3. ЗАХИСТ ДАНИХ

3.1. Створення резервних копій файлів. Зберігання копій.

3.2. видалення та відновлення даних.

3.3.Основні поняття криптографії. Шифрування та маскування даних.

3.1. Створення резервних копій файлів. Зберігання копій.

Для захисту інформації необхідно забезпечити її конфіденційність, цілісність та доступність. Одним із найвідоміших та простих методів запобігання втрати важливих даних є резервне копіювання файлів або бекап.

Даний процес забезпечує зберігання будь-якого важливого документа або інформації в окремому місці від оригіналу для уникнення втрати інформації. Якщо вихідний документ пошкоджений, можна відновити інформацію завдяки наявності копії, яка зберігалася в іншому безпечному місці.

Розрізняють такі типи резервних копій:

- резервна копія операційної системи;
- резервна копія логічного диску (розділу);
- резервна копія окремих файлів та папок — найпоширеніший спосіб резервного копіювання.

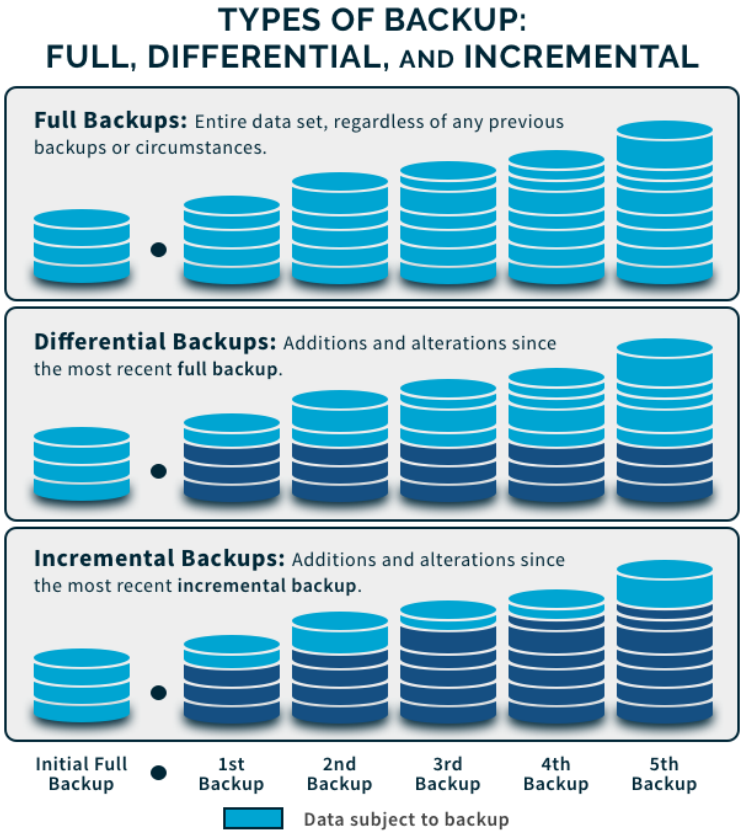
Можна навести й іншу класифікацію резервного копіювання.

Повне резервне копіювання (Full Backup або L0) – повна копія даних. Рівень, який забезпечує створення повної копії об’єкту резервного копіювання.

Цей рівень дозволяє забезпечити максимальну відповідність оригіналу даних його копії.

Диференційне резервне копіювання (Differential Backup або L1) – копіювання змін, що були зроблені після створення останньої повної копії. Створення такої копії потребує більше часу та займає більший об’єм, ніж додаткове копіювання, але дозволяє пришвидшити процес відновлення. Загалом є альтернативою між створенням повної або додаткової копії.

Додаткове резервне копіювання (Incremental Backup або L2) – копіювання змін, що відбулись із часу повного, диференційного або додаткового копіювання. Загалом на додаткове копіювання затрачається менше часу, бо копіюється менше файлів. Однак процес відновлення даних займає більше часу, оскільки повинні спочатку відновлюватися дані останньої повної копії і після цього — всі резервні копії, від яких залежить додаткова копія.



Компанія Eset надає такі поради. Після вибору типу бекапа, який найкраще підходить для Ваших потреб, важливо вирішити, яким чином слід зберігати. Протягом останніх 20 років типи носіїв, які найчастіше використовуються для зберігання даних, змінювалися та вдосконалювалися.

Найвідомішими серед них є перфокарти, дискети, оптичні носії, такі як CD, DVD та Blu-Ray, стрічки, зовнішні жорсткі диски, зберігання даних у хмарі. Під час вибору носія для зберігання власних резервних копій варто в першу чергу врахувати тривалість її зберігання відповідно до Ваших потреб. Наприклад, CD/CD-ROM, MD (Mini Disc) та DVD служать довше – 25-50 років. Після них йдуть HDD, SSD, USB флеш-накопичувачі та карти пам'яті з тривалістю зберігання 10 років. І найменший життєвий цикл до 10 років мають дискети та Blu-Ray диски.

Поширені помилки при резервному копіюванні файлів.

1. Невиконання процесу резервного копіювання важливих файлів. Такі дії – найпоширеніша помилка. Дуже часто резервне копіювання не було виконано через те, що інформація здавалася не важливою до моменту, поки вона не була втрачена.

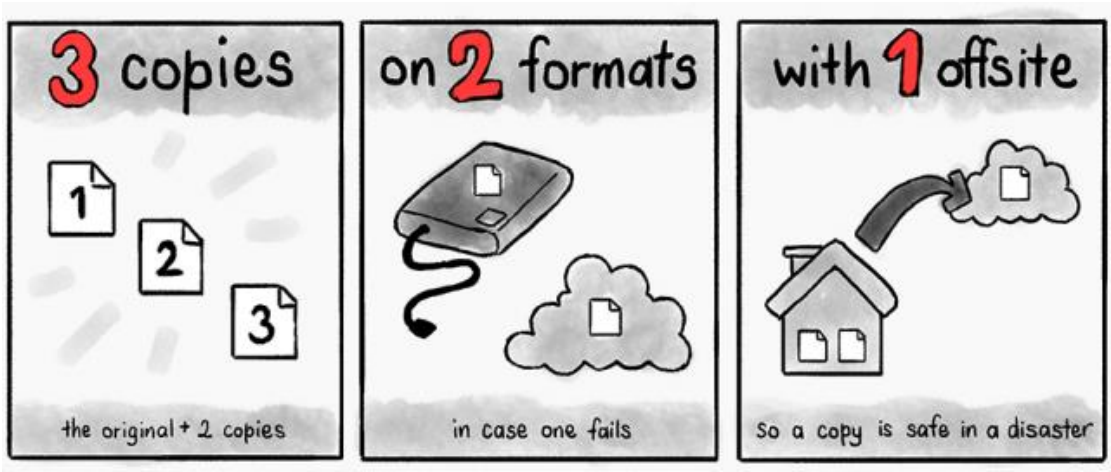
2. Збереження резервних копій на тому ж пристрої, що й оригінальні файли. Копія повинна зберігатися окремо від оригінальних документів. Якщо вони зберігаються на одному пристрої та обладнання пошкоджено, то резервні копії можуть бути втрачені разом із оригіналами.

3. Відсутність тестування. Створення резервної копії включає ряд процесів. Недостатньо просто створити копію – потрібно перевірити файли, щоб переконатися, що збережені дані фактично доступні в разі потреби. Оскільки під час зберігання вони можуть бути пошкоджені, то в цьому випадку потрібно зробити нове резервне копіювання.

4. Здійснення бекапа недостатньо часто. Важливо регулярно створювати резервні копії, особливо якщо інформація часто оновлюється.

5. Відсутність маркування файлів резервного копіювання. Під час бекапа важливо фіксувати, на якому обладнанні зберігаються певні дані. У разі необхідності відновлення даних записи допоможуть прискорити цей процес.

Фахівці радять для зберігання критично важливих даних керуватися законом «3-2-1»: три копії зберігати на двох різних носіях, один із яких – в офлайні.

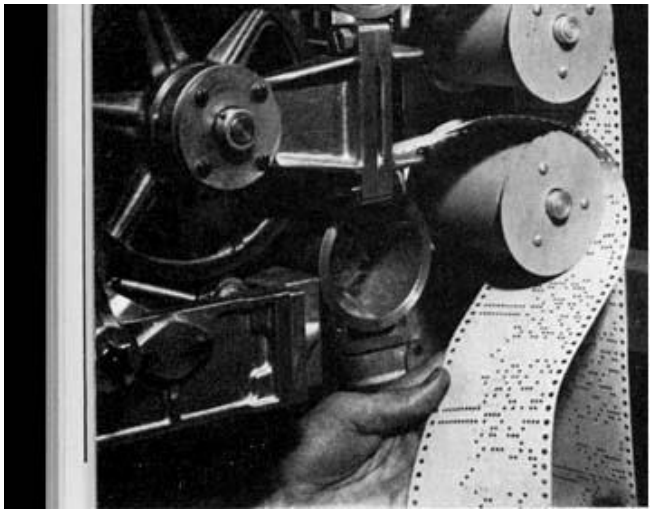


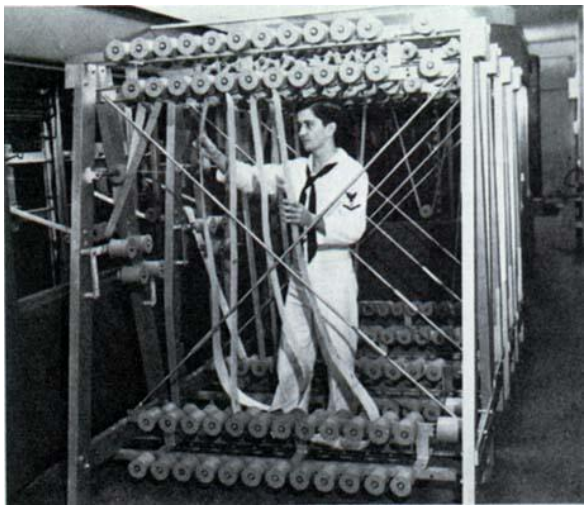
Слід уникати нестандартних способів зберігання (у всякому разі, як єдиного способу), рідких та пропрієтарних форматів, мов (наприклад, для документів краще використовувати ODF і TXT, а не DOCX чи DOC). Зберігати інформацію слід у стиснутих форматах і незашифрованому вигляді – інакше, навіть незначне пошкодження цілісності даних може зробити всю інформацію

недоступною. Наприклад, якщо потрібно надовго зберегти медіа файли, то для звуку краще буде WAV, для фотографій – RAW, TIFF та BMP.

З іншого боку, відсутність шифрування особливо важливих файлів може бути небезпечною!

Ще одна проблема – з часом пристрої зчитування інформації з носіїв стають застарілими.





1. Початковий рівень. Хмарні сховища. Наприклад, сервіс Mega. Безкоштовний акаунт дозволяє зберігати до 50 Гб інформації. Сервіс пропонує зручний десктоп-додаток. Він автоматично копіює в хмару всі зміни в папці. Інший, дуже популярний варіант – Googke-диск.

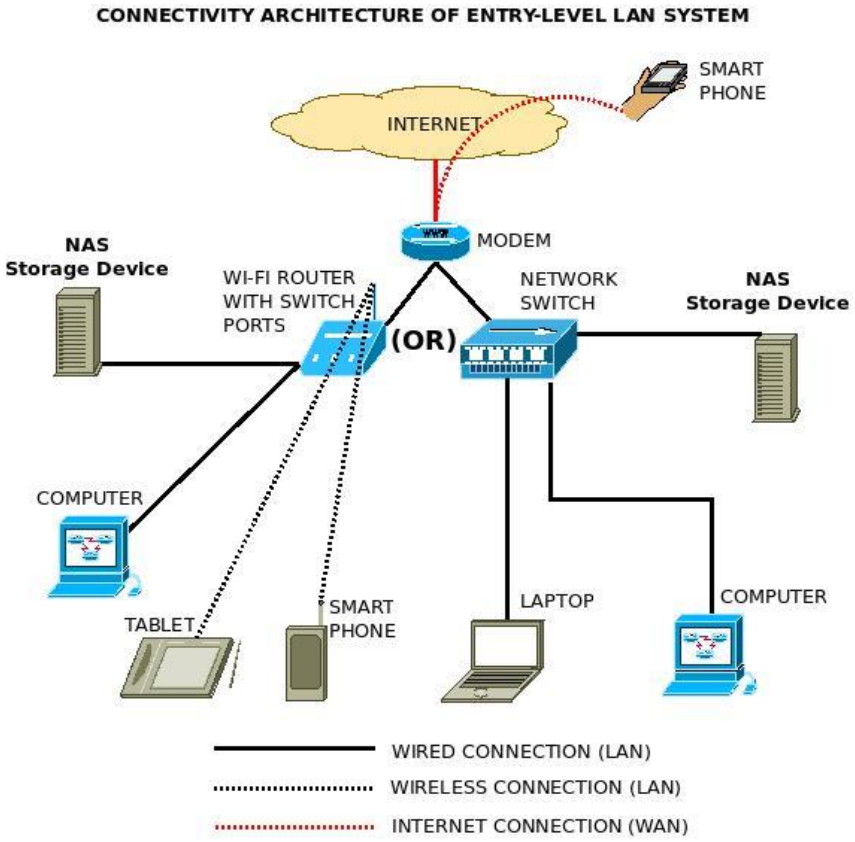
2. Напівпрофесійний рівень. Резервний жорсткий диск. Більшість фахівців із відновлення даних рекомендують для резервування критично важливих файлів використовувати додатковий жорсткий диск, причому саме HDD, а не SSD.

Фахівці не радять зберігати важливу інформацію на SSD-дисках, SD-картах т а USB-флешках, оскільки відновити інформацію з таких типів носіїв складно та вони мають менший термін працездатності в порівнянні з HDD.

3. Професійний рівень.

1) Для більш надійного зберігання доцільно скористатися сховищем даних типу NAS – Network Attached Storage. Жорсткі диски для NAS

відрізняються від інших великим ресурсом і спеціальними алгоритмами оптимізації читання та запису. Недоліком NAS є його висока ціна.



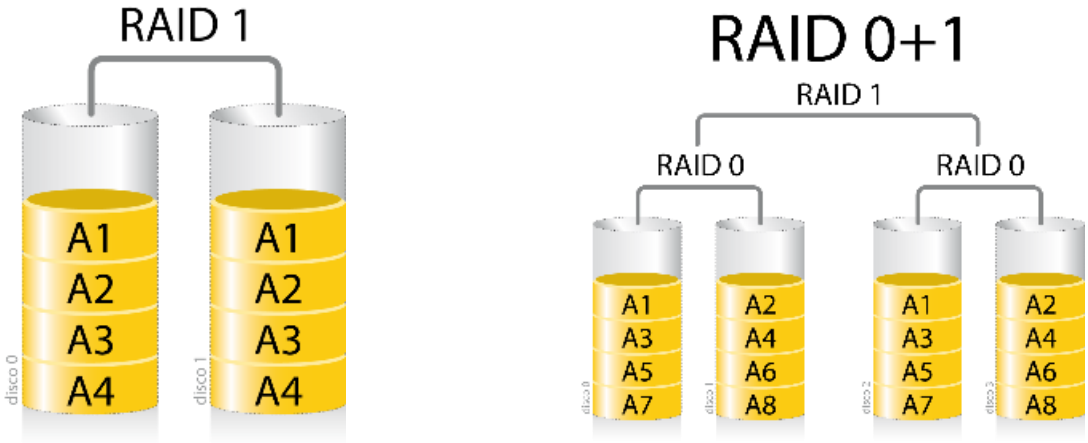
2) Технологія RAID (Redundant Array of Independent Disks) – це дисковий масив, об'єднання декількох жорстких дисків, для операційної системи вони будуть функціонувати як один, підвищуючи швидкість читання даних або надійність їх збереження. Всього існує 7 основних (типових) конфігурації (з номерами від 0 до 6) а також кілька комбінованих варіацій, наприклад, RAID 10 – комбінує розширюваність RAID 0 і надійність RAID 1.

Дискові масиви RAID 0 будуються мінімум із 2 дисків й використовують усі диски одночасно для зберігання на них файлів. Технологія за якою працює цей масив називається data striping, або розбивка даних. Суть полягає в тому що дані розбиваються на блоки фіксованого розміру і по черзі складаються на кожен диск. Тобто один файл може лежати шматочками на усіх дисках масиву. Таким чином досягається дуже висока швидкість читання, адже файл «збирається» вже не з одного (часто фрагментованого) диска, а одразу з декількох, хоча при запису швидкість, звичайно, менша ніж при роботі з одним

диском. При втраті одного диска з масиву дані безповоротно пошкоджуються, оскільки практично всі файли лежать одразу по всіх дисках.

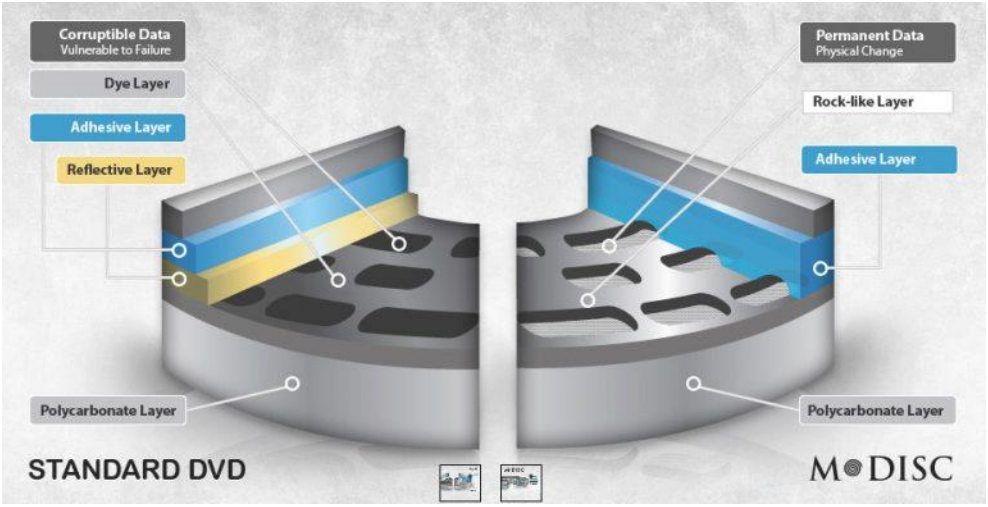
Масиви RAID 1 також будуються мінімум із 2 дисків. Технологія за якою працюють дискові масиви типу RAID 1 називається mirroring, або віддзеркалювання. Суть технології полягає в тому що всі дані лежать на одному диску, а інший працює як «двійник» тримаючи на собі повну копію основного диска. Таким чином, дана технологія забезпечує збереженість даних навіть при виході з ладу одного диска в масиві, що робить її ідеальною для зберігання на ній важливих даних, яким між тим не потрібен дуже швидкий доступ, оскільки в швидкості читання/запису вона програє навіть одиночним (які не стоять в RAID) дискам.

Доцільно, за можливості, поєднувати обидві технології.



4. Суто професіональний рівень.

1) M-Disc:



2) LTO-стрімер (стандарт Linear Tape-Open):

3.2. Видалення та відновлення даних.

З метою захисту файлів від видалення чи копіювання можна скористатися як засобами операційної системи так і допомогою спеціальних програм.

Для захисту комп’ютера від копіювання файлів на знімні носії необхідно внести певні зміни до реєстру операційної системи. Якщо необхідно заборонити видалення деяких файлів, то достатньо створити на локальному диску спеціальну папку, в якій будуть зберігатися файли, втрата яких є небажаною.

Окрім штатних засобів Windows, розроблена достатня кількість сторонніх програм, які можуть захистити файли від копіювання та видалення.

Відновлення видалених даних або, навпаки, видалення даних без можливості їх відновлення, суттєво залежить від типу накопичувача.

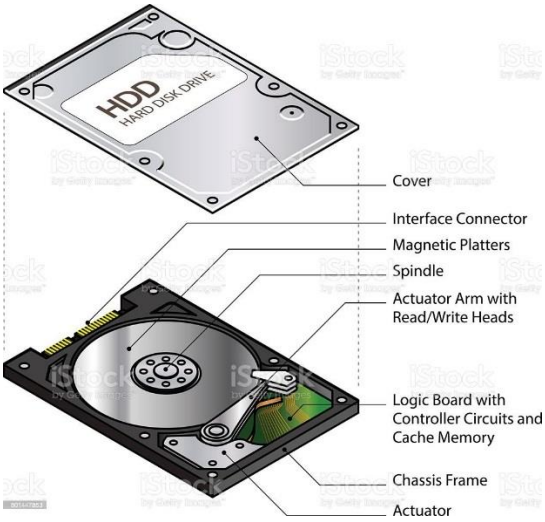
Дисковий накопичувач типу HDD (hard (magnetic) disk drive).

Процедура знищення певного файлу відбувається у кілька етапів:

1. ви видаляєте файл «X» (наприклад, через Кошик), і для користувача він зникає з папки.

2. Фізично «X» залишається на диску, але комірка, де він зберігається, отримує статус вільної.

3. При записі на диск нових файлів, комірка зі статусом «вільна» заповнюється, й відбувається затирання файлу «X» новим. Якщо ж комірка при збереженні нового файлу не використовувалася, то видалений раніше файл «X» продовжує фізично перебувати на жорсткому диску.



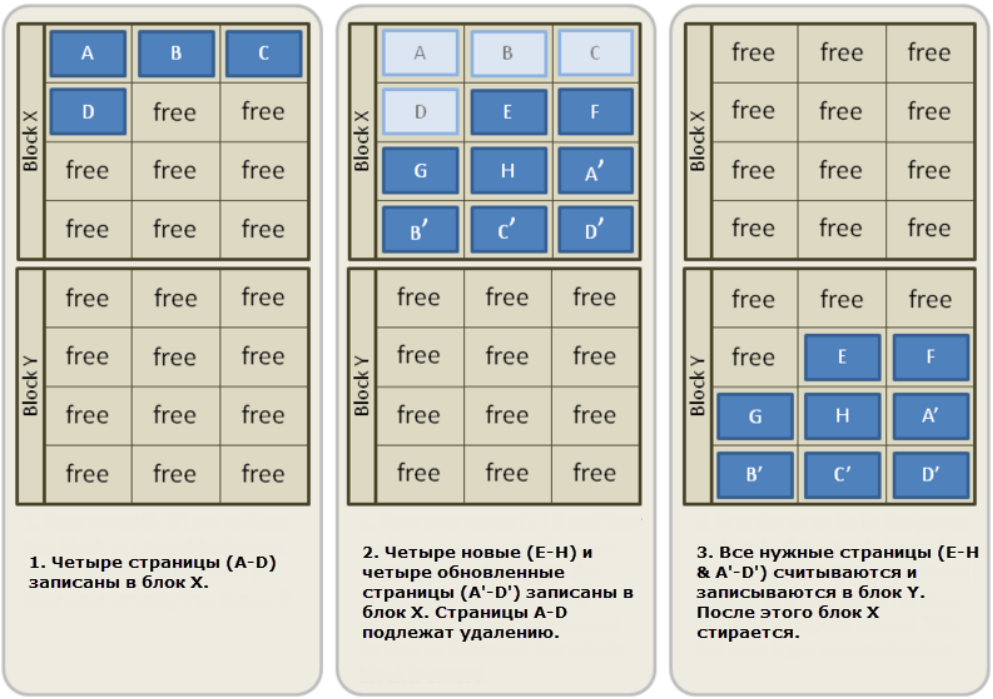
4. Після багаторазового перезапису даних у комірці (2-3 рази) видалений файл «X» буде остаточно знищенно. Якщо ж файл займає більше місця, ніж одна комірка, то, в такому випадку, буде знищено лише фрагмент файлу «X».

Отже, існує можливість досить легко відновити видалені файли за допомогою спеціальних програм. На успіх відновлення прямо впливає період часу від знищення до початку процедури відновлення, та інші чинники – кількість вільного місця на диску, чи записували ви великі файлі після знищення.

З іншого боку, для гарантованого видалення файлу, без подальшого відновлення, необхідно ініціювати його примусовий перезапис. Для цього існує чимало утиліт, проте найпростіше скористатися штатними засобами Вашої операційної системи.

Жорстки диски типу SSD (solid-state drive). Твердотілий накопичувач розбито на блоки (обсягом декілька мегабайт), блоки, у свою чергу, поділено на сторінки (обсягом декілька десятків кілобайт кожна). Сторінка може бути заповнена даними лише один раз, при цьому сторінки в межах блоку повинні програмуватися строго в порядку зростання їх номерів. Для повторного заповнення сторінки необхідно повністю стерти весь блок. Стерти лише частину блоку неможливо.

Логіка роботи накопичувача побудована таким чином, що сторінка, яка була видалена користувачем, фактично продовжує зберігати записану інформацію. Для запису нової інформації контролер ініціює процедуру, відому як Garbage Collection/TRIM, яка видаляє непотрібні дані й перерозподіляє існуючі. Для цього всі сторінки, за винятком непотрібної, копіюються на інший, вільний блок, тоді як перший блок повністю стирається. Далі актуальні сторінки переносяться назад до першого блоку, видаляються з другого, і лише після цього нові дані остаточно займають своє місце.



Для прискорення роботи SSD, при наявності вільного місця, нові файли відразу записуються на вільні сторінки, а оптимізація сміття відкладається до моменту простою накопичувача.

висновки:

1. Якщо інформація була дійсно фізично знищена в пам’яті накопичувача, вона не підлягає відновленню за жодних обставин.

2. Навіть якщо процедуру оптимізації сміття не було завершено, користувач не зможе отримати доступ до неочищених сторінок (за винятком наявності спеціального обладнання).

3. В абсолютній більшості випадків відновити файли, які були видалені з SSD-накопичувача, не вдасться.

4. Якщо накопичувач чи операційна система (наприклад, Windows XP) чи протокол (наприклад, при роботі з usb) не підтримує команду TRIM, або вона не включена, то відновлення видаленої інформації можливе.

5. Для видалення даних без можливості їх подальшого відновлення необхідно виконати форматування диску чи скористатися відповідною утілитою від виробника.

USB flash-накопичувач, карта пам’яті. Ці накопичувачі мають наступні правила: пам’ять розділена на блоки розміром декілька мегабайт; перед

записом у блок пам’яті його необхідно очистити від вже існуючих даних; блок складається зі сторінок, розміром у десятки кілобайт; запис даних у блок проводиться сторінками, одночасно може бути записана відразу вся сторінка даних; сторінки даних усередині одного блоку повинні записуватись строго у порядку зростання їх номерів; кожна сторінка після стирання блоку може бути записана лише один раз до наступного стирання.

Отже, при видаленні файлу фактично він не знищується. Натомість система позначає його як видалений, а відповідну частину дискового простору – як вільне місце для використання новими файлами. Доки ці кластери не будуть перезаписані іншими файлами, видалений файл можна відновити, особливо, якщо накопичувач має багато вільного місця, а процедура відновлення проводиться негайно після видалення.

Методи відновлення/знищення даних засновані на певних фізичних процесах, із використанням відповідного обладнання чи на застосуванні спеціалізованого програмного продукту (наприклад, Transcend RecoveRx, Recuva, Ashampoo Undeleter, MiniTool Power Data Recovery).

Принцип роботи програм відновлення даних наступний: необхідно визначити носій, на якому розташовано видалені файли. Це може бути весь жорсткий диск, USB-накопичувач або лише певні папки. Доцільно максимально звузити пошук. Введіть індивідуальні умови пошуку та встановіть різні фільтри, такі як тип інформації: музика, відео або контакти. Також можна вказати розмір файлу або дату, наприклад, певний період часу. Після цього почніть пошук. Далі з’явиться індикатор стану чи кількість результатів, вони будуть показані відповідно до різних критеріїв. Програми відновлення даних зазвичай вказують ймовірність повного відновлення та збереження файлу. виберіть потрібні файли та вкажіть папку, в яку вони мають бути відновлені, а далі дотримуйтесь інструкцій на екрані.

Важливо: не відновлювати інформацію на той самий носій, де вона зберігалася до видалення.

Для надійного видалення інформації використовується наступна процедура: на носій здійснюється запис випадковим чином згенерованої інформації, запис виконується декілька разів (залежно від обраного режиму), наприклад, алгоритм Міністерства оборони США DoD 5220.22-M: перезапис комбінаціями цифр, що передбачає до 7 циклів чи алгоритм за методом Гутмана, перезапис комбінаціями цифр у 35 циклів. Вважається, що однократного перезапису недостатньо для гарантованого знищення даних. Збалансованим з точки зору пари «час – надійність» є трикратний цикл перезапису. Метод Гутмана триває дуже довго, переважно більше доби, але це максимально безпечний алгоритм.

Приклади програм для видалення інформації: CCleaner, Eraser, File Shredder, Alternate File Shredder.

Програма Eraser, наприклад, надійно видаляє файли і папки, очищає вільний дисковий простір. Користувач може вибирати один із 14 алгоритмів видалення на власний розсуд. Програма вбудовується в контекстне меню операційної системи.

Важливо: єдиний надійний спосіб видалити всі дані з жорсткого диска без можливості відновлення – проведення повного форматування зі зміною типу файлової системи. Наприклад, якщо необхідно видалити без можливості відновлення зображення, але при цьому в ОС включено відображення ескізів, то просте видалення файлу не допоможе. Обізнана людина зможе відновити його, використовуючи файл Thumbs.db, що зберігає в собі ескізи фото. Аналогічна ситуація і з файлом підкачки та іншими системними документами, які містять у собі копії чи ескізи даних користувача.

3.3.Основні поняття криптографії. Шифрування та маскування даних.

Криптографія – наука про математичні методи забезпечення конфіденційності, цілісності та автентичності інформації. виникла з практичної потреби передавати важливі відомості найнадійнішим чином. Тривалий час під

криптографією розумілось лише шифрування – процес перетворення звичайної інформації в абстрактні конструкції.

Відкритий (вихідний) текст – дані (не обов’язково текстові), що передаються без використання криптографії.

Шифротекст, шифрований (закритий) текст – дані, отримані після застосування криптосистеми (зазвичай – з деяким ключем).

Ключ – параметр шифру, що визначає вибір конкретного перетворення даного тексту.

Шифр, криптосистема – сімейство оборотних перетворень відкритого тексту в шифрований.

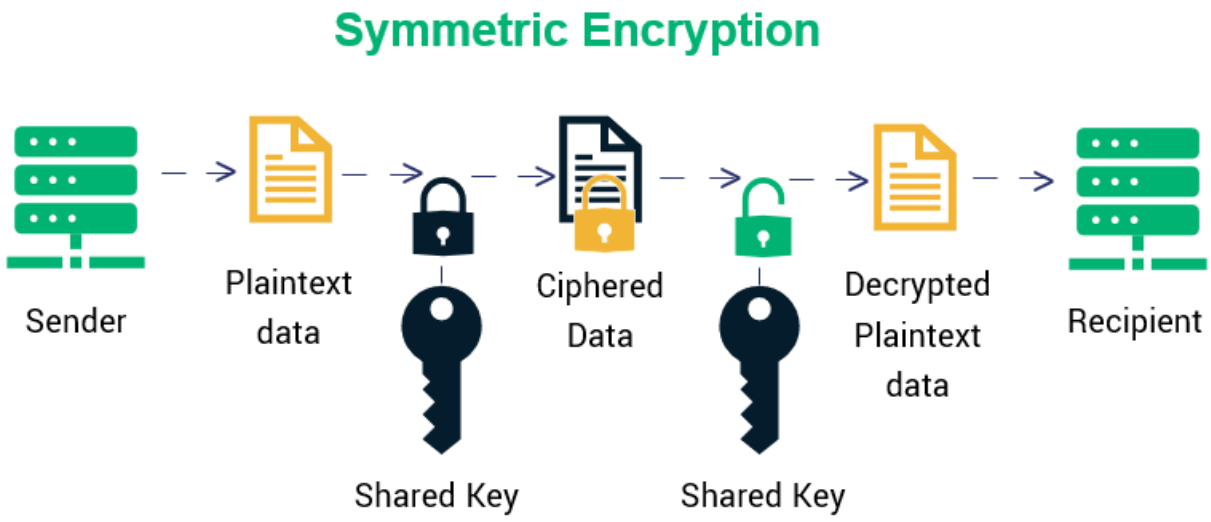
Шифрування – процес нормального застосування криптографічного перетворення відкритого тексту на основі алгоритму та ключа, в результаті якого виникає шифрований текст. Розшифрування – процес нормального застосування криптографічного перетворення шифрованого тексту у відкритий.

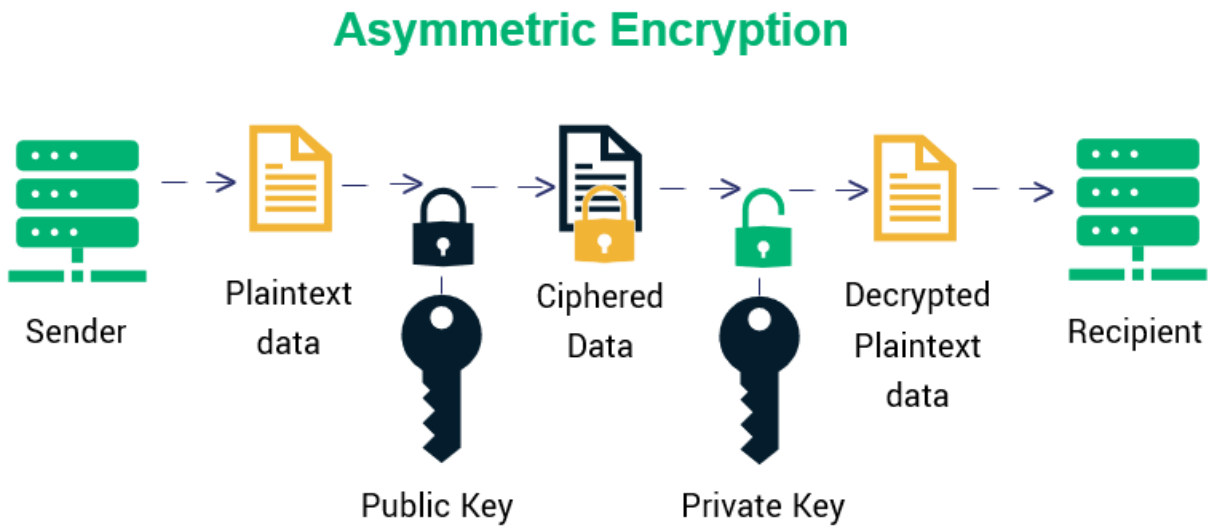
В симетричних криптосистемах для шифрування та розшифровуння інформації використовується один і той же загальний секретний ключ, яким взаємодіючі сторони заздалегідь обмінюються по деякому захищеному каналу.

Асиметричні криптосистеми характерні тим, що в них використовуються різні ключі для шифрування та розшифровуння інформації:

- закритий ключ (private key) – ключ, що відомий лише своєму власнику, одержувач, будучи монопольним власником закритого ключа (для розшифровування), буде єдиним, хто зможе розшифрувати призначені для нього повідомлення;

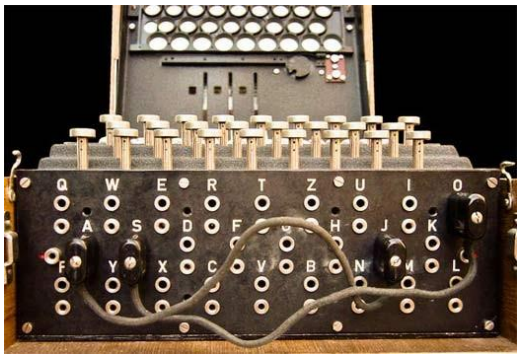
- відкритий ключ (public key) – ключ, який є загальнодоступним, будь-хто може зашифровувати повідомлення для певного одержувача.





Головна властивість ключової пари: по закритому ключу легко обчислюється відкритий ключ, але, маючи відкритий ключ практично неможливо вирахувати закритий ключ.

В алгоритмах, що використовуються для реалізації цифрового підпису ролі закритого та відкритого ключів змінюються на протилежні: візування електронного документа відбувається приватним ключем автора документа, а перевіряється загальнодоступним публічним ключем. Таким чином будь-хто може перевірити достовірність авторства певної особи. Таким чином, асиметричні алгоритми, можуть забезпечувати не тільки конфіденційності та цілісності інформації, але і її автентичність.



Зазвичай пакети офісних програм (зокрема, Microsoft Office, LibreOffice) мають засоби для захисту текстових документів, електронних таблиць, презентацій тощо шляхом шифрування. В залежності від цілей користувача, передбачено захист файлу від відкриття чи захист від редагування. В останньому випадку передбачаються такі ступені захисту:

- лише перегляд змісту;
- заборона змін, окрім коментарів;
- фіксування записи виправлень – внесення змін дозволено, але вони фіксуються і можуть бути скасовані автором;
- дозвіл введення даних тільки в поля форм (у вибіркові розділи документа).

Утілити-архіватори та програми перегляду файлів формату pdf також можуть встановлювати парольний захист на відкриття чи редагування документів.

Можна скористатися й онлайн-сервісами для встановлення парольного захисту документів.

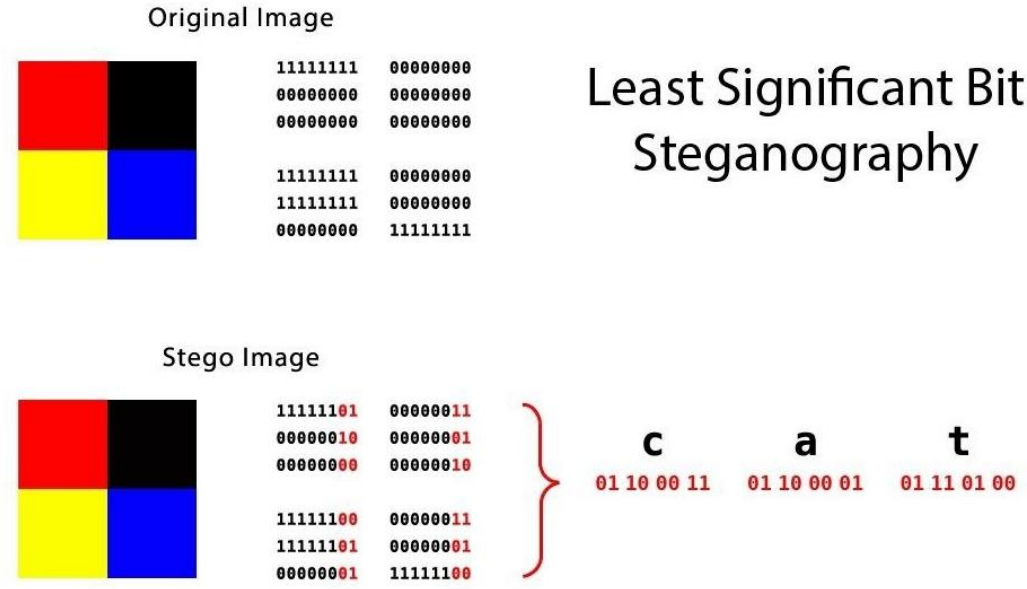
Важливо: такий захист є не дуже надійним й може бути скасований, в окремих випадках, навіть без застосування спеціальних інструментів.

При виборі програми для шифрування файлів та дисків доцільно обрати ту, яка існує вже багато років, поширюється у вигляді вихідних текстів, використовує стійкі алгоритми, коректно їх реалізує, причому ця реалізація була проаналізована кількома незалежними фахівцями з криптографії. Наприклад, Encrypto, VeraCrypt AxCrypt.

Стеганографія – це наука про приховану передачу інформації шляхом збереження в таємниці самого факту передачі. На відміну від криптографічного захисту, коли у зловмисника існує можливість знайти, перехопити та зробити спробу дешифрувати криптограму, стеганографічні методи дозволяють вмонтувати інформацію, що передається, в невинні на вигляд послання так, щоб не можна було навіть запідозрити існування підтексту.

Шанси знайти приховане повідомлення невеликі, але на той випадок, якщо повідомлення буде виявлено, його можна ще додатково зашифрувати. У цьому випадку стеганографія являє собою більш високий рівень захисту інформації в порівнянні з методами криптографії.

Науково-технічний прогрес дозволив стеганографії зайняти певну нішу у галузі захисту інформації, з'явився такий напрям в області захисту інформації, як комп'ютерна стеганографія. Комп'ютерна стеганографія, враховуючи природні неточності пристроїв дискретизації і надмірність аналогового відео або аудіо сигналу, дозволяє приховувати повідомлення в комп'ютерних файлах (контейнерах, наприклад, зображення чи звуковий файл – у файлі WAV, MP3 або у відео файлі).



Також треба зазначити, що без спеціальних засобів збережену інформацію не можливо отримати із файла-контейнера.

У сучасному інформаційному просторі стеганографічні системи активно використовуються для вирішення таких основних завдань:

1) захист конфіденційної інформації від несанкціонованого доступу;

2) подолання систем моніторингу та управління мережевими ресурсами;

3) камуфлювання програмного забезпечення;

4) захист авторського права на деякі види інтелектуальної власності.

Стеганографічні методи також спрямовані на протидію системам моніторингу та управління мережевими ресурсами промислового шпигунства, дозволяють протистояти спробам контролю над інформаційним простором при проходженні інформації через сервери керування локальних і глобальних обчислювальних мереж. Для корпорацій та державних відомств, що зберігають важливі масиви даних, це одна із неоціненних функції стеганографії.

Іншим важливим завданням стеганографії є камуфлювання програмного забезпечення. У тих випадках, коли використання ПЗ незареєстрованими користувачами є небажаним, воно може бути закамуфльовано під стандартні універсальні програмні продукти (наприклад, текстові редактори) або приховано в файлах мультимедіа (наприклад, у звуковому супроводі комп'ютерних ігор).

Прикладом використання стеганографії у захисті авторського права від піратства є нанесення спеціальної мітки на комп'ютерні графічні зображення. Мітка залишається невидимою для очей людини, але розпізнається спеціальним ПЗ, яке вже використовується в комп'ютерних версіях деяких журналів. Даний напрямок стеганографії призначений не тільки для обробки зображень, але і для файлів з аудіо- та відео-інформацією й забезпечує захист інтелектуальної власності.

Для приховування інформації у цифровому вигляді за допомогою стеганографії існують спеціальні алгоритми. Внесення нової інформації у вже наявні файли (наприклад, мультимедійні) призводить до спотворенн, які перебувають нижче порогу чутливості людини, тому це не викликає помітних змін у сприйнятті вхідних файлів.

На тепер найбільш поширеним, але найменш стійким є метод заміни найменших значущих бітів або LSB-метод (Least Significant Bit, найменший значущий біт). Він полягає у використанні похибки дискретизації, яка завжди існує в оцифрованих зображеннях, аудіо– або відеофайлах. Дана похибка дорівнює найменшому значущому розряду числа, що визначає величину колірної складової елемента зображення (пікселя). Тому модифікація молодших бітів в більшості випадків не викликає значної трансформації зображення і не виявляється візуально. Так, наприклад, одна секунда оцифрованого звуку з частотою дискретизації 44100Гц та 8-бітним рівнем відліку у стереорежимі дозволяє приховати за рахунок зміни найменш значимих молодших розрядів повідомлення у 10 Кбайт.

Іншим популярним методом вбудовування повідомлень є використання особливостей форматів даних із стисненням з втратою даних (наприклад JPEG). Цей метод (на відміну від LSB) більш стійкий до геометричних перетворень і виявленню при передачі, так як є можливість в широкому діапазоні варіювати якість стислого зображення, що робить неможливим визначення походження спотворення.

При побудові стегосистеми необхідно враховувати:

1) зловмисник має повне уявлення про стегосистему і деталі її реалізації, єдиною інформацією, яка залишається невідомою, є ключ, за допомогою якого тільки його власник може встановити факт наявності і зміст прихованого повідомлення;

2) якщо зловмисник якимось чином дізнається про факт існування прихованого повідомлення, це не повинно дозволити йому отримати подібні повідомлення в інших даних до тих пір, доки ключ зберігається у таємниці;

3) потенційний зловмисник повинен бути позбавлений будь-яких технічних та інших переваг у розпізнаванні або розкритті змісту таємних повідомлень.

У якості контейнера (повідомлення) може використовуватися будь-яка інформація призначена для приховування таємних повідомлень.

Повідомленням може бути як текст або зображення, так і, наприклад, аудіодані (файли мультимедіа) тощо. Порожній контейнер – контейнер без вбудованого повідомлення; заповнений контейнер (стег) – контейнер, що містить вбудовану інформацію. Вбудоване (приховане) повідомлення – повідомлення, яке вбудовується в контейнер. Стеганографічний канал або просто стегоканал – канал передачі стег. Стегоключ або просто ключ – секретний ключ, необхідний для приховування інформації. В залежності від кількості рівнів захисту (наприклад, вбудовування попередньо зашифрованого повідомлення) в стегосистеми може бути один або декілька стегоключів.

За аналогією з криптографією, за типом стегоключа стегосистеми можна поділити на системи з секретним ключем та системи з відкритим ключем.

Отже, стегосистема має відповідати таким вимогам:

1) властивості контейнера повинні бути модифіковані таким чином, щоб зміни неможливо було виявити при візуальному контролі, що визначає якість приховування повідомлення (для безперешкодного проходження стегоповідомлення каналами зв’язку воно не повинно привернути увагу);

2) стегоповідомлення повинно бути стійким до спотворень, в тому числі і до зловмисних (у процесі передачі зображення, звука або використання інших контейнерів можуть відбуватися різні трансформації зі зменшення або збільшення, перетворення в інший формат, ущільнення, в тому числі і з використанням алгоритмів з втратою даних тощо);

3) для збереження цілісності вбудованого повідомлення необхідно використовувати коди з виправленням помилок;

4) для підвищення надійності вбудоване повідомлення має бути продубльовано.