень, що мають однаковий хеш.

Хешування застосовується для порівняння: якщо у двох масивів даних хеш-коди різні, масиви гарантовано розрізняються; якщо однакові – масиви, швидше за все, однакові.

Однією з найважливіших характеристик хеш-функцій, що зумовили їхнє широке впровадження у практику, виявилася здатність отримувати з відкритого тексту великої довжини (наприклад в хеш-функції SHA максимальна довжина відкритого тексту обмежена 2^{64} бітами) хеш-коду набагато меншої довжини (у російському стандарті ГОСТ Р 34.11–94 довжина хеш-коду становить 256 біт, західні хеш-функції мають переважно хеш-код довжиною 160...180 біт), що в певних випадках дозволяє дуже ефективно скоротити мережний трафік. Застосовування хеш-функцій надає можливість усувати надлишковість відкритого тексту, що при подальшому криптографічному перетворенні хеш-коду відкритого тексту позитивно позначається на криптографічних властивостях зашифрованого повідомлення.

Взагалі існує безліч алгоритмів хешування з різними характеристиками (розрядність, обчислювальна складність, криптостійкістю тощо). Вибір тієї чи іншої хеш-функції визначається специфікою розв'язуваної задачі. Найпростішим прикладом хеш-функції може служити ***контрольна сума***. Прикладом такого алгоритму є поділ повідомлення на 32- або 16- бітні слова і їх підсумовування, що застосовується, наприклад, у протоколі TCP/IP. По швидкості обчислення такі алгоритми в сотні разів швидше, ніж алгоритми для обчислення криптографічних хеш-функцій, і значно простіше в апаратній реалізації.

Платою за таку високу швидкість є відсутність криптостійкості – легка можливість підігнати повідомлення на заздалегідь відому суму. Тому такі швидкі і прості алгоритми використовуються тільки для захисту від ненавмисного перекручування інформації.

Однак, слід зазначити, що не доведено існування повністю криптостійких (необоротних) хеш-функцій, для яких обчислення якогось прообразу заданого значення хеш-функції теоретично неможливе. Зазвичай знаходження зворотного значення є лише обчислювально складним завданням.

Для криптографічних хеш-функцій також важливо, щоб при найменшій зміні аргументу значення функції сильно змінювалося (лавинний ефект). Зокрема, значення хешу не повинно давати витоку інформації навіть про окремі біти аргументу. Ця вимога є запорукою криптостійкості алгоритмів хешування.

Найбільш відомі алгоритми отримування хеш-образів повідомлень представлені в табл. 3.2 – CRC, ADLER-32, MD5, SHA-1, RIPEMD, ГОСТ 34.311, TIGER, HAVAL.

Таблиця 13.2. Алгоритми отримування хеш-образів повідомлень

CRC	Алгоритм знаходження контрольної суми, призначений для перевірки цілісності даних. CRC є практичним додатком завадостійкого кодування, заснованим на певних математичних властивостях циклічного коду.
ADLER-32	Довжина хеш-коду - 32 біт. Обчислює значення контрольної суми відповідно до RFC 1950 для масиву байтів або його фрагмента. Даний алгоритм розрахунку контрольної суми відрізняється від CRC32 продуктивністю.
MD5	Довжина хеш-коду - 128 біт. Представник сімейства алгоритмів обчислення хеш-функцій MD (Message Digest Algorithm), запропонованого Р. Рівестом; розроблено 1991 р.; найбільш розповсюджене використання – спільно з RSA.
RIPEMD	Довжина хеш-коду - 128 (RIPEMD-128) або 160 біт (RIPEMD-160). розроблено в межах європейського проекту RIPE (Race Integrity Primitives Evaluation) Європейського співтовариства; є модифікацією алгоритму MD4.

TIGER	Довжина хеш-коду - 192 біт. Розроблено Р. Андерсоном та Е. Біхемом; призначений для реалізації на 64-розрядних комп'ютерах.
HAVAL	Довжина хеш-коду - 128, 160, 192, 224 або 256 біт. Односпрямована хеш-функція змінної довжини. Функція HAVAL є модифікацією функції MD5. Алгоритм HAVAL опрацьовує повідомлення блоками розміром у 1024 розряди, що є удвічі більше, аніж в алгоритмі MD5. У HAVAL використовується вісім 32-розрядних змінних зчеплення, тобто удвічі більше, аніж в алгоритмі MD5, і змінна кількість раундів опрацювання – від трьох до п'яти (на кожному раунді виконується 16 кроків).
SHA-1	Довжина хеш-коду - 160 біт. Призначена для використання в стандарті DSS. Використовує принципи, закладені в MD4, MD5.
ГОСТ 34.311	Довжина хеш-коду - 256 біт. Побудована на основі оригінальних перетворень. Використовує, у тому числі алгоритм шифрування ГОСТ 28147-89. Застосовується спільно з Національним стандартом ДСТУ 4145-2002.

В якості прикладу розглянемо достатньо поширений алгоритм обчислення хеш-функції *Adler-32*. Цей алгоритм розроблений Марком Адлером і є модифікацією хеш-функції Fletcher, що працює на основі обчислення контрольної суми.

Adler-32 обчислюється за формулою:

$$Adler-32(D)=B\times 2^{16}+A, \qquad 13.5$$

де D – байт-коди символів вихідного тексту; A, B – допоміжні коефіцієнти, які обчислюються ітераційно по байт-кодам символів вихідного тексту:

$$A_0=1;$$

$$B_0=0;$$

$$A_i=(A_{i-1}+D_i)\bmod 65521; \qquad 13.6$$

$$B_i=(B_{i-1}+A_i)\bmod 65521. \qquad 13.7$$

Число 65521 – це найбільше просте число менше, ніж $2^{16}(65536)$. Результат зазвичай перетворюють в 16-річну систему числення (hex). Приклад обчислення хеш-функції *Adler-32* наведено в табл. 13.3.

Таблиця 13.3. Приклад обчислення хеш-функції Adler-32

Вихідний текст, D	Код *ASCII*[9]	Коеф. *A*	Коеф. *B*	*Adler-32*
		1	0	
K	75	76	76	
y	121	197	273	

[9] Коди ASCII взяті з табл. 13.4.

r	114	311	584	
y	121	432	1016	
c	99	531	1547	
h	104	635	2182	
o	111	746	2928	
k	107	853	3781	
				247792469_{10} $EC50355_{16}$

В даному прикладі операція mod не знадобилася, оскільки всі коефіцієнти менші 65521. Якщо змінити вихідний текст *D* хоча б на 1 (наприклад, замість 99 ввести 100), то значення хеш-функції Adler-32 змінюється на 248054614. Ця суттєва зміна підтверджує лавинний ефект, необхідний для криптографічних хеш-функцій.

Таблиця 13.4. Коди ASCII

ASCII Table

Dec	Hex	Oct	Char	Dec	Hex	Oct	Char	Dec	Hex	Oct	Char	Dec	Hex	Oct	Char
0	0	0		32	20	40	[space]	64	40	100	@	96	60	140	`
1	1	1		33	21	41	!	65	41	101	A	97	61	141	a
2	2	2		34	22	42	"	66	42	102	B	98	62	142	b
3	3	3		35	23	43	#	67	43	103	C	99	63	143	c
4	4	4		36	24	44	$	68	44	104	D	100	64	144	d
5	5	5		37	25	45	%	69	45	105	E	101	65	145	e
6	6	6		38	26	46	&	70	46	106	F	102	66	146	f
7	7	7		39	27	47	'	71	47	107	G	103	67	147	g
8	8	10		40	28	50	(	72	48	110	H	104	68	150	h
9	9	11		41	29	51	)	73	49	111	I	105	69	151	i
10	A	12		42	2A	52	*	74	4A	112	J	106	6A	152	j
11	B	13		43	2B	53	+	75	4B	113	K	107	6B	153	k
12	C	14		44	2C	54	,	76	4C	114	L	108	6C	154	l
13	D	15		45	2D	55	-	77	4D	115	M	109	6D	155	m
14	E	16		46	2E	56	.	78	4E	116	N	110	6E	156	n
15	F	17		47	2F	57	/	79	4F	117	O	111	6F	157	o
16	10	20		48	30	60	0	80	50	120	P	112	70	160	p
17	11	21		49	31	61	1	81	51	121	Q	113	71	161	q
18	12	22		50	32	62	2	82	52	122	R	114	72	162	r
19	13	23		51	33	63	3	83	53	123	S	115	73	163	s
20	14	24		52	34	64	4	84	54	124	T	116	74	164	t
21	15	25		53	35	65	5	85	55	125	U	117	75	165	u
22	16	26		54	36	66	6	86	56	126	V	118	76	166	v
23	17	27		55	37	67	7	87	57	127	W	119	77	167	w
24	18	30		56	38	70	8	88	58	130	X	120	78	170	x
25	19	31		57	39	71	9	89	59	131	Y	121	79	171	y
26	1A	32		58	3A	72	:	90	5A	132	Z	122	7A	172	z
27	1B	33		59	3B	73	;	91	5B	133	[	123	7B	173	{
28	1C	34		60	3C	74	<	92	5C	134	\	124	7C	174	|
29	1D	35		61	3D	75	=	93	5D	135	]	125	7D	175	}
30	1E	36		62	3E	76	>	94	5E	136	^	126	7E	176	~
31	1F	37		63	3F	77	?	95	5F	137	_	127	7F	177	

13.5.2. Електронний цифровий підпис

Електронний цифровий підпис – це засіб, що дозволяє на основі криптографічних методів надійно встановити авторство і справжність електронного документа. Електронний цифровий підпис дозволяє замінити при безпаперовому документообігу традиційні печатку та підпис. Проставляння

підпису під документом не змінює самого документа, а тільки дає можливість перевірити достовірність та авторство отриманої інформації. Таким чином, досягається *автентичність* (справжність) та цілісність повідомлення. З юридичної точки зору це означає, що автор повідомлення не зможе від нього відмовитися.

Оскільки ЕЦП багато в чому є аналогом рукописного підпису – тому, до нього пред'являються практично аналогічні загальні вимоги:

1) цифровий підпис має доводити, що саме законний автор, і ніхто інший, свідомо підписав документ;

2) цифровий підпис має представляти собою невід'ємну частину документа. Має бути неможливим відокремлення підпису від документа і використання його для підписання інших документів;

3) цифровий підпис повинен забезпечувати неможливість зміни підписаного документа (*в тому числі і для самого автора*);

4) факт підписання документа повинен бути юридично-доказовим (забезпечення автентичності).

Спочатку були спроби створення механізму ЕЦП на основі алгоритмів симетричного шифрування, але потім, використовуючи переваги двох ключів, механізм функціонування ЕЦП повністю перейшов на алгоритми асиметричного шифрування.

Секретний (закритий) ключ підпису використовується для створення електронного цифрового підпису. Лише збереження особою у таємниці свого секретного ключа гарантує неможливість (точніше – велику обчислювальну складність) підробки зловмисником документа і цифрового підпису від імені автора.

Відкритий ключ підпису формується як значення деякої функції від секретного ключа, але знання відкритого ключа не дозволяє визначити секретний ключ. Відкритий ключ може бути опублікований і використовується для перевірки достовірності підписаного документа, а також для попередження шахрайства з боку автора у вигляді відмови його від підписаного ним документа.

В якості електронного цифрового підпису може виступати сам текст, зашифрований закритим ключем відправника. Однак такий варіант не використовується через його неефективність. По-перше, шифрування /розшифрування тексту займає дуже багато часу. По-друге, довжина ЕЦП в цьому випадку буде дорівнювати (і навіть перевищувати) довжині вихідного повідомлення, що створює незручність при пересиланні. Тому сучасні алгоритми електронного цифрового підпису базуються на використанні, раніше згаданих, *хеш-функцій*.

Підписання електронного документу ЕЦП. При підписанні електронного документу його початковий зміст не змінюється, а додається блок даних, так званий Електронний цифровий підпис. Отримання цього блоку можна розділити на два етапи (рис. 13.3):

На першому етапі за допомогою програмного забезпечення і спеціальної математичної функції обчислюється так званий «відбиток повідомлення» (message digest).

Цей відбиток має такі особливості:

- фіксовану довжину, незалежно від довжини повідомлення;
- унікальність відбитку для кожного повідомлення;
- неможливість відновлення повідомлення по його відбитку.

Таким чином, якщо документ був модифікований, то зміниться і його відбиток, що відобразиться при перевірці ЕЦП.

На другому етапі відбиток документу шифрується за допомогою програмного забезпечення (алгоритму ЕЦП) і особистого ключа автора, перетворюючись в ЕЦП.

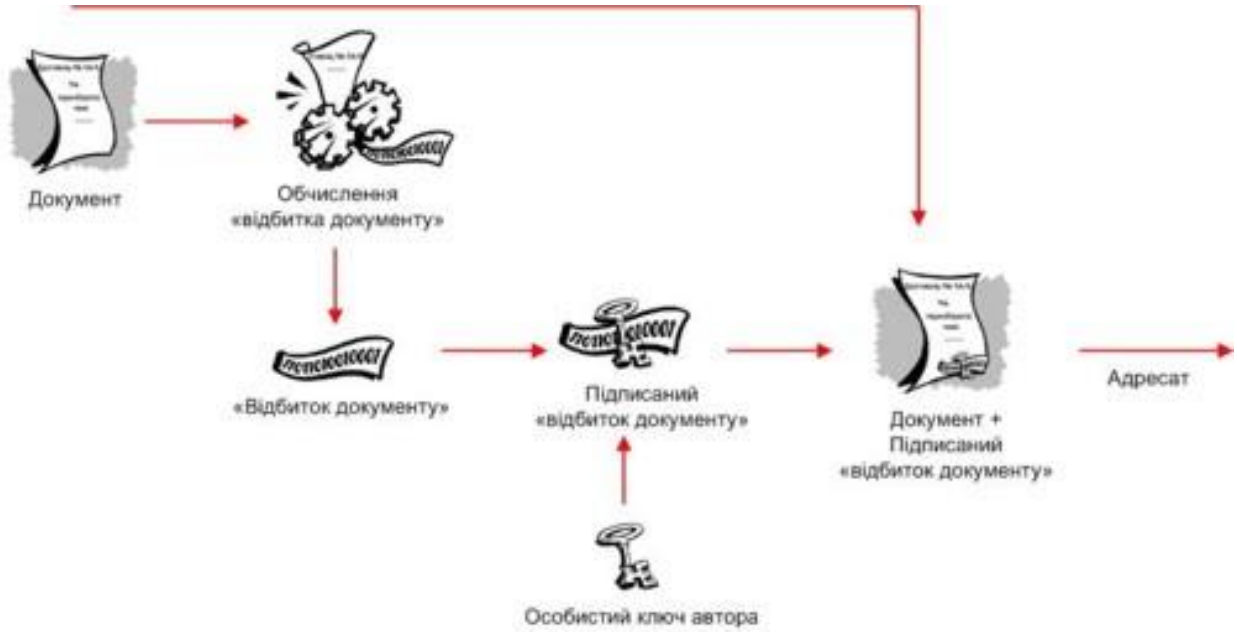


Рис. 13.3. Підписання електронного документу ЕЦП

Розшифрувати ЕЦП і одержати початковий відбиток, який відповідатиме документу, можна тільки використовуючи *Сертифікат* відкритого ключа автора.

Таким чином, обчислення відбитку документу захищає його від модифікації сторонніми особами після підписання, а шифрування особистим ключем автора підтверджує авторство документу.

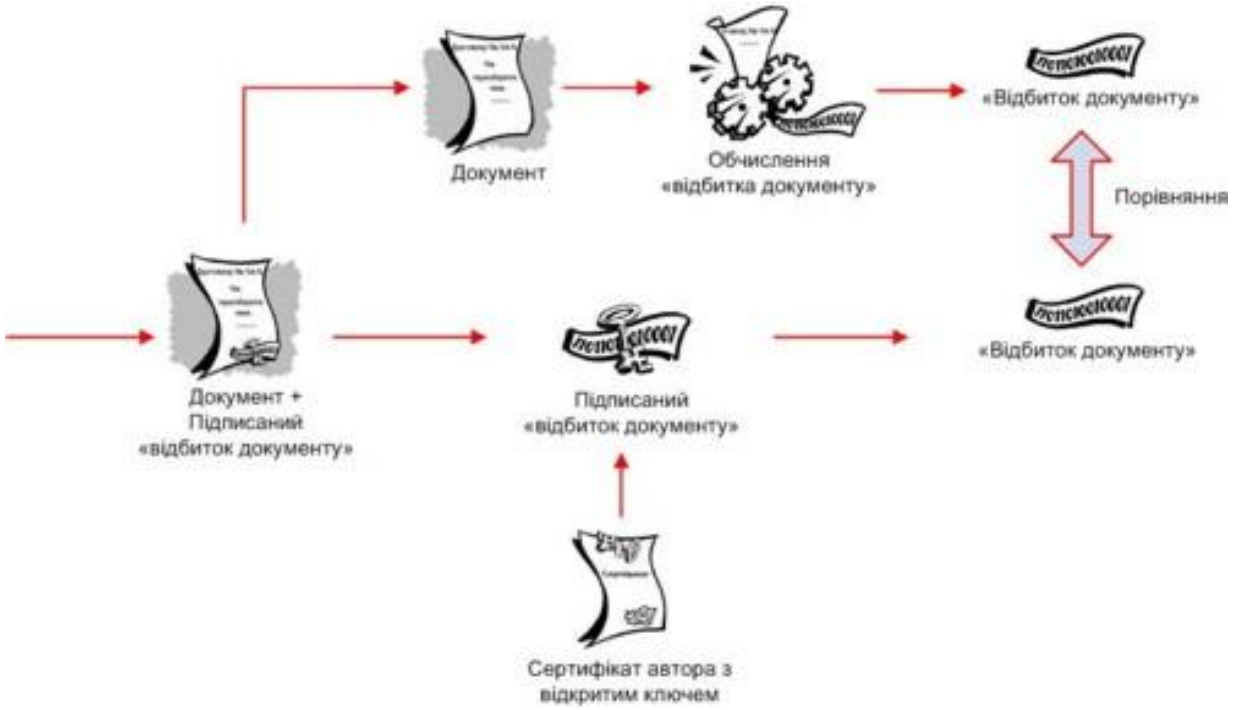


Рис. 13.4. Перевірка ЕЦП одержаного документу

Перевірка ЕЦП одержаного документу. Перевірка ЕЦП одержаного документу проводиться також в декілька етапів (рис. 13.4):

1. На першому етапі адресат за допомогою програмного забезпечення сертифікатом відкритого ключа автора розшифровує підписаний відбиток і одержує відбиток початкового документа.

2. За допомогою програмного забезпечення і спеціальної математичної функції з документу, який був одержаний, обчислюється його відбиток.

3. При перевірці ЕЦП порівнюються відбитки початкового і одержаного документів. Результат перевірки - одна з відповідей: «вірний»/«невірний».

Таким чином, ЕЦП підтверджує достовірність і цілісність документа. Якщо в нього в процесі пересилки були внесені які-небудь зміни, нехай навіть зовсім незначні, то підміна відразу ж буде виявлена.

13.5.3. Коди автентифікації (MAC-коди)

Часто криптографічні хеш-функції використовуються в якості засобів контрольного підсумовування: наприклад, для деякого файлу, поміщеного в публічний доступ на ftp-сервері, може бути наведено його хеш, виміряний з використанням деякого алгоритму (найчастіше в таких випадках використовується алгоритм md5). У цьому випадку користувач, що завантажив файл може пересвідчитися в його справжності, однак у цьому випадку зловмисник може підмінити файл і привести хеш, відповідний новому файлу – виявити подібні маніпуляції, використовуючи звичайні хеш-функції,

неможливо. Захист від подібного роду атак забезпечується шляхом застосування кодів автентифікації.

Коди автентифікації, або *MAC-коди*, являють собою криптографічні хеш-функції, для обчислення яких необхідно знати секретний ключ. Використання ключа дозволяє гарантувати неможливість підміни захищених об'єктів: зловмисник, який не знає секретного ключа, не зможе перерахувати хеш для нового файлу.

В якості кодів автентифікації часто використовуються модифікації симетричних криптографічних систем.

Порядок виконання лабораторної роботи №13:

1. Включити ПК.
2. Ознайомитися з короткими теоретичними відомостями.
3. Зашифрувати вручну свої дані методом перестановки: «прізвище ім'я по батькові» за допомогою ключів k_1 та k_2, заданих в табл. 13.5. При цьому, спершу, необхідно підібрати розмір шифротаблиці під довжину своїх даних.
4. У вашій компанії виникла необхідність обміну конфіденційною інформацією. Тому, на основі отриманих результатів, використовуючи шифрування методом перестановки, вам потрібно змоделювати в MS Excel[10] симетричну криптосистему обміну повідомленнями в ІТС. Першим повідомленням має бути ваше «прізвище ім'я по батькові». При моделюванні дозволяється користуватися зразком який наведений в додатку 5.
5. Обчислити вручну значення хеш-функції Adler-32 для свого прізвища та ім'я, записаних на латиниці. Коди ASCII взяти з табл. 13.4.
6. Оформити звіт згідно до вимог (додаток 1) та прикріпити файл(-и) створеної симетричної криптосистеми обміну повідомленнями.
7. Відповісти на контрольні питання та підготуватися до письмового опитування.

Зміст звіту:

1. Титульний лист.
2. Постановка завдання.
3. Сформована шифротаблиця (або декілька) для свого «прізвища ім'я по батькові» та результат шифрування методом перестановки.
4. Програмний код (та скріншот зовнішнього вигляду), з описом та коментарями вже змодельованої симетричної криптосистеми обміну повідомленнями.
5. Результат обчислення хеш-функції Adler-32 у вигляді таблиці.

[10] Симетрична криптосистема обміну повідомленнями також може бути змодельована за допомогою будь-якої іншої мови програмування.

6. Висновки.

Завдання на виконання лабораторної роботи №13

Таблиця № 13.5 (варіант відповідно до номера за списком у журналі)

Номер варіанта	**Ключ k_1**	**Ключ k_2**
1	6–5–1–3–2–4	4–2–3–1
2	6–1–4–3–2–5	1–3–2–4
3	5–1–4–3–6–2	1–2–4–3
4	4–1–6–3–2–5	2–3–1–4
5	3–1–4–5–2–6	2–4–3–1
6	2–1–4–3–6–5	2–3–4–1
7	6–5–4–1–2–3	2–4–1–3
8	6–5–1–3–2–4	3–4–2–1
9	6–1–4–3–2–5	3–2–4–1
10	5–6–4–3–2–1	3–1–4–2
11	4–5–6–3–2–1	3–1–2–4
12	3–5–4–6–2–1	1–4–2–3
13	2–5–4–3–6–1	4–3–2–1
14	1–5–4–3–2–6	4–3–1–2
15	6–5–4–3–2–1	4–2–3–1
16	3–1–4–2–6–5	4–1–2–3
17	3–2–1–6–5–4	1–3–2–4
18	5–2–6–4–1–3	1–2–4–3
19	4–1–3–2–5–6	2–3–2–4
20	4–2–1–3–5–6	2–4–3–1
21	5–2–4–3–6–1	2–3–4–1
22	5–2–3–4–6–1	2–4–1–3
23	5–2–4–3–1–6	3–4–2–1
24	6–2–5–4–3–1	3–2–4–1
25	6–2–3–4–5–1	3–1–4–2
26	1–6–3–4–5–2	3–1–2–4
27	1–2–6–4–5–3	1–4–2–3

Контрольні питання:

1. Надати визначення наступним поняттям: криптографічна система, криптографічні засоби, криптографічне перетворення інформації.

2. Перерахувати всі основні задачі захисту інформації, які вирішуються шляхом застосування криптографічних перетворень.
3. Описати основні характеристики криптографічних методів захисту інформації.
4. Описати процедуру шифрування та розшифрування.
5. Охарактеризувати симетричне та асиметричне шифрування.
6. Визначити основні недоліки симетричних та асиметричних алгоритмів шифрування.
7. Що таке функція хешування? Назвати основні її властивості.
8. Що таке ЕЦП? Перерахувати основні вимоги до ЕЦП.
9. Описати процедури підписання та перевірки електронного документу ЕЦП.

Лабораторна робота №14
«Професійний засіб криптографічного захисту – програмний засіб PGP»

Мета роботи:

1. Освоїти основні прийоми використання програмного засобу криптографічного захисту PGP Desktop для виконання операцій шифрування і цифрового підпису повідомлень, файлів та іншої інформації, представленої в електронному вигляді.

Стислі теоретичні відомості:

В даний час розроблено і достатньо широко використовується велика кількість програмних, апаратних і програмно-апаратних засобів криптографічного захисту інформації. Серед програмних засобів найбільш відома криптографічна програма PGP Філа Циммермана, яка спочатку розповсюджувалася безкоштовно. Але зараз – це комерційний продукт з можливістю безкоштовного використання або в режимі обмеженої функціональності, або протягом 30 днів в повнофункціональному режимі.

В Україні найбільшу популярність мають апаратні засоби захисту компанії «Інститут інформаційних технологій» (м. Харків), які визнані офіційно на державному рівні і використовуються урядовими організаціями, банками, великими корпораціями (https://iit.com.ua/).

Другими за поширеністю є апаратно-програмні засоби фірми «АВТОР» http://www.author.kiev.ua/). Їх продуктова лінійка включає в себе засоби аутентифікації (SecureToken-337, CryptoCard-337), засоби шифрування дисків (CryptoGuard), засоби захисту IP-трафіку (CryptoIP), систему мобільних та інтернет платежів (ПлатиМО!), програмно-технічний комплекс Центр сертифікації ключів («CryptoKDC»), а також всілякі карт-рідери і смарт-карти.

14.1. Криптографічний пакет PGP Desktop

PGP (Pretty Good Privacy) – це криптографічне (шифрувальне) програмне забезпечення з високим ступенем надійності, яке дозволяє користувачам обмінюватися інформацією в електронному вигляді в режимі повної конфіденційності. У PGP застосовується принцип використання двох взаємопов'язаних ключів: відкритого і закритого. До закритого ключа маєте доступ лише Ви, а свій відкритий ключ Ви поширюєте серед своїх респондентів.

Головна перевага цієї програми полягає в тому, що для обміну зашифрованими повідомленнями користувачам непотрібно передавати один одному таємні ключі оскільки дана програма побудована на новому принципі роботи – публічній криптографії або обміні відкритими (публічними) ключами. Користувачі цього пакету можуть відкрито посилати один одному свої публічні ключі за допомогою мережі Інтернет і при цьому не турбуватися про можливість несанкціонованого доступу будь-яких третіх осіб до їх конфіденційних повідомлень. Розшифрувати їх можна тільки другим (секретним) ключем, який нікому не надсилається, а зберігається лише у людини-генератора пари ключів.

Розробник PGP Філіп Ціммерман відкрито опублікував код своєї програми, який неодноразово був досліджений фахівцями криптоаналітиками найвищого класу і жоден з них не знайшов в програмі будь-яких слабких місць. Спочатку програма PGP поширювалася абсолютно безкоштовно, але потім автор продав своє право фірмі *PGP Corporation* за 1 млн. доларів, яка в подальшому на основі цієї програми створила комерційний пакет *PGP Desktop*. Але навіть при комерційному поширенні залишилася можливість безкоштовного використання цього пакету в режимі обмеженої функціональності, який цілком достатній для вивчення у вузі і виконання лабораторних робіт.

У повному обсязі пакет PGP Desktop дозволяє шифрувати повідомлення електронної пошти, будь-які файли, в тому числі і графічні, папки і весь вміст дисків. Також пакет надає всі необхідні сервіси для електронного цифрового підпису та гарантованого знищення файлів. У режимі обмеженої функціональності пакет дозволяє шифрувати тільки текстові файли.

14.1.1. Принципи роботи PGP

Програмне забезпечення PGP базується на використанні методів асиметричного шифрування, при яких важливо правильне використання пари

ключів. Для цього визначимо ролі відправника та одержувача. Людина, яка генерує пару ключів (закритий і відкритий) називається ***резидентом***. Резидент зберігає закритий ключ тільки у себе (для розшифрування повідомлень, які приходять йому), а відкритий ключ вільно передає ***респондентам***. Респондент – це особа, яка шифрує повідомлення для резидента отриманим від нього відкритим ключем.

Таким чином, як нам вже відомо, з минулого заняття, у криптографічній системі з відкритим ключем кожен має два взаємно-пов'язаних ключа: відкритий ключ (який публікується) і секретний ключ. Однак знання відкритого ключа не дозволяє вам обчислити відповідний секретний ключ. І саме тому, відкритий ключ може публікуватися і широко розповсюджуватися через відкриті (не захищені) комунікаційні мережі. Такий протокол забезпечує таємність без необхідності використовувати спеціальних каналів зв'язку, які так необхідні для стандартних криптографічних систем.

Хто завгодно може використовувати відкритий ключ одержувача, щоб зашифрувати повідомлення йому, а одержувач використовує його власний відповідний секретний ключ для розшифрування повідомлення. Ніхто, крім одержувача, не може розшифрувати його, тому що ніхто більше не має доступу до секретного ключа. Навіть той, хто шифрував повідомлення, вже не матиме можливості розшифрувати його.

Крім того, забезпечується також встановлення автентичності повідомлення. Власний секретний ключ відправника може бути використаний для «підпису» самого повідомлення. Так створюється електронний цифровий підпис повідомлення, який одержувач може перевіряти, використовуючи відкритий ключ відправника і таким чином підтверджуючи його автентичність. Підробка підписаного повідомлення неможлива, і до того ж відправник вже не зможе змінити свій підпис.

Ці два процеси можуть бути об'єднані для забезпечення і секретності, і встановлення автентичності: спочатку підписується повідомлення вашим власним ключем, а потім шифрується вже підписане повідомлення відкритим ключем одержувача. Одержувач робить навпаки: розшифровує повідомлення за допомогою власного секретного ключа, а потім перевіряє підпис за допомогою вашого відкритого ключа. Ці кроки виконуються автоматично за допомогою програмного забезпечення PGP.

Відкриті ключі зберігаються у вигляді «сертифікатів ключів», які включають в себе ідентифікатор користувача власника ключа (зазвичай це ім'я користувача), тимчасову мітку, яка вказує час генерації пари ключів, і власне ключі. Сертифікати відкритих ключів містять відкриті ключі, а сертифікати секретних ключів – секретні. Кожен секретний ключ також шифрується

окремим паролем. Файл ключів, або каталог ключів («кільце з ключами» – «keyring») містить один або кілька таких сертифікатів. У каталогах відкритих ключів зберігаються сертифікати відкритих ключів, а в каталогах секретних – сертифікати секретних ключів.

Також необхідно відзначити, що PGP використовує «дайджести повідомлень» для формування підпису. Дайджест повідомлення, як нам вже відомо, це криптографічно потужна одностороння хеш-функція від повідомлення. Вона дещо нагадує контрольну суму, або CRC код і забезпечує перевірку цілісності повідомлення. На відміну від CRC коду, дайджест не дозволяє створити два повідомлення з однаковим дайджестом. Дайджест повідомлення шифрується секретним ключем для створення електронного підпису повідомлення.

Документи підписуються за допомогою додавання перед ними засвідчуючого підпису, який містить ідентифікатор ключа, використаного для підпису, підписаний секретним ключем дайджест повідомлення і мітку дати і часу, коли підпис був згенерований. Ідентифікатор ключа використовується одержувачем повідомлення, щоб знайти відкритий ключ для перевірки підпису. Програмне забезпечення одержувача автоматично шукає відкритий ключ відправника і ідентифікатор користувача в каталозі відкритих ключів одержувача.

Використання цих двох типів каталогів ключів і є головним принципом збереження і роботи з відкритими і секретними ключами. Замість того, щоб зберігати індивідуальні ключі в окремих файлах ключів, вони збираються в каталогах ключів для полегшення автоматичного пошуку ключів або за ідентифікатором ключа, або за ідентифікатором користувача. Кожен користувач зберігає свою власну пару каталогів ключів.

Індивідуальний відкритий ключ тимчасово зберігається в окремому файлі, досить компактному для відправлення його вашим респондентам, які зможуть додати його в свої каталоги ключів.

14.1.2. Порядок використання програмного пакету PGP Desktop

1) Встановлення та першочергове налаштування PGP Desktop.

Процес встановлення PGP Desktop є досить стандартним (як і встановлення будь-якого іншого програмного забезпечення) і тому він не розглядається детально.

В разі успішного встановлення – нас просять перезавантажитися, щоб запустилися встановлені служби, необхідні для коректної роботи програми. І після перезавантаження системи з’являється вікно налаштування (рис. 14.1), в

якому запитується щодо відкриття доступу до PGP для даного користувача (акаунта).

Рис. 14.1. Початкове вікно першочергового налаштування PGP

Наступними етапами є заповнення реєстраційної форми (рис. 14.2) та введення ліцензійного ключа (рис 14.3).

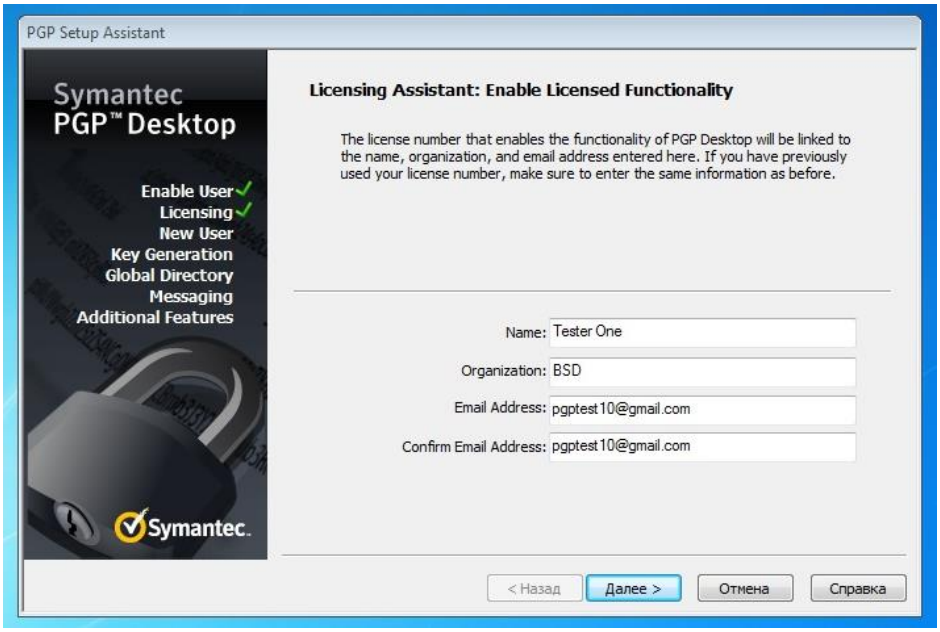


Рис. 14.2. Вікно реєстраційної форми PGP

Рис. 14.3. Вікно введення ліцензійного ключа для активації PGP Desktop

В подальшому нас запитують чи користувалися ми даним програмним продуктом раніше, чи використовуємо вперше, для того щоб дізнатися чи є у нас пара ключів, чи її потрібно генерувати (рис. 14.4).

Рис. 14.4. Вікно визначення типу користувача PGP Desktop

Оскільки програмний продукт використовується вперше, далі розглянемо більш детально процес створення пари ключів. Отже, обравши «Нового користувача» та підтвердивши необхідність створення нової пари ключів з’являється наступне вікно налаштування, а точніше вікно генерації пари ключів (рис. 14.5).

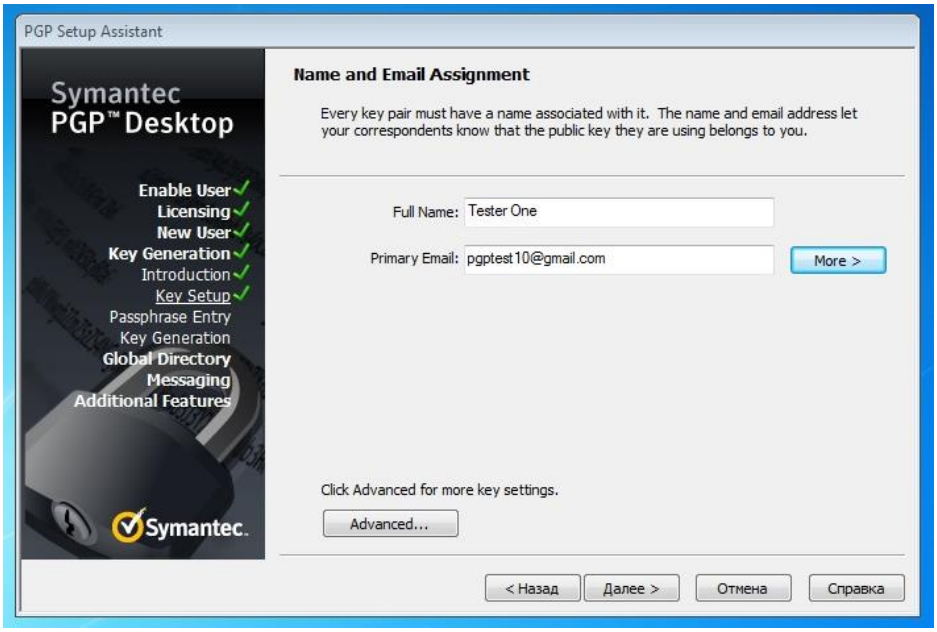


Рис. 14.5. Вікно генерації пари ключів

Для налаштування безпосередньо самої пари ключів необхідно відкрити нове вікно налаштування ключів (рис. 14.6), натиснувши кнопку ***«Advanced».*** В даному вікні потрібно налаштувати всі параметри вашої ключової пари. Вибравши тип ключа (RSA або Diffie-Helman / DDS), розмір ключа підпису, розмір ключа шифрування, термін дійсності пари ключів, шифр, хеш та стиснення.

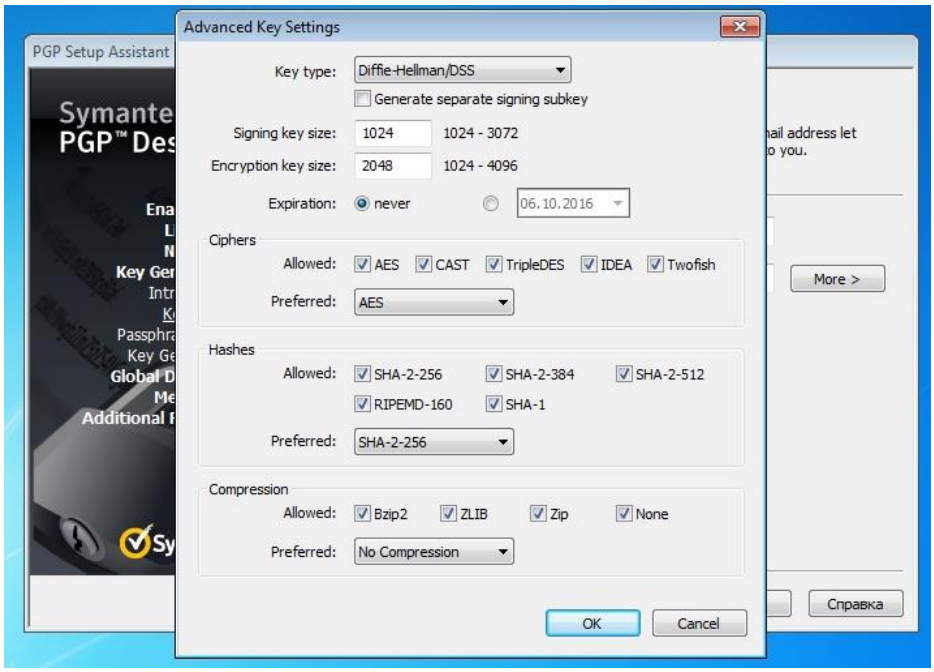


Рис. 14.6. Вікно налаштування ключової пари

Після підтвердження всіх налаштувань з’являється наступне вікно «Ключова фраза» (рис. 14.7), в якому необхідно ввести ключову фразу (пароль) для захисту вашого таємного ключа. При цьому необхідно пам’ятати, що загублений, забутий пароль відновленню не підлягає і якщо Ви забудете

пароль, то доведеться створювати нові ключі заново, потім розсилати всім новий публічний ключ і просити замінити його. Насправді ж, страшного нічого не станеться, якщо Ви забудете пароль. Пару ключів можна буде згенерувати заново, але старі зашифровані повідомлення та файли Ви вже ніколи не відкриєте! І якщо хтось забуде видалити ваш старий ключ і зашифрує ним повідомлення, то ви не зможете його прочитати.

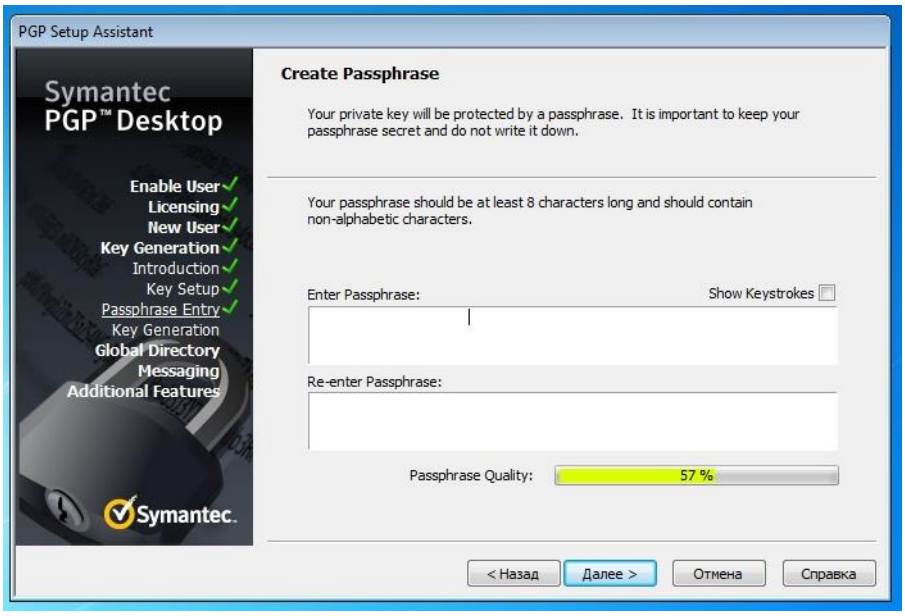


Рис. 14.7. Вікно створення ключової фрази для Вашого таємного ключа

Після генерації ключової пари Global directory assistant допомагає нам опублікувати відкритий ключ в PGP (рис. 14.8). Процес публікації включає поновлення ключа та подання його на Global Directory server.

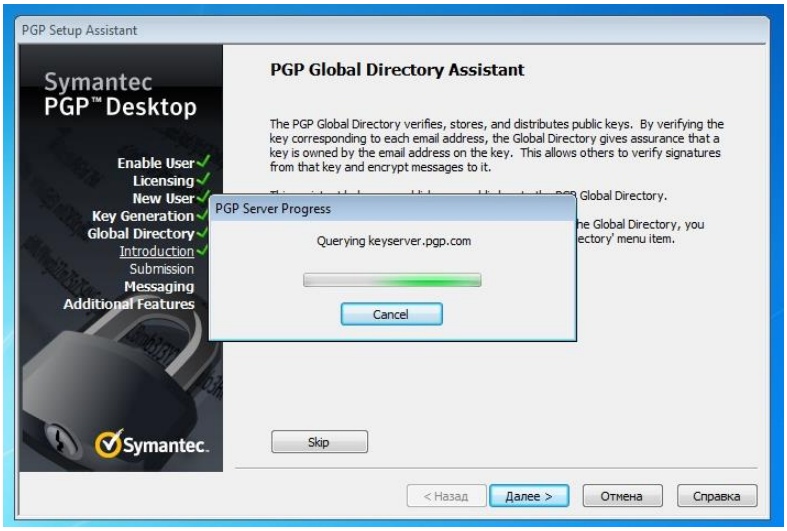


Рис. 14.8. Вікно публікації вашого відкритого ключа

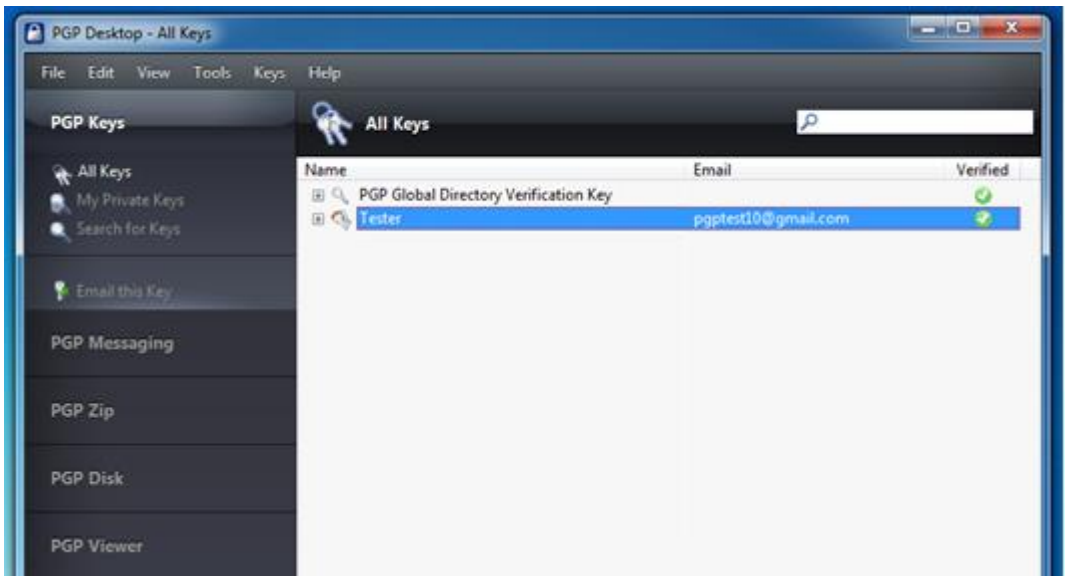


Рис. 14.9. Стартове вікно програми PGP Desktop

2) Створення (генерація) закритого та відкритого ключа (ключової пари).

Перед тим, як почати використовувати програму PGP, вам необхідно згенерувати пару ключів. Вона складається із закритого ключа, до якого маєте доступ лише Ви, і відкритого ключа, який Ви копіюєте і вільно передаєте іншим людям (Вашим респондентам).

Генерація ключів вже була розглянута при першочерговому налаштуванні PGP, тому розгляд даного етапу пропустимо, оскільки генерація нової пари ключів відбувається таким же чином як і при першочерговому налаштуванні. Вам лише необхідно:

1. Переконатися, що ви перебуваєте в робочій зоні PGP Keys.
2. Вибрати File > New PGP Key або натиснути Ctrl + N, після чтого з'явиться перше вікно помічника PGP Key Generation Assistant.

3) Поширення свого відкритого ключа серед своїх респондентів.

Ваш відкритий ключ – це невеликий файл з розширенням ***.asc***, який з'являється після виконання команди ***Export***[11] (команда, яка виконується над закритим ключам). Після чого Ви можете поширювати свій відкритий ключ різними способами:

- опублікувати ключ на PGP Global Directory (взагалі жоден з інших методів не потрібно, як тільки ваш ключ публікується в цьому каталозі);
- прикріпивши ваш відкритий ключ (тільки не переплутайте з файлом де зберігаються ваші обидва ключа) до повідомлення електронної пошти;

[11] Експортувати файл відкритого ключа необхідно без опції «Include Private Key(s)», оскільки при ввімкненні даної опції в експортований файл буде включений також Ваш секретний ключ.

- можна експортувати ваш відкритий ключ на знімні носії або скопіювати його в текстовий файл.

4) Отримання відкритих ключів від своїх резидентів.

Спершу необхідно отримати файл з розширенням .asc від своїх резидентів і виконати для нього команду ***Import*** (рис. 14.10), при цьому необхідно упевнитися у достовірності відкритого ключа. Як тільки Ви отримаєте відкриті ключі своїх резидентів, то їх можна додати в «кільце відкритих ключів». Після цього вам необхідно переконатися в тому, що у Вас дійсно відкритий ключ Вашого резидента. Ви можете це зробити, зв'язавшись з цим резидентом і попросивши його зачитати вам по телефону «відбитки пальців» (унікальний ідентифікаційний номер або список слів) його відкритого ключа (рис. 14.11 та рис. 14.12). До того ж Ви можете відразу повідомити йому номер Вашого відкритого ключа. Як тільки Ви переконаєтесь в тому, що ключ дійсно належить йому, Ви можете його підписати і таким чином підтвердити свою довіру до цього ключа.

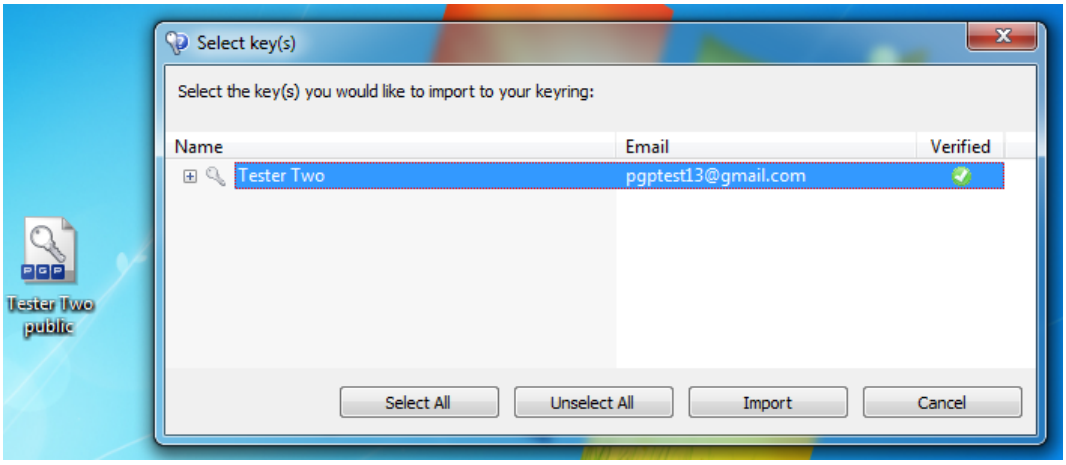


Рис. 14.10. Вікно з відкритим ключем, отриманим респондентом

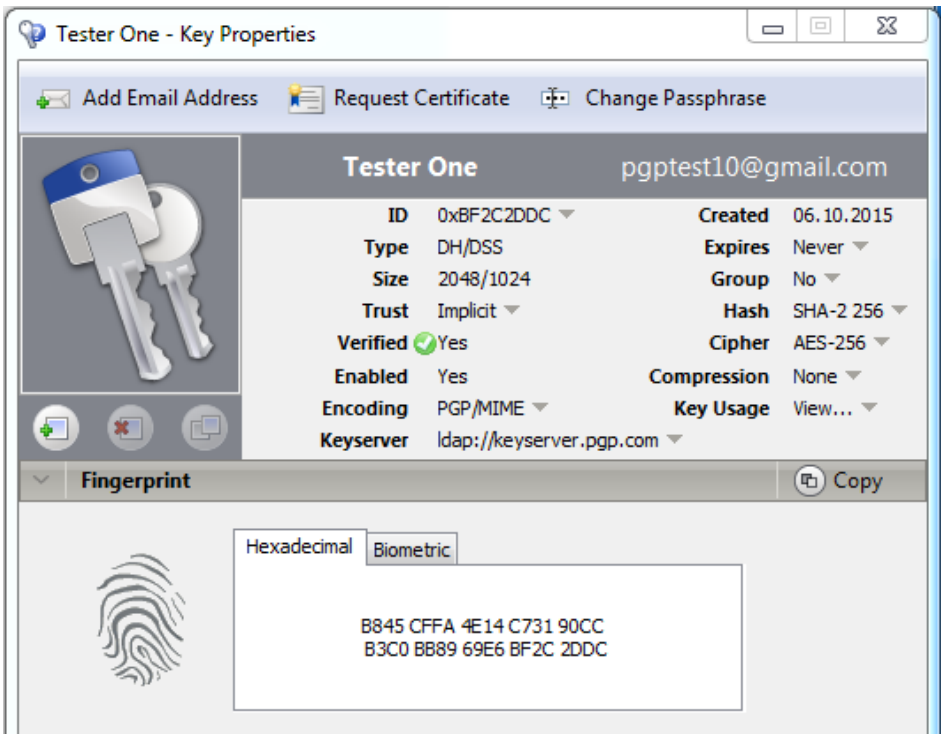


Рис. 14.11. Вікно з «відбитком пальців» у шістнадцятковому форматі

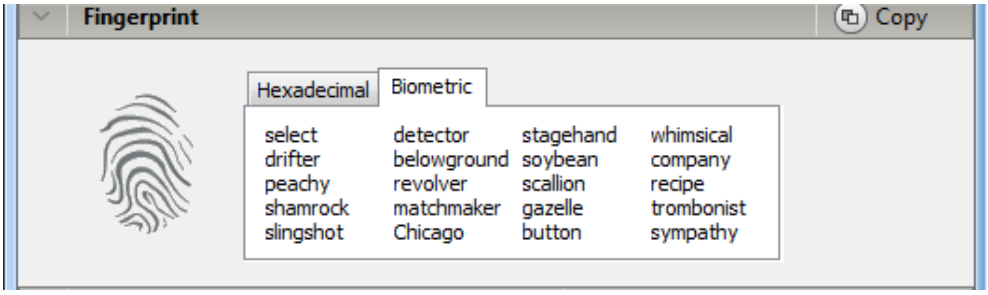


Рис. 14.12. Вікно з «відбитком пальців» у вигляді унікального списку слів

5) *Шифрування і/або засвідчення своєї кореспонденції Вашим цифровим підписом.*

Після генерації пари ключів і обміну відкритими ключами Ви можете почати шифрування і/або засвідчення Ваших повідомлень і файлів своїм цифровим підписом. Якщо Ви використовуєте поштову програму, яка підтримується програмою PGP, то Ви можете шифрувати і дешифрувати всю Вашу кореспонденцію, перебуваючи прямо в цій програмі. Якщо ж Ваша поштова програма не підтримується програмою PGP або ви користуєтеся звичайними електронними поштовими сервісами, то Ви можете шифрувати Вашу кореспонденцію іншими способами (через буфер обміну або шифруванням файлів цілком).

Щоб зашифрувати і підписати повідомлення, вам потрібно:

1) Скопіювати текст повідомлення в буфер обміну, а потім через іконку PGP Desktop в треї обрати ***Clipboard > Encrypt & Sign*** (рис. 14.13).

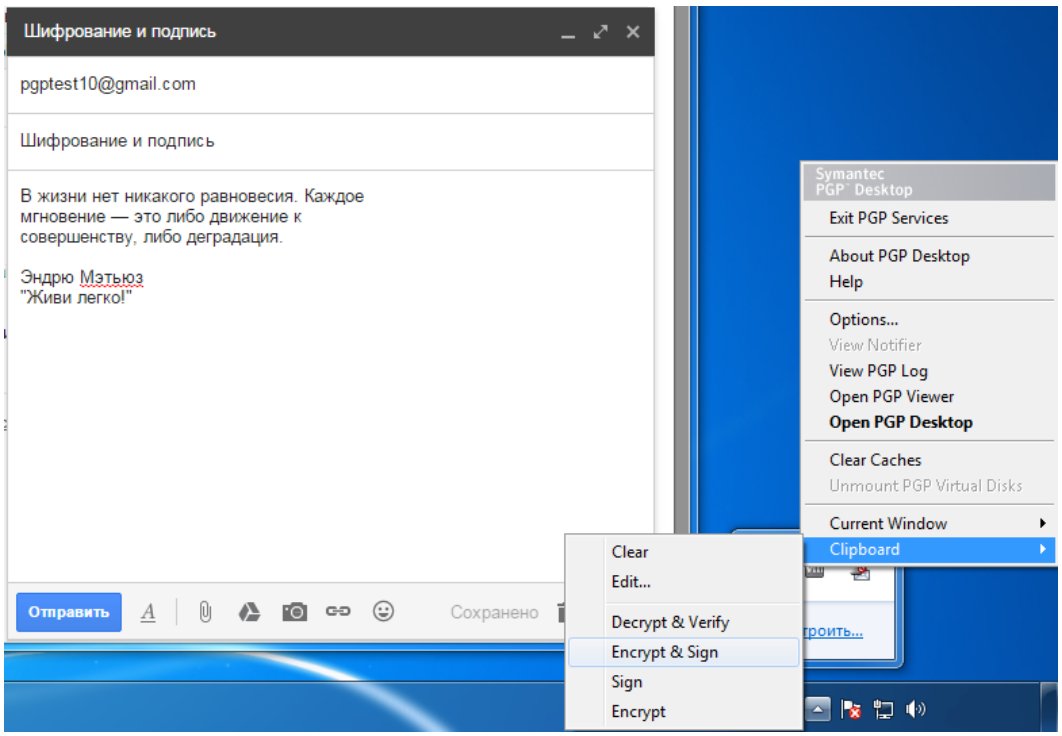


Рис. 14.13. Шифрування та підпис повідомлення через буфер обміну

2) Після чого з'явиться вікно, в якому вам необхідно перетягнути відкритий ключ одержувача в поле ***Recipients***, за допомогою якого дане повідомлення буде зашифровано (рис. 14.14).

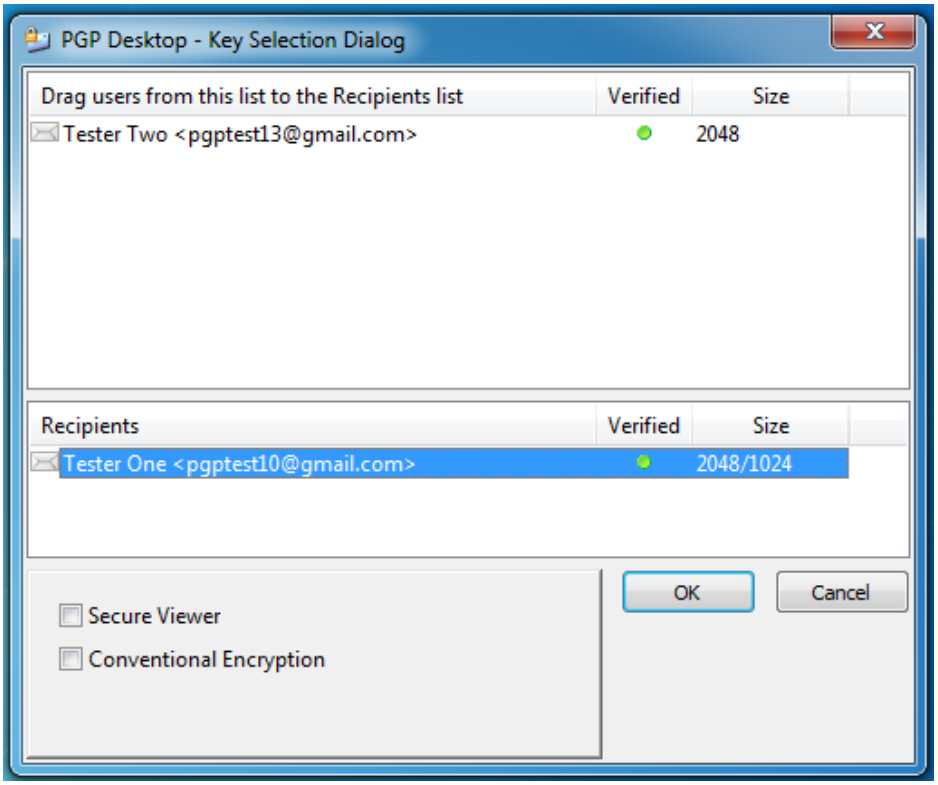


Рис. 14.14. Вікно вибору відкритого ключа одержувача для шифрування Вашого повідомлення

3) Наступним кроком відбувається підпис вашого електронного повідомлення, для чого вам необхідно буде ввести пароль свого закритого

ключа (якщо пароль вже вводився раніше, він зберігається в кеші і вводити заново вже не потрібно) у вікні PGP Desktop – Enter Passphrase.

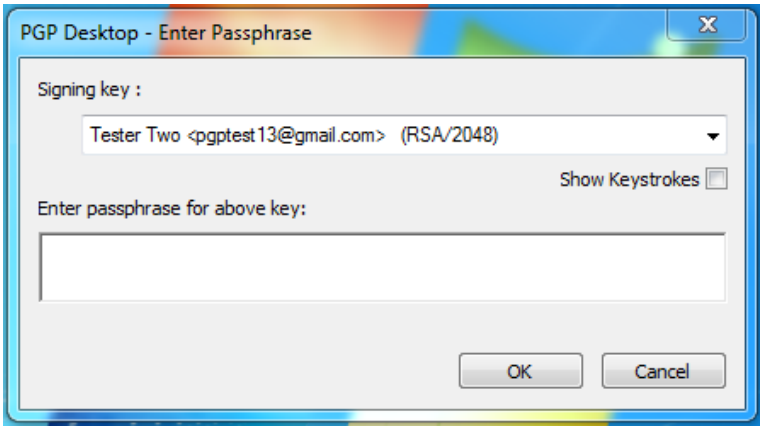


Рис. 14.15. Вікно введення ключової фрази Вашого закритого ключа

4) Після чого Ваше повідомлення буде зашифровано і підписано, і ви повертаєте його з буфера обміну, в свій електронний лист, замінюючи старий текст.

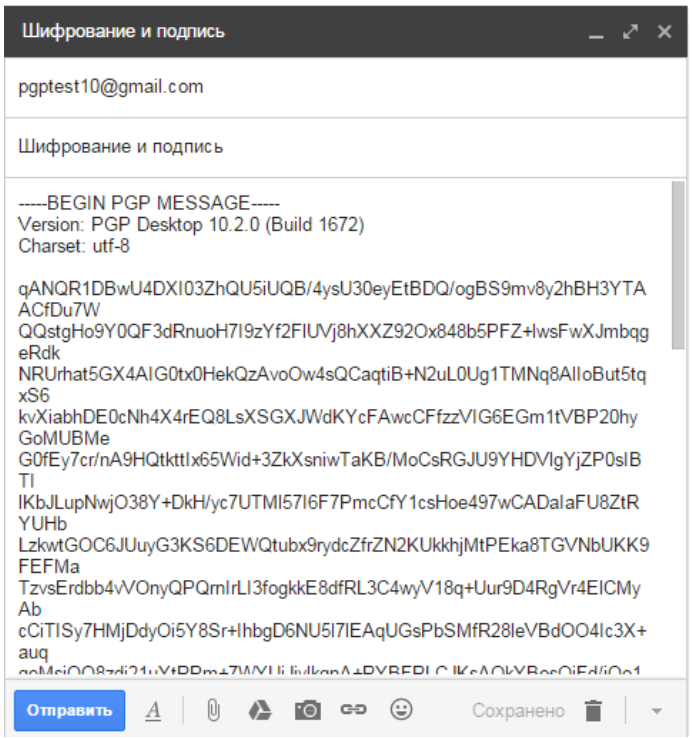


Рис. 14.16. Вікно вже зашифрованого та підписаного електронного листа

Якщо вам необхідно лише підписати повідомлення або лише зашифрувати його, вам необхідно скопіювати текст повідомлення в буфер обміну, а потім через іконку PGP Desktop в треї обрати ***Clipboard*** **>** ***Encrypt*** (для шифрування повідомлення) або ***Sign*** (для підпису електронного повідомлення).

6) Розшифрування повідомлень респондента, які надходять до Вас та/або перевірка справжність ЕЦП відправника.

Коли будь-хто висилає вам зашифроване повідомлення, Ви можете розшифрувати його або перевірити справжність відправника цього повідомлення і цілісність самого повідомлення. Якщо Ваша поштова програма не підтримується PGP, то Ви також можете зробити це через буфер обміну.

Для того щоб перевірити підпис, розшифрувати або після перевірки підпису і розшифрувати повідомлення електронної пошти (без поштового клієнта) вам необхідно:

1) Відкрити отримане електронне повідомлення.

2) Скопіювати текст повідомлення в буфер обміну, а потім через іконку PGP Desktop в треї обрати ***Clipboard > Decrypt & Verify***.

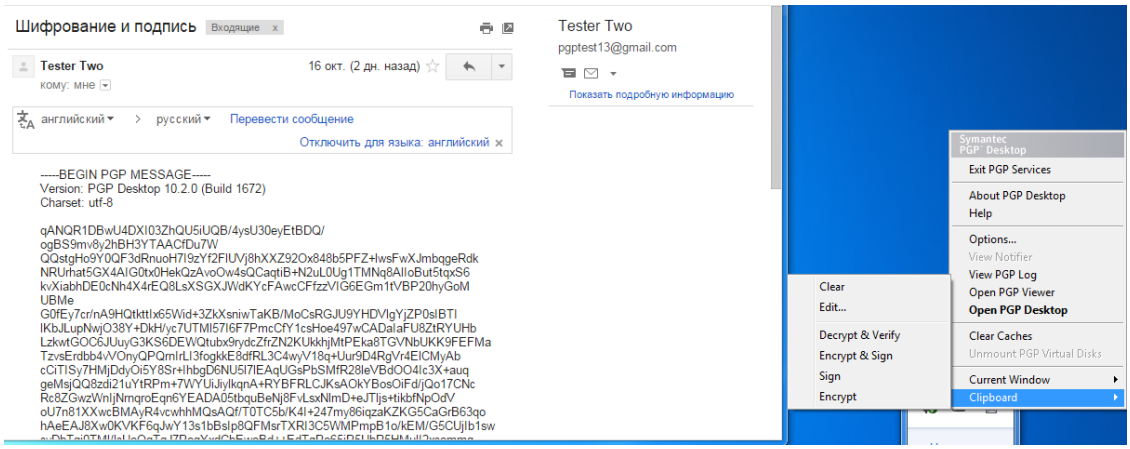


Рис. 14.17. Вікно отриманого зашифрованого та підписаного електронного листа

3) Після чого з’явиться вікно в якому вам необхідно ввести пароль свого закритого ключа, за допомогою якого дане повідомлення буде розшифровано і перевірений підпис вхідного повідомлення.

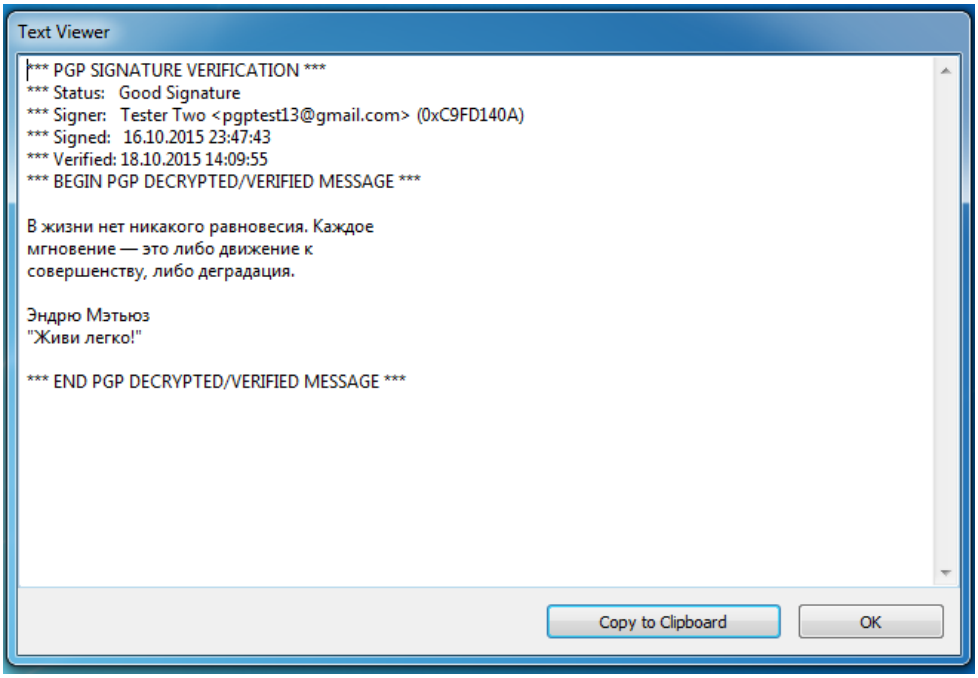


Рис. 14.18. Вікно розшифрованого повідомлення з відображенням перевірки ЕЦП

Порядок виконання лабораторної роботи №14[12]:

1. Включити ПК.
2. Ознайомитися з короткими теоретичними відомостями.
3. Виконати наступні завдання[13]:

1) Завантажити найновішу версію PGP Desktop, встановити, здійснити першочергове налаштування та ознайомитися з інтерфейсом і функціоналом даного програмного продукту.

2) Після встановлення програми PGP Desktop, якщо Ви ще не згенерували ключову пару, необхідно створити пару ключів під своїм прізвищем.

3) Виконати роль резидента X. Для цього вам необхідно, передати (експортувати) відкритий ключ респонденту, отримати від нього зашифроване повідомлення, розшифрувати. Звірити з респондентом вихідний текст для контролю правильності виконання завдання.

4) Виконати роль респондента Y. Для цього вам необхідно отримати відкритий ключ від резидента і імпортувати його, зашифрувати цим ключем повідомлення та передати його резиденту. Звірити з резидентом вихідний текст для контролю правильності виконання завдання.

5) Виконати роль зловмисника-резидента Z-X. Для цього перехопити (взяти) файл респондента X1, який працює з резидентом Y1, і спробувати його розшифрувати своїм закритим ключем[14].

6) Виконати роль зловмисника-респондента Z-Y. Для цього зашифрувати файл своїм відкритим ключем і відправити (передати) його чужому резиденту X1.

4. Оформити звіт згідно до вимог (додаток 1).
5. Відповісти на контрольні питання.

Зміст звіту:

1. Титульний лист.
2. Постановка завдання.
3. Протокол виконання лабораторної роботи, що містить скріншоти та опис всіх виконуваних дій та отриманих результатів.
4. Висновки та відповіді на контрольні питання.

Контрольні питання:

[12] Перед виконанням даної лабораторної роботи необхідно поділитися на бригади по 2 чоловіки.
[13] Усі виконувані дії описувати в звіті та супроводжувати скріншотами.
[14] Під користувачами X1 та Y1 маються на увазі студенти з іншої бригади.

1. Назвіть відомі вам українські компанії, які займаються криптографічним захистом інформації.
2. Охарактеризуйте програмний пакет PGP.
3. Опишіть основний принцип роботи програмного забезпечення PGP Desktop.

Лабораторна робота №15
«Інформаційна безпека на рівні операційної системи Windows»

Мета роботи:

1. Ознайомлення з принципами побудови архітектури підсистеми безпеки сучасних операційних систем.
2. Вивчення моделі безпеки операційної системи Windows та отримання практичних навиків у використанні засобів забезпечення її безпеки.

Стислі теоретичні відомості:

15.1. Аналіз захищеності сучасних операційних систем

При оцінці ступеня захищеності операційних систем діє нормативний підхід, згідно з яким сукупність завдань, що виконується системою безпеки, повинна задовольняти певні вимоги. Їх перелік визначається загальноприйнятими стандартами, наприклад, TCSEC («Помаранчева книга») або «Загальні критерії оцінки безпеки інформаційних технологій». В Україні також діють подібні критерії, які визначені в НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу (НСД)». Такі стандарти складають основу *політики безпеки* системи, яка в свою чергу передбачає відповіді на наступні питання: яку інформацію захищати, якого роду загрози можуть бути реалізовані в системі та які саме засоби планується використовувати для захисту від кожного типу атак.

На сьогоднішній день, до сучасних популярних операційних систем прийнято відносити два сімейства: Windows та Linux. Так, наприклад, зі сторони сімейства Windows, після еволюції від однокористувацької моделі до багатокористувацької, розробники операційної системи приділили серйозну увагу забезпеченню безпеки роботи користувачів. Це підтверджується категоріями, присвоєними різним версіями цієї операційної системи за тими чи іншими міжнародними і національними критеріями оцінки безпеки. Так, за класифікацією «Помаранчевої книги» ОС Windows NT 4 ще в 1999 році отримала клас безпеки C2, за стандартом ISO/IEC 15408 Common Criteria for Information Technology Security Evaluation (Загальні критерії оцінки безпеки

інформаційних технологій) клієнтські і серверні версії від Windows 2000 до Windows 10, від Windows Server 2008 до Windows Server 2013 отримали рівень безпеки EAL4+. А взагалі, необхідно відзначити, що обидва сімейства операційних систем, переважно задовольняють вимоги класу C2 TCSEC, згідно яким, система повинна забезпечувати:

- безпечний вхід в систему, який забезпечує точну ідентифікацію користувачів ОС і надає їм можливість доступу до ресурсів комп'ютера тільки після проходження процедури аутентифікації. У Windows за ідентифікацію та аутентифікацію користувачів відповідають процеси *Winlogon.exe* і *Lsass.exe*;
- управління доступом – надання користувачам можливості захисту приналежних їм даних, що дозволяє власникові ресурсу (файлу, розділу реєстру, об'єкту ядра та ін) визначити, хто має право на доступ до ресурсу, а також уточнити суть цих прав (читання, зміна, запуск тощо). При використанні дискреційної моделі доступу для ущільнення матриці доступу власник може наділяти правами, які надають різні види доступу до об'єкта, як окремого користувача, так і групу користувачів. Безпечний доступ в ОС Windows реалізується за допомогою компонента *Security Reference Monitor* виконавчої системи *Ntoskrnl.exe*;
- системний аудит – здатність системи проводити докладний аудит дій, виконуваних користувачами і самою операційною системою;
- аудит безпеки, який дозволяє реєструвати всі події, що відносяться до питань безпеки. Ідентифікація користувачів при вході в систему дозволяє прив'язувати всі події безпеки в системі до конкретного користувача. У Windows аудит підтримується *SRM* і *Lsass.exe*;
- захист об'єктів від повторного використання – здатність системи запобігати доступу користувача до інформаційних ресурсів, з якими до цього працював інший користувач, тобто система не дозволяє користувачам переглядати дані, видалені іншим користувачем, а також не дозволяє звертатися до пам'яті, яка раніше була використана, а потім звільнена іншим користувачем. У Windows звільнена пам'ять очищується системним потоком *обнулення сторінок*, працюючим під час простою системи (з нульовим пріоритетом);
- захист самої системи від зовнішнього впливу або нав'язування, такого, як модифікація завантаженої системи або системних файлів, що зберігаються на диску.

15.2. Підсистема захисту в ОС Windows

Вивчення структури системи захисту допомагає зрозуміти особливості її функціонування. Незважаючи на слабку документованість ОС Windows за непрямими джерелами, можна судити про особливості її функціонування.

Для захисту даних Windows використовує наступні основні механізми:

- аутентифікація і авторизація користувачів;
- аудит подій в системі;
- шифрування даних;
- підтримка інфраструктури відкритих ключів;
- вбудовані засоби мережного захисту.

Ці механізми підтримуються такими підсистемами ОС Windows як LSASS (Local Security Authority Subsystem Service, локальна підсистема безпеки) – слідкує за процесом аутентифікації, доступом користувачів та аудитом в системі, SAM (Security Account Manager, менеджер локальних записів безпеки) – забезпечує підтримку аутентифікаційної бази даних SAM, SRM (Security reference Monitor, монітор контролю безпеки) – перехоплює звернення користувачів до об'єктів захисту і передає їх на обробку LSASS. SRM виконується в режимі ядра ОС, Active Directory (служба каталогів), EFS (Encrypting File System, файлова система шифрування) та ін. Для більш детального розгляду, на рисунку 15.1. схематично відображено структуру системи захисту ОС сімейства Windows, яка фактично складається з наступних компонентів:

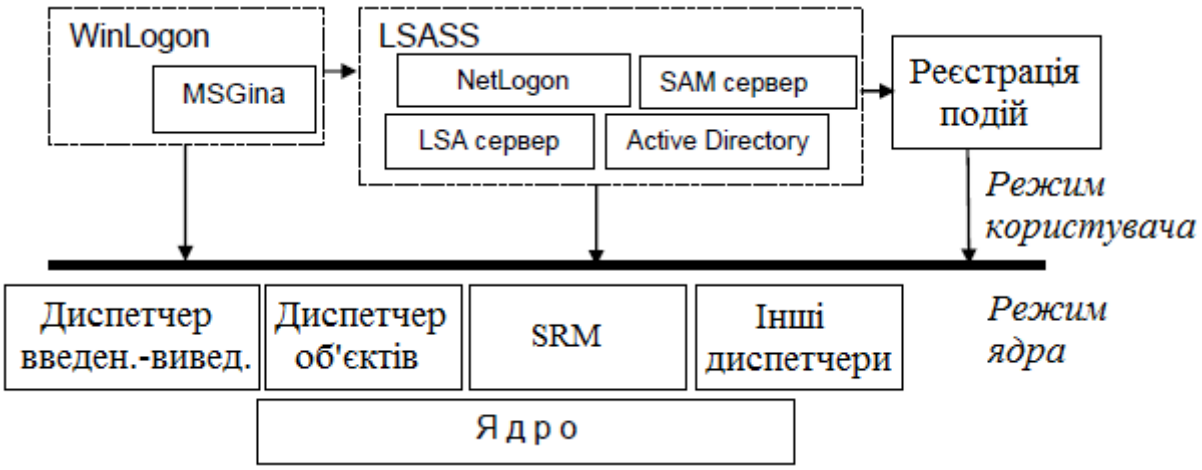


Рис. 15.1. Система захисту ОС Windows.

Процедура реєстрації (Logon Processes), яка обробляє запити користувачів на вхід у систему. Вона запускає початкову інтерактивну процедуру діалогу із користувачем на екрані, і віддалену процедуру входу, яка дозволяє віддаленим користувачам отримати доступ з робочої станції мережі до серверних процесів Windows. Процес *Winlogon* реалізований у файлі Winlogon.exe і виконується як процес режиму користувача. Стандартна бібліотека аутентифікації *Gina* реалізована у файлі Msgina.dll.

Локальний адміністратор безпеки (Local Security Authority, LSA), який гарантує, що користувач має дозвіл на доступ у систему. Цей компонент – центральний для системи захисту ОС Windows. Він формує маркери доступу, керує локальною політикою безпеки і надає користувачам аутентифікаційні послуги. LSA також контролює політику аудиту і веде журнал, в якому зберігаються повідомлення, що формуються диспетчером доступу. Основна частина функціональності реалізована в Lsasrv.dll.

Менеджер локальних записів безпеки (Security Account Manager, SAM) керує базою даних обліку користувачів, яка містить інформацію про всіх користувачів ОС, в тому числі і про групи користувачів. Ця служба реалізована в Samsrv.dll і виконується в процесі LSASS.

Монітор контролю безпеки (Security Reference Monitor, SRM), який перевіряє, чи має користувач право на доступ до об'єкта, а також право на виконання тих дій, які він намагається зробити. Цей компонент забезпечує легалізацію доступу і політику аудиту, що визначаються LSA. Він надає послуги для програм супервізорного режиму і режиму користувача та гарантує, що користувачі і процеси, які здійснюють спроби доступу до об'єкта, мають необхідні права. Також він формує повідомлення служби аудиту, коли це необхідно. Це компонент ядра системи: Ntoskrnl.exe.

Усі компоненти активно використовують базу даних LSASS, що містить параметри політики безпеки локальної системи, яка зберігається в розділі *HKLM\SECURITY* реєстру.

Як уже зазначалося раніше, захист об'єктів і аудит дій з ними в ОС Windows організовані на основі виборчого (дискреційного) доступу, коли права доступу (читання, запис, видалення, зміна атрибутів) суб'єкта до об'єкта відкрито задаються в спеціальній матриці доступу. Для укрупнення матриці користувачі можуть об'єднуватися в групи. Взагалі необхідно відзначити, що реалізація моделі дискреційного доступу пов'язана з функціонуванням SRM, який, згідно з описом, забезпечує також управління ролевим і привілейованим доступом. При спробі суб'єкта (одного з потоків процесу, запущеного від його імені) отримати доступ до об'єкта вказуються, які операції користувач збирається виконувати з об'єктом. Якщо подібний тип доступу дозволений, потік отримує *специфікатор* (***дескриптор безпеки***) об'єкта і всі потоки процесу можуть виконувати операції з ним. Подібна схема доступу, очевидно, вимагає аутентифікації кожного користувача, який отримує доступ до ресурсів та його надійну ідентифікацію в системі, а також механізмів опису прав користувачів і груп користувачів в системі, опису та перевірки дискреційних прав доступу користувачів до об'єктів. Тому, в наступному підрозділі розглянемо,

як в ОС Windows організована ідентифікація, аутентифікація та авторизація користувачів.

15.2.1. Ідентифікація та аутентифікація користувача. Вхід в систему.

Всі діючі в системі суб'єкти (користувачі, групи, локальні комп'ютери, домени) ідентифікуються в Windows не по іменах, унікальність яких не завжди вдається досягти, а по ***ідентифікаторах безпеки*** (Security Identifiers, ***SID***). SID являє собою числове значення змінної довжини:

$$S-R-I-S0-S1-\ldots-Sn-RID$$

S – незмінний ідентифікатор строкового подання SID;

R – рівень ревізії (версія). На сьогодні 1.

I – (identifier-authority) ідентифікатор повноважень. Являє собою 48-бітний рядок, що ідентифікує комп'ютер або мережу, який(а) видав SID об'єкту. Можливі значення:

- 0 (SECURITY_NULL_SID_AUTHORITY) – використовуються для порівнянь, коли невідомі повноваження ідентифікатора;
- 1 (SECURITY_WORLD_SID_AUTHORITY) – застосовуються для конструювання ідентифікаторів SID, які представляють всіх користувачів. Наприклад, ідентифікатор SID для групи *Everyone* (Всі користувачі) – це *S-1-1-0*;
- 2 (SECURITY_LOCAL_SID_AUTHORITY) – використовуються для побудови ідентифікаторів SID, що представляють користувачів, які входять на локальний термінал;
- 5 (SECURITY_NT_AUTHORITY) – сама операційна система. Тобто, даний ідентифікатор випущений комп'ютером або доменом.

Sn – 32-бітові коди (кількістю 0 і більше) субагентів, яким було передано право видати SID. Значення перших підлеглих повноважень загальновідомо. Вони можуть мати значення:

- 5 – ідентифікатори SID присвоюються сеансам реєстрації для видачі прав будь-якому додатку, що запускається під час певного сеансу реєстрації. У таких ідентифікаторах SID перші підлеглі повноваження встановлені як 5 і приймають форму *S-1-5-5-x-y*;
- 6 – коли процес реєструється як служба, він отримує спеціальний ідентифікатор SID у свій маркер для позначення даної дії. Цей ідентифікатор SID має підпорядковані повноваження 6 і завжди буде мати вигляд *S-1-5-6*;
- 21 (SECURITY_NT_NON_UNIQUE) – позначають ідентифікатор SID користувача та ідентифікатор SID комп'ютера, які не є унікальними в глобальному масштабі;

- 32 (SECURITY_BUILTIN_DOMAIN_RID) – позначають вбудовані ідентифікатори SID. Наприклад, відомий SID для вбудованої групи адміністраторів *S-1-5-32-544*;
- 80 (SECURITY_SERVICE_ID_BASE_RID) – позначають ідентифікатор SID, який належить службі.

Інші підлеглі повноваження ідентифікатора спільно позначають домен або комп'ютер, який видав ідентифікатор SID.

RID – 32-бітний відносний ідентифікатор. Він є ідентифікатором унікального об'єкта безпеки в області, для якої був визначений SID. Наприклад, 500 – позначає вбудований обліковий запис *Administrator*, 501 – позначає вбудований обліковий запис *Guest*, а 502 – RID для квитка на отримання квитків протоколу Kerberos.

При генерації SID Windows використовує генератор випадкових чисел, щоб забезпечити унікальність SID для кожного користувача. Зокрема, якщо видалити користувача в системі, а потім створити його під тим же ім'ям, то SID створеного користувача буде вже іншим. Як приклад, для деякого довільного користувача SID може виглядати так:

S-1-5-21-1690090054-2308632580-4048739682-1000

Визначеним користувачам і групам Windows видає характерні SID, що складаються з SID комп'ютера або домену та зумовленого RID. В таблиці 15.1 наведено перелік деяких загальновідомих SID.

Таблиця 15.1. Загальновідомі SID Windows

SID	Назва	Опис
S-1-1-0	Все	Група, в яку входять всі користувачі.
S-1-5-2	Мережа	Група, в яку входять всі користувачі, що зареєструвались в системі з мережі.
S-1-5-7	Анонімний вхід	Група, в яку входять всі користувачі, що увійшли в систему анонімно.
S-1-5-домен-500	Адміністратор	Обліковий запис адміністратора системи. За замовчуванням цей запис забезпечує повний контроль системи.
S-1-5-домен-501	Гість	Обліковий запис користувача – гостя.

Повний список загальновідомих SID можна подивитися в документації Platform SDK. Дізнатися SID конкретного користувача в системі, а також SID груп, в які він включений, можна, використовуючи консольну команду ***whoami***:

whoami /user *або* ***whoami /groups***

Відповідність імені користувача і його SID можна відстежити також в ключі реєстру **HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ ProfileList**.

Згідно з політикою безпеки, для доступу до комп'ютера користувач повинен пройти процедуру аутентифікації. Ця процедура ініціюється комбінацією клавіш «CTRL+ALT+DEL». Дана комбінація клавіш, відома як SAS (secure attention sequence), завжди перехоплюється драйвером клавіатури, який викликає при цьому справжню (а не «троянського коня») програму аутентифікації. Процес користувача не може сам перехопити цю комбінацію клавіш або відмінити чи скасувати її обробку драйвером. Кажучи мовою стандартів, в системі реалізована функціональність захищеного каналу (trusted path functionality). Ця особливість відповідає вимогам захисту рівня В «Помаранчевої книги».

Процедурою аутентифікації користувача в системі управляє програма, WinLogon.exe, яка за допомогою інтерактивної процедури відображає початковий діалог із користувачем на екрані. Процес WinLogon активно взаємодіє з бібліотекою GINA (Graphical Identification and Authentication – графічною бібліотекою ідентифікації і аутентифікації). Одержавши ім'я і пароль користувача від GINA, WinLogon викликає модуль LSASS для аутентифікації цього користувача. В разі успішного входу в систему, Winlogon отримує з реєстру профіль користувача, визначає тип оболонки і запускає її.

Комбінація SAS може бути одержана системою не лише на етапі входу користувача в систему. Якщо ж користувач уже увійшов до системи, то після натиснення клавіш «*CTRL+ALT+DEL»* він отримує наступні можливості: подивитися список активних процесів, ініціювати перезавантаження або вимкнення комп'ютера, змінити свій пароль і заблокувати робочу станцію. У свою чергу, якщо робоча станція заблокована, то після введення SAS користувач має можливість її розблокування. Іноді може бути здійснене примусове виведення користувача із системи з подальшим входом у неї адміністратора.

Після аутентифікації користувача процесом Winlogon, всі процеси, запущені від імені цього користувача будуть ідентифікуватися спеціальним об'єктом, званим ***маркером доступу*** (access token). При формуванні маркера використовуються ключі SECURITY і SAM реєстру. Перший ключ визначає загальну політику безпеки, а другий ключ містить інформацію про захист для індивідуальних користувачів. Якщо процес користувача запускає дочірній процес, то його маркер успадковується, тому маркер доступу уособлює користувача для системи в кожному запущеному від його імені процесі. Основні елементи маркера представлені на рис. 15.2.

SID користувача	SID1 ... SIDn Ідентифікатори груп користувача	DACL за замовчуванням	Привілеї	Інші параметри

Рис. 15.2. Узагальнена структура маркера доступу.

Маркер доступу містить ідентифікатор доступу самого користувача та всіх груп, в які він включений. В маркер включений також DACL за замовчуванням – список дискреційного контролю доступу, який приєднується до створюваних користувачем об'єктів. Ще одна важлива для визначення прав користувача в системі частина маркера – *список його привілеїв*, призначення і відкликання яких є прерогативою локального адміністратора безпеки LSA. ***Привілеї*** – це права довіреного об'єкта на здійснення будь-яких дій по відношенню до всієї системи. У таблиці 15.2 перераховані деякі привілеї, які можуть бути надані користувачеві.

Таблиця 15.2. Привілеї, якими можуть бути наділені користувачі

Ім'я та ідентифікатор привілею	Опис привілею
SeIncreaseBasePriorityPrivilege Збільшення пріоритету диспетчирування	Користувач, що володіє даним привілеєм може змінювати пріоритет диспетчирування процесу за допомогою інтерфейсу Диспетчера завдань.
SeLockMemoryPrivilege Закріплення сторінок в пам'яті	Процес отримує можливість зберігати дані фізичної пам'яті, не вдаючись до кешування даних у віртуальній пам'яті на диску.
SeAuditPrivilege Управління аудитом та журналом безпеки	Користувач отримує можливість вказувати параметри аудиту доступу до об'єкта для окремих ресурсів, таких як файли, об'єкти Active Directory, ключі реєстру.
SeTakeOwnershipPrivilege Оволодіння файлами або іншими об'єктами	Користувач отримує можливість ставати власником будь-яких об'єктів безпеки системи, включаючи об'єкти Active Directory, файли і папки NTFS, принтери, розділи реєстру, служби, процеси і потоки.
SeShutdownPrivilege Завершення роботи системи	Користувач отримує можливість завершувати роботу операційної системи на локальному комп'ютері.
SeChangeNotifyPrivilege Обхід перехресної перевірки	Використовується для обходу перевірки дозволів для проміжних каталогів при проході багаторівневих каталогів.

Управління привілеями користувачів здійснюється в оснащенні **«Групова політика»**, розділ ***Конфігурація Windows/Локальні політики/Призначення прав користувача.***

Щоб подивитися привілеї користувача, можна також використовувати команду ***whoami:***

whoami /all

Інші параметри маркера носять інформаційний характер і визначають, наприклад, яка підсистема створила маркер, унікальний ідентифікатор маркера безпеки, час його дії. Необхідно також відзначити можливість створення *обмежених маркерів* (restricted token), які відрізняються від звичайних тим, що з них видаляються деякі привілеї та його SID-ідентифікатори перевіряються тільки на заборонні правила.

Принцип мінімальних привілеїв рекомендує виконання всіх операцій із мінімальними привілеями, необхідними для досягнення результату. Це дозволяє зменшити втрати від спроб навмисного збитку й уникнути випадкових втрат даних. Наприклад, користувачу не рекомендується реєструватися як адміністратор системи без необхідності. Таким чином, обмежені маркери використовуються для процесів, які підміняють клієнта і виконують небезпечний код.

Створити обмежений маркер можна програмно, використовуючи API-функцію ***CreateRestrictedToken***, а можна запустити процес з обмеженим маркером, використовуючи пункт контекстного меню Windows ***«Запуск від імені іншого користувача»*** (рис.15.3).

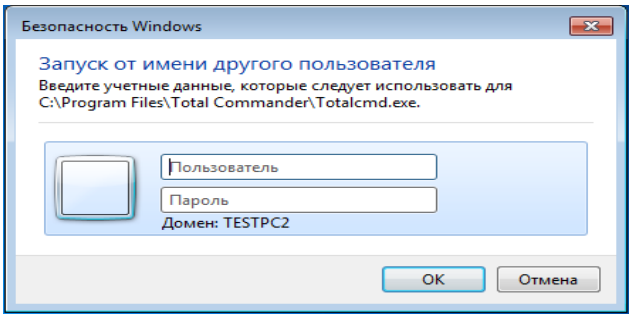


Рис. 15.3. Запуск процесу з обмеженим маркером

Також необхідно відзначити, що маркер доступу може бути створений не тільки при первинному вході користувача в систему. Windows надає можливість запуску процесів від імені інших користувачів, створюючи для цих процесів відповідний маркер. Для цих цілей можна використовувати:

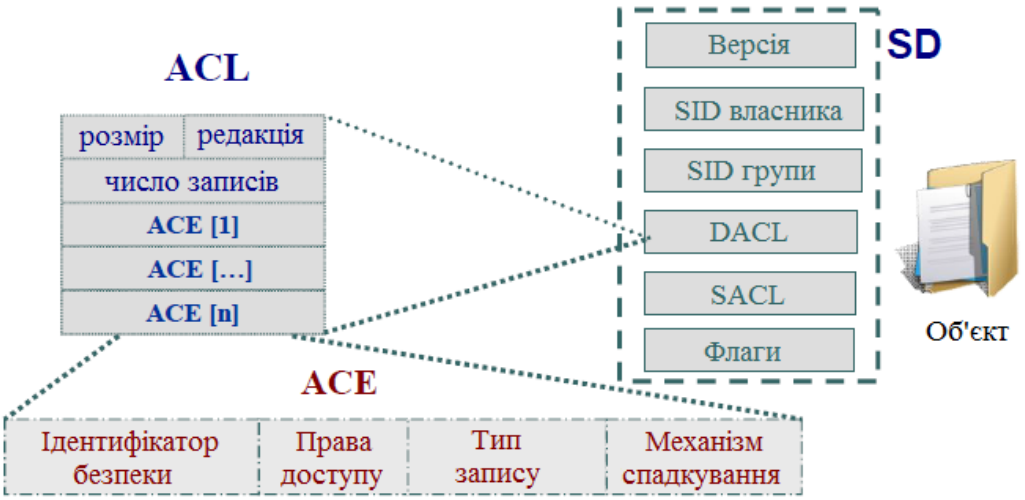
- API-функції ***CreateProcessAsUser, CreateProcessWithLogon***;
- віконний інтерфейс (рис. 4.3), який ініціюється при виборі пункту контекстного меню ***«Запуск від імені іншого користувача»***;
- консольну команду ***runas***:

runas /user: username program,

де *username* – ім’я облікового запису користувача, який буде використаний для запуску програми в форматі *користувач@домен* або *домен\користувач*;

program – команда або програма, яка буде запущена за допомогою облікового запису, зазначеного в параметрі ***/user***.

У будь-якому варіанті запуску процесу від імені іншого облікового запису, потрібно задати його пароль.



15.2.2. Захист об’єктів системи

Маркер доступу ідентифікує суб’єктів – користувачів системи. З іншого боку, кожний об’єкт системи, що потребує захисту, містить опис прав доступу до нього користувачів. Для цих цілей використовується ***дескриптор безпеки*** (Security Descriptor, ***SD***). Кожному об’єкту системи, включаючи файли, принтери, мережні служби, контейнери Active Directory та інше, присвоюється дескриптор безпеки, який визначає права доступу до об’єкта і містить наступні основні атрибути (рис. 15.4):

- SID власника, що ідентифікує обліковий запис користувача – власника об’єкта;
- список дискреційного контролю доступу (Discretionary Access Control List, DACL), який дозволяє відстежувати права та обмеження, встановлені власником даного об’єкта. DACL може бути змінений користувачем, який вказаний як поточний власник об’єкта.
- список системного контролю доступу (System Access Control List, SACL), що визначає перелік дій над об’єктом, які підлягають аудиту;
- флаги, які визначають атрибути об’єкта.

Рис. 15.4. Структура дескриптора безпеки об’єкта ОС Windows

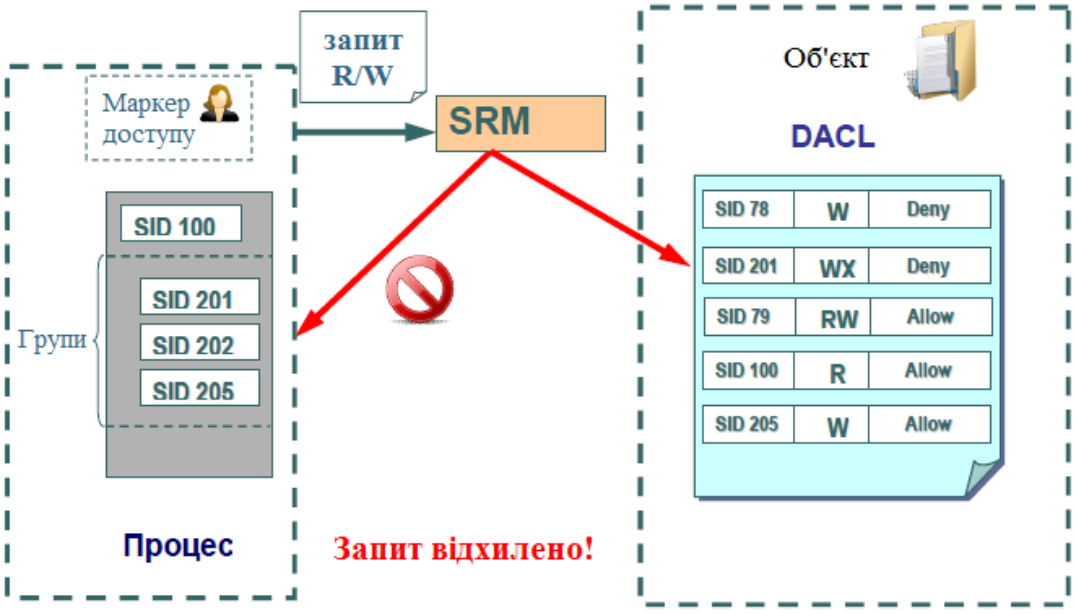
Авторизація Windows заснована на зіставленні маркера доступу суб’єкта з дескриптором безпеки об’єкта. Керуючи властивостями об’єкта, адміністратори можуть встановлювати дозволи, призначати право володіння і відстежувати доступ користувачів.

Список дискреційного контролю доступу містить набір записів ACE (Access Control Entries). У DACL кожен ACE складається з чотирьох частин: у першій зазначаються користувачі або групи, до яких належить даний запис, у другій – права доступу, а третя інформує про те, надаються ці права чи відбираються. Четверта частина являє собою набір флагів, що визначають, як даний запис буде успадковуватися вкладеними об'єктами (актуально, наприклад, для папки файлової системи, розділів реєстру).

Якщо список ACE в DACL порожній, до нього немає доступу ні у одного користувача (тільки у власника на зміну DACL). Якщо відсутній сам DACL в SD об'єкта, в такому разі всі користувачі мають повний доступ до нього.

Якщо який-небудь потік запросив доступ до об'єкта, підсистема SRM здійснює перевірку прав користувача, що запустив потік, на даний об'єкт, переглядаючи його список DACL. Перевірка здійснюється до появи дозвільних прав ***на всі*** запитані операції. Якщо зустрінеться забороняюче правило хоча б ***на одну*** запитану операцію, доступ не буде наданий.

Докладніше розглянемо приклад на рис.15.5. Процес намагається отримати доступ до об'єкта з заданим DACL. В маркері процесу вказані SID користувача який запустив його, а також SID груп, в які він входить. У списку



DACL об'єкта присутні правила, що дозволяють здійснювати читання для користувача з SID=100, і запис для групи з SID=205. Однак, в доступі користувачу буде відмовлено, оскільки раніше зустрічається забороняюче запис правило для групи з SID=201.

Рис. 15.5. Перевірка прав доступу користувача до об'єкту

Необхідно відзначити, що забороняюче правило поміщено в списку DACL на рисунку не випадково. Забороняючі правила завжди розміщуються перед дозвільними, тобто є домінуючими при перевірці прав доступу.

Для визначення і перегляду прав доступу користувачів до ресурсів можна використовувати як графічні засоби контролю, так і консольні команди. Стандартне вікно властивостей об’єкта файлової системи (диску, папки, файлу) на вкладці ***Безпека*** (рис. 15.6) дозволяє переглянути поточні дозволи для користувачів і груп користувачів, редагувати їх, створювати нові або видаляти існуючі.

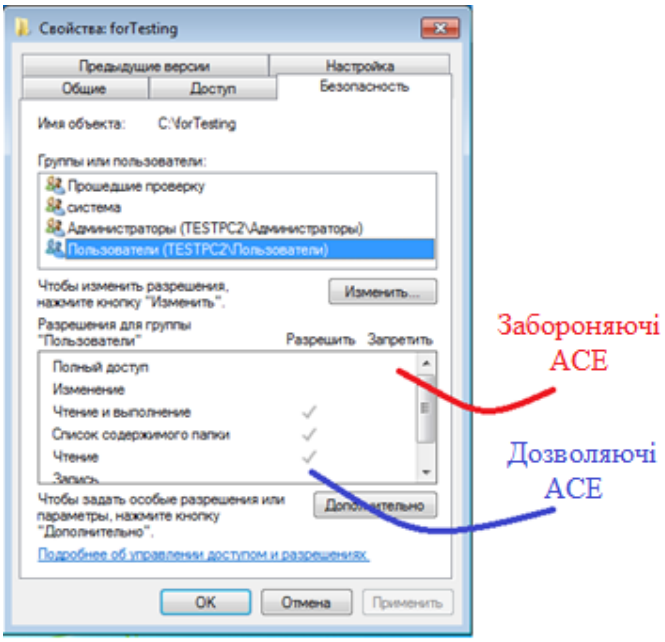


Рис. 15.6. GUI-інтерфейс Windows для зміни прав доступу до об’єктів

При визначенні прав доступу до об’єктів можна задати правила їх успадкування в дочірніх контейнерах. У вікні додаткових параметрів безпеки на вкладці ***Дозволу*** при виборі опції ***«Додавати дозволи, які успадковуються від батьківських об’єктів»*** (рис. 15.7) можна успадкувати дозволи і обмеження, задані для батьківського контейнера, поточному об’єкту.

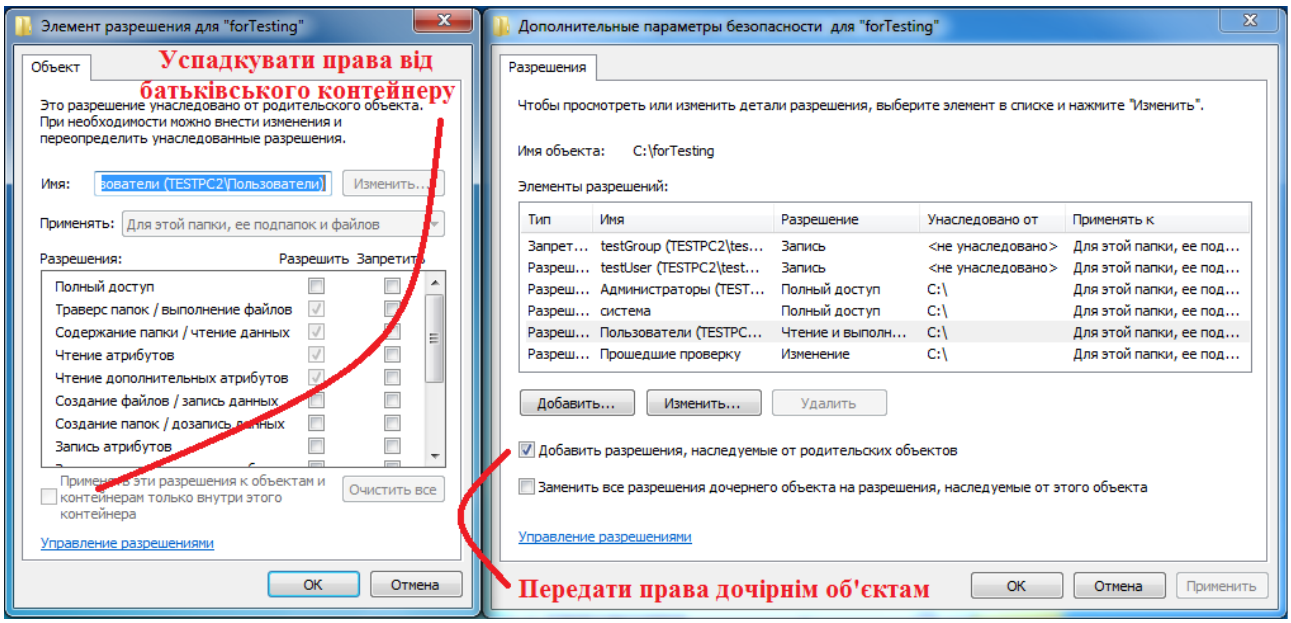


Рис. 15.7. Визначення параметрів успадкування прав доступу до об’єктів

При виборі опції ***«Застосовувати ці дозволи до об’єктів і контейнерів тільки усередині цього контейнера»*** дозволяється передача визначених для об’єкта-контейнера правил доступу його дочірнім об’єктам.

В цьому ж вікні на вкладці «***Власник»*** можна дізнатися власника об’єкта і замінити його. Власник об’єкта має право на зміну списку його DACL, навіть якщо до нього заборонений будь-який тип доступу. Адміністратор має право ставати власником будь-якого об’єкта.

З урахуванням можливості входження користувача у різні групи і незалежності визначення прав доступу до об’єктів для груп і користувачів, часто буває складно визначити кінцеві права користувача на доступ до об’єкту: потрібно переглянути забороняючі правила, визначені для самого об’єкта, для всіх груп, в які він включений, потім те ж саме зробити для дозвільних правил. Автоматизувати процес визначення дозволених користувачеві видів доступу до об’єкта можна з використанням вкладки ***«Чинні дозволи»*** вікна додаткових параметрів безпеки об’єкта (рис. 15.8).

Для перегляду та зміни прав доступу до об’єктів в режимі командного рядка призначена команда ***icacls*** (***cacls*** в Windows XP).

ICACLS *i’мя [/grant[:r] Sid:perm[...]] [/deny Sid:perm [...]] [/remove[:g|:d]] Sid[...]] [/T] [/C] [/L] [/Q] [/setintegritylevel Level:policy[...]]*

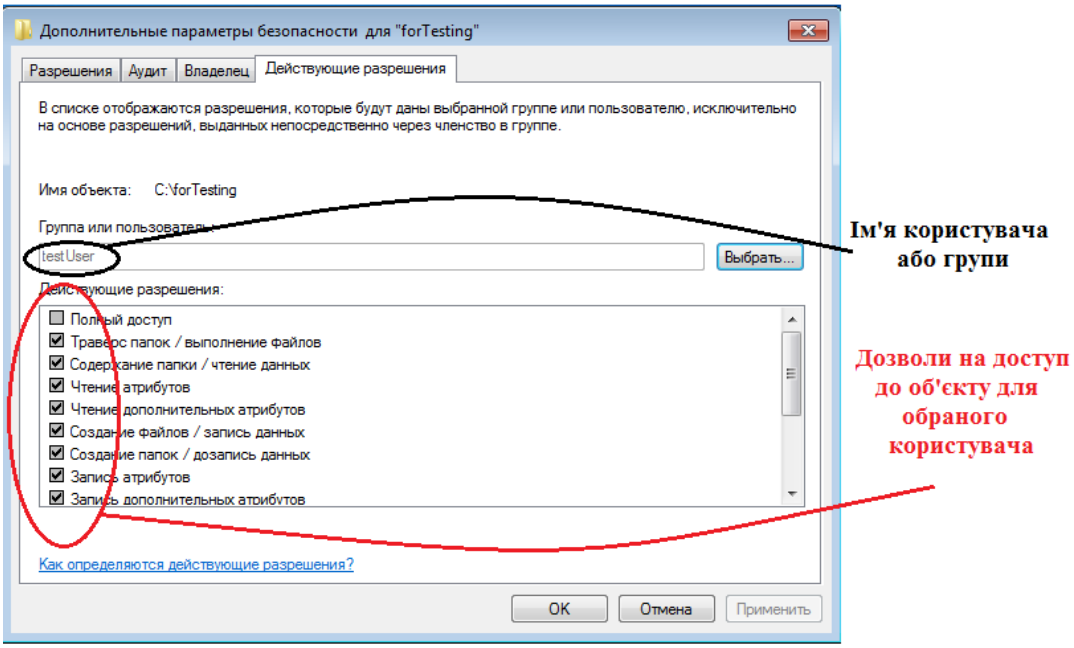


Рис. 15.8. Визначення ефективних прав доступу користувача (групи) до об’єкту

Призначення параметрів команди наведені в таблиці 15.3.

Таблиця 15.3. Параметри команди *icacls*

<ім’я>	Задає файл або папку, права доступу до якої необхідно переглянути/змінити (допустимо використовувати шаблони з символами * та ?).
/grant[:r] Sid:perm	Надання зазначених прав доступу користувача. З параметром *:r* ці дозволи замінюють усі раніше надані дозволи. Без параметра *:r* дозволи додаються до будь-яких раніше наданих дозволів.
/deny Sid:perm	Відгук зазначених прав доступу користувача. Додається ACE відкликання для заявлених дозволів з видаленням цих дозволів у будь-якому представленні.
/remove[:[g|:d]] Sid	Видалення всіх входжень SID в ACL. З параметром *:g* видаляються всі входження наданих прав у цьому SID. З параметром *:d* видаляються всі входження відкликаних прав у цьому SID.
/setintegritylevel	Lодавання ACE рівня цілісності до всіх відповідних файлів.

Для вказівки прав, які додаються або віднімаються використовуються такі значення:

F – повний доступ;

DE – видалення;

WD – запис;

RC – читання;

N – немає доступу.

Розглянемо кілька прикладів:

icacls c:\test – видасть список DACL для папки test.

icacls c:\test /deny ім'я_комп'ютера \ім'я_користувача:(WD) – заборонить запис до об'єкту для зазначеного користувача.

icacls c:\test /grant ім'я_комп'ютера \і'мя_групи:(F)– надасть повний доступ до папки c:\test і її підпапок всім членам зазначеної групи.

Для програмного перегляду і зміни списків DACL можна використовувати API-функції ***AddAccessAllowedAce, AddAccessDeniedAce, SetSecurityInfo***.

Розглянуті способи роботи з списком дискреційного доступу ілюструють реалізацію в Windows моделі довільного доступу. Але починаючи з Windows Vista фірма Microsoft реалізувала елементи мандатного доступу для контролю доступу до об'єктів. За цей рівень забезпечення безпеки відповідає *Windows Integrity Control (WIC)*. Концепція WIC вторить раніше згаданим принципам примусового (мандатного) управління доступом і заснована на побудові довірчих відносин між об'єктами і управлінні діями з ними користувачів на основі їх рівня довіри. Базовим поняттям WIC є ***рівень цілісність*** (integrity level) об'єкта. WIC присвоює контрольованим об'єктам один з шести доступних рівнів цілісності:

- ***Untrusted*** – анонімні процеси автоматично потрапляють в цю категорію.
- ***Low*** – стандартний рівень при роботі з Інтернетом. Якщо браузер Internet Explorer запущений в захищеному режимі, всі файли і процеси, асоційовані з ним, призначаються в цю категорію. Деякі папки, такі як, наприклад, Temporary Internet Folder, також за замовчуванням наділяються *Низьким рівнем довіри*.
- ***Medium*** – в даному контексті працює більшість об'єктів. Ординарні користувачі отримують *Середній рівень* і якщо не вказано який-небудь інший, тоді всім об'єктам присвоюється даний рівень доступу.
- ***High*** – рівень, асоційований у системі з *Адміністраторами*. Об'єкти *Високого рівня* недоступні звичайним користувачам.
- ***System*** – рівень для роботи ядра операційної системи та її служб.
- ***Installer*** – вершина в ієрархії рівнів WIC. Його об'єкти можуть редагувати і видаляти файли всіх попередніх рівнів.

Контроль за рівнями цілісності при доступі до об'єкту також здійснюється на основі правил ACE. Але це спеціалізовані ACE, які починаючи з ОС Windows Vista зберігаються в списку SACL дескриптора безпеки об'єкта поряд з правилами аудиту. Рівень цілісності користувача (процесу, що виконується від його імені) зберігається в його ***токені безпеки***. При доступі процесу до об'єкта монітор безпеки порівнює рівень цілісності в токені з рівнем

цілісності в дескрипторі об’єкта (у SACL). Система видає права доступу в залежності від того, вище чи нижче рівень цілісності суб’єкта по відношенню до об’єкта, а також залежно від флагів політики цілісності у відповідному ACE об’єкта. Рівні цілісності (***IL***) користувача описуються в його ідентифікаторі безпеки, точніше – в його RID-частині:

SID = S-1-16-0x0 – рівень Untrusted

SID = S-1-16-0x1000 – рівень Low

SID= S-1-16-0x2000 – рівень Medium

SID= S-1-16-0x3000 – рівень High

SID= S-1-16-0x4000 – рівень системи

Для зміни рівня цілісності об’єктів можна використовувати наступні інструменти:

- вже розглянуту команду *icacls* з ключем /setintegitylevel. Наприклад, ось так можна присвоїти файлу низький (*L*) рівень цілісності:

icacls c:\forTesting /setintegritylevel L

- використовуючи спеціальні утиліти *Chml* («change mandatory label») для зміни рівня цілісності файлів та папок, і *Regil* («Registry integrity levels») для роботи з рівнями цілісності ключів реєстру.

Змінити рівень цілісності процесу можна, наприклад, запустивши його утилітою ***psexec.exe*** з відповідним ключем. Ось як можна запустити блокнот з високим рівнем цілісності:

psexec –h notepad.exe

Очевидно, що змінювати рівень цілісності процесів, що запускаються потенційно небезпечна операція, тому її можуть запускати тільки процеси, у яких в маркері доступу встановлений привілей *SeRelabelPrivilege*.

Дізнатися, який рівень цілісності має процес можна, наприклад, запустивши утиліту ***ProcessExplorer*** з набору *Sysinternals* (рис. 15.9).

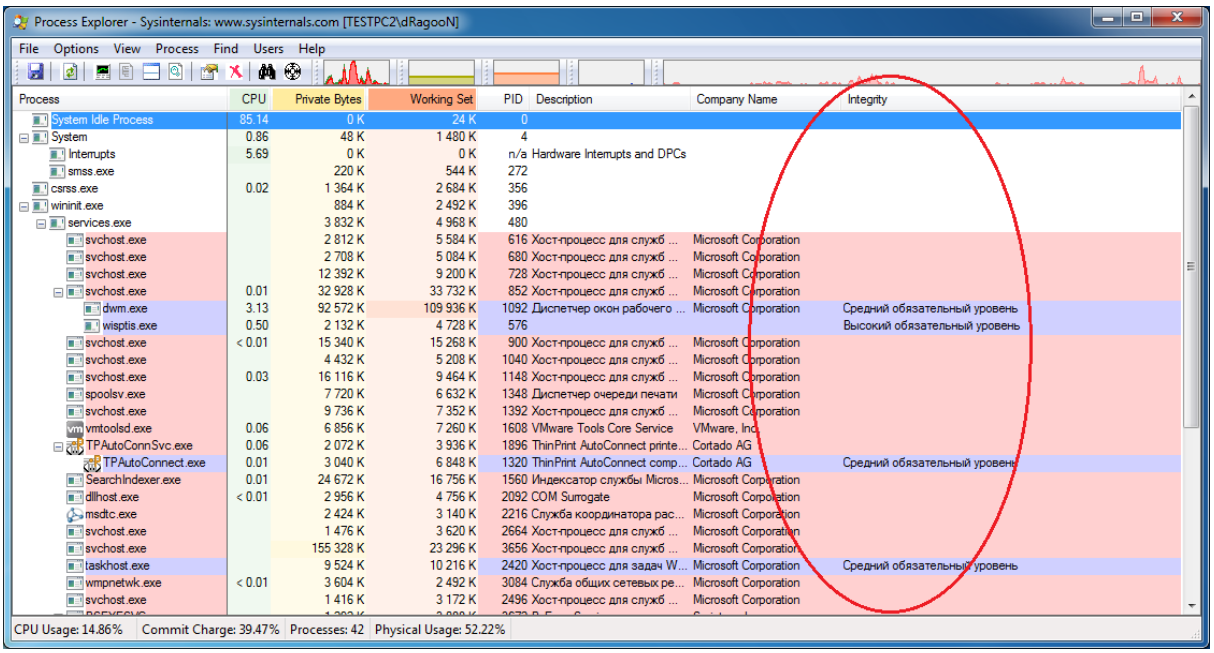


Рис. 15.9. Рівень цілісності запущених процесів в інтерфейсі ProcessExplorer

Необхідно відзначити, що контроль рівнів цілісності має більш високий пріоритет при перевірці прав доступу до об’єкта перед дискреційної таблицею.

15.2.3. Підсистема аудиту

Навіть найкраща система захисту рано чи пізно буде зламана, тому виявлення спроб вторгнення – найважливіше завдання системи захисту. Основним інструментом виявлення вторгнень є аудит подій в системі, який є важливим елементом політики безпеки. Окремі дії користувачів протоколюються, а одержаний протокол використовується для виявлення вторгнень. ОС Windows веде аудит подій за 9 категоріями:

1. Аудит подій входу в систему.
2. Аудит управління обліковими записами.
3. Аудит доступу до служби каталогів.
4. Аудит входу в систему.
5. Аудит доступу до об’єктів.
6. Аудит зміни політики.
7. Аудит використання привілеїв.
8. Аудит відстеження процесів.
9. Аудит системних подій.

Розглянемо більш докладно, які події відстежує кожна з категорій.

Аудит подій входу в систему. Аудит спроб користувача увійти в систему з іншого комп’ютера або вийти з неї, за умови, що цей комп’ютер використовується для перевірки справжності облікового запису.

Аудит управління обліковими записами. Аудит подій, пов'язаних з управлінням обліковими записами на комп'ютері: створення, зміна або видалення облікового запису користувача або групи; перейменування, відключення або включення облікового запису користувача; встановлення або зміна пароля.

Аудит доступу до служби каталогів. Аудит подій доступу користувача до об'єкта каталогу Active Directory, для якого заданий власний список системного контролю доступу (SACL).

Аудит входу в систему. Аудит спроб користувача увійти в систему з комп'ютера або вийти з неї.

Аудит доступу до об'єктів. Аудит подій доступу користувача до об'єкта – наприклад, файлу, папки, розділу реєстру, принтера і т. п., – для якого заданий власний список системного контролю доступу (SACL).

Аудит зміни політики. Аудит фактів зміни політик, призначення прав користувачів, політик аудиту або політик довірчих відносин.

Аудит використання привілеїв. Аудит спроб користувача скористатися наданим йому правом.

Аудит відстеження процесів. Аудиту таких подій, як активізація програми, завершення процесу, повторення дескрипторів і непрямий доступ до об'єкта.

Аудит системних подій. Аудит подій перезавантаження або вимикання комп'ютера, а також подій, які впливають на системну безпеку або на журнал безпеки.

Рішення про аудит конкретного типу подій безпеки приймаються у відповідності з політикою аудиту локальної системи. Політика аудиту, також звана *локальною політикою безпеки* (local security policy), є частиною політики безпеки, підтримуваної LSASS в локальній системі, і налаштовується за допомогою редактора локальної політики безпеки (Оснащення ***gpedit.msc, Конфігурація комп'ютера – Конфігурація Windows – Параметри безпеки – Локальні політики – Політика аудиту***, рис. 15.10).

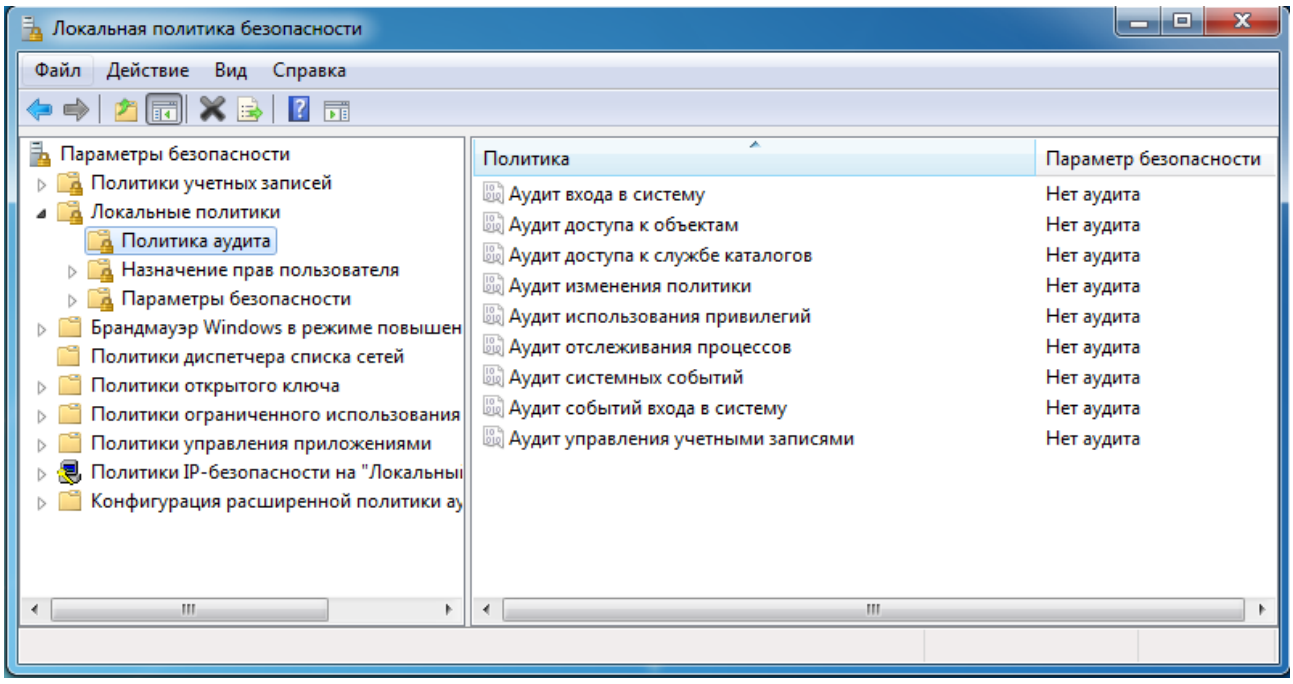


Рис. 15.10. Конфігурація політики аудиту редактора локальної політики безпеки

Для кожного об’єкта в SD міститься список SACL, що складається із записів ACE, які регламентують запис у журнал аудиту вдалих або невдалих спроб доступу до об’єкта. Ці ACE визначають, які операції, що виконуються над об’єктами конкретними користувачами або групами, підлягають аудиту. Інформація аудиту зберігається в системному журналі аудиту. Аудиту можуть підлягати як успішні, так і невдалі операції. Подібно записам ACE DACL, правила аудиту об’єктів можуть успадковуватись дочірніми об’єктами. Процедура спадкування визначається набором флагів, які є частиною структури ACE.

Налаштування списку SACL може бути здійснене у вікні додаткових властивостей об’єкта (пункт ***«Додатково»***, закладка ***«Аудит»***, рис. 15. 11).

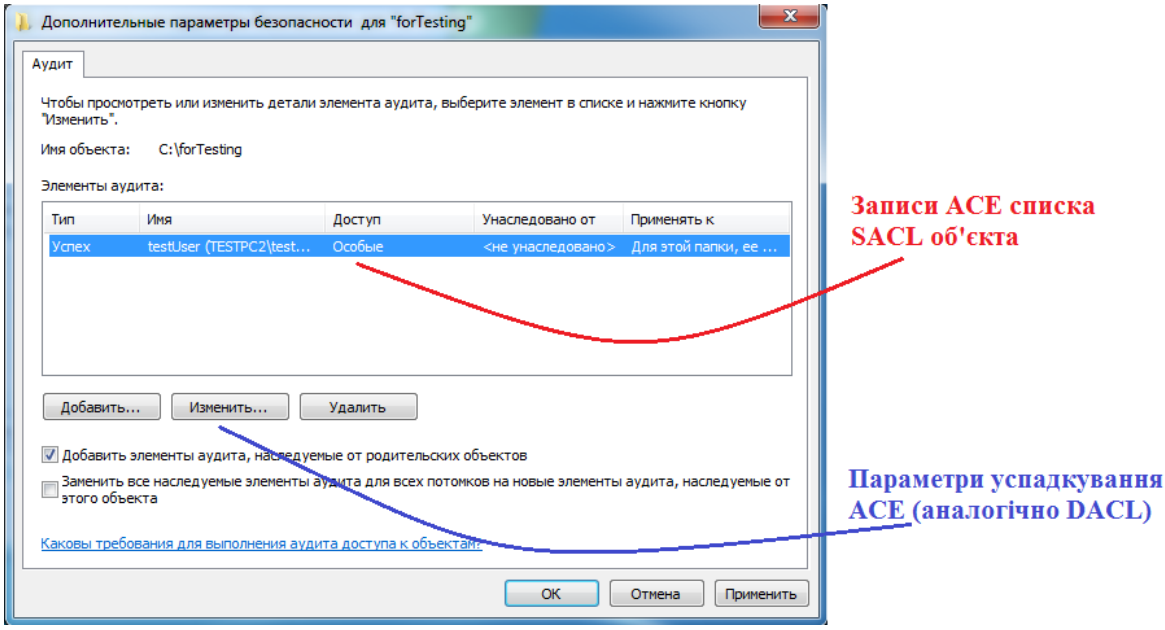


Рис. 15.11. Інтерфейс редагування правил аудиту для об’єкта

Для програмного перегляду і зміни списків SACL можна використовувати API-функції ***GetSecutityInfo*** і ***SetSecutityInfo***.

При ініціалізації системи і зміні політики LSASS посилає SRM повідомлення, які інформують його про поточну політику аудиту. LSASS відповідає за прийом записів аудиту, які генеруються на основі подій аудиту від SRM, їх редагування і передачу Event Logger (реєстратору подій). SRM посилає записи аудиту LSASS через своє LPC-з’єднання. Після цього Event Logger заносить записи в журнал безпеки.

Починаючи з Windows Vista підтримуються дві категорії журналів подій: «***журнали Windows»*** і «***журнали додатків і служб»***. ***Журнали Windows*** – реєструють загальносистемні подій, і ведуться самою ОС. ***Журнали додатків і служб*** – індивідуальні для конкретних типів додатків і компонентів (Internet Explorer, MediaCenter, PoerShell та ін). Події аудиту записуються в журнали Windows наступних типів (на прикладі Windows 7):

1. ***Журнал додатків.*** В журналі додатків містяться дані, що відносяться до роботи додатків і програм.
2. ***Журнал безпеки.*** Журнал безпеки містить записи про такі події, як успішні і невдалі спроби доступу в систему, а також про події, що відносяться до використання ресурсів.
3. ***Журнал системи.*** У журналі містяться події системних компонентів Windows. Наприклад, в журналі системи реєструються збої при завантаженні драйвера або інших системних компонентів при запуску системи.
4. ***Журнал установки.*** Фіксує події, пов’язані із встановленням або видаленням компонентів системи.
5. ***Журнал перенаправлення.*** Фіксує події, перенаправлені з сусідніх комп’ютерів.

Перегляд журналу безпеки здійснюється у вікні «Перегляд подій» (***eventvwr.msc***, рис. 15.12). Самі журнали зберігаються у файлах з розширенням *evtx* в папці ***%SystemRoot%\System32\Winevt\Logs\.***

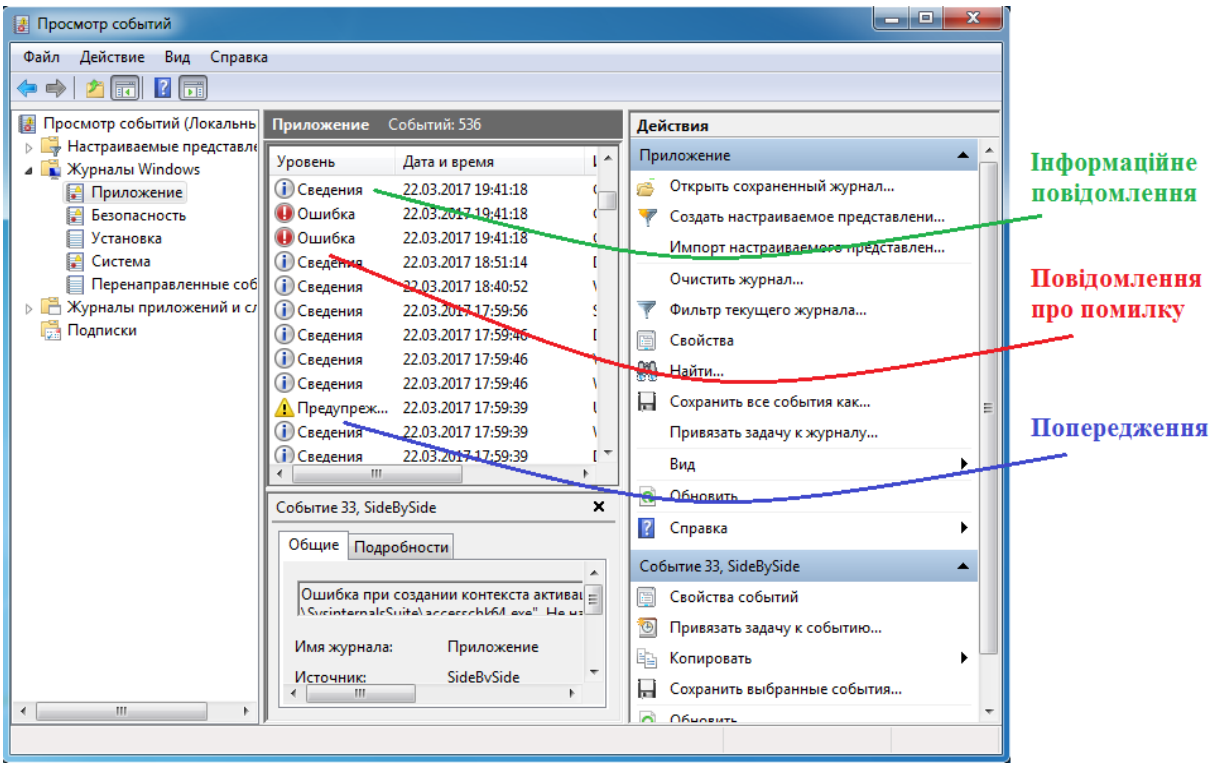


Рис. 15.12. Вікно Windows «Перегляд подій»

У журналі реєструються події різних типів:

- ***Відомість*** – сигналізує про зміну в додатку або компоненті, наприклад, успішний доступ до ресурсу, запуск програми або служби;
- ***Попередження*** – сигналізує про потенційно небезпечні події, що виникли в додатку або компоненті, які не заважають його роботі, але можуть стати причиною проблем у майбутньому;
- ***Помилка*** – сигналізує про проблему, яка впливає на програму або компоненту;
- ***Критична помилка*** – відповідає збою, критичному для додатка або компонента, після якого вони не можуть продовжувати роботу;

15.2.4. Файлова система шифрування.

Починаючи з версії Windows 2000, в операційних системах сімейства Windows NT підтримується шифрування даних на розділах файлової системи NTFS з використанням *файлової системи шифрування* (***Encrypted File System, EFS***). Основна її перевага полягає в забезпеченні конфіденційності даних на дисках комп'ютера за рахунок використання надійних симетричних алгоритмів шифрування даних в режимі реального часу.

Для шифрування даних EFS використовує симетричний алгоритм шифрування (AES або DESX) з випадковим ключем для кожного файлу (***File Encryption Key, FEK***). За замовчуванням дані шифруються в Windows 2000 і Windows XP за алгоритмом DESX, а в Windows XP з Service Pack 1 (або вище)

та Windows Server 2003 – по алгоритму AES. У версіях Windows, дозволених для експорту за межі США, драйвер EFS реалізує 56-бітний ключ шифрування DESX, тоді як у версії, що підлягає використанню тільки в США, і у версіях з пакетом для 128-бітного шифрування довжина ключа DESX дорівнює 128 бітам. Алгоритм AES в Windows використовує 256-бітові ключі.

При цьому для забезпечення секретності самого ключа FEK шифрується асиметричним алгоритмом RSA відкритим ключем користувача, результат шифрування FEK – ***Data Decryption Field, DDF*** – додається в заголовок зашифрованого файлу (рис. 15. 13). Такий підхід забезпечує надійне шифрування без втрати ефективності процесу шифрування: дані шифруються швидким симетричним алгоритмом, а для гарантії секретності симетричного ключа використовується асиметричний алгоритм шифрування.

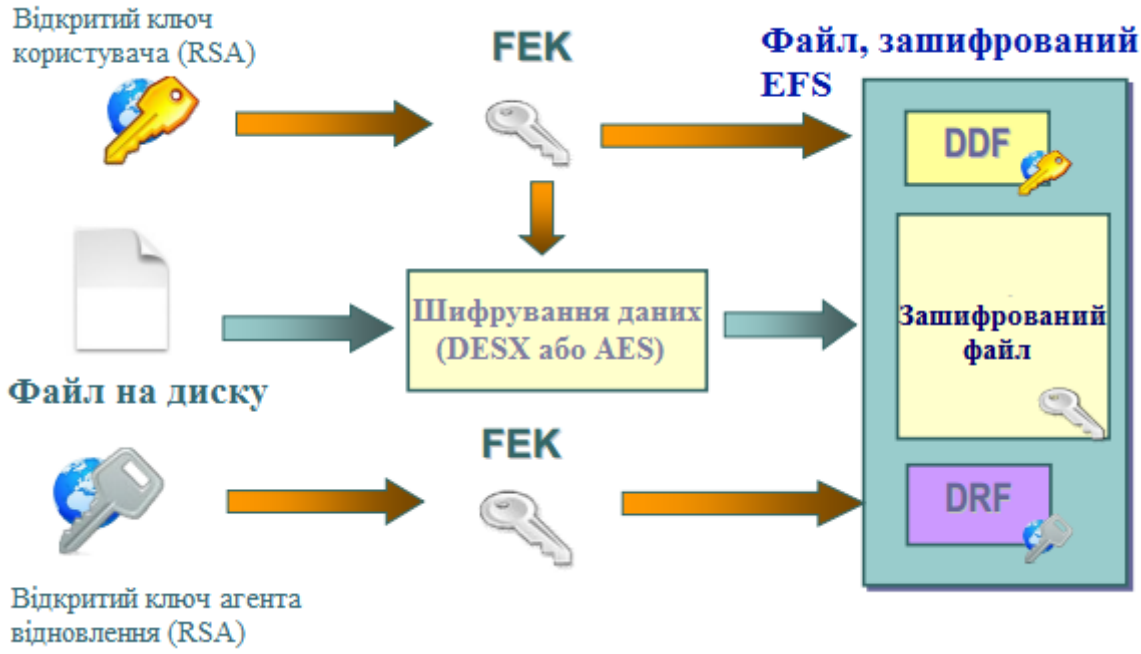


Рис. 15.13. Схема шифрування файлу в EFS

Для шифрування файлів з використанням EFS можна використовувати графічний інтерфейс або команду ***cipher***.

Графічний інтерфейс доступний в стандартному вікні властивостей об’єкта по натисненню кнопки ***«Додатково»*** (рис. 15.14). Зашифровані об’єкти в стандартному інтерфейсі Windows Explorer відображаються зеленим кольором, а при спробі відкрити зашифрований файл іншим користувачем відбувається «Відмова в доступі».

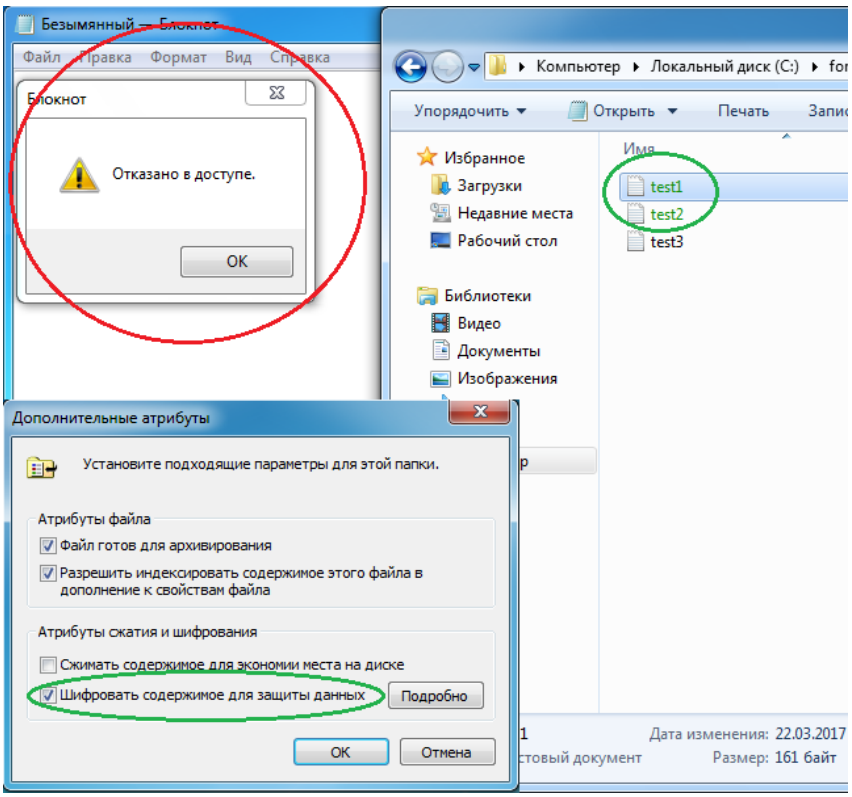


Рис. 15.14. Графічний інтерфейс шифрування файлу з використанням EFS

Необхідно відзначити, що EFS дозволяє розділяти зашифрований файл між декількома користувачами. У цьому випадку FEK шифрується відкритими ключами всіх користувачів, яким дозволений доступ до файлу, і кожен результат шифрування додається в DDF.

Шифрування файлу з використанням EFS захищає файл комплексно: користувачу, який не має права на розшифрування файлу, неприпустимі, в тому числі, такі операції, як видалення, перейменування і копіювання файлу. Необхідно пам’ятати, що EFS є частиною файлової системи NTFS, і в разі копіювання захищеного файлу авторизованим користувачем на інший том з файловою системою, яка не підтримує EFS (наприклад, FAT32), він буде розшифрований і збережений на цільовому томі у відкритому вигляді.

Консольна команда ***cipher*** може бути використана для шифрування/розшифрування файлів з командного рядка або в bat-сценарії.

cipher [{***/e***|***/d***}] [***/s***:каталог] [***/a***] [***/i***] [***/f***] [***/q***] [***/h***] [***/k***] [***/u***[***/n***]] [шлях [...]] | [***/r***:і’мя_файлу_без_розширення]

Призначення параметрів команди наведені в таблиці 15.4.

Таблиця 15.4. Параметри команди **cipher**

/e	Шифрує вказані папки. Папки позначаються таким чином, щоб файли, які будуть додаватися в папку пізніше, також шифрувалися.
/d	Розшифровує вказані папки. Папки позначаються таким чином,

	щоб файли, які будуть додаватися в папку пізніше, не будуть шифруватися
/s: *каталог*	Виконує обрану операцію над зазначеною папкою і всіма підпапками в ній.
/a	Виконує операцію над файлами і каталогами.
/i	Продовження виконання зазначеної операції навіть після виникнення помилок. За замовчуванням виконання ***cipher*** припиняється після виникнення помилки.
/f	Виконання повторного шифрування або розшифрування вказаних об'єктів. За замовчуванням вже зашифровані або розшифровані файли пропускаються командою ***cipher***
/k	Створення ключа шифрування файлу для користувача, який виконав команду ***cipher***. Якщо використовується цей параметр, всі інші параметри команди ***cipher*** не враховуються.
/u	Оновлення ключа шифрування файлу користувача або ключа агента відновлення на поточні ключі до всіх зашифрованих файлів на локальному диску (якщо ці ключі були змінені). Цей параметр використовується тільки разом з параметром ***/n***.
/n	Заборона оновлення ключів. Даний параметр служить для пошуку всіх зашифрованих файлів на локальних дисках. Цей параметр використовується тільки разом з параметром ***/u.***
шлях	Вказує шаблон, файл або папку.
/r: *і'мя_файлу*	Створення нового сертифіката агента відновлення і закритого ключа з наступним їх записом у файлі з іменем, вказаним в параметрі *ім'я_файлу* (без розширення). Якщо використовується даний параметр, всі інші параметри команди ***cipher*** не враховуються.

Наприклад, щоб визначити, зашифрована якась папка чи ні, необхідно використовувати команду:

cipher шлях\ім'я_папки

Команда ***cipher*** без параметрів виводить статус (зашифрований чи ні) для всіх об'єктів поточної папки.

Для шифрування файлу необхідно використовувати команду:

cipher /e /a шлях\ім'я_файлу

Для розшифрування файлу, відповідно, використовується команда:

cipher /d /a шлях\ім'я_файлу

Допустиме шифрування/розшифрування групи файлів по шаблону:

cipher /e /a d:\work*.doc

Пара відкритий і закритий ключ для шифрування FEK створюються для користувача автоматично при першому шифруванні файлу з використанням EFS.

Якщо деякий користувач або група користувачів зашифрували файл з використанням EFS, то його вміст доступно тільки їм. Це призводить до ризиків втрати доступу до даних в зашифрованих файлах у разі втрати пароля даними користувачами (працівник забув пароль, звільнився тощо). Для запобігання подібних проблем адміністратор може визначити деякі облікові записи в якості *агентів відновлення*.

Агенти відновлення (Recovery Agents) визначаються в політиці безпеки ***Encrypted Data Recovery Agents*** (Агенти відновлення зашифрованих даних) на локальному комп'ютері або в домені. Ця політика доступна через оснащення ***Групова політика (gpedit.msc)*** розділ ***«Параметри безпеки»*** >> ***«Політика відкритого ключа»*** >> ***«Файлова система EFS»***. Пункт меню ***«Дія»*** >> ***«Додати агент відновлення даних»*** відкриває *«майстер додавання нового агента»*.

Додаючи агентів відновлення можна вказати, які криптографічні пари (позначені їхніми сертифікатами) можуть використовувати ці агенти для відновлення зашифрованих даних (рис. 15.15). Сертифікати для агентів відновлення створюються командою ***cipher*** з ключем ***/r*** (див. табл. 15.4). Для користувача, який буде агентом відновлення, необхідно імпортувати закритий ключ агента відновлення із сертифікату, створеного командою ***cipher***. Це можна зробити у вікні *«майстра імпорту сертифікатів»*, що автоматично завантажується при подвійному клацанні по файлу ****.pfx***.

EFS створює ***DRF (Data Recovery Field)*** – елементи ключів для кожного агента відновлення, використовуючи провайдер криптографічних сервісів, зареєстрований для EFS-відновлення. DRF додається в зашифрований файл і може бути використаний як альтернативний засіб вилучення FEK для розшифрування вмісту файлу.

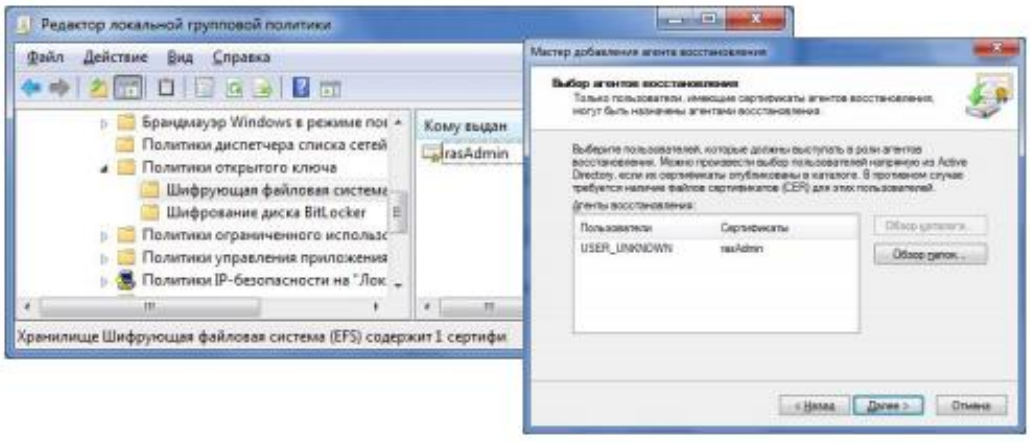


Рис. 15.15. Додавання нового агента відновлення EFS

Windows зберігає закриті ключі в підкаталозі ***Application Data\Microsoft\Crypto\RSA*** каталогу профілю користувача. Для захисту закритих ключів Windows шифрує всі файли в папці RSA на основі симетричного ключа, що генерується випадковим чином; такий ключ називається ***майстер-ключем користувача***. Майстер-ключ має довжину в 64 байти і створюється стійким генератором випадкових чисел. Майстер-ключ також зберігається в профілі користувача в каталозі ***Application Data\Microsoft\Protect*** і шифрується за алгоритмом 3DES з допомогою ключа, який частково заснований на паролі користувача. Коли користувач змінює свій пароль, майстер-ключі автоматично розшифровуються, а потім заново зашифровуються з урахуванням нового пароля.

Для розшифрування FEK EFS використовує функції ***Microsoft CryptoAPl (CAPI)***. CryptoAPI складається з DLL провайдерів криптографічних сервісів (cryptographic service providers, CSP), які забезпечують програмам доступ до різних криптографічних сервісів (шифруванню, розшифруванню і хешуванню). EFS спирається на алгоритми шифрування RSA, що надаються провайдером ***Microsoft Enhanced Cryptographic Provider***.

Шифрування та розшифрування файлів можна здійснювати програмно, використовуючи API-функції ***EncryptFile*** і ***DecryptFile***.

Порядок виконання лабораторної роботи №15:

1. Включити ПК.
2. Ознайомитися з короткими теоретичними відомостями.
3. Виконати наступні завдання:

1) При виконанні лабораторної роботи на комп'ютерах у навчальній лабораторії використовуйте раніше створену (на лабораторній роботі №6) віртуальну машину ***Test PC1 Win*** або створіть та запустіть нову віртуальну машину. Увійдіть в систему під обліковим записом адміністратора. Всі дії в наступних підпунктах виконуйте в системі, що працює на віртуальній машині.

2) Створіть обліковий запис нового користувача, наприклад, ***testUser*** розділ ***«Керування комп'ютером»*** (***compmgmt.msc***). При створенні нового облікового запису забороніть користувачеві зміну пароля і зніміть обмеження на термін дії його пароля. Створіть нову групу, наприклад, ***«testGroup»*** і включіть в неї нового користувача. Видалити користувача з усіх інших груп. Створіть на диску C: папку ***forTesting***. Створіть або скопіюйте в папку кілька текстових файлів (*.txt).

3) З допомогою команди *runas* запустити сеанс командного рядка (**cmd.exe**) від імені новоствореного користувача. Командою *whoami*

подивіться SID користувача і всіх його груп, а також поточні привілеї користувача. Рядок запуску і результат роботи цієї і ***BCIX*** наступних консольних команд записати у файл протоколу лабораторної роботи, або відобразити у вигляді скріншотів.

4) Переконайтеся у відповідності імені користувача та отриманого SID в реєстрі Windows. (Використовуйте ключ реєстру HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList).

5) Командою *whoami* визначте перелік поточних привілеїв користувача ***testUser***. В сеансі командного рядка користувача спробуйте змінити системний час командою *time*. Щоб надати користувачу такий привілей, запустіть оснащення ***«Локальні параметри безпеки»*** (***secpol.msc***). Додайте користувача в список параметрів політики ***«Зміна системного часу»*** розділу ***Локальні політики*** >> ***Призначення прав користувача***. Після цього перезапустіть ваш сеанс командного рядку від імені користувача, переконайтеся, що у списку привілеїв додався ***SeSystemtimePriviege***. Спробуйте змінити системний час командою ***time***.

6) Переконайтеся, що привілей ***«Завершення роботи системи»*** (SeShutdown-Privilege) наданий користувачу ***testUser*** . Після цього спробуйте завершити роботу системи з сеансу командного рядка користувача командою *shutdown –s.* Додайте йому привілей «***Примусове віддалене завершення» (SeRemoteShutdownPrivilege)***. Спробуйте завершити роботу консольною командою ще раз (скасувати команду завершення до її безпосереднього виконання можна командою *shutdown –a*).

7) Ознайомтеся з довідкою по консольній команді *icacls*. Використовуючи цю команду, перегляньте дозволу на папку c:\forTesting. Поясніть всі позначення в описах прав користувачів і груп у видачі команди.

8) Дозвольте користувачеві ***testUser*** запис в папку ***forTesting***, але забороніть запис для групи ***testGroup***. Спробуйте записати файли чи папки в ***forTesting*** від імені користувача ***testUser***. Поясніть результат. Подивіться надані дозволи користувача ***testUser*** до папки ***forTesting*** у вікні властивостей папки.

9) Використовуючи стандартне вікно властивостей папки, виберіть для користувача ***testUser*** такі права доступу до папки, щоб він міг записувати інформацію в папку ***forTesting***, але не міг переглядати її вміст. Переконайтеся, що папка ***forTesting*** є тепер для користувача ***testUser*** «сліпою», запустивши, наприклад, від його імені файловий менеджер і спробувавши записати файли в папку, переглянути її вміст, видалити файл з папки.

10) Для вкладеної папки ***forTesting\Docs*** зніміть спадкування ACL від батька і дозвольте користувачеві перегляд, читання і запис в папку. Перевірте, що для користувача папка ***forTesting\Docs*** перестала бути «сліпою» (наприклад, зробіть її поточною в сеансі роботи файлового менеджера від імені користувача і створіть у ній новий файл).

11) Зніміть заборону на читання папки ***forTesting*** для користувача ***testUser***. Використовуючи команду *icacls* забороніть цьому користувачеві доступ до файлів з розширенням ***txt*** в папці ***forTesting***. Переконайтеся в недоступності файлів для користувача.

12) Командою *icacls* забороніть користувачеві всі права на доступ до папки ***forTesting*** і дозвольте повний доступ до вкладеної папки ***forTesting\Docs***. Переконайтеся, що теки forTesting\Docs є доступною для користувача. Поясніть результат.

13) Від імені користувача ***testUser*** зашифруйте який-небудь файл на диску. Переконайтеся, що після цього був створений сертифікат користувача, запустивши оснастку ***certmgr.msc*** від імені користувача (розділ ***Особисті***). Перегляньте основні параметри сертифіката відкритого ключа користувача ***testUser*** (термін дії, використовувані алгоритми).

14) Створіть у папці ***forTesting*** нову папку ***Encrypt***. У папці ***Encrypt*** створіть або скопіюйте в неї текстові файли. Зашифруйте папку ***Encrypt*** і весь її вміст із меню властивості папки від імені адміністратора. Спробуйте переглянути або скопіювати який-небудь файл цієї папки від імені користувача ***testUser***. Поясніть результат.

15) Скопіюйте зашифрований файл в незашифровану папку (наприклад, ***forTesting***). Переконайтеся, що він залишився зашифрованим. Додайте користувача ***testUser*** у список користувачів які мають доступу до файлу у вікні властивостей шифрування файлу. Повторіть спробу отримати доступ до файлу від імені користувача ***testUser***.

8. Оформити звіт згідно до вимог (додаток 1).

9. Відповісти на контрольні питання та підготуватися до письмового опитування.

Зміст звіту:

1. Титульний лист.
2. Постановка завдання.
3. Протокол виконання лабораторної роботи, що містить результати роботи всіх консольних команд або відповідні скріншоти з поясненням отриманих результатів.

4. Висновки та відповіді на контрольні питання.

Контрольні питання:

1. До якого класу безпеки відноситься ОС Windows за різними критеріями оцінки?
2. Яким чином користувачі ідентифікуються в ОС Windows?
3. Що таке списки DACL і SACL?
4. Як відбувається перевірка прав доступу користувача до ресурсів ОС Windows?
5. Що таке маркер безпеки, і яка його роль у моделі безпеки Windows?
6. Що таке рівень цілісності? Як він впливає на права доступу суб'єктів до об'єктів ОЗ? Як можна дізнатися і задати рівень цілісності для об'єктів і суб'єктів?
7. Які події підлягають аудиту в ОС Windows?
8. Яким чином зашифровуються файли у файловій системі EFS? Що таке FEK? DDF?
9. Які алгоритми шифрування використовуються в EFS?

Лабораторна робота №16
«Механізми безпеки операційної системи Linux»

Мета роботи:

1. Ознайомлення з принципами побудови архітектури підсистеми безпеки сучасних операційних систем.
2. Вивчення моделі безпеки операційної системи Linux та отримання практичних навиків у використанні засобів забезпечення її безпеки.

Стислі теоретичні відомості:

16.1. Порівняння архітектури ОС Windows та Linux

Віруси, троянські коні та інші деструктивні програми вражають ПК з встановленою на них ОС Windows внаслідок цілої низки причин, властивих Windows та не властивих Linux:

1) ОС Windows порівняно недавно еволюціонувала від однокористувацької моделі до багатокористувацької.

2) ОС Windows за своєю архітектурою є монолітною, а не модульною системою.

3) В ОС Windows надто широко використовується RPC-механізм.

4) Windows фокусується на відомому графічному інтерфейсі для ПК.

Розглянемо вказані причини детальніше.

ОС Windows порівняно недавно еволюціонувала від однокористувацької моделі до багатокористувацької. Система Windows з самого початку була розроблена, щоб забезпечити користувачам та програмам вільний доступ до усієї системи, а це означає, що хто завгодно міг скомпрометувати критичнно важливу системну програму або файл. Це також значить, що віруси та інші деструктивні програми могли зробити те ж саме, тому що ОС Windows не ізолювала користувачів та прикладне програмне забезпечення від критичних ділянок операційної системи.

Операційна система Windows XP стала першою версією Windows, де з'явилися суттєві результати спроб ізолювання користувачів від системи, таким чином, щоб кожен користувач мав свої власні особисті файли та обмежені системні повноваження. Однак платою за це стало те, що програмні продукти, розроблені для попередніх версій перестали працювати. Саме тому в Windows XP було передбачено режим сумісності, тобто режим, який дозволяє програмам працювати так, ніби вони функціонують в однокористувацькому середовищі. Windows XP – це прогрес, однак і Windows XP не можна назвати дійсно багатокористувацькою системою.

Windows Server 2003 – це наступний крок до істинно багатокористувацької системи, але навіть у Windows Server 2003 не вдалося ліквідувати усі «діри» (уразливості) в системі захисту. Саме тому в Windows Server 2003 довелося відключити використання «за замовчуванням» деяких функцій web-браузера (наприклад, ActiveX, написання сценаріїв тощо). Якщо б Microsoft переписала ці функції для роботи у безпечному режимі в істинно багатокористувацькому середовищі, вони не створювали б таких серйозних загроз, перед якими беззахисна ОС Windows.

Windows за своєю архітектурою є монолітною, а не модульною системою. Монолітна система – це система, де більшість функцій інтегровано в єдиний модуль. Протилежністю такої системи є така система, в якій функції розподілено за кількома рівнями, причому кожен рівень має обмежений доступ до інших.

Взаємозалежності такого типу мають два негативних каскадних побічних ефекта. По-перше, в монолітній системі кожна «діра» в одній частині системи впливає на усі сервіси та додатки, які залежать від цієї частини системи. Інтегрувавши Internet Explorer в операційну систему, Microsoft створила систему, де будь-яка «діра» в Інтернет Explorer створює загрози для комп'ютера з ОС Windows в цілому.

Така архітектурна модель впливає набагато більше, ніж здається на перший погляд. Таким чином, у монолітній системі вразливості в системі захисту виявляються набагато критичнішими, ніж можна було очікувати.

Проілюструвати це зможе проста аналогія. Уявимо собі ідеальну ОС, яка складається з трьох сфер: одна в центрі; друга, більшого діаметру, охоплює першу; а третя сфера охоплює дві перших. Користувач бачить лише третю сферу. Це рівень, де він запускає додатки, наприклад, текстові процесори. Вони використовують необхідні функції, що надаються другою сферою, наприклад, засоби візуалізації графічних зображень або форматування текстів. Ця друга сфера (спеціалісти називають її «користувацькими процесами») не має прямого доступу до критичних частин системи. Щоб виконати певну операцію, вона має запитати дозволу у внутрішньої сфери. Внутрішня сфера виконує найважливіші функції, тому, що має безпосередній доступ до усіх критичних частин системи. Вона керує пам'яттю, дисками та рештою важливих частин системи. Ця сфера називається «ядром» і є серцем ОС.

У такій архітектурі «діра» в програмі графічного відображення не може нанести глобальної шкоди комп'ютеру, оскільки функції візуалізації не мають прямого доступу до найкритичніших частин системи. Навіть якщо користувач завантажить у текстовий процесор зображення з втіленим вірусом, цей вірус не зможе пошкодити нічого окрім власних файлів користувача, оскільки функція графічного відображення не має доступу до жодної критичної частини системи.

Проблема ОС Windows полягає в тому, що в ній не дотримуються розумних конструкторських принципів розділення функцій по відповідних описаних рівнях. ОС Windows реалізує занадто багато функцій у ядрі, центральній сфері, в якій реалізація тієї чи іншої загрози може призвести до критичних наслідків. Наприклад, якщо інтегрувати графічні функції в ядро, ці функції зможуть нашкодити усій системі. Таким чином, як тільки виявиться «діра» в алгоритмі графічного відображення, надмірно інтегрована архітектура ОС Windows полегшить використання цієї «діри» для отримання повного контролю над системою і ймовірно подальшого руйнування всієї системи.

Монолітна система нестабільна за самою своєю природою. Коли в системі так багато взаємозв'язків, зміна однієї з її частин породжує багато загроз. Одна зміна в системі може вплинути (і вона таки впливає) на усі сервіси та додатки, які залежать від цієї частини системи. Саме тому оновлення, які виправляють одну частину ОС Windows, часто порушують роботу інших сервісів та додатків. Для прикладу можна навести такий факт: для пакета оновлень Windows XP Service Pack 2 було створено список випадків, коли його встановлення призвело до виходу з ладу програм сторонніх виробників. Таке явище в монолітній системі звичайна справа.

В ОС Windows занадто широко використовується RPC-механізм. Абревіатура RPC означає «віддалений виклик процедур» (Remote Procedure Call), що має на увазі ситуацію коли одна програма відправляє через мережу вказівку іншій програмі виконати певну дію. Віддаленим викликом процедури цей механізм називається тому, що не має значення, функціонують ці програми на одному й тому ж комп'ютері, чи на різних, підключених до мережі Інтернет.

RPC-механізми – це потенціальна загроза ІБ, оскільки їх призначення – дозволити комп'ютерам, які знаходяться десь у мережі, віддавати даному комп'ютеру вказівки виконати ті, чи інші дії. Як тільки знаходиться вразливість в програмі, що використовує RPC-механізм, будь-хто з мережі може скористатися цією вразливістю, щоб змусити уражений комп'ютер виконати якісь дії. На жаль, користувачі ОС Windows не можуть заблокувати RPC-механізм, оскільки ОС Windows використовує його, навіть якщо комп'ютер не підключений до мережі. Дивно, але деякі з найбільш серйозних вразливостей у Windows Server 2003 – наслідок «дір» у самих RPC-функціях ОС Windows, а не в програмних продуктах, що їх використовують.

Важливо зазначити, що RPC-механізми не завжди необхідні, і не зрозуміло, чому Microsoft так широко їх використовує.

16.1.1. Особливості архітектури ОС Linux

За даними статистичних опитувань Evans Data Linux Developers Survey, 92 % респондентів ніколи не зіштовхувалися з випадками зараження ОС Linux вірусами, троянськими та іншими деструктивними програмами.

Той факт, що віруси, троянські та інші деструктивні програми дуже рідко можуть (якщо взагалі можуть) заразити Linux-системи, частково можна пояснити такими причинами:

1. ОС Linux має довгу історію використання ретельно проробленої багатокористувацької архітектури.
2. За своєю архітектурою ОС Linux є, в основному, модульною системою.
3. Функціонування ОС Linux не залежить від RPC-механізму, а сервіси зазвичай за замовчуванням налаштовані не використовувати RPC-механізми.
4. Сервери Linux ідеально підходять для віддаленого адміністрування.

Розглянемо ці причини детальніше.

ОС Linux має довгу історію використання ретельно проробленої багатокористувацької архітектури. ОС Linux ніколи не була однокористувацькою системою. Тому в ній з самого початку закладено принцип ізолювання користувачів від додатків, файлів та каталогів, що

впливають на ОС в цілому. Кожному користувачу надається користувацький каталог, де зберігаються усі його файли даних, конфігураційні файли, що належать цьому користувачу. Коли користувач запускає якийсь додаток (наприклад, текстовий процесор), він запускається з обмеженими повноваженнями. Цей додаток має право на запис лише у власний каталог цього користувача і не може нічого записати у системні файли, і навіть у каталог іншого користувача, якщо тільки адміністратор явним чином не надасть цьому користувачеві таке право.

Ще важливіше, що ОС Linux надає практично усі функціональні можливості (наприклад, візуалізацію зображень JPEG) у вигляді модульних бібліотек. Тому, коли текстовий процесор відображає JPEG-зображення, відповідні функції запускаються з тими ж обмеженими повноваженнями, що й сам текстовий процесор. Якщо в програмах візуалізації JPEG-зображень є «діра», зловмисник зможе використати її лише для отримання таких самих повноважень, як і у цього користувача, що значно обмежує масштаби можливих збитків. У цьому переваги модульних систем, вони ближчі до раніше описаного ідеалу ОС.

Навіть сервіси, наприклад, web-сервери, зазвичай запускаються як користувачі з обмеженими повноваженнями. Так, наприклад, Debian GNU/Linux запускає web-сервер Apache як користувача «www-data», що належить до такої самої групи. Якщо зловмисник на комп'ютері з Debian отримає повний контроль над web-сервером Apache, він зможе впливати лише на файли, які належать користувачу «www-data», тобто на web-сторінки. В свою чергу, MySQL, запускається з повноваженнями користувача «mysql». Навіть, якщо Apache та MySQL разом обслуговують web-сторінки, зловмисник, отримавши контроль над Apache, не буде мати повноважень, які дозволяють використати цю вразливість для отримання контролю над сервером баз даних, тому що він «належить» іншому користувачу. Крім того, такі облікові записи конфігуруються без можливості доступу до командного рядка, а отже, не зможуть подати довільну команду серверу Linux.

За своєю архітектурою Linux є модульною, а не монолітною системою. Linux – це ОС, сконструйована, в основному, за модульним принципом, від ядра до різних додатків. В ОС Linux практично немає нероздільних зв'язків між компонентами. Немає й єдиного web-браузера, який використовується системою або програмами електронної пошти. Отже, «діра» у web-браузері не обов'язково небезпечна для інших додатків.

Однак, необхідно відзначити, що, хоча, ядро ОС Linux підтримує модульні драйвери, але значною мірою все ж таки є монолітним ядром, оскільки сервіси в цьому ядрі взаємозалежні. Усі негативні наслідки

монолітності мінімізуються тим, що ядро ОС Linux, наскільки це можливо, розроблено як найменша частина системи. Розробники Linux фанатично притримуються такого принципу: «Якщо задача може бути вирішена за межами ядра, вона обов'язково повинна бути виконана поза ним». Це значить, що в Linux майже кожна корисна функція («корисна» – означає «для кінцевого користувача») не має доступу до вразливих частин ОС Linux.

Сервери Linux ідеально підходять для віддаленого адміністрування. Сервер Linux можна, а зачастіше й необхідно, інсталювати без монітора та адмініструвати віддалено, оскільки при такому стилі адміністрування він не піддається таким загрозам як при локальному адмініструванні.

Можливо, це одна з найголовніших відмінностей ОС Linux від Windows, тому, що цей фактор зводить нанівець багато критичних вразливостей, загальних для ОС Linux та Windows, наприклад, вразливості web-браузера Mozilla та Internet Explorer.

16.2. Основні принципи та механізми забезпечення безпеки в ОС Linux

Розглянувши всі переваги архітектури ОС Linux перейдемо до детального розгляду безпосереднь методів забезпечення безпеки ОС Linux.

Забезпечення безпеки в ОС Linux коротко можна описати за допомогою структурної схеми системи безпеки ОС Linux, яка відображена на рис. 16.1 (SELinux).

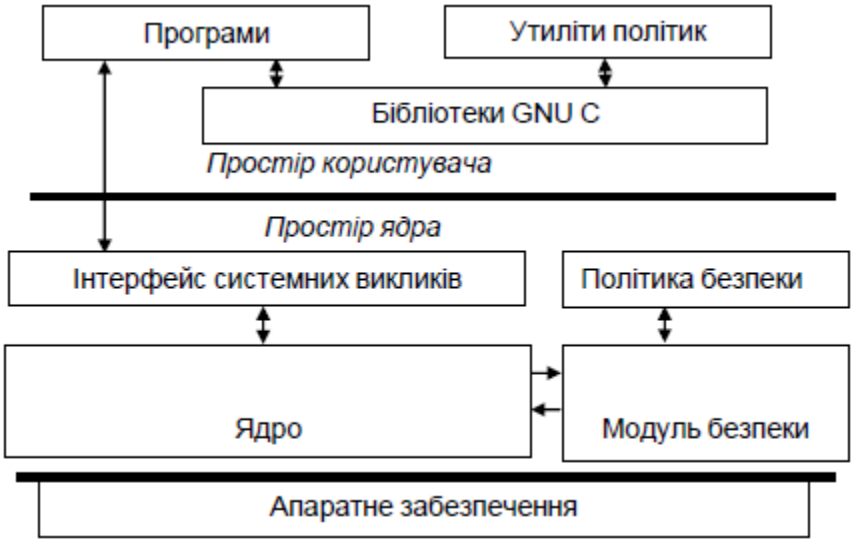


Рис. 16.1. Структурна схема системи безпеки ОС Linux

Як бачимо, система, завдяки своїй модульній структурі, дозволяє змінювати модулі безпеки та утиліти політик безпеки (дана функція притаманна усім версіям Linux), які зосереджені поза межами мікроядра, що

позитивно впливає на безпеку системи в цілому, а також на можливість вдосконалення цієї системи без втручання в роботу ядра.

ОС SELinux є на сьогодні однією з найбільш захищених середовищ, але, безумовно, не єдиною. Альтернативою SELinux є ***бібліотеки AppArmor***, в якій також використовується інфраструктура модуля LSM (Linux Security Module). Причиною створення AppArmor стало те, що SELinux виявився надто складним для пересічного користувача. AppArmor має повністю налаштовувані модулі безпеки та режим навчання, який допомагає налаштувати систему безпеки. Ще однією перевагою AppArmor є те, що вона не залежить від типу файлової системи (ФС), тоді як SELinux вимагає підтримки ФС додаткових атрибутів.

16.2.1. Основні принципи організації доступу в ОС Linux

Розглянемо основні принципи організації доступу в Linux. Як відомо, основні версії Linux підтримують дискреційну модель доступу, яка реалізується файловою системою extX (ext 2, 3, 4). Основні параметри доступу Linux зводяться до наступного.

Кожен користувач має ***унікальний ідентифікатор користувача (UID)***, а група, до якої він належить – ***ідентифікатор групи (GID)***. Для автентифікації користувачів використовуються дві утиліти: *getty*, яка приймає логін користувача, і утиліта *login*, яка приймає пароль і виконує аутентифікацію. Паролі в Linux також зберігаються у вигляді хеш-образів. У перших версіях хешування виконувалося алгоритмом DES, зараз – MD5. Облікові записи зберігаються в папці */etc/passwd/*.

Структура записів бази даних така:

Ім'я користувача:хеш_пароля:sid:gid:дод._інф.:home_dir:shell

Приклади:

petrenko:1QRxtta36BD:340:120:Петренко_В.І.:/home/Petrenko:/bin/bash

root: Ep6mckrOLChF:0:0:root:/root:/bin/bash

або:

petrenko:x:340:120: Петренко_В.І.:/home/ Petrenko:/bin/bash

root:x:0:0: root: /root:/bin/bash

Символи «*x*» на місці пароля означають, що у системі застосований більш сучасний метод зберігання паролів: вони зберігаються у файлі тіньових паролів – ***/etc/shadow*.** Власником файлу */etc/shadow* є користувач *root* і тільки він має право читати інформацію з нього.

Формат записів у цьому файлі має наступний вигляд, як приклад:

petrenko: 1QRxtta36BD.:10063:0:99999:7:::
root: Ep6mckrOLChF:10792:0::7:7::
shutdown:U:10811:0:-1:7:7:-1:134531940

Призначення першого поля файла *shadow* таке ж, як і у першого поля файла – ім'я користувача. Друге поле містить хеш-образ пароля. Реалізація тіньових паролів дозволяє збільшити довжину паролів від 13 до 24 символів. Символи для використання у паролях, беруться з набору який складається з 52 літер англійського алфавіту, цифр та спецсимволів "(" та ")". Разом виходить 64 символи.

З третього поля починається інформація про термін дії пароля. Це – кількість днів з 1 січня 1970 року до дня зміни цього пароля.

Четверте поле (*мінімальний термін дії пароля*) вказує на кількість днів, яка повинна пройти, перш ніж можна буде змінювати пароль. Таким чином, поки з дня останньої зміни пароля не пройде зазначена у цьому полі кількість днів, знову змінювати пароль не можна.

П'яте поле (*максимальний термін дії пароля*) задає максимальну кількість днів, протягом яких можна використовувати пароль, після чого він має бути обов'язково змінений. Якщо в даному полі стоїть додатня величина, то при спробі користувача зайти до системи після цього терміну призведе до того, що команду password буде запущено у режимі обов'язкової зміни пароля.

Значення з шостого поля визначає, за скільки днів до закінчення терміну дії пароля слід попереджати користувача про це.

Сьоме поле (*дата блокування облікового запису*) задає число днів, починаючи з дня обов'язкової зміни пароля, коли цей обліковий запис блокується. Іншими словами, якщо після цієї кількості днів користувач не зайде до системи і не змінить свій пароль, то його обліковий запис буде заблоковано.

Останнє ж поле залишається зарезервованим і поки що не використовується.

У файлі ***etc/groups*** описано групи користувачів. *Структура цього файла подібна до файла паролів, наприклад:*

root::0:
wheel::10:
bin::1:bin,daemon
daemon::2:bin,daemon

Спершу вказується ім'я групи (воно повинне бути унікальним); потім йде запис пароля (як правило, паролі для груп не використовуються, тому, воно практично завжди порожнє); після чого вказується ідентифікатор ідентифікатор

групи, gid (він також має бути унікальним, хоча це і не є обов'язковим); і в останньому відображається список користувачів, що входять до цієї групи (імена користувачів пишуться через кому без пробілів).

Взагалі, кожен користувач має створену за замовчуванням групу, яка створюється при реєструванні користувача, так звану групу входу. Ім'я цієї групи співпадає з іменем користувача. Якщо користувач або адміністратор не вкаже інакше, система призначає цю групу групою-власником усіх його файлів, що дозволяє автоматично обмежити доступ інших користувачів до його інформації, оскільки вони належать до інших груп користувачів.

Щоб визначити UID користувача, GID та ім'я його основної групи, а також список інших груп, до якого включено користувач, можна використовувати команду *id*. У разі її використання без аргументів, команда виведе інформацію про поточного користувача. Якщо ж вказати в якості аргументу ім'я іншого зареєстрованого користувача, вивід команди буде відповідати зазначеному користувачеві.

Окремим випадком команди *id* є команда *groups*. Вона видає список імен всіх груп, в яких розташований поточний або вказаний користувач.

Введення команди *who* без аргументів дозволяє отримати список користувачів, що працюють в даний момент в системі. Якщо ж набрати *whoami*, система виведе інформацію про поточного користувача.

16.2.2. Файли та права доступу

ОС Linux, в принципі, підтримує багато файлових систем. Однак, як зазначалося раніше, основними є ФС типу extX (ext 2, 3, 4). Дві останні – журнальні ФС, які дозволяють відновлювати втрачену інформацію, звісно ж, до певної межі.

В останніх версіях ОС Linux використовується ext 4. Особливості цих ФС полягають в тому, що файли, каталоги та пристрої вважаються файлами. Кожному пристрою відповідає свій файл. Файли та пристрої для використання задіюються операцією монтування. Точка монтування визначається при поданні довільної команди, а керує цим ядро системи. Коли користувач хоче отримати доступ до пристрою, ядро визначає, чи має він відповідні права, при цьому виконується аналіз ідентифікатора користувача та ідентифікатори усіх груп, до яких він належить. На основі цього аналізу і виноситься рішення про надання доступу.

Також, необхідно відзначити, що сам файловий простір Linux-систем є ієрархією файлів (рис. 16. 2), яка має єдиний спільний корінь – так званий кореневий каталог, що позначається знаком слеша "/". Щоб однозначно

ідентифікувати будь-який файл, можна вказати шлях до цього файлу від кореневого або поточного каталогу. Всі елементи шляху відокремлюються один від одного слешами, і якщо перший символ рядка також слеш, то шлях бере початок в кореневому каталозі, в іншому випадку – в поточному. Шлях з єдиним ім'ям позначає файл в поточному каталозі. *Приклади:*

- *docs.ps* - файл з ім'ям *docs.ps* в поточному каталозі;
- */usr/doc/FAQ/README* – файл з ім'ям *README* в каталозі */Usr/doc/FAQ*;
- *work/thesis.tex* – файл *thesis.tex* в підкаталозі *work* поточного каталогу.

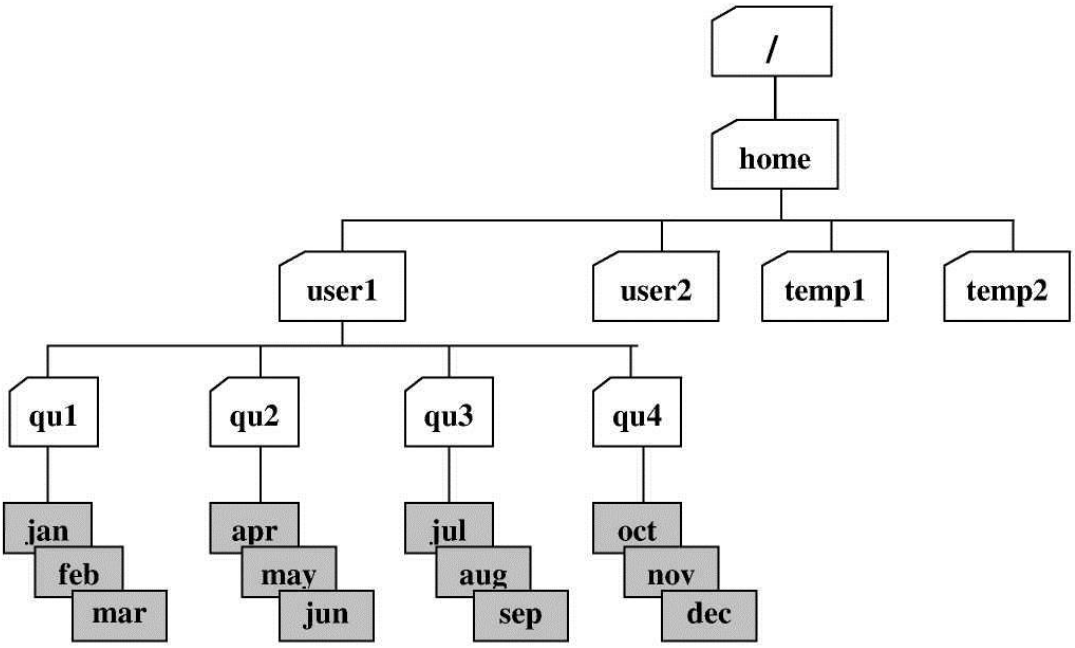


Рис. 16.2. Приклад ієрархії файлового простору Linux-системи

Для того щоб отримати детальну інформацію про окремий файл, необхідно ввести команду *ls -l*. В результаті, спершу йде вказівка на тип файла, а саме: d – directory (каталог); c – символьний пристрій (аналог COM-порта в Windows); b – блоковий пристрій (жорсткий диск 0 – перший жорсткий диск системи); s – сокет; p – іменований канал; l – символьне посилання; "-" – простий файл користувача; після чого вказуються права доступу (літери до числа, так звана тріади дозволів); потім кількість посилань на файл; ім'я власника файлу та ім'я групи, до якої він належить; розмір файлу в байтах, дата і час останньої зміни і, нарешті, повне ім'я файлу. Ім'я групи позначає групу, якій надається доступ за категорією «група». І для кращого розуміння нижче наведені *приклади:*

```
drwxr-xr-x 2 roman roman 4096 Jul 25 15:37 Desktop
drwxr-xr-x 2 roman roman 4096 Jul 25 15:37 Documents
drwxr-xr-x 2 roman roman 4096 Jul 25 15:37 Downloads
```

- rw- r-- r-- 1 roman roman 8980 Jul 25 15:37 gunz

Однак, якщо ввести команду *ls -i*, то отримаємо щось подібне наступному:

786723 Desktop 786725 Downloads
786769 Documents 786792 gunz

Відразу ж можна помітити, що зліва з'явилося число, яке вказує номер індексного дескриптора файла, в якому записано всю важливу інформацію про файл, в тому числі (в останніх версіях) підтримуються списки контролю доступу, чого раніше в Linux не було.

Списки контролю доступу розширюють можливість тріад доступу. Їх використовують, коли деяким користувачам необхідно надати доступ до файлу без зміни групових налаштувань.

Як можна спостерігати, у вище зазначеному приклады, після індексного дескриптора йде мітка звичайного файла, потім тріади дозволів: 1-а тріада – дозволи для власника файла; друга – для його групи; третя – для усіх інших (решта). Значення "r" – дозвіл на читання; "w" – на запис; "x" – на виконання; "-" – дозволу на цю операцію немає.

Однак дозволи для каталогів трактуються інакше, ніж для файлів: дозвіл на читання – дозволяється продивлятися вміст каталогу, тобто отримати список файлів, що містяться у цьому каталозі, однак самі файли можуть бути недоступними для читання; дозвіл на запис для каталогу означає, що туди можна записувати файли або створювати нові, однак зміна існуючих файлів може виявитися недоступною; наявність права на виконання дозволяє зайти в цей каталог за допомогою команди *cd*. Можна читати список файлів з каталогу або записувати туди нові файли, але зайти в нього без дозволу на виконання не можна.

Також, очевидно, що при створенні нових файлів і каталогів вони вже будуть володіти певним набором прав доступу. Ці права доступу, що встановлюються за замовчуванням, визначаються значенням маски прав доступу, яка встановлюється командою *umask*. При введенні команди *umask* без аргументів вона виведе поточне значення маски, при використанні восьмизначного числа в якості аргументу буде встановлено нове значення.

Маска прав доступу визначає, які права мають бути видалені з повного набору прав, тобто маска прав доступу є в деякому роді зворотним значенням прав доступу. Наприклад, маска 022 призведе до скидання бітів запису для групи власника та інших користувачів. Зауважимо, що для звичайних файлів (*НЕ каталогів*) всі біти виконання (x) в правах за замовчуванням будуть скинуті незалежно від поточної маски.

Приклад, що демонструє ефект команди *umask*:

$ umask 002
$ mkdir dir1
$ ls -l
drwxrwxr-x 2 user1 users 1024 Jul 25 16:19 dir1
$ umask 072
$ mkdir dir2
$ ls -l
drwxrwxr-x 2 user1users 1024 Jul 25 16:19 dir1
drwx --- r-x 2 user1users 1024 Jul 25 16:20 dir2

Порядок виконання лабораторної роботи №16:

1. Включити ПК.
2. Ознайомитися з короткими теоретичними відомостями.
3. Виконати наступні завдання:

1) При виконанні лабораторної роботи на комп'ютерах у навчальній лабораторії використовуйте раніше створену (на лабораторній роботі №6) віртуальну машину ***Test PC2 Lin*** або створіть та запустіть нову віртуальну машину. Увійдіть в систему під обліковим записом адміністратора. Всі дії в наступних підпунктах виконуйте в системі, що працює на віртуальній машині.

2) Створити обліковий запис нового користувача, наприклад, ***testUser*** за допомогою команди *useradd*. При створенні нового облікового запису заборонити користувачеві зміну пароля і змінити обмеження на термін дії його пароля. Створити нову групу, наприклад, ***«testGroup»*** і включити в неї нового користувача.

3) Ознайомитися з командами визначення прав доступу до файлів і їх зміни (команди: *id, groups, ls -l, stat, chmod, chown, chgrp, umask*).

4) Знайти запис у файлі ***/etc/passwd***, що відповідає вашому реєстраційному імені.

5) Визначити свій ***UID***, дізнатися, до яких груп належить ваше реєстраційне ім'я, пояснити вивід команд *id, groups*.

6) Визначити список груп, в які входить користувач ***root***.

7) Дізнатися, якими правами доступу володіють новостворювані файли і каталоги[15].

[15] Пояснення: тобто, вам спершу необхідно створити новий файл і новий каталог, і вже потім переглянути для них права доступу.

8) Визначити значення ***umask***, при якому новостворювані файли і каталог будуть недоступні для читання, запису і виконання, нікому, окрім власника.

9) Зробити свій домашній каталог відкритим (доступним для перегляду) для всіх користувачів групи ***users***.

10) Створити в домашньому каталозі підкаталог ***tmp***, файли в якому зможе створювати, видаляти і перейменовувати будь-хто, хто входить до групи ***users***, при цьому вміст цього підкаталогу не повинен бути доступним для перегляду всім іншим користувачам.

11) Після виконання всіх завдань, видаліть всі створені файли, каталоги, групу та користувача.

4. Оформити звіт згідно до вимог (додаток 1).
5. Відповісти на контрольні питання та підготуватися до письмового опитування.

Зміст звіту:

1. Титульний лист.
2. Постановка завдання.
3. Протокол виконання лабораторної роботи, що містить результати роботи всіх консольних команд або відповідні скріншоти з поясненням отриманих результатів.
4. Висновки та відповіді на контрольні питання.

Контрольні питання:

1. В чому полягають основні відмінності між ОС Windows та Linux?
2. Назвіть та поясніть основні особливості архітектури ОС Linux.
3. Опишіть підсистему захисту в ОС Linux.
4. Назвіть основні принципи організації доступу в ОС Linux?
5. Для яких цілей можуть використовуватися «тіньові» каталоги?
6. Опишіть структуру файлового простору ОС Linux.
7. Які права по відношенню до файлів і каталогів вам необхідно мати для копіювання файлу? Як змінюються при цьому атрибути копії?

Лабораторна робота №17
«Комп’ютерні віруси та інше шкідливе програмне забезпечення. Боротьба з malware»

Мета роботи:

1. Закріплення знань про існуючі «комп'ютерні віруси» та інше шкідливе програмне забезпечення.
2. Вивчення загальноприйнятої класифікації вірусів та деяких алгоритмів їх поведінки, способів поширення «комп'ютерних вірусів» і механізмів їх впровадження в систему.
3. Знайомство з деякими алгоритмами попередження і виявлення вірусних загроз, та розгляд основних функцій, достоїнств і недоліків сучасного антивірусного програмного забезпечення.

Стислі теоретичні відомості:

17.1. Умови існування шкідливих програм та загальні відомості про комп'ютерні віруси

На сьогоднішній день, комп'ютерні віруси, мережеві хробаки, троянські програми існують для десятків операційних систем і додатків. Однак, в той же час існує величезна кількість інших операційних систем і додатків, для яких шкідливих програми поки ще не виявлено.

Причиною появи шкідливих програм в конкретній операційній системі або додатку є одночасне виконання наступних умов:

- популярність, широке поширення даної системи;
- наявність різноманітної і достатньо повної документації по системі;
- незахищеність системи або існування відомих уразливостей в системі безпеки.

Кожна перерахована умова є необхідною, а виконання всіх трьох умов одночасно є достатнім для появи різноманітних шкідливих програм.

Умова популярності системи необхідна для того, щоб вона зацікавила комп'ютерних хуліганів або хакерів (крекєрів). Якщо виробник системи домігся її масового поширення, то очевидно, що рано чи пізно хакери і творці комп'ютерних вірусів спробують використати її у своїх інтересах. Звідси логічним висновком буде: чим популярніша операційна система або програма, тим частіше вона буде ставати жертвою вірусної атаки. І практика це підтверджує – розподіл кількості шкідливого програмного забезпечення для ОС Windows і Linux практично збігається з частками ринку, які займають ці операційні системи.

Наявність повної документації необхідна для існування вірусів з природної причини – створення програм (включаючи вірусні) неможливе без технічного опису використання сервісів операційної системи та правил написання додатків.

Під *захищеністю системи* розуміються архітектурні рішення, які не дозволяють новому (невідомому) додатку отримати повний або достатньо широкий доступ до файлів на диску (включаючи інші додатки) і потенційно

небезпечним сервісам системи. Подібне обмеження фактично блокує будь-яку вірусну активність, але при цьому, зазвичай, накладає істотні обмеження на можливості звичайних програм.

Офіційна поява першого комп'ютерного вірусу датується 1981 роком, задовго до виходу першої версії Microsoft Windows. Цей вірус, замаскований під комп'ютерну гру, атакував найбільш популярний комп'ютер того часу – Apple II, хоча поширювався він з черепашачою швидкістю (за допомогою дискет).

Згідно з підрахунками експертів, обсяг ***malware*** (загальноприйнята назва всіх видів шкідливих програм) зростає більш ніж на 15 % в рік. Згідно з даними компанії *Symantec*, розробника антивірусних програм, кожен день з'являється приблизно 30 нових вірусів, а перелік активних вірусів поповнюється 10 тис. нових найменувань на рік.

Історично перше визначення комп'ютерного вірусу було наведено ще в 1984 р. Фредом Коеном: «***Комп'ютерний вірус*** – це програма, яка може заражати інші програми, модифікуючи їх за допомогою включення в них своєї, можливо модифікованої копії, причому остання зберігає здатність до подальшого розмноження». Це означає, що програма, будучи запущеною, здатна створювати свої копії (можливо, модифіковані) і поширювати їх певним чином з комп'ютера на комп'ютер. При цьому, як правило, впровадження вірусу на комп'ютер і його запуск відбувається без відома (і всупереч бажанням) власника комп'ютера.

Структурно, можна уявити, що комп'ютерний вірус складається з двох частин: *голови* і *хвоста (тіла)*. *Головою* називається частина вірусу, яка отримує управління першою. *Хвіст вірусу* – це частина вірусу, розташована в тексті інфікованої програми окремо від голови. У найпростішому випадку вірус може складатися лише з однієї голови (переважно файлові віруси). Такі віруси ще називаються *несегментованими*. На відміну від них, *сегментовані* віруси мають і хвіст, і голову.

Також необхідно відзначити, що комп'ютерний вірус складається з *механізму розмноження* і «*начинки»*. Механізм розмноження визначає спосіб, яким копії вірусу створюються, розповсюджуються і запускаються. «Начинка», в свою чергу, містить в собі додаткові функції вірусу, які реалізуються на зараженому комп'ютері.

«Начинка» деяких вірусів є цілком нешкідливою (наприклад, виведення повідомлення на екран), а інших – достатньо небезпечною: знищення даних, викрадення інформації або використання комп'ютера в якості плацдарму для DOS-атаки. У будь-якому випадку вірус чинить негативний вплив, витрачаючи ресурси процесора, оперативну пам'ять та дисковий простір. Крім того, масштабна епідемія вірусу, що розмножується по мережі, коли виявляються

зараженими тисячі комп'ютерів, це може призвести до того, що мережа вийде з ладу через перевантаження. З цієї причини віруси називають шкідливими програмами.

Також необхідно відмітити, що окрім «начинки» і механізму розмноження інтерес становлять прийоми, за допомогою яких віруси приховують свою присутність в системі, з тим, щоб протриматися в ній як можна довше.

Стелс-вірус – вірус, повністю або частково приховує свою присутність шляхом перехоплення звернень до операційної системи, які здійснюють читання, запис, читання додаткової інформації про заражені об'єкти (завантажувальні сектори, елементи файлової системи або пам'яті і т. д.) Наприклад, файловий вірус може перехоплювати функції читання/запису в файл, читання каталогу і т. д., щоб приховати збільшення розміру заражених програм; перехоплює функції читання/запису файлу в пам'ять, щоб приховати факт зміни файлу.

Поліморфні віруси – віруси, які модифікують свій код в заражених програмах таким чином, що два екземпляри одного і того ж вірусу можуть не співпадати ні в одному біті. Це ускладнює аналіз і виявлення його антивірусом. Для модифікації коду використовується шифрування (рис. 17.1). Тобто вірус містить шифратор, причому при розмноженні кожна копія вірусу шифрується новим випадковим ключем, а розшифровує вірус сам себе вже під час виконання. Природно, дешифратор при цьому не шифрується, але поліморфні віруси зазвичай містять код генерації дешифратора, щоб, виконуючи одні і ті ж функції, ця частина в кожній копії вірусу мала різний вигляд.

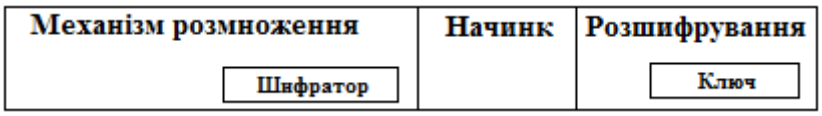


Рис. 17.1. Структура поліморфного вірусу

Таким чином, на сьогоднішній день, під *комп'ютерним вірусом* (або просто вірусом) розуміється автономно функціонуюча програма, що володіє здатністю до самостійного, скритного впровадження в тіла інших програм і подальшого самовідтворення та саморозповсюдження в інформаційно-обчислювальних мережах і окремих ЕОМ. Окрім цього, слід доповнити, що вірус може бути наділений деструктивними функціями.

Інше визначення ***комп'ютерного вірусу*** (яке, використовується в Україні, згадується в НД ТЗІ 1.1-003-99) – програма, що володіє здатністю до самовідтворення і, як правило, здатна здійснювати дії, які можуть порушити функціонування КС і/або зумовити порушення політики безпеки.

17.2. Класифікація шкідливого програмного забезпечення

До шкідливого ПЗ належать програми, які отримали такі назви, як: класичні комп'ютерні віруси, мережеві хробаки, троянські програми, утиліти хакерів та інші. Всі вони завдають або явну шкоду комп'ютеру, на якому запускаються на виконання, або завдають шкоди іншим комп'ютерам в мережі, чи виконують інші несанкціоновані дії. До дій, які не завдають прямої шкоди, можна віднести розсилку спаму, настирливу рекламу, передачу конфіденційної інформації користувача зловмисникові та інше. Далі розглянемо більш детально кожен з різновидів комп'ютерних вірусів.

17.2.1. Класичні комп'ютерні віруси.

До даної категорії відносяться програми, які дописують свій код в тіло якої-небудь відомої програми. Зазвичай це файли типу exe, com, bat. Отримавши управління, класичні віруси можуть не відразу наносити шкоду, а витримують деякий час, який називають ***періодом латентності.***

Наприклад, відомий вірус Win95.CIH (Чорнобиль), написаний тайванським студентом Чень Інхао в червні 1998 року, масове розповсюдження якого відбулося 1999 року, спрацьовував лише в річницю найбільшої аварії на Чорнобильській АЕС. При запуску перевіряв системну дату комп'ютера і лише 26 квітня активував механізм знищення даних на жорсткому диску. При цьому здійснював спроби записати «сміття» у FLASH BIOS комп'ютера. Деякі старі моделі це дозволяли, після чого відновити материнську плату можна було тільки за допомогою заміни мікросхеми. Інший вірус, Klez.E, викликав епідемію в 2002 році. Він спрацьовував на шостий день кожного непарного місяця і заповнював файли певних форматів (.doc, .txt та ін.) випадковим вмістом, після чого їх відновлення ставало неможливим. У першу чергу такі програми поширюють свої копії по ресурсам локального комп'ютера з метою:

- запуску свого коду при будь-яких діях користувача;
- подальшого впровадження в інші ресурси комп'ютера;
- нанесення шкоди після закінчення періоду латентності.

На відміну від хробаків, віруси не використовують мережевих сервісів для проникнення на інші комп'ютери. Копія вірусу потрапляє на віддалені комп'ютери тільки в тому випадку, якщо заражений об'єкт з яких-небудь не залежних від функціоналу вірусу причин виявляється активізованим на іншому комп'ютері, наприклад:

- при зараженні доступних дисків вірус проник у файли, які розташовані на мережевому ресурсі;
- вірус скопіював себе на зовнішній носій або заразив файли на ньому;

- користувач відіслав електронний лист із зараженим вкладенням.

Деякі віруси містять у собі властивості інших різновидів шкідливого програмного забезпечення, наприклад, бекдор-процедуру (скритне віддалене управління комп'ютером) або іншу троянську компоненту.

Класифікація класичних комп'ютерних вірусів

Типи комп'ютерних вірусів розрізняються між собою за такими основним ознаками:

1) середовище існування;
2) спосіб зараження.

Під «*середовищем існування*» розуміються системні області комп'ютера, операційні системи або програми, в компоненти (файли) яких впроваджується код вірусу. Під «*способом зараження*» розуміються різні методи проникнення вірусного коду в об'єкти з ціллю їхнього зараження.

Таким чином, за середовищем існування віруси можна розділити на:

- файлові;
- завантажувальні;
- макровіруси;
- скриптові.

Файлові віруси при своєму розмноженні тим або іншим способом використовують файлову систему якоїсь (або яких-небудь) ОС. Вони:

- різними способами проникають у виконувані файли на комп'ютері (найбільш поширений тип вірусів);
- створюють файли-двійники (компаньйон-віруси);
- створюють свої копії в різних каталогах;
- використовують особливості організації файлової системи (link-віруси).

Зазвичай, поширення таких вірусів відбувається через заражені файли. Досить принести один такий файл на незаражений комп'ютер і запустити його, щоб вірус почав діяти. Через короткий час всі виконувані файли на комп'ютері виявляються зараженими і при запуску будь-якої програми разом з нею спрацьовує і вірус.

За механізмами зараження файлові віруси можна поділити на:

- віруси, що перезаписуються (overwriting);
- паразитичні віруси (parasitic);
- віруси-компаньйони (companion);
- віруси-посилання (link);
- віруси, що заражають об'єктні модулі (OBJ);
- віруси, що заражають бібліотеки компіляторів (LIB);

- віруси, що заражають вихідні тексти програм.

Overwriting. Даний метод зараження є найпростішим: вірус записує свій код замість коду цільового файлу, знищуючи його вміст. Природно, що при цьому файл перестає працювати і не відновлюється. Такі віруси дуже швидко розкривають себе, тому що операційна система і додатки досить швидко перестають працювати.

Parasitic. До паразитичних відносяться всі файлові віруси, які при поширенні своїх копій обов'язково змінюють вміст файлів, залишаючи самі файли, при цьому повністю або частково працездатними.

Основними типами таких шкідливих програм є віруси, які записуються в початок файлів (prepending), у кінець файлів (appending) і в середину файлів (inserting). У свою чергу, впровадження вірусів в середину файлів відбувається різноманітними методами – шляхом переносу частини файлу в його кінець або копіювання свого коду в свідомо невикористовуванні дані файлу (cavity-віруси).

Впровадження вірусу в початок файлу. Відомі два способи впровадження паразитичного файлового вірусу в початок файлу. Перший спосіб полягає в тому, що вірус переписує початок цільового файлу в його кінець, а сам копіюється в звільнене місце. При зараженні файлу другим способом вірус дописує файл, який піддається зараженню, до свого тіла.

Таким чином, при запуску зараженого файлу першим управління отримує код вірусу. При цьому віруси, щоб зберегти працездатність програми, або лікують заражений файл, повторно запускають його, чекають закінчення його роботи і знову записуються в його початок (іноді для цього використовується тимчасовий файл, в який записується знешкоджений файл), або відновлюють код програми в пам'яті комп'ютера і налаштовують необхідні адреси в її тілі (тобто дублюють роботу ОС).

Впровадження вірусу в кінець файлу. Найбільш поширеним способом упровадження вірусу у файл є дописування вірусу в його кінець.

При цьому вірус змінює початок файлу таким чином, що першими командами програми, які виконуються є команди вірусу.

Для того щоб отримати управління при запуску файлу, вірус коригує стартову адресу програми (адресу точки входу). Для цього вірус виконує необхідні зміни в заголовку файлу.

Впровадження вірусу в середину файлу. Існує кілька методів впровадження вірусу в середину файлу. У найбільш простому з них вірус переносить частину файлу у його кінець або «розсовує» файл і записує свій код у звільнений простір. Цей спосіб багато в чому аналогічний методам, перерахованим вище. Деякі віруси при цьому спресовують блок файлу, який переносять, таким чином, щоб довжина файлу при зараженні не змінювалася.

Другим є метод «cavity», при якому вірус записується в області файлу, які фактично не використовуються. Вірус може бути скопійований в незадіяні області заголовку EXE-файлу, в «діри» між секціями EXE-файлів або текстових повідомлень популярних компіляторів. Існують віруси, що заражають тільки ті файли, які містять блоки, заповнені якимось постійним байтом, при цьому вірус записує свій код замість такого блоку.

Крім того, копіювання вірусу в середину файлу може статися в результаті помилки вірусу, в цьому випадку файл може бути безповоротно зіпсований.

Віруси без точки входу. Окремо слід відзначити досить незначну групу вірусів, що не мають «точки входу» (EPO-віруси – Entry Point Obscuring viruses). До них відносяться віруси, що не змінюють адресу точки старту в заголовку EXE-файлів. Такі віруси записують команду переходу на свій код в яке-небудь місце в середину файлу і отримують управління безпосередньо не при запуску зараженого файлу, а при виклику процедури, яка містить код для передачі управління на тіло вірусу. Причому ця процедура може виконуватися вкрай рідко (наприклад, при виведенні повідомлення про будь-яку специфічну помилку). В результаті вірус може довгі роки «спати» всередині файлу і реалізуватися тільки при деяких обмежених умовах.

Перед тим, як записати у середину файлу команду переходу на свій код, вірусу необхідно вибрати «правильний» адреса в файл – інакше заражений файл може бути зіпсований. Відомі кілька способів, за допомогою яких віруси визначають такі адреси всередині файлів, наприклад, пошук у файлі послідовності стандартного коду заголовків процедур мов програмування, дизасемблювання коду файлу або заміна адрес функцій, які імпортуються.

Companion. До категорії «companion» відносяться віруси, що не змінюють заражених файлів. Алгоритм роботи цих вірусів полягає в тому, що для цільового файлу створюється файл-двійник, причому при запуску зараженого файлу керування одержує саме цей двійник, тобто вірус.

До вірусів даного типу відносяться ті з них, які при зараженні перейменовують файл в яке-небудь інше ім’я, запам’ятовують його (для подальшого запуску файлу-господаря) і записують свій код на диск під ім’ям цільового файлу. Наприклад, файл NOTEPAD.EXE перейменовується в NOTEPAD.EXD, а вірус записується під ім’ям NOTEPAD.EXE. При запуску управління отримує код вірусу, який потім запускає оригінальний NOTEPAD.

Інші способи зараження. Існують віруси, які жодним чином не пов’язують свою присутність із яким-небудь виконуваним файлом. При розмноженні вони усього лише копіюють свій код у які-небудь каталоги дисків в надії, що ці нові копії будуть коли-небудь запущені користувачем. Іноді ці

віруси дають своїм копіям «спеціальні» імена, щоб підштовхнути користувача на запуск своєї копії – наприклад, INSTALL.EXE або WINSTART.BAT.

Деякі віруси записують свої копії в архіви (ARJ, ZIP, RAR). Інші записують команду запуску зараженого файлу в BAT-файли.

Link-віруси також не змінюють фізичного вмісту файлів, проте при запуску зараженого файлу «змушують» ОС виконати свій код. Цієї мети вони досягають за допомогою модифікації необхідних полів файлової системи.

Файлові віруси були достатньо поширені в 90-х роках, коли програми були невеликими і поширювалися «з рук в руки» на дискетах. В даний час ці віруси непопулярні, оскільки їх достатньо легко виявити: по-перше, збільшується розмір усіх виконуваних файлів, а по-друге, багато програм при запуску перевіряють свою цілісність (наприклад, за розміром або за допомогою контрольної суми) і сигналізують про її порушення. Тим не менш, небезпека завантажити з Інтернету заражений файл залишається.

Завантажувальні віруси прописують себе або в завантажувальний сектор диска (boot-сектор), або в сектор, що містить системний завантажувач вінчестера (Master Boot Record), або змінюють покажчик на активний boot-сектор. Принцип дії завантажувальних вірусів заснований на алгоритмах запуску операційної системи при включенні або перезавантаженні комп’ютера – після необхідних тестів встановленого обладнання (оперативної пам’яті, дисків і т. п.) програма системної загрузки зчитує перший фізичний сектор завантажувального диску та передає на нього управління.

Сама ця програма переміщується в інше місце, а при завантаженні з зараженого носія спочатку запускається вірус та закріплюється в оперативній пам’яті з ціллю отримання контролю над системою, після чого дозволяє завантажуватися стандартному завантажувачу. Даний тип вірусів був досить поширений у 1990-х рр., але практично зник з переходом на 32-бітні операційні системи і відмовою від використання дискет як основного способу обміну інформацією. Однак в останні роки з’явилася варіація вірусів (які також можна назвати завантажувальними), що поширюються через флеш-накопичувачі.

Такий вірус являє собою звичайний виконуваний файл з атрибутом «прихований», який записується в кореневий каталог флешки або в приховану папку, емулюючий кошик Windows або іншу системну папку. Крім цього в кореневому каталозі розміщується файл autorun.inf з посиланням на вірус. Вірус активується, якщо у флешки спрацьовує автозапуск, а це зазвичай відбувається автоматично, якщо відкривати флешку подвійним клацанням по її ярлику, за умови, що налаштування Windows встановлені за замовчуванням. Вірус залишає свої копії (разом з autorun.inf) на всіх розділах жорсткого диска і, таким чином, отримує управління під час кожного сеансу роботи користувача,

коли той випадково активує автозапуск на одному з цих розділів. Після чого вірус постійно знаходиться в оперативній пам'яті, виконує свій код («начинку»), а також відстежує підключення до комп'ютера нових переносних носіїв і заражає їх.

Для профілактики таких вірусів (крім антивірусного захисту) необхідно відкривати переносні пристрої таким чином, щоб не дозволити спрацювання автозапуску. Наприклад, відкривати їх через оболонку типу Total Commander, або через адресний рядок провідника Windows (але не подвійним клацанням по ярлику).

Макровіруси не відрізняються за механізмом розмноження від файлових вірусів; їх особливість в тому, що заражають вони не виконувані файли, а файли деяких популярних форматів документів (зокрема .doc і .xls). Макровіруси виявилися достатньо небезпечними, адже користувачі вже звикли до думки, що зараженою може бути тільки програма і не боялися отримати вірус разом з документом.

Макровіруси використовують можливості деяких програм (текстових, графічних, табличних редакторів, систем проектування, СУБД тощо) впроваджувати в документи, створювані цими програмами для автоматизації виконання повторюваних дій, так звані макроси – процедури, написані на вбудованій в них мові програмування і виконуються у відповідь на певні події (натискання користувачем кнопки або відкриття документа). Наприклад, Microsoft Office підтримує вбудовану мову програмування Visual Basic for Applications (VBA).

Таким чином, *макровірус* являє собою програму створену за допомогою мови макросів, впроваджену в документ відповідного формату, яка зазвичай автоматично запускається при відкритті документа. Після запуску вірус шукає інші доступні документи цього формату і впроваджується в них, а також реалізує свій код, тобто виконує свою «начинку» (можливостей сучасних макромов цілком вистачає, щоб ця «начинка» могла містити серйозні деструктивні функції).

В даний час макровіруси також непопулярні, оскільки сучасні версії програм, що підтримують макромови, попереджають користувача про макроси в документі. Більше того, щоб дозволити макросу запуститися, від імені користувача нерідко потрібно змінити налаштування програми.

Слід зазначити також існування ***скрипт-вірусів***, які є підгрупою файлових вірусів. Дані віруси, написані на різних скрипт-мовах (VBS, JS, PHP, PHP тощо). Вони заражають інші скрипт-програми (командні та службові файли MS Windows або Linux), які є частинами багатокомпонентних вірусів. Також, дані віруси можуть заражати файли інших форматів (наприклад, HTML), якщо в них можливе виконання скриптів.

17.2.2. Мережеві хробаки

Сучасні віруси не зацікавлені в тому, щоб заразити якомога більше файлів на комп'ютері (і тим самим підвищити вірогідність свого запуску і розмноження). З повсюдним проникненням Інтернету, найбільш привабливa мета для вірусів є проникнення на якомога більше число комп'ютерів в локальних і/або глобальних мережах з метою:

- проникнення на віддалені комп'ютери;
- запуск своєї копії на віддаленому комп'ютері;
- подальшого поширення на інші комп'ютери в мережі.

При цьому достатньо, щоб на кожному комп'ютері містився лише один екземпляр вірусу, але з обов'язковим дотриманням двох наступних умов:

1) вірус повинен автоматично запускатися (бажано одночасно із запуском операційної системи);

2) файл, який містить вірус повинен бути надійно прихований від користувача.

Віруси, які автоматично запускаються в момент старту операційної системи і, таким чином, постійно функціонують в оперативній пам'яті, називають ***резидентними***. Віруси, які розповсюджують свої копії по локальній мережі або через Інтернет, називаються ***мережними хробаками***. Більшість мережевих хробаків є резидентними.

Для свого поширення мережеві хробаки використовують різноманітні комп'ютерні і мобільні мережі: електронну пошту, системи обміну миттєвими повідомленнями, файлообмінні (P2P) і IRC-мережі (груповий чат), LAN (локальні мережі), мережі обміну даними між мобільними пристроями (смартфонами, кишеньковими комп'ютерами) і т. д.

Більшість відомих хробаків розповсюджуються за допомогою *соціального інжинірингу* у вигляді прикріпленого до електронного листа файлового вкладення, посилання на заражений файл на якому-небудь веб- або FTP-ресурсі в ICQ і IRC-повідомленнях, яке довірливі й халатні користувачі, що мають низьку культуру в області інформаційної безпеки, з цікавості запускають, віддаючи тим самим свій комп'ютер під контроль вірусу.

Цьому сприяє той факт, що лист з вірусним вкладенням може прийти зі знайомої поштової адреси. Дійсно, заразивши комп'ютер, поштовий вірус, як правило, обробляє файл, в якому міститься адресна книга поштової програми, і витягує з неї адреси постійних кореспондентів користувача, після чого їм надсилаються автоматично згенеровані листи з копією вірусу.

Один з найгучніших мережевих хробаків – вірус «*I love you*», епідемія якого почалася 4 травня 2000 року. Після відкриття файлу, прикладеного до

електронного листа, вірус знищував або змінював деякі файли на зараженій машині, а крім того відразу ж, у момент запуску, розсилав себе за всіма адресами адресної книги користувача. За оцінками різних компаній, ураження зазнало величезна кількість комп'ютерних мереж (в окремих країнах – від 30 до 80 відсотків). Кількість одержувачів «любовних листів» оцінюється в 45 мільйонів чоловік, загальні збитки – до 10 мільярдів доларів США. Адресат отримував листа такого змісту:

Тема: «ILOVEYOU»

Повідомлення: «kindly check the attached LOVELETTER coming from me.»

Приєднаний файл: «LOVE LETTER-FOR-YOU.TXT.vbs»

Незважаючи на те, що механізм проникнення вірусів через поштові вкладення має досить поважний вік і широко відомий, користувачі все ще заражаються поштовими вірусами, необережно запускаючи вкладення.

Деякі хробаки (так звані «безфайлові» або «пакетні» хробаки) поширюються у вигляді мережевих пакетів, проникають безпосередньо в пам'ять комп'ютера і активізують свій код.

Інший механізм зараження – *недоліки в конфігурації мережі* (наприклад, копіювання на диск, відкритий на повний доступ), помилки в мережевих програмах, помилки в налаштуваннях безпеки операційних систем і додатків, що дозволяють шкідливій програмі проникати на комп'ютер користувача і отримувати на ньому управління без будь-яких дій з боку самого користувача. Такі віруси з'являються значно рідше (оскільки виявлення подібних помилок та написання програми, яка буде використовувати їх, достатньо складна задача). Проте, з'явившись, такі програми викликають серйозну вірусну епідемію (як вірус *MsBlast* у 2003 році), яка припиняється лише тоді, коли випускається патч (програма, яка виправляє вразливість) і його встановлюють більшість користувачів.

Єдиний спосіб хоч якось протистояти подібним вірусам – своєчасна установка оновлень.

Розглянемо тепер резидентні віруси. Їх характерною особливістю є автоматичний запуск після завантаження операційної системи. Більшість резидентних вірусів під Windows забезпечує виконання цієї умови, прописуючи себе в розділи автозавантаження в реєстрі:

HKEY_LOCAL_MACINE\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

При цьому багато вірусів, резидентно знаходячись в пам'яті, стежать за реєстром і якщо користувач видаляє відповідний запис (ключ), відновлюють його. Тому щоб видалити вірус вручну, необхідно провести завантаження ОС в безпечному режимі.

Маскуються мережеві хробаки в більшості випадків в системних папках Windows (наприклад, System32) серед сотень файлів, призначення яких користувачеві невідомо.

До того ж необхідно відмітити, що деякі хробаки володіють також властивостями інших різновидів шкідливого програмного забезпечення. Наприклад, деякі хробаки містять троянські функції або здатні заражати виконувані файли на локальному диску, тобто мають властивість троянської програми та/або комп'ютерного вірусу.

17.2.3. Троянські програми

У цю категорію входять програми, що здійснюють різні несанкціоновані користувачем дії: збір інформації і передача її зловмисникові, її руйнування або зловмисну модифікацію, порушення працездатності комп'ютера, використання ресурсів комп'ютера, впровадження іншого шкідливого ПЗ та інше. Вони, як правило, не містять механізму саморозповсюдження, натомість вони маскуються під програми, що виконують корисні функції. Таким чином, поширення троянських коней часто відбувається за допомогою самих користувачів, які скачують з Інтернету або один у одного, не здогадуючись про наслідки.

Особлива небезпека в тому, що користувачі приймають їх за легальні програми, оскільки, часто троянські програми не порушують працездатність зараженого комп'ютера, а використовують його ресурси в інших злочинних цілях (наприклад, троянські програми, розроблені для масованих DOS-атак на віддалені ресурси мережі). *Троян* – це не вірус в його класичному розумінні, а невеличка програмка, яку ще називають «Утилітою віддаленого адміністрування комп'ютером». Трояни розрізняються між собою за тими діями, які вони виконують на зараженому комп'ютері.

Backdoor – троянські утиліти віддаленого адміністрування комп'ютерів в мережі. По своїй функціональності вони багато в чому нагадують різні системи адміністрування, які розробляються та розповсюджуються фірмами-виробниками програмних продуктів.

Єдина особливість цих програм, яка змушує класифікувати їх як шкідливі троянські програми: відсутність попередження про інсталяції і запуску. При запуску троянська програма встановлює себе в систему і потім стежить за нею, при цьому користувачеві не видається ніяких повідомлень про її дії в системі. Більше того, посилання на троянську програму може бути відсутнім в списку активних додатків. В результаті користувач може не знати про її присутність в системі, в той час як його комп'ютер відкритий для віддаленого управління.

Утиліти прихованого управління дозволяють робити з комп'ютером все, що в них заклав автор: приймати або відсилати файли, запускати і знищувати їх, виводити повідомлення, видаляти інформацію, перезавантажувати комп'ютер і т. д. В результаті ці троянці можуть бути використані для виявлення і передачі конфіденційної інформації, для запуску вірусів, знищення даних і т. п. – уражені комп'ютери виявляються відкритими для зловмисних дій хакерів.

Таким чином, троянські програми даного типу є одним з найбільш небезпечних видів шкідливих програм, оскільки в них закладена можливість найрізноманітніших злочинних дій, властивих іншим видам троянських програм.

Окремо слід відзначити групу бекдорів, здатних поширюватися по мережі і впроваджуватися в інші комп'ютери, як це роблять комп'ютерні хробаки. Відрізняє такі троянські програми від хробаків той факт, що вони поширюються по мережі не мимовільно (як хробаки), а тільки за спеціальною командою.

Trojan-PSW. Дане сімейство об'єднує троянські програми, які крадуть різну інформацію з зараженого комп'ютера, зазвичай – системні паролі (PSW – Password-Stealing-Ware). При запуску PSW-троянці шукають системні файли, що зберігають різну конфіденційну інформацію (зазвичай номери телефонів і паролі доступу до Інтернету) і відсилають її за вказаною в коді троянської програми електронною адресою або адресами.

Існують PSW-троянці, які повідомляють і іншу інформацію про заражений комп'ютер, наприклад, інформацію про систему (наприклад, розмір пам'яті і дискового простору, версію операційної системи, тип використовуваного поштового клієнта, IP-адресу тощо). Деякі троянські програми даного типу крадуть реєстраційну інформацію до різного програмного забезпечення, коди доступу до мережевих ігор та інше.

Trojan-Clicker – Інтернет-клікери. Сімейство троянських програм, основна функція яких – організація несанкціонованих звернень до Інтернет-ресурсів (зазвичай до веб-сторінок). Досягається це або посиланням відповідних команд браузеру, або заміною системних файлів, в яких вказані стандартні адреси Інтернет-ресурсів (наприклад, файл hosts в MS Windows).

У зловмисника можуть бути наступні цілі для подібних дій:

- збільшення відвідуваності будь-яких сайтів з метою збільшення переглядів реклами;
- організація DoS-атаки (Denial of Service) на який-небудь сервер;
- залучення потенційних жертв для зараження вірусами або троянськими програмами.

Trojan-Downloader – доставка шкідливих програм. Троянські програми цього класу призначені для завантаження та встановлення на комп'ютер-жертву нових версій зловмисних програм, встановлення троянських програм або

рекламних систем. Завантажені з Інтернету програми потім запускаються на виконання, або реєструються троянською програмою на автозавантаження відповідно з можливостями операційної системи. Дані дії при цьому відбуваються без відома користувача.

Інформація про імена і місця розташування завантажуваних програм міститься в коді та даних троянської програми або завантажується їй з керуючого Інтернет-ресурсу (зазвичай з веб-сторінки).

Trojan-Dropper – інсталятори шкідливих програм. Троянські програми цього класу написані у цілях прихованої інсталяції програм і практично завжди використовуються для впровадження на комп'ютер-жертву вірусів або інших троянських програм.

Дані троянці зазвичай без будь-яких повідомлень (або з фальшивими повідомленнями про помилку в архіві або невірної версії операційної системи) скидають на диск в який-небудь каталог (корінь диска C:, в тимчасовий каталог, каталоги Windows) інші файли і запускають їх на виконання.

Trojan-Proxy – троянські проксі-сервера. Сімейство троянських програм, що таємно здійснюють анонімний доступ до різних Інтернет-ресурсів. Зазвичай використовуються для розсилки спаму.

Trojan-Spy – шпигунські програми (відомі також під назвою *Key Logger*). Дані троянці здійснюють електронне шпигунство за користувачем зараженого комп'ютера: вся інформація, яка вводиться з клавіатури, знімки екрану, список активних додатків і дії користувача з ними зберігаються в якомусь файлі на диску і періодично відправляються зловмисникові.

Троянські програми цього типу часто використовуються для крадіжки інформації користувачів різних систем онлайнових платежів та банківських систем.

Rootkit – приховування присутності в операційній системі. Поняття *rootkit* походить з UNIX систем. Спочатку це поняття використовувалося для позначення набору інструментів, що застосовуються для отримання прав root.

Так як інструменти типу rootkit на сьогоднішній день є і на інших ОС (у тому числі, на Windows), то слід визнати подібне визначення rootkit морально застарілим.

Таким чином, ***rootkit*** – програмний код або техніка, спрямована на приховування присутності в системі заданих об'єктів (процесів, файлів, ключів реєстру тощо).

Trojan-Notifier – оповіщення про успішну атаку. Троянці даного типу призначені для повідомлення про заражений комп'ютер. При цьому на адресу власника троянця («господаря») відправляється інформація про комп'ютер, наприклад, IP-адреса комп'ютера, номер відкритого порту, адресу електронної пошти і т. п. Відсилання здійснюється різними способами: електронним

листом, спеціально оформленим зверненням до веб-сторінки «господаря», ICQ-повідомленням та інше.

Дані троянські програми використовуються в багатокомпонентних троянських наборах для сповіщення свого «господаря» про успішну інсталяцію троянських компонент в цільову систему (на яку проводилася атака).

17.2.4. Хакерські утиліти та інші шкідливі програми

До даної категорії відносяться:

- утиліти автоматизації створення вірусів, хробаків і троянських програм (конструктори);
- програмні бібліотеки, розроблені для створення шкідливих програм;
- хакерські утиліти приховування коду заражених файлів від антивірусної перевірки (шифрувальники файлів);
- «злі жарти», що ускладнюють роботу з комп'ютером;
- програми, які повідомляють користувачеві завідомо невірну інформацію про свої дії в системі;
- інші програми, які тим або іншим способом навмисно завдають прямий або опосередкований збиток цьому або віддаленому комп'ютеру.

Exploit, Worm – зломщики віддалених комп'ютерів. Хакерські утиліти цього класу призначені для проникнення на віддалені комп'ютери з метою подальшого управління ними (використовуючи методи троянських програм типу «backdoor») або для впровадження в зламану систему інших шкідливих програм.

Хакерські утиліти типу «backdoor» при цьому використовують уразливості в операційних системах або додатках, встановлених на комп'ютері, на який здійснюється атака.

Constructor. Конструктори вірусів і троянських програм – це утиліти, призначені для створення нових комп'ютерних вірусів та троянських програм. Вони дозволяють генерувати вихідні тексти вірусів (ASM-файли), об'єктні модулі і/або безпосередньо заражені файли.

Деякі конструктори забезпечені стандартним віконним інтерфейсом, де за допомогою системи меню можна вибрати тип вірусу, цільові об'єкти (які будуть піддаватися атакам), наявність або відсутність самошифровки, протидія відладчику, внутрішні текстові рядки, також можна вибрати ефекти, що супроводжують роботу вірусу і т. п. Інші конструктори не мають інтерфейсу і зчитують інформацію про тип вірусу з конфігураційного файлу.

17.3. Тенденції сучасних комп'ютерних вірусів і боротьба з ними

Розглянемо характерні риси, які за останні роки найбільш чітко проявилися в сучасних вірусах:

- найбільше поширення отримали мережеві хробаки;
- віруси активно використовують уразливості в різних операційних системах і програмному забезпеченні;
- для швидкого поширення вірусів використовуються спам-технології;
- один вірус поєднує в собі безліч технологій: поліморфних, стелс, бекдор;
- замість пересилання свого тіла по електронній пошті часто відправляється посилання на веб-сайт або на заражений раніше комп'ютер;
- збільшується кількість вірусів для нових платформ: стільникових телефонів, смартфонів і комунікаторів, при цьому активно використовуються бездротові середовища передачі даних (Bluetooth, Wi-Fi).

Непрофесіоналові важко виявити присутність вірусів на комп'ютері, оскільки вони вміло маскуються серед звичайних файлів. Саме тому далі розглянемо ознаки зараження комп'ютера, а також способи відновлення даних після вірусної атаки і заходи щодо запобігання їх ураження шкідливими програмами.

Можна відзначити ряд ознак, що свідчать про зараження комп'ютера шкідливими програмами:

- виведення на екран непередбачених повідомлень або зображень;
- подача непередбачених звукових сигналів;
- зміна дати і часу модифікації файлів
- несподіване відкриття і закриття лотка DVD-ROM-пристрою;
- довільний, без вашої участі, запуск на комп'ютері будь-яких програм;
- зникнення файлів і каталогів або перекручування їхнього вмісту;
- часті зависання і збої у роботі комп'ютера;
- повільна робота комп'ютера;
- неможливість завантаження ОС;
- істотне зменшення розміру вільної оперативної пам'яті;
- припинення роботи або неправильна робота програм, які раніше функціонували нормально;
- зміна розмірів файлів;
- несподіване значне збільшення кількості файлів на диску;
- часте звертання до жорсткого диска (часто блимає лампочка на системному блоці);
- Інтернет-браузер «зависає» або веде себе несподіваним чином (наприклад, вікно програми неможливо закрити);

- при наявності на вашому комп'ютері міжмережевого екрану, поява попереджень про спробу будь-якої з програм вашого комп'ютера вийти в Інтернет, хоча ви це не ініціювали та інше.

Але мало виявити той факт, що комп'ютерна система піддалася впливу шкідливого ПЗ, необхідно виявити та нейтралізувати джерело загрози. Для боротьби з вірусами використовується спеціальне програмне забезпечення – ***антивіруси***. Для кращого розуміння, що таке антивірусне програмне забезпечення, далі розглянемо основні методи виявлення антивірусом своїх жертв.

Метод виявлення, заснований на сигнатурах – метод роботи антивірусів і систем виявлення вторгнень, при якому антивірус, переглядаючи файл (або пакет, який передається по мережі), звертається до словника, в якому містяться сигнатури відомих атак або вірусів. Під *сигнатурою* розуміється фрагмент коду, який однозначно ідентифікує вірус. Наприклад, вірус Email-Worm.Win32.Happy містить рядок «Happy New Year 1999!!», який лише з досить низькою ймовірністю може зустрітися в іншій програмі.

Основний принцип, за яким виділяється сигнатура – вона повинна містити унікальні рядки з цього файлу, настільки характерні, щоб гарантувати мінімальну можливість помилкового спрацьовування. Розробка сигнатур здійснюється вручну шляхом ретельного дослідження декількох файлів, заражених одним вірусом. Автоматична генерація сигнатур (особливо в умовах поліморфних вірусів) поки не дає задовільних результатів.

Кожен сучасний антивірус має велику (кількасот тисяч) базу сигнатур, яка регулярно оновлюється. Проблема виявлення заснована на сигнатурах полягає в тому, що новий вірус (сигнатури якого ще немає в базі) може безперешкодно обійти антивірусний захист. При цьому створення та доставка сигнатури користувачам займає від 11 до 97 годин в залежності від виробника у той час як, теоретично, вірус може захопити весь інтернет менше, ніж за 30 секунд.

Метод виявлення підозрілої поведінки програми. Антивірус простежує поведінку всіх працюючих програм і намагається виявити дії, характерні для вірусу (наприклад, запис даних в exe-файл). Однак цей метод часто викликає помилкові спрацьовування (в результаті користувачі перестають звертати увагу на попередження). Різновид цього методу – *емуляція програми*: перед запуском програми антивірус намагається імітувати його поведінку з метою відстеження підозрілих дій. Даний метод найбільш вимогливий до ресурсів.

Метод «білого списку». Запобігання виконанню всіх комп'ютерних кодів крім тих, які були раніше позначені системним адміністратором як безпечні.

Евристичне сканування – метод, заснований на сигнатурах і евристиці, покликаний поліпшити здатність сканерів застосовувати сигнатури і розпізнавати модифіковані версії вірусів в тих випадках, коли сигнатура

збігається з тілом невідомої програми не на 100 %, але в підозрілій програмі присутня більшість загальних ознак вірусу. Однак, дана технологія, застосовується в сучасних програмах дуже обережно, так як може підвищити кількість помилкових спрацювань.

Фахівці антивірусних технологій виділяють п’ять типів антивірусного ПЗ за функціями, які вони виконують: сканери, монітори, ревізори змін, імунізатори і поведінкові блокатори.

Сканер. Принцип роботи антивірусного сканера полягає в тому, що він переглядає файли, оперативну пам’ять і завантажувальні сектори дисків на предмет наявності вірусних масок, тобто унікального програмного коду вірусу. Вірусні маски (опис) відомих вірусів містяться в антивірусній базі даних сканера, і якщо він зустрічає програмний код, який збігається з одним з цих описів, то він видає повідомлення про виявлення відповідного вірусу.

Програми-детектори забезпечують пошук і виявлення віруси в оперативній пам’яті, на зовнішніх носіях, і при виявленні видають відповідне повідомлення. Розрізняють детектори універсальні і спеціалізовані. *Універсальні* детектори в своїй роботі використовують перевірку незмінності файлів шляхом підрахунку і порівняння з еталоном контрольної суми. Недолік універсальних детекторів пов’язаний з неможливістю визначення причин викривлення файлів. *Спеціалізовані* детектори здійснюють пошук відомих вірусів за їх *сигнатурою* (повторюваної ділянки коду). Недолік таких детекторів полягає в тому, що вони нездатні виявляти всі відомі віруси.

Програми-доктори (фаги) не тільки знаходять заражені вірусами файли, але і «лікують» їх, тобто видаляють з файлу тіло програми-вірусу, повертаючи файли в початковий стан. На початку своєї роботи фаги шукають віруси в оперативній пам’яті, знищуючи їх, і тільки потім переходять до «лікування» файлів. Серед фагів також можна виділяють полі-фаги, тобто програми-доктори, призначені для пошуку і знищення великої кількості вірусів.

Ревізори (CRC-сканери) відносяться до найнадійніших засобів захисту від вірусів. Ревізори запам’ятовують початковий стан об’єктів (програм, каталогів і системних областей диска) незараженої системи і періодично або за бажанням користувача порівнюють поточний стан з вихідним. Виявлені зміни виводяться на екран відео-монітора. Як правило, порівняння станів проводиться відразу після завантаження операційної системи. При порівнянні перевіряються довжина файлу, код циклічного контролю (контрольна сума файлу), дата і час модифікації та інші параметри.

Програми-ревізори мають досить розвинуті алгоритми, виявляють стелс-вірусів і можуть навіть відрізнити зміни версії програми, що перевіряється, від змін, внесених вірусом.

Програми-фільтри *(сторожа)* являють собою невеликі резидентні програми, призначені для виявлення підозрілих дій при роботі комп'ютера, характерних для вірусів. Такими діями можуть бути:

- спроби корекції файлів з розширеннями COM і EXE;
- зміна атрибутів файлів;
- прямий запис на диск за абсолютною адресою;
- запис в завантажувальні сектори диска;
- завантаження резидентної програми.

При спробі якої-небудь програми зробити зазначені дії «сторож» посилає користувачеві повідомлення і пропонує заборонити або дозволити відповідну дію. Програми-фільтри досить корисні, оскільки здатні виявити вірус на самій ранній стадії його існування до початку розмноження. Однак вони не «лікують» файли і диски. Для знищення вірусів потрібно застосувати інші програми, наприклад фаги. До недоліків програм-сторожів можна віднести їх «настирливість» (наприклад, вони постійно видають попередження про будь-яку спробу копіювання виконуваного файлу), а також можливі конфлікти з іншим програмним забезпеченням.

Імунізатори (вакцини) – резидентні програми, що запобігають зараженню файлів. Імунізатори застосовують, якщо відсутні програми-доктори, які «лікують» цей вірус. Вакцинація можлива тільки від відомих вірусів. Вакцина модифікує програму або диск таким чином, щоб це не відображалось на їх роботі, а вірус буде сприймати їх вже зараженими і тому не буде намагатися проникнути. В даний час програми-вакцини мають обмежене застосування.

Істотним недоліком таких програм є їх обмежені можливості щодо запобігання зараження від великої кількості різноманітних вірусів.

Таким чином, на сьогоднішній день перелік доступних антивірусних програм досить широкий. Вони розрізняються як за ціною (від достатньо дорогих – комерційних до абсолютно безкоштовних), так і по своїм функціональним можливостям. Найбільш потужні (і, як правило, найбільш дорогі) антивірусні програми являють собою насправді пакети спеціалізованих утиліт (багатофункціональні програмні комплекси), здатних при спільному їх використанні виявляти, лікувати (видаляти) віруси, а також перешкоджати їх проникненню на комп'ютер.

Сучасні антивіруси можуть працювати в двох режимах. В режимі *монітора* антивірус постійно працює, відстежуючи всі звернення до файлів, вклинюючись в цей процес і перевіряючи ці файли на предмет зараження. Таким чином, при першій спробі вірусу активувати антивірус блокує цю спробу і видає попередження. При використанні режиму монітора робота комп'ютера

сповільнюється (так як частина обчислювальних ресурсів витрачається на роботу антивірусу, а будь-яке звернення до файлів і деяким іншим об'єктам супроводжується процедурою сканування). Крім того, якщо на комп'ютері присутні заражені файли, які не проявляють активності і звернення до них не відбувається, вони залишаться непоміченими.

В режимі *сканера* антивірус перевіряє всі файли в заданій області (певний каталог, розділ жорсткого диска або всі пристрої зберігання інформації) і видаляє/лікує заражені (або просто сповіщає про них – в залежності від налаштувань сканера). Перевірка всіх даних на комп'ютері може зайняти значний час (кілька годин). Крім того, вірус може потрапити в систему відразу після сканування.

Для надійного захисту рекомендується застосування обох режимів: постійна робота антивірусу в режимі монітора і регулярна (наприклад, раз в тиждень) перевірка всіх даних за допомогою сканера (зазвичай сканування запускається на ніч).

Однак необхідно відзначити, що 100 % захисту жодне антивірусне ПЗ не забезпечує. Це пов'язано з тим, що будь-який розробник антивірусного ПЗ може оновити свою вірусну базу лише після того, як хтось з постраждалих надішле файл заражений раніше невідомим вірусом. Після цього потрібно ще деякий час для аналізу та створення сигнатури, за допомогою якої можливе знешкодження нового вірусу і час на оновлення антивірусних баз користувачів. У кращому випадку це приблизно 12 годин, за які новий вірус може встигнути поширитися по мережі Інтернет. Але, тим не менш, застосовувати антивірусне ПЗ необхідно, тому що крім нових вірусів система Інтернет наповнена великою кількістю старих вірусів, від яких вже захист є гарантованим.

До найбільш потужних і популярних антивірусних пакетів сьогодення відносяться: антивірус Касперського (AVP), Doctor WEB, NOD32, Norton Antivirus корпорації Symantec, McAfee VirusScan від компанії Network Associates, Panda Antivirus, Avast! Antivirus (останній є безкоштовним для домашнього використання).

Останнім часом також з'явився новий вид антивірусних послуг: онлайн перевірка документів або підозрілих файлів на віруси через Інтернет за допомогою спеціальних сервісів. Це, наприклад, Kaspersky VirusDesk від лабораторії Касперського (рис. 17.2) або сервіс від VirusTotal (рис. 17.3)

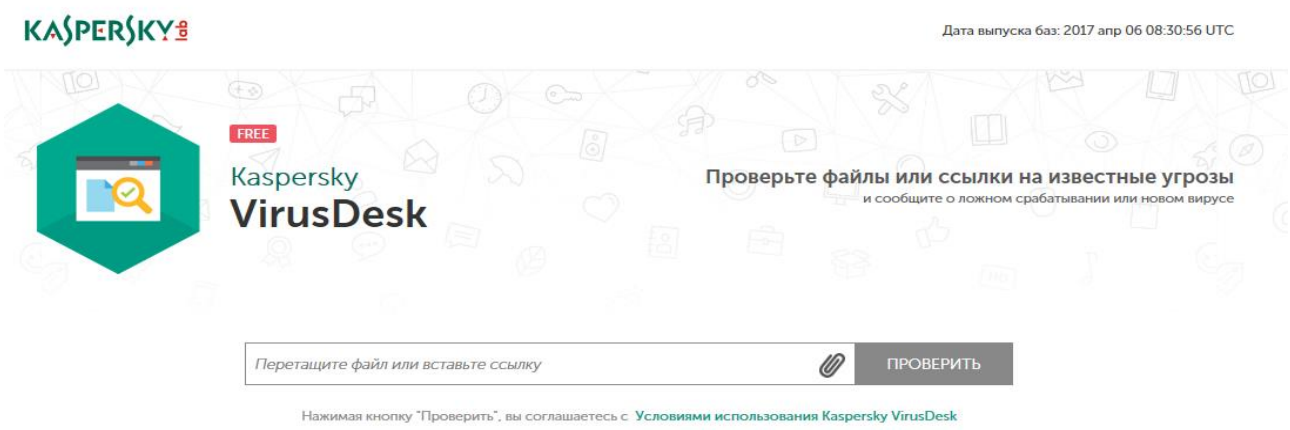


Рис. 17.2.Онлайн перевірка на віруси лабораторії Касперського

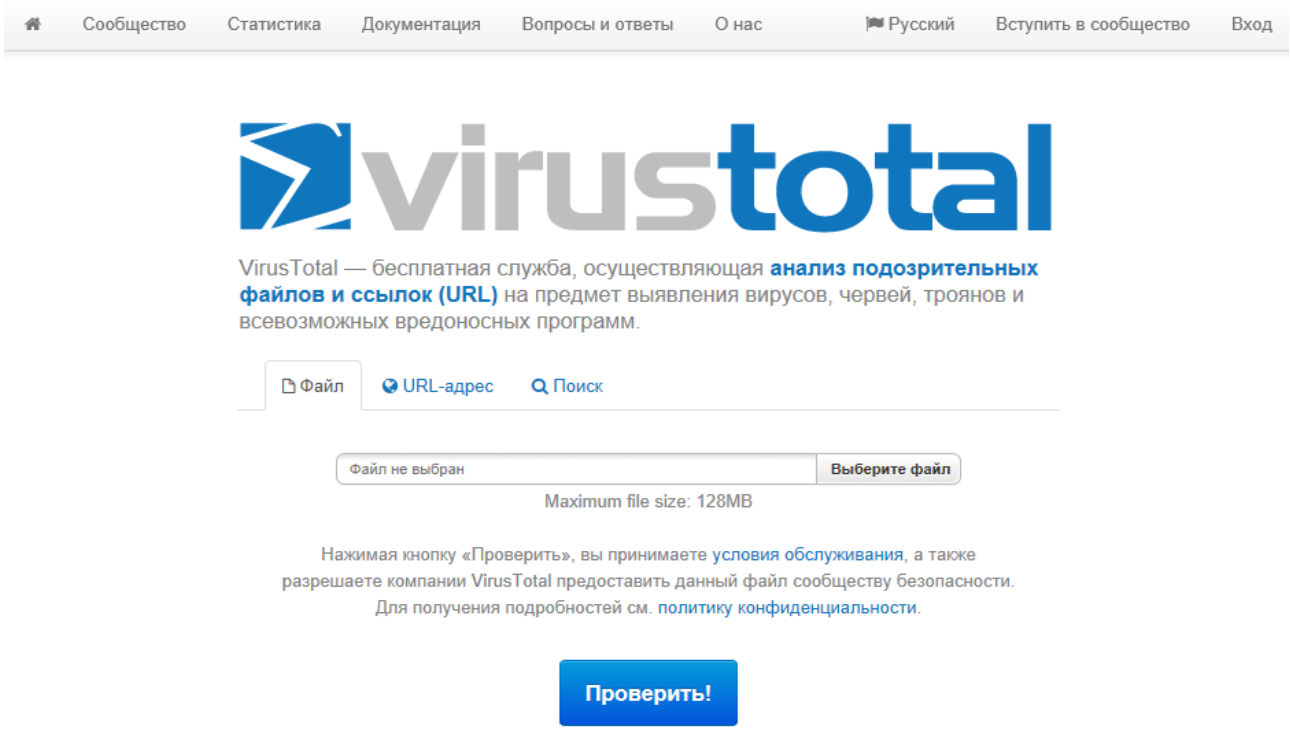


Рис. 17.3. Онлайн перевірка на віруси сервісом VirusTotal

Порядок виконання лабораторної роботи №17:

1. Включити ПК.
2. Ознайомитися з короткими теоретичними відомостями.
3. Підготувати коротку письмову доповідь по заданому пакету антивірусного програмного забезпечення (згідно варіанту в табл. 17.1), використовуючи будь-які доступні джерела інформації, описати основні функції, переваги та недоліки;
4. Виконайте наступні завдання:

1) При виконанні лабораторної роботи на комп'ютерах у навчальній лабораторії використовуйте раніше створену (на лабораторній роботі №6) віртуальну машину *Test PC1 Win* або створіть та запустіть нову віртуальну машину. Увійдіть в систему під обліковим записом

адміністратора. Всі дії в наступних підпунктах виконуйте в системі, що працює на віртуальній машині.

2) Інсталювати та ознайомитися з усіма функціями і можливостями антивірусного ПЗ згідно свого варіанту;

3) Навчитися грамотної експлуатації встановленої версії антивірусного ПЗ та провести його тестування (випробування)[16];

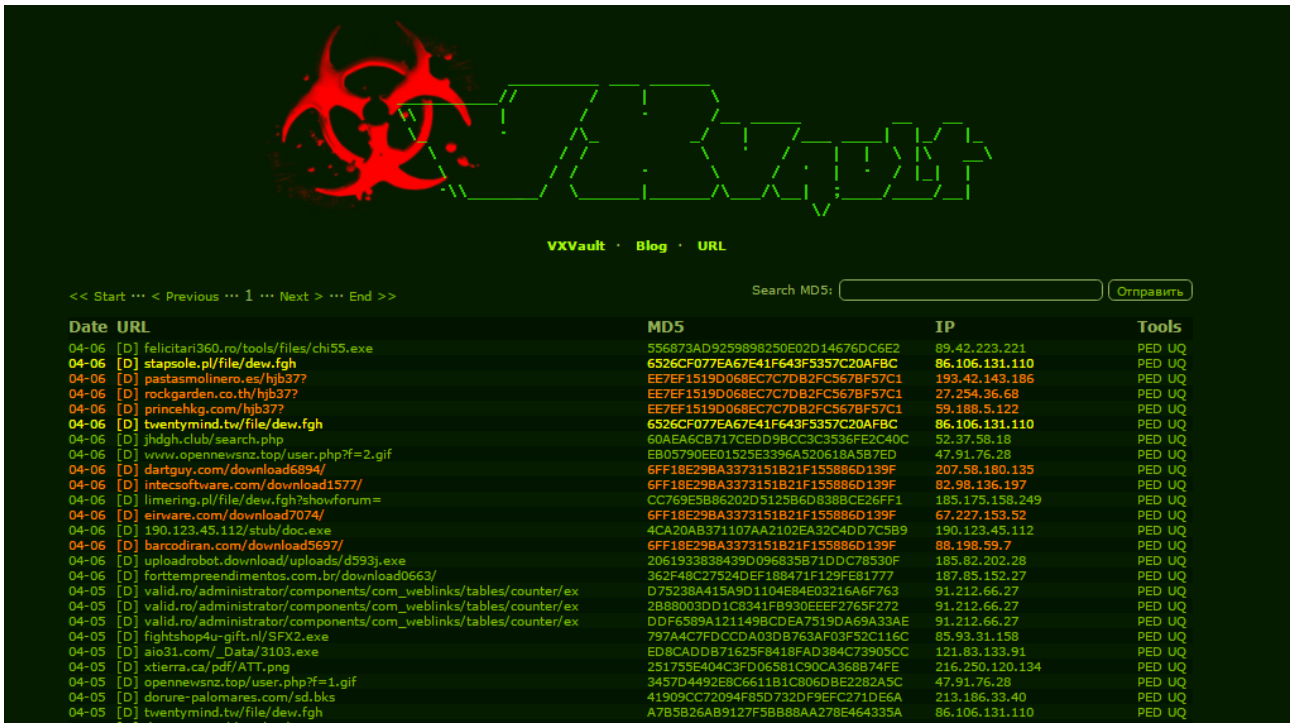


Рис. 17. 4. Бібліотека шкідливого програмного забезпечення *Vxvault*

В даному списку все шкідливе програмне забезпечення підсвічується трьома кольорами:

- жовтий – означає, що шкідник, скоріш за все, вже видалений;
- темно-жовтий – означає, що шкідник видалений;
- зелений – означає, що шкідник доступний для скачування (Link).

Окрім цього сайт відображає хеш файлу, IP-адресу та вказує базові інструменти для вивчення і дослідження *malware.*

Завантаживши, за посиланням ***Link*** (рис. 17.5), шкідливе програмне забезпечення, його можна перевірити та отримати більш детальну інформацію використовуючи онлайн інструменти, наприклад *VirusTotal* (рис. 17.6), *Kaspersky VirusDesk* (рис. 17.7).

[16] Для тестування можна використовувати сервіс **Vxvault.net** – сайт зі списком шкідливого програмного забезпечення (рис. 17.4), який оновлюється щоденно, майже в реальному часі.

Рис. 17. 5. Сторінка бібліотеки *Vxvault* з конкретним malware

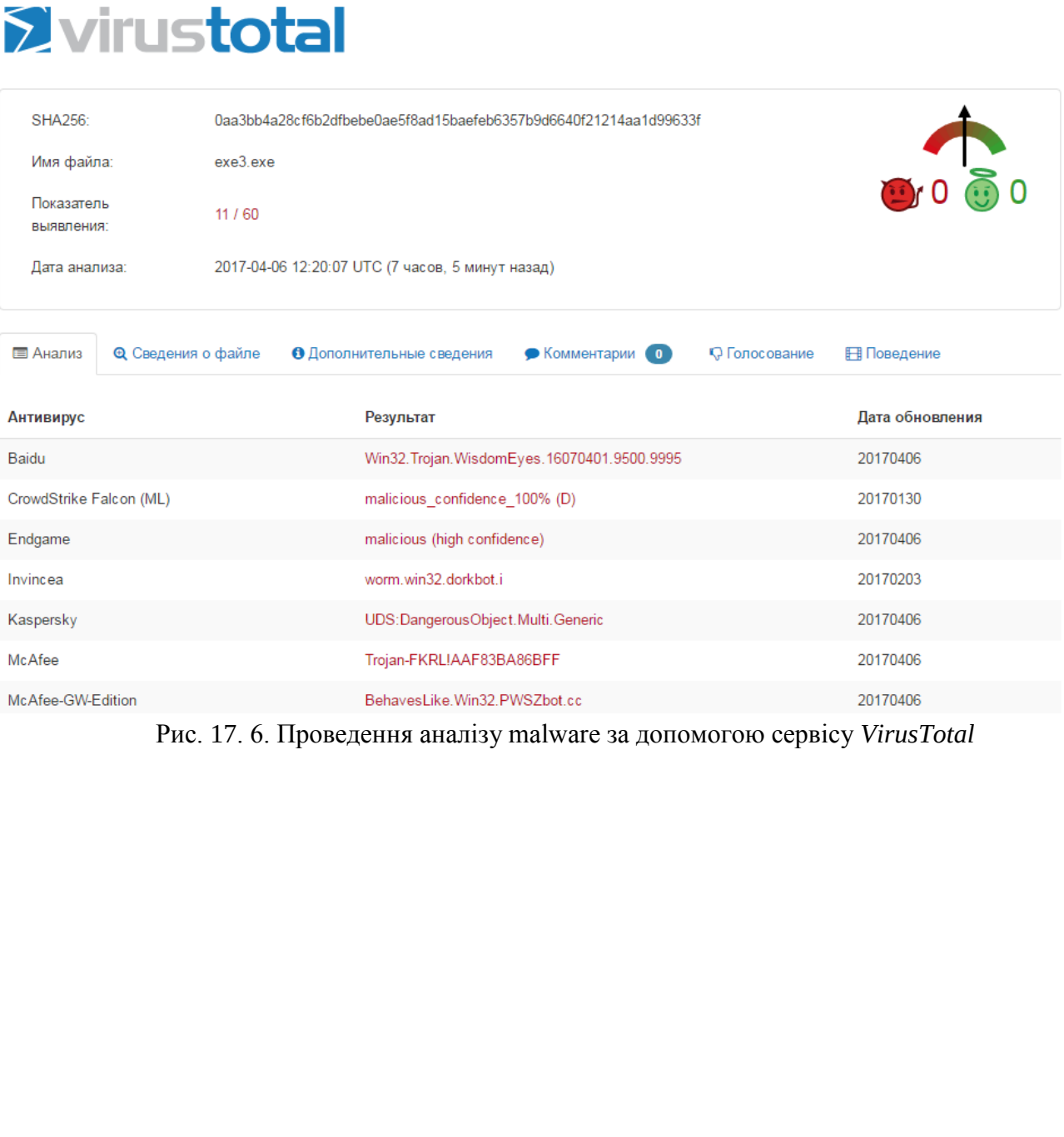


Рис. 17. 6. Проведення аналізу malware за допомогою сервісу *VirusTotal*

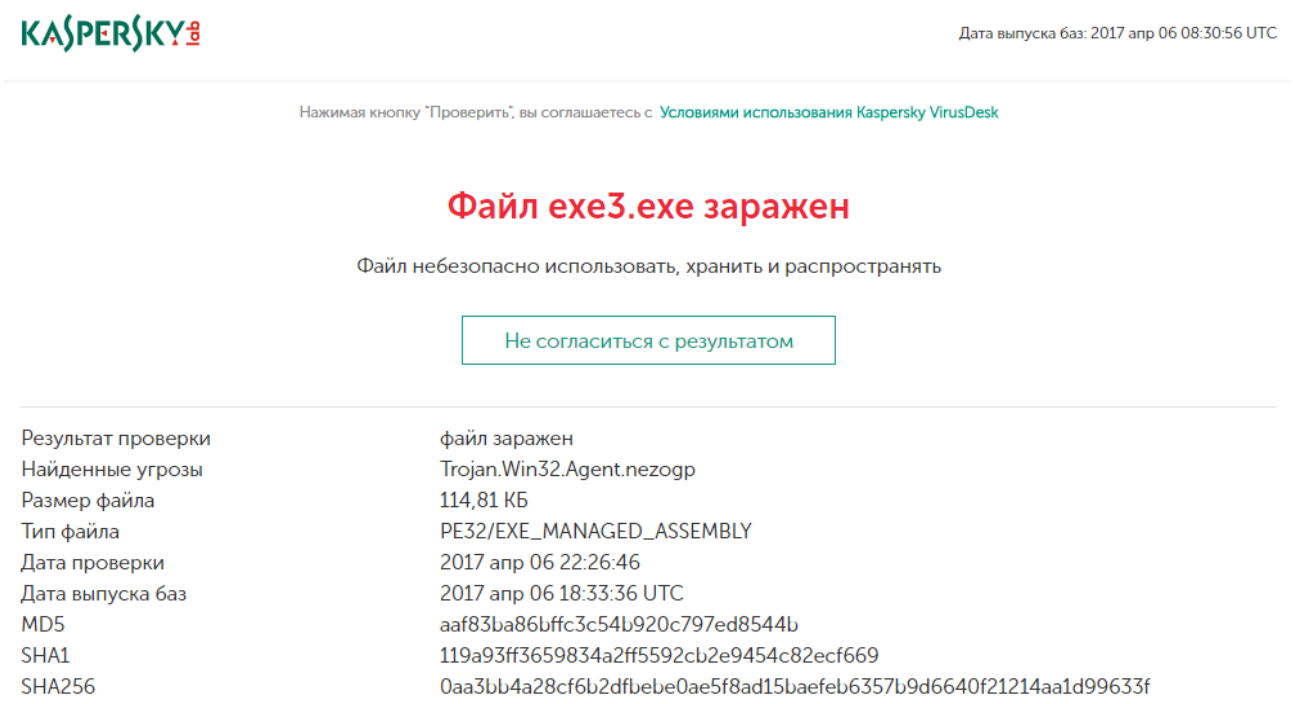


Рис. 17. 7. Проведення аналізу malware за допомогою сервісу *Kaspersky VirusDesk*

4) Описати виявлене шкідливе програмне забезпечення.

6. Оформити звіт згідно до вимог (додаток 1).

7. Відповісти на контрольні питання та підготуватися до письмового опитування.

Зміст звіту:

1. Титульний лист.
2. Постановка завдання.
3. Коротка письмова доповідь по заданому пакету антивірусного програмного забезпечення.
4. Протокол виконання лабораторної роботи, що містить результати проведеного тестування встановленої версії антивірусного ПЗ з відповідними скріншотами та описом завантажених malware.
5. Висновки.

Завдання на виконання лабораторної роботи №17

Таблиця № 17.1 (варіант відповідно до номера за списком у журналі)

Номер варіанта	Назва антивірусного вендору
1	Agnitum, Росія
2	Avast Software, Чехія
3	AVG Technologies, Чехія
4	Avira, Німеччина
5	BitDefender, Румунія
6	Доктор Веб, Росія

7	Emsisoft, Австрія
8	Eset, Словаччина
9	F-Secure, Фінляндія
10	Лабораторія Касперського, Росія
11	McAfee, США
12	Panda Security, Іспанія
13	Qihoo 360, Китай
14	Symantec, США
15	Trend Micro, Японія
16	TrustPort, Чехія
17	ВірусБлокАда, Білорусь
18	Comodo, США
19	Check Point, Ізраїль
20	G Data, Німеччина
21	Online Solutions, Росія
22	Zillya!, Україна
23	Microsoft, США

Контрольні питання:

1. Назвіть програми, які відносяться до так званого шкідливого програмного забезпечення та надайте визначення поняттю «комп'ютерний вірус».
2. Перерахуйте основні причини появи та існування шкідливих програм.
3. Класифікуйте класичні віруси та надайте кожному з видів коротку характеристику.
4. Опишіть основні механізми зараження файлів комп'ютерними вірусами.
5. Опишіть тип шкідливого ПЗ: мережеві хробаки.
6. Опишіть тип шкідливого ПЗ: троянські програми.
7. Назвіть основні ознаки зараження комп'ютера.
8. Назвіть та коротко опишіть основні методи виявлення вірусів.
9. Назвіть основні типи антивірусного програмного забезпечення та коротко опишіть принцип їх роботи.

Лабораторна робота №18
«Основи забезпечення мережевої безпеки інформаційно-телекомунікаційної системи»

Мета роботи:

1. Ознайомлення з основними принципами захисту інформації при підключенні ІТС до мережі Інтернет.
2. Вивчення принципів функціонування міжмережевих екранів різних класів.

Стислі теоретичні відомості:

У сучасному глобальному світі мережева безпека має вирішальне значення. Підприємствам необхідно забезпечувати безпечний доступ для співробітників до мережевих ресурсів в будь-який час, для чого сучасна стратегія забезпечення мережевої безпеки повинна враховувати ряд таких факторів, як збільшення надійності мережі, ефективне управління безпекою та захист від динамічно зростаючих загроз і нових методів атак.

18.1. Основні принципи захисту інформації при підключення ІТС до мережі Інтернет

Для підключення будь-якої організації до мережі Інтернет необхідно прийняти ряд певних організаційно-технічних заходів для її захисту.

При побудові захисту варто враховувати, що будь-який захист ускладнює використання системи за прямим призначенням, обмежує функціональні можливості, споживає обчислювальні й трудові ресурси, а також, вимагає певних фінансових витрат на створення та експлуатацію. Таким чином, можна стверджувати наступне: чим надійніший захист, тим дорожчою у побудові та обслуговуванні стає система і тим менш вона зручна для безпосередніх користувачів. Тому, захищаючи мережу, варто виходити з доцільної вартості захисту. Тобто витрати на захист повинні бути пропорційні цінності ресурсів, які підлягають захисту. В зв'язку з цим, далі буде розглянуто ряд основних принципів, що дозволяють організувати досить безпечне підключення до мережі Інтернет порівняно простими засобами.

18.1.1. Міжмережеве екранування

Основним загальновизнаним засобом захисту інформації при підключенні ІТС до мережі Інтернет є міжмережевий екран (*Брандмауер – Firewall*).

Міжмережевий екран (МЕ) виконує функції розмежування інформаційних потоків на кордоні ІТС, що захищається. Це дозволяє:

- підвищити безпеку об'єктів внутрішнього середовища за рахунок ігнорування неавторизованих запитів із зовнішнього середовища;
- контролювати інформаційні потоки в зовнішнє середовище;

- забезпечити реєстрацію процесів інформаційного обміну.

Таким чином міжмережевий екран встановлюється між внутрішньою мережею та мережею Інтернет і виконує роль мережевого фільтра (рис. 18.1).

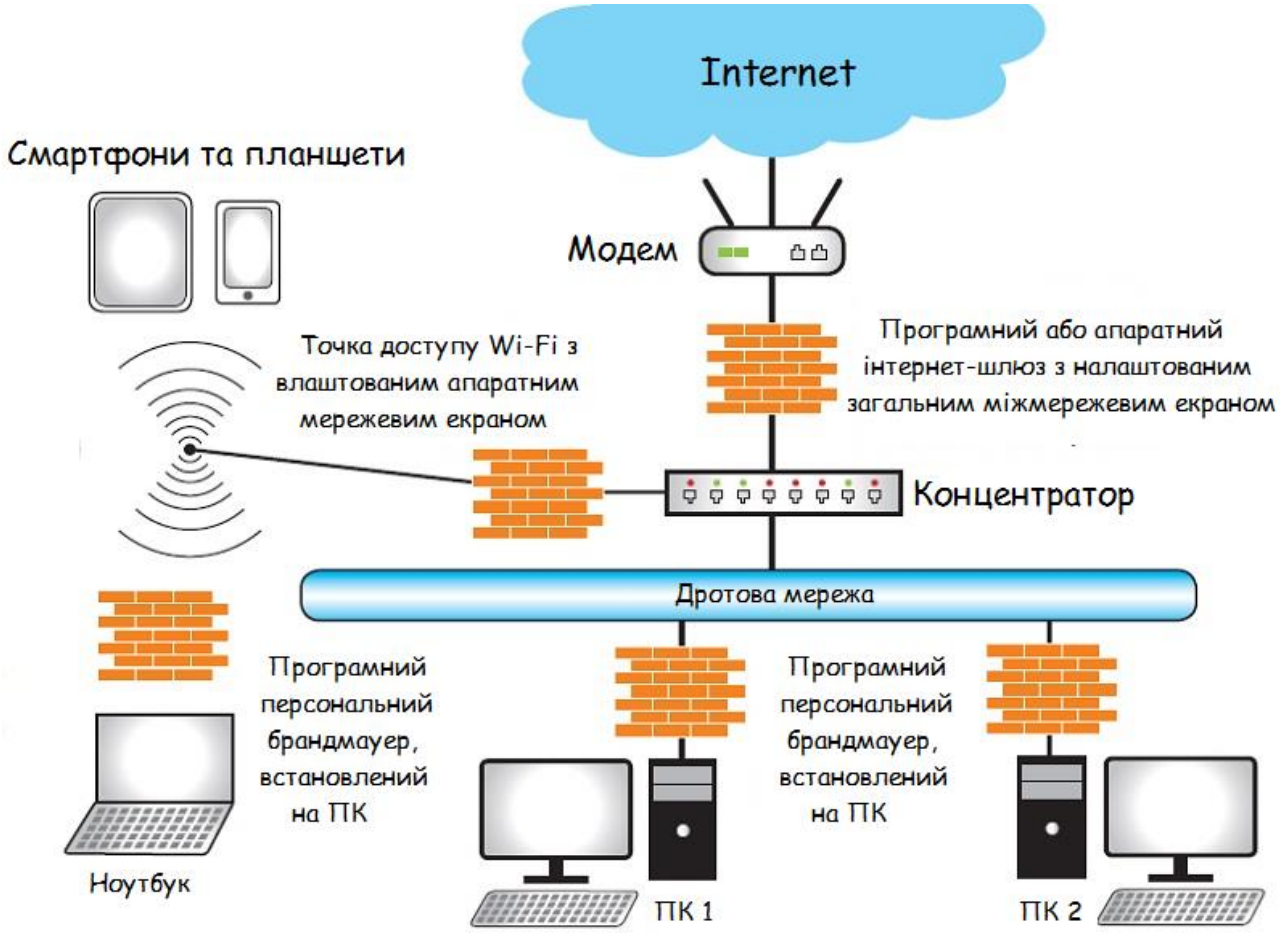


Рис. 18.1. Типова схема використання брандмауера в ІТС з підключенням до Інтернету

Контроль інформаційних потоків проводиться за допомогою фільтрації інформації, тобто аналізу її за сукупністю критеріїв (відповідно до політики інформаційної безпеки організації) і прийняття рішення щодо пропуску допустимого трафіку від користувачів мережі до служб мережі Інтернет і назад; та відповідно обмежити трафік з боку мережі Інтернет до внутрішньої мережі, яка потребує захисту, лише необхідними службами, наприклад: smtp, dns, ntp.

Залежно від принципів функціонування та застосування різних технологій мережевого захисту, виділяють кілька класів міжмережевих екранів, а саме:

- пакетний фільтр (Packet-filtering);
- шлюз додатків (Application-gateway);
- брандмауер рівня з'єднання (Circuit-level);
- брандмауер перевірки стану (Stateful Inspection).

Найпростішим класом залишаються ***пакетні фільтри*** в яких фільтрація пакетів зазвичай здійснюється за наступними критеріями:

- IP-адреса джерела;
- IP-адреса одержувача;
- порт джерела;
- порт одержувача;
- специфічні параметри заголовків мережевих пакетів.

Сама ж фільтрація реалізується шляхом порівняння перерахованих параметрів заголовків мережевих пакетів з базою правил фільтрації.

Ще одним досить поширеним класом МЕ є ***шлюз додатків*** – модель більшості персональних брандмауерів. Також дані види брандмауерів іноді називаються *проксі-брандмауерами*, оскільки вони можуть фільтрувати, ґрунтуючись на IP-адресах і певних функціях, які намагається виконати той чи інший додаток. Наприклад, ці брандмауери можуть не пропустити певні програми, такі, як Microsoft NetMeeting, PCAnywhere або FTP. Переглядаючи функції конкретного додатку, брандмауер може навіть дозволити виконувати деякі операції цьому додатку, в той же час блокуючи інші. Один із прикладів цього – FTP-сайт, який дозволяє вам завантажити файли в зазначені директорії без дозволу переглядати або змінювати файли в цих директоріях.

Брандмауери рівня з'єднань пропускають потік трафіку з попередньо схвалених IP-адрес, мереж або постачальників Інтернет-послуг.

Брандмауери перевірки стану замість обмеженої перевірки пакетів на відповідність вимогам порту або додатку вивчають весь пакет цілком і аналізують його вміст. Брандмауери даного класу намагаються визначити тип даних, які передаються і таким чином, якщо розглянуті дані не несуть загрози, брандмауери дозволяють їм пройти.

18.1.2. Технологія NAT

Другою цеглинкою забезпечення захищеності мережі є «заміна мережевої адреси» – Network Address Translation, або NAT (також має назви IP Masquerading, Network Masquerading і Native Address Translation.) – це механізм, який використовується в мережах TCP/IP, що дозволяє перетворювати IP-адреси транзитних пакетів (див. рис. 18.2).

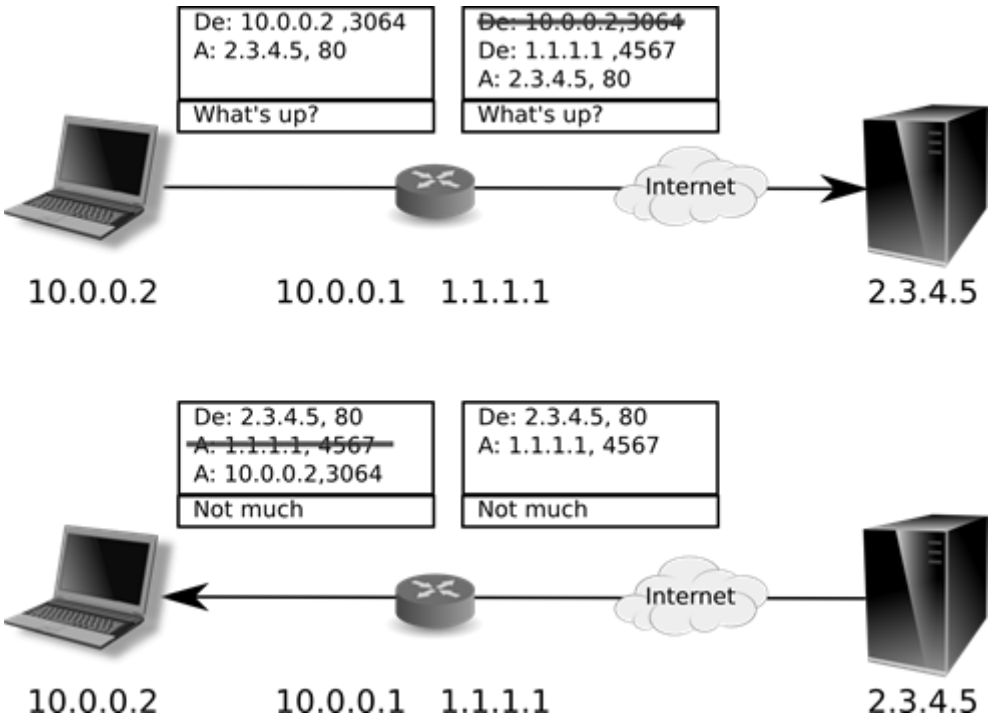


Рис. 18.2. Принцип роботи NAT

Перетворення адрес методом NAT може проводитися майже будь-яким маршрутизуючим пристроєм – маршрутизатором, сервером доступу, міжмережевим екраном, т.д. Найбільш популярним є ***SNAT (source NAT)***, суть механізму якого полягає в заміні адреси джерела (англ. *source*) при проходженні пакета в один бік і зворотної заміні адреси призначення (англ. *destination*) у відповідному пакеті. Поряд з адресами джерело/призначення можуть також замінюватися номера портів джерела і призначення.

Приймаючи пакет від локального комп'ютера, роутер дивиться на IP-адресу призначення. Якщо це локальна адреса, то пакет пересилається іншому локальному комп'ютеру. Якщо ж ні, то пакет пересилається назовні, в мережу Інтернет. Але ж зворотнім адресом у пакеті вказано локальний адрес комп'ютера, який з мережі Інтернет буде недоступний. Саме тому роутер «на льоту» виробляє трансляцію IP-адреси і порту і запа'ятовує цю трансляцію у себе в тимчасовій таблиці. Через деякий час після того, як клієнт і сервер закінчать обмінюватися пакетами, роутер зітре у себе в таблиці запис про *n-ий* порт за строком давності.

Крім *source NAT* (надання користувачам локальної мережі з внутрішніми адресами доступу до мережі Інтернет) часто застосовується також ***destination NAT***, коли звернення ззовні транслюються міжмережевим екраном на комп'ютер користувача в локальній мережі, що має внутрішню адресу і тому недоступний безпосередньо (без NAT) ззовні мережі.

Існує 3 базових концепції трансляції адрес: статична (Static Network Address Translation), динамічна (Dynamic Address Translation) та маскарадна (NAPT, NAT Overload, PAT).

Статичний NAT – трансляція незареєстрованої IP-адреси у зареєстровану IP-адресу на підставі один до одного. Особливо корисно, коли пристрій повинен бути доступним зовні мережі, однак дана трансляція є найбільш слабкою з точки зору безпеки мережі. Оскільки, при цьому, противник безперешкодно «бачить» такий комп'ютер у зовнішній мережі, тому що йому однозначно відповідає певна зовнішня адреса.

Динамічний NAT – трансляція незареєстрованої IP-адреси у зареєстровану адресу від групи зареєстрованих IP-адрес. Тобто внутрішній комп'ютер, виходячи в Інтернет, одержує вільну у цей момент адресу з бази даних. При цьому адреси підмінюються динамічно, і кожне нове *TCP*-з'єднання може бути встановлене з іншою IP-адресою. Це також створює додаткові труднощі противнику, тому що позбавляє його можливості атакувати будь-який внутрішній комп'ютер прицільно.

Перевантажений NAT (NAPT, NAT Overload, PAT) – форма динамічного NAT, який відображає кілька незареєстрованих адрес в єдину зареєстровану IP-адресу, використовуючи різні порти. Відомий також як PAT (Port Address Translation). При перевантаженні кожен комп'ютер у приватній мережі транслюється в ту ж саму адресу, але з різним номером порту. При цьому всі внутрішні комп'ютери можуть працювати з Інтернетом одночасно, а маршрутизатор розрізняє, кому яка відповідь перетрансльовується за службовими даними *TCP*-з'єднання. У зовнішній мережі створюється враження, що до неї звертається тільки один комп'ютер. Така заміна істотно ускладнює життя противнику, тому що повністю приховує внутрішні комп'ютери й перешкоджає «вирахуванню» жертви (рис. 18.3). Навіть, якщо противник має змогу переглядати трафік, що виходить із внутрішньої мережі, не може визначити, від якого комп'ютера він виходить. Крім того, це виключає можливість ініціативного обігу ззовні до внутрішнього комп'ютера, тому що для маршрутизатора в цьому випадку відсутнє правило прив'язки зовнішньої адреси до внутрішньої. Зокрема виключається можливість сканування ззовні внутрішньої мережі.

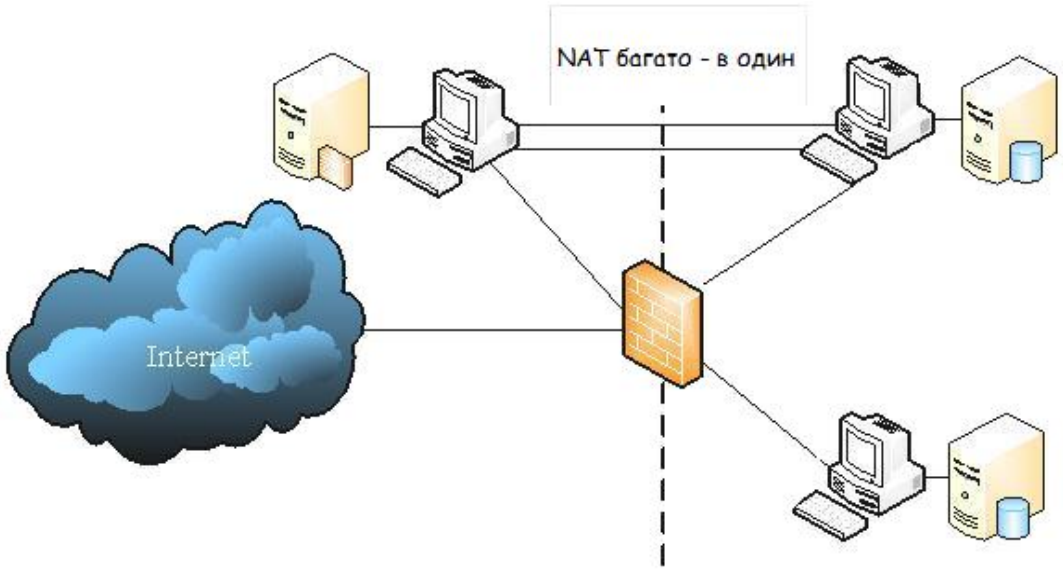


Рис. 18.3. Трансляція групи внутрішніх адрес в одну зовнішню

18.1.3. Демілітаризована зона

В більшості випадків, організації потрібно мати у себе деякі мережні ресурси, до яких відкритий доступ з мережі Інтернет. Як правило, це поштовий, dns і web-сервери. Механізм їх роботи допускає, що до них повинен бути дозволений вільний або слабко обмежений обіг з Інтернету. Відповідно ймовірність їх зламу вища, ніж інших комп'ютерів мережі. Із цієї причини розміщати їх усередині зони, що захищається, недоцільно з погляду безпеки, тому що у випадку зламу вони можуть стати воротами для атаки внутрішніх комп'ютерів. Для мінімізації ризику і збереження функціональності такі сервери встановлюють за основним шлюзом мережі, але перед міжмережевим екраном, що забезпечує захист внутрішніх комп'ютерів. Логічну область їх розміщення називають демілітаризованою зоною (рис. 18.4).

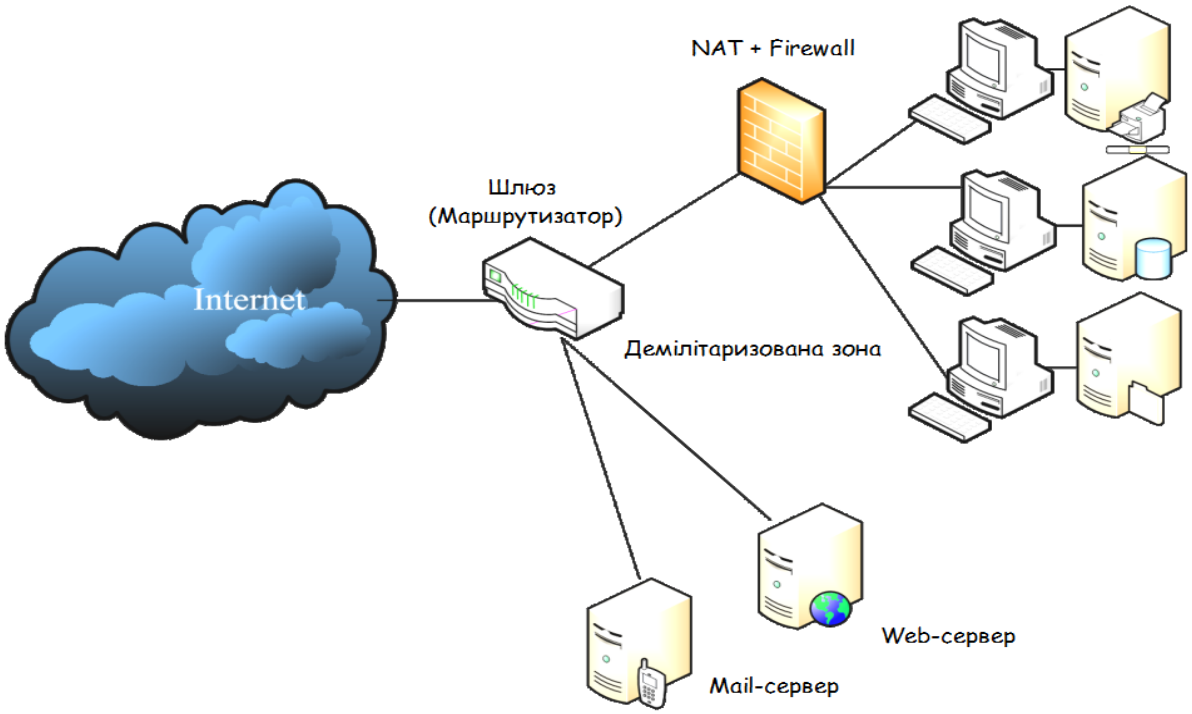


Рис. 18.4. Структурна схема ІТС з демілітаризованою зоною

Порядок виконання лабораторної роботи №18:

1. Включити ПК.
2. Ознайомитися з короткими теоретичними відомостями та основним сценарієм даної лабораторної роботи, який полягає в наступному:

В раніше згадуваній компанії «Cyberstec» виникла необхідність в підвищенні мережевої безпеки компанії. Головна вимога вказана в нижченаведеному електронному листі.

Посилення безпеки мережі

Cyberstec <CBS@cyberstec.com> 21 червня 2017, 12:15

Доброго дня, у нас виникли деякі проблеми з безпекою мережі. Нам би хотілося заборонити зловмисникам використовувати програму ping.exe в нашій мережі. Як вам відомо, за допомогою ping.exe зловмисники можуть визначити підключені до мережі сервери і скористатися додатковими уразливостями цих серверів, застосовуючи інші засоби.

Чи могли б ви нам допомогти у вирішенні даної проблеми?

*З повагою, виконавчий директор «*Cyberstec*», Parker Riss.*

3. Допомогти у вирішенні проблеми посилення безпеки мережі в компанії «Cyberstec», при цьому всі прийняті рішення необхідно спершу протестувати на лабораторному стенді, який був створений під час виконання лабораторної роботи №6 (за умови, що ваша хостова машина – ПК

зловмисника, а *Test PC1 Win* та *Test PC2 Lin* – ПК компанії «Cyberstec»). У звіті відобразити усі прийняті рішення (з поясненнями та відповідними скріншотами виконуваних дій) щодо посилення безпеки мережі.

4. Оформити звіт згідно до вимог (додаток 1).
5. Відповісти на контрольні питання та підготуватися до письмового опитування.

Зміст звіту:

1. Титульний лист.
2. Постановка завдання.
3. Протокол виконання лабораторної роботи, що містить результати вирішення проблеми посилення безпеки мережі в компанії «Cyberstec» з усіма поясненнями того чи іншого рішення, та з супроводом скріншотів проведеного тестування прийнятих рішень.
4. Висновки та відповіді на контрольні питання.

Контрольні питання:

1. Назвіть основні принципи захисту інформації при підключення ІТС до мережі Інтернет.
2. Поясніть, що таке міжмережевий екран та опишіть типову схему його використання.
3. Назвіть та коротко опишіть основні класи міжмережевих екранів.
4. Надайте визначення технології NAT та поясніть принцип її роботи.
5. Назвіть та опишіть базові концепції трансляції IP-адрес.
6. Поясніть, що таке демілітаризована зона та схематично відобразіть її використання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Законом України «Про захист персональних даних».
2. Законі України «Про інформацію».
3. Закону України «Про основні засади забезпечення кібербезпеки України».
4. Кодекс України «Про адміністративні правопорушення».
5. Кримінальний кодекс України.
6. Критерии оценки безопасности компьютерных систем МО США («Оранжевая книга») TCSTC (Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STD, 1983).
7. НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу».
8. СОУ Н НБУ 65.1 СУІБ 1.0:2010 – Методи захисту в банківській діяльності. Система управління інформаційною безпекою. Вимоги.
9. СОУ Н НБУ 65.1 СУІБ 2.0:2010 – Методи захисту в банківській діяльності. Звід правил для управління інформаційною безпекою.
10. ISO/IEC 15408-1999 «Common Criteria for Information Technology Security Evaluation»
11. ISO/IEC 17799:2005 «Information technology – Security techniques – Code of practice for information security management»
12. ISO/IEC 27001:2005 «Information technology – Security techniques – Information security management systems – Requirements»
13. Аверченков В. И. Системы защиты информации в ведущих зарубежных странах: учебное пособие для вузов / В. И. Аверченков, М. Ю. Рытов, Г. В. Кондрашин, М. В. Рудановский. – Брянск: БГТУ, 2007. – 225 с.
14. Анин Б. Ю. Защита компьютерной информации / Б. Ю. Анин – Санкт-Петербург: БХВ-Санкт-Петербург, 2000. – 384 с.
15. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: посібник / В. Л. Бурячок, С. В. Толюпа, В. В. Семко, Л. В. Бурячок, П. М. Складанний, Н. В. Лукова-Чуйко. – Київ: ДУТ – КНУ, 2016. – 178 с.
16. Бурячок В. Л. Модель формування дерева атак для одержання інформації в інформаційно-телекомунікаційних системах і мережах при вилученому доступі / В. Л. Бурячок // Науковий журнал «Інформатика та математичні методи в моделюванні» Одеського національного політехнічного університету. – № 2, 2013, с. 123 – 131

17. Гулак Г. М. Основи криптографічного захисту інформації: підручник / Г. М. Гулак, В. А. Мухачов, В. О. Хорошко, Ю. Є. Яремчук. – Вінниця: ВНТУ, 2011. – 199 с.

18. Кавун С. В. Інформаційна безпека. Навчальний посібник. Ч. 2 / С. В. Кавун, В. В. Носов, О. В. Манжай. – Харків: ХНЕУ, 2008. – 196 с

19. Мельник С. В. До проблеми формування понятійно-термінологічного апарату кібербезпеки / С.В. Мельник, О.О. Тихомиров, О.С. Лєнков // Збірник наукових праць Військового інституту КНУ ім. Тараса Шевченка. – Київ. : ВІКНУ, 2011. – Вип. 30. – с. 159-165.

20. Остапов С. Е. Технології захисту інформації: навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Харків: ХНЕУ, 2013. – 476 с.

21. Силаенков А. Н. Проектирование системы информационной безопасности: учебное пособие / А. Н. Силаенков – Омск: Изд-во ОмГТУ, 2009. – 128 с.

22. Сухов А. М. Механизмы безопасности в Linux: Методические указания к лабораторной работе / А. М. Сухов. – Самара: СГАУ, 2010. – 24 с.

23. Сычев Ю. Н. Основы информационной безопасности: учебно-практическое пособие / Ю. Н. Сычев – Москва: Изд. центр ЕАОИ, 2007. – 300 с

24. Хамухин А. А. Практикум по информационной безопасности: учебное пособие / А. А. Хамухин, А. А. Захарова – Томск: ТПУ, 2011. – 196 с.

25. Цирлов В. Л. Основы информационной безопасности автоматизированных систем. Краткий курс / В. Л. Цирлов. – Ростов-на-Дону: Феникс, 2008. – 253 с.

26. Cardwell Kevin. Building Virtual Pentesting Labs for Advanced Penetration Testing / K. Cardwell – Birmingham: Packt Publishing Ltd, 2014. – 412 с.

27. Кузьменко Б. В. Захист інформації / Б. В. Кузьменко, О. А. Чайковська. – Київ: Видавничий відділ КНУКіМ, 2009. – 69 с.

Додаток 1

Вимоги до оформлення

Текст лабораторної роботи слід друкувати, додержуючись таких розмірів полів: верхнє і нижнє – не менше 20 мм, ліве – 25 мм, праве – 15 мм. Шрифт текстового редактору MS Word – Times New Roman, розмір шрифту – 14 пунктів, інтервал – 1,15, абзац – 1,25, вирівнювання за шириною.

Додаток 2

Таблиця аналізу інцидентів ІБ та виявлених загроз

№	Інцидент ІБ	Тип виявленої (реалізованої) загрози	Джерело загрози та тип порушника	Спосіб реалізації загрози	Використані уразливості	Вид активів, які підлягають захисту	Наслідки (порушення)		
							К	Ц	Д
1.	злам сервера Hotmail.com	упровадження програмних закладок або комп'ютерних вірусів.	антропогенне джерело – група хакерів «Hackers Unite»; зовнішній порушник з високим потенціалом.	одержання зловмисником інформації про програмно-апаратне середовище, тип та параметри засобів обчислювальної техніки, тип та версії операційної системи, склад прикладного програмного забезпечення та інше.	- уразливості системного ПЗ; - уразливості прикладного ПЗ; - уразливості в апаратних засобах.	конфіденційні дані користувачів Hotmail – почтові скриньки.	+		+
2.									
3.									

Додаток 3

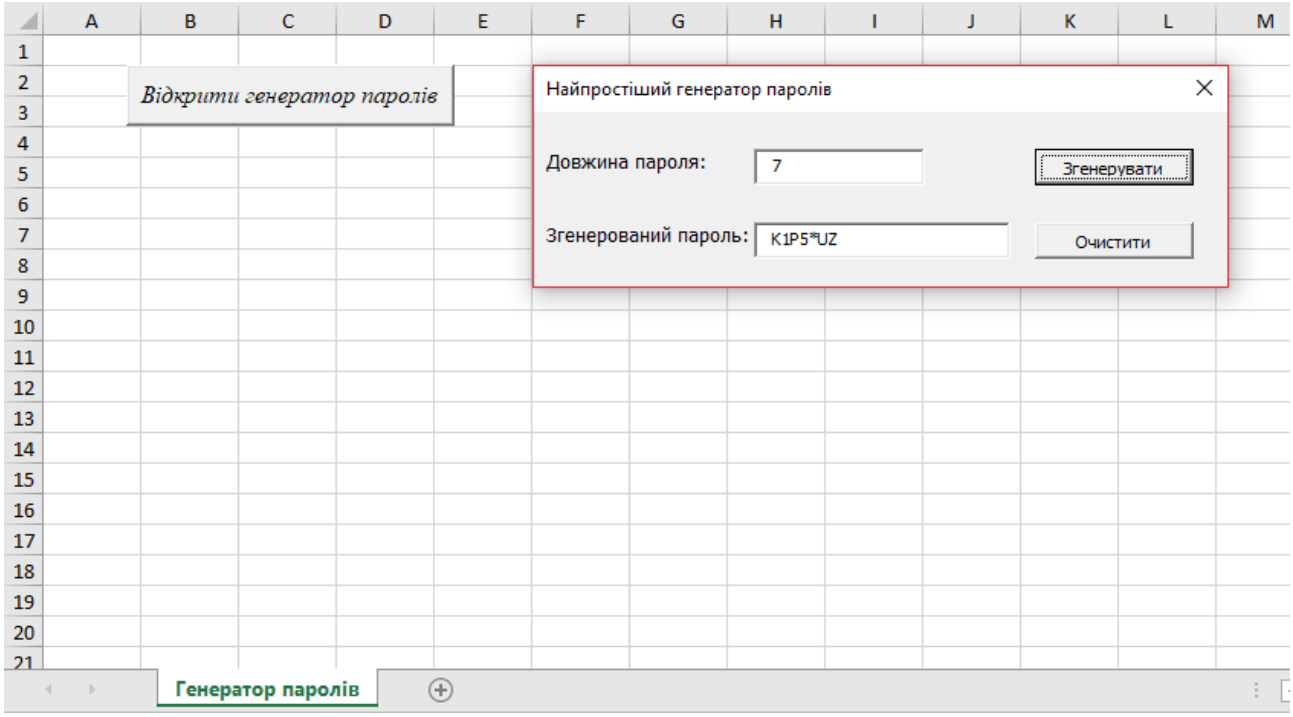


Рис. Зразок реалізації генератора паролів в MS Excel

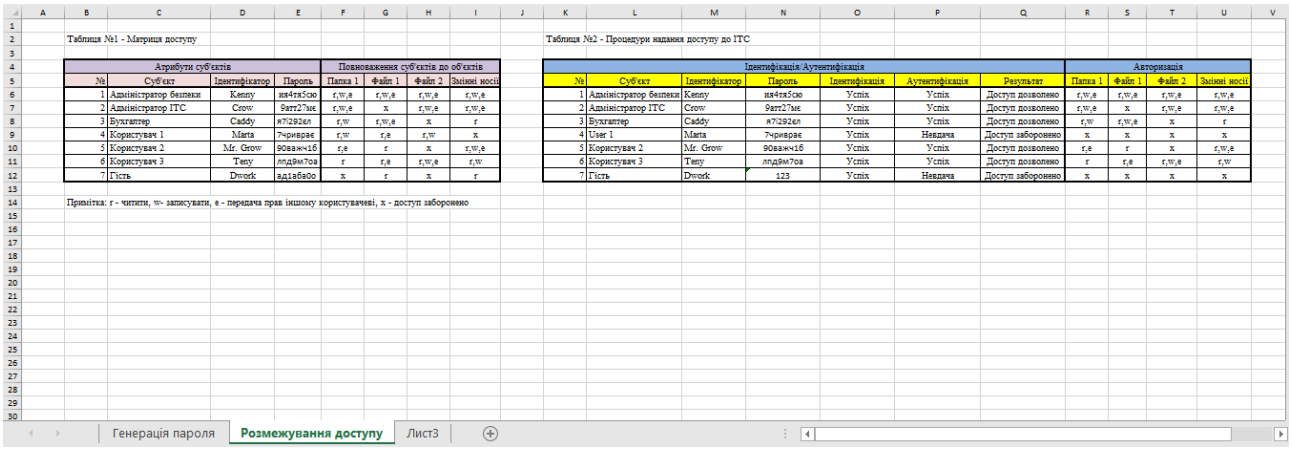
Лістинг реалізованого генератора паролів в MS Excel за допомогою Microsoft Visual Basic, з можливістю регулювання довжини пароля, який складається з цифр, латинських літер верхнього регістру та спец. символів[17]*:*

```
Dim i As Byte
Dim FinalPassword As String

Randomize
FinalPassword = ""

 If Not IsNumeric(TextBox1.Text) Then
   MsgBox ("Ви не вказали довжину пароля!")

    ElseIf TextBox1.Text > 0 Then
      Select Case Rnd(1) * 10 Mod 3
    Case 0:
       For i = 1 To TextBox1
          If i = 1 Or i = 4 Or i = 8 Then
          FinalPassword = FinalPassword + Chr(Int(10 * Rnd + 48))
```

[17] Підказка: в програмному коді використовується зведена таблиця кодів ASCII

```
            ElseIf i = 3 Or i = 10 Then
            FinalPassword = FinalPassword + Chr(Int(10 * Rnd + 33))
            Else
            FinalPassword = FinalPassword + Chr(Int(26 * Rnd + 65))
            End If
        Next
        TextBox2.Text = FinalPassword
    Case 1:
        For i = 1 To TextBox1
            If i = 2 Or i = 3 Or i = 9 Or i = 12 Then
            FinalPassword = FinalPassword + Chr(Int(10 * Rnd + 48))
            ElseIf i = 4 Or i = 7 Then
            FinalPassword = FinalPassword + Chr(Int(10 * Rnd + 33))
            Else
            FinalPassword = FinalPassword + Chr(Int(26 * Rnd + 65))
            End If
        Next
        TextBox2.Text = FinalPassword
    Case 2:
        For i = 1 To TextBox1
            If i = 2 Or i = 4 Or i = 13 Then
            FinalPassword = FinalPassword + Chr(Int(10 * Rnd + 48))
            ElseIf i = 5 Or i = 8 Then
            FinalPassword = FinalPassword + Chr(Int(10 * Rnd + 33))
            Else
            FinalPassword = FinalPassword + Chr(Int(26 * Rnd + 65))
            End If
        Next
        TextBox2.Text = FinalPassword
    End Select

    Else
    MsgBox ("Довжина пароля повинна бути більше 0")
End If
```

Додаток 4



Таблиця №1 - Матриця доступу

Атрибути суб'єктів				Повноваження суб'єктів до об'єктів			
№	Суб'єкт	Ідентифікатор	Пароль	Папка 1	Файл 1	Файл 2	Змінні носії
1	Адміністратор безпеки	Kenny	ия4тя5сю	r,w,e	r,w,e	r,w,e	r,w,e
2	Адміністратор ІТС	Crow	9ятт27ме	r,w,e	x	r,w,e	r,w,e
3	Бухгалтер	Caddy	я7ї292ел	r,w	r,w,e	x	r
4	Користувач 1	Marta	7чиврає	r,w	r,e	r,w	x
5	Користувач 2	Mr. Grow	90важч16	r,e	r	x	r,w,e
6	Користувач 3	Tony	лпдйм7оа	r	r,e	r,w,e	r,w
7	Гість	Dwork	ад1аба0о	x	r	x	r

Примітка: r - читати, w- записувати, e - передача прав іншому користувачеві, x - доступ заборонено

Таблиця №2 - Процедури надання доступу до ІТС

			Ідентифікація/Аутентифікація				Авторизація			
№	Суб'єкт	Ідентифікатор	Пароль	Ідентифікація	Аутентифікація	Результат	Папка 1	Файл 1	Файл 2	Змінні носії
1	Адміністратор безпеки	Kenny	ия4тя5сю	Успіх	Успіх	Доступ дозволено	r,w,e	r,w,e	r,w,e	r,w,e
2	Адміністратор ІТС	Crow	9ятт27ме	Успіх	Успіх	Доступ дозволено	r,w,e	x	r,w,e	r,w,e
3	Бухгалтер	Caddy	я7ї292ел	Успіх	Успіх	Доступ дозволено	r,w	r,w,e	x	r
4	User 1	Marta	7чиврає	Успіх	Невдача	Доступ заборонено	x	x	x	x
5	Користувач 2	Mr. Grow	90важч16	Успіх	Успіх	Доступ дозволено	r,e	r	x	r,w,e
6	Користувач 3	Tony	лпдйм7оа	Успіх	Успіх	Доступ дозволено	r	r,e	r,w,e	r,w
7	Гість	Dwork	123	Успіх	Невдача	Доступ заборонено	x	x	x	x

Генерація пароля | Розмежування доступу | Лист3

Рис. Зразок реалізації моделі DAC в MS Excel

Додаток 5

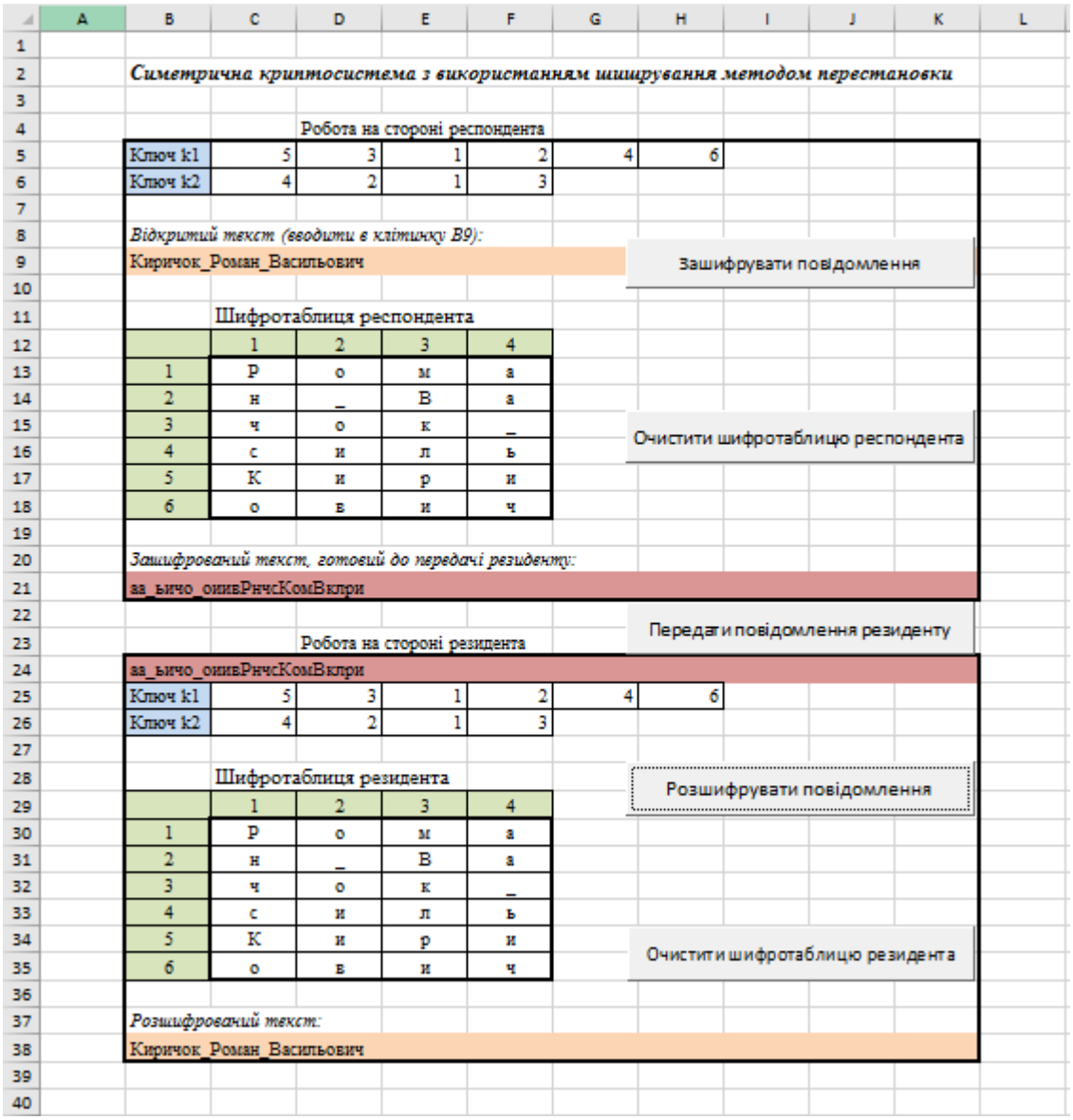


Рис. Зразок змодельованої симетричної криптосистеми обміну повідомленнями в ІТС

Лістинг змодельованої симетричної криптосистеми обміну повідомленнями в ІТС з використанням шифрування методом перестановки:

Визначення змінних:

```
Dim Tabl1(6, 4), Tabl2(6, 4) As String
Dim IshodnText, ShifText, DeshifText, Sim As String
Dim k1(6), k2(4) As Byte
```

Шифрування на стороні респондента:

```
Private Sub CommandButton1_Click() ‘Шифрування
‘Зчитуємо ключ на стороні респондента
For i = 1 To 6
```

```
k1(i) = Cells(5, i + 2).Value
Next i
For j = 1 To 4
k2(j) = Cells(6, j + 2).Value
Next j
‘Читаємо відкритий текст
IshodnText = Range("B9").Value
Schet = 1 ‘Лічильник символів для шифрування
‘Заповнюємо шифротаблицю в масив
For i = 1 To 6
 i1 = k1(i)
  For j = 1 To 4
     Tabl1(i1, j) = Mid(IshodnText, Schet, 1)
    Schet = Schet + 1
   Next j
Next i
‘Виводимо шифротаблицю на лист
For i = 1 To 6
  For j = 1 To 4
       Cells(i + 12, j + 2) = Tabl1(i, j)
    Next j
Next i
‘Читаємо шифротаблицю по стовпцях та формуємо зашифрований рядок тексту
Schet = 1
ShifText = ""
Sim = ""
 For j = 1 To 4
    j1 = k2(j)
     For i = 1 To 6
         Sim = Tabl1(i, j1)
         ShifText = ShifText + Sim
         Schet = Schet + 1
       Next i
Next j
Range("B21").Value = ShifText
End Sub
```

Очищення шифротаблиці та відправки повідомлення:

```
Private Sub CommandButton2_Click() ‘Очистити шифротаблицю респондента
 For i = 1 To 6
  For j = 1 To 4
    Cells(i + 12, j + 2) = ""
  Next j
Next i
Range("B21").Value = ""
End Sub

Private Sub CommandButton3_Click() ‘Відправка повідомлення
Range("B24").Value = Range("B21").Value
End Sub
```

Розшифрування на стороні резидента:

```
Private Sub CommandButton4_Click() ‘Розшифрувати
‘Зчитуємо ключ на стороні резидента
For i = 1 To 6
 k1(i) = Cells(25, i + 2).Value
Next i
For j = 1 To 4
 k2(j) = Cells(26, j + 2).Value
Next j
‘Зчитуємо зашифрований текст
ShifText = Range("B24").Value
Schet = 1 ‘Лічильник символів шифрування
‘Заповнюємо шифротаблицю в масив в зворотньому порядку
Schet = 1
 For j = 1 To 4
    j1 = k2(j)
    For i = 1 To 6
     Tabl1(i, j1) = Mid(ShifText, Schet, 1)
     Schet = Schet + 1
    Next i
Next j
‘Виводимо шифротаблицю на лист
For i = 1 To 6
  For j = 1 To 4
    Cells(i + 29, j + 2) = Tabl1(i, j)
  Next j
```

```
        Next i
        ‘Читаємо шифротаблицю по рядкам та формуємо розшифрований рядок тексту
        Schet = 1
        DeshifText = ""
        Sim = ""
            For i = 1 To 6
            i1 = k1(i)
             For j = 1 To 4
               Sim = Tabl1(i1, j)
               DeshifText = DeshifText + Sim
               Schet = Schet + 1
            Next j
            Next i
        Range("B38").Value = DeshifText
        End Sub
```

Очищення шифротаблиці резидента:

```
        Private Sub CommandButton5_Click() ‘Очистити шифротаблицю резидента
        For i = 1 To 6
          For j = 1 To 4
             Cells(i + 29, j + 2) = ""
           Next j
         Next i
         Range("B24").Value = ""
         Range("B38").Value = ""
        End Sub
```