**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ**

**КАФЕДРАКОМП’ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ**

ДОПУСТИТИ ДО ЗАХИСТУ

Завідувач кафедри

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.В. Ільєнко

«\_\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_ 2020 р.

**МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА**

**ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ**

**«МАГІСТР»**

Тема: «Розподілена система резервного копіювання з шифруванням»

Виконав: студент 241-М групи \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Слободянюк Б.О.

Керівник: д.ф.-м.н., професор\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Азаренко О.В.

Нормоконтроль з ЄСКД (ЄСПД):\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Єгоров С.В.

**Київ 2020**

**НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ**

**Факультет:** Кібербезпеки, комп’ютерної та програмної інженерії

**Кафедра:** Компютеризованих систем захисту інформації

**Освітній ступінь:** Магістр

**Спеціальність:** 125 «Кібербезпека»

**Освітньо-професійна програма**: «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ

Завідувач кафедри

\_\_\_\_\_\_\_\_\_\_\_\_\_ А.В. Ільєнко

«\_\_» \_\_\_\_\_\_\_\_\_ 2020 р.

**ЗАВДАННЯ**

**на виконання магістерської атестаційної роботи**

**магістранта Слободянюка Богдана Олеговича**

1. Тема роботи «Розподілена система резервного копіювання з шифруванням»

затверджена наказом ректора від 02.10.2019 р. № 2265/ст.

1. Термін виконання роботи: з 16.10.2019 р. по 10.02.2020 р.
2. Вихідні дані роботи: дані про інформаційно-комунікаційну систему та локальну мережу для забезпечення збереження резервних копій.
3. Зміст пояснювальної записки: аналітичний огляд літературних джерел з тематики диплому. Проведення аналізу нормативно-правового забезпечення України та міжнародних стандартів в сфері захисту інформації. Надання рекомендацій щодо посилення захисту системи. Опис процесу розробки програмного додатку мовою програмування Java.
4. Перелік обов'язкового ілюстративного матеріалу: презентація PowerPoint.
5. Календарний план-графік

|  |  |  |  |
| --- | --- | --- | --- |
| № пор | Завдання | Термін виконання | Відмітка про виконання |
| 1 | Уточнення постановки задачі | 16.10.2019 | *Виконано* |
| 2 | Аналіз літературних джерел | 16.10.2019 - 22.10.2019 | *Виконано* |
| 3 | Обґрунтування вибору рішення | 22.10.2019 -24.10.2019 | *Виконано* |
| 4 | Збір інформації | 25.10.2019 - 15.11.2019 | *Виконано* |
| 5 | Аналіз даних та їх класифікація | 16.11.2019 - 27.11.2019 | *Виконано* |
| 6 | Ознайомлення із поширеними методами реалізації резервного копіювання | 28.11.2019 - 08.12.2019 | *Виконано* |
| 7 | Розробка структурно-логічної моделі програмного додатку | 09.12.2019 – 18.12.2019 | *Виконано* |
| 8 | Створення програмної реалізації розробленої моделі | 19.12.2019 – 27.12.2019 | *Виконано* |
| 9 | Тестування та оцінка ефективності створеного додатку | 28.12.2019 – 22.01.2020 | *Виконано* |
| 10 | Проаналізувати існуючі аналоги | 23.01.2020 – 25.01.2020 | *Виконано* |
| 11 | Перевірка на антиплагіат | 26.01.2019 – 27.01.2020 | *Виконано* |
| 12 | Оформлення і друк пояснювальної записки | 28.01.2020 | *Виконано* |
| 13 | Оформлення презентації | 29.01.2020 | *Виконано* |
| 14 | Отримання рецензій від рецензента | 30.01.2020 | *Виконано* |
| 15 | Захист в ЕК | 05.02.2020 | *Виконано* |

Магістрант Б. Слободянюк

(підпис, дата)

Науковий керівник О. Азаренко

(підпис, дата)

**РЕФЕРАТ**

Магістерська атестаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатків і має 72 сторінки основного тексту, 15 рисунків, 2 таблиці, к сторінки додатків. Список використаних джерел містить 42 найменування і займає 4 сторінки. Загальний обсяг роботи 90 сторінок.

Предмет дослідження: захищеність даних від втрати, що забезпечується завдяки резервному копіюванню.

Об’єкт дослідження: дані або сукупності даних, процес створення резервних копій та відновлення даних.

Мета дипломної роботи: вирішення задачі зберігання та відновлення даних без використання спеціальних серверів та послуг, що надаються сторонніми компаніями, а також розробка програмного додатку для обміну резервними копіями між комп’ютерами локальної мережі peer-to-peer.

Методи дослідження: аналіз, порівняння.

Технічні та програмні засоби: ОС сімейства Windows, IntellijIDEA.

Отримані результати та їх новизна: проаналізовано існуючі рішення задачі резервного копіювання в мережахpeer-to-peer, розроблено програмний додаток, що дозволяє створювати резервні копії файлів та зберігати їх на інших комп’ютерах мережі у зашифрованій формі.

Значущість виконаної роботи та висновки: реалізовано можливістьзбереження та відновлення окремого файлу або цілої папки на вказаний момент часу, створено зручний для користувача інтерфейс.

Рекомендації щодо використання результатів: розроблене програмне забезпечення є готовим продуктом, який може використовуватися як рядовими користувачами, так і комерційними організаціями з метою збереження і захисту інформації.

Галузь застосування та ступінь впроваження матеріалів дипломної роботи: інформаційні технології.

**ЗМІСТ**

[ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ 7](#_Toc30032384)

[ВСТУП 8](#_Toc30032385)

[РОЗДІЛ 1 10](#_Toc30032386)

[ОСНОВНІ ШЛЯХИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ. 10](#_Toc30032387)

[1.1 Основні шляхи забезпечення безпеки інформації. 10](#_Toc30032388)

[1.1.1 Концепція захисту інформації 10](#_Toc30032389)

[1.1.2 Стратегія та архітектура захисту інформації 11](#_Toc30032390)

[1.1.3 Політика безпеки інформації 13](#_Toc30032391)

[1.1.4 Види забезпечення безпеки інформації 19](#_Toc30032392)

[1.2 Нормативно-правова база у сфері захисту інформації 22](#_Toc30032393)

[1.2.1 Закон України «Про інформацію» 22](#_Toc30032394)

[1.2.2 Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» 31](#_Toc30032395)

[1.3 Висновки по розділу 37](#_Toc30032396)

[РОЗДІЛ 2 38](#_Toc30032397)

[РЕЗЕРВНЕ КОПІЮВАННЯ ТА ВІДНОВЛЕННЯ ДАНИХ. ЗАХИСТ ДАНИХ 38](#_Toc30032398)

[2.1 Визначення даних 38](#_Toc30032399)

[2.2 Резервне копіювання 39](#_Toc30032400)

[2.2.1 Об'єкти резервного копіювання 39](#_Toc30032401)

[2.2.2 Вимоги для відновлення даних. 39](#_Toc30032402)

[2.2.3 Рівні резервного копіювання. 40](#_Toc30032403)

[2.2.4 Ціліснісність резервних копій даних. 41](#_Toc30032404)

[2.2.5 Методи передачі резервних копій. 42](#_Toc30032405)

[2.2.6 Методи створення копії даних. 42](#_Toc30032406)

[2.2.7 Зберігання резервної копії. 43](#_Toc30032407)

[2.3 Відновлення даних 44](#_Toc30032408)

[2.3.1 Способи відновлення. 44](#_Toc30032409)

[2.4.1 Оцінка ризику 51](#_Toc30032410)

[2.4.2 Створення плану ВД 52](#_Toc30032411)

[1.Планування 53](#_Toc30032412)

[2.Визначення КД 54](#_Toc30032413)

[3.Створення необхідних політик та процедур 56](#_Toc30032414)

[4.Визначення типу (типів) резервних копій 56](#_Toc30032415)

[5.Розробка процесів відновлення 57](#_Toc30032416)

6.[Варіанти збереження даних 57](#_Toc30032417)

[2.5 Висновки по розділу 63](#_Toc30032418)

[РОЗДІЛ 3 65](#_Toc30032419)

[РОЗРОБКА ПРОГРАМНОГО ДОДАТКУ 65](#_Toc30032420)

[3.1 Платформа реалізації 65](#_Toc30032421)

[3.2 Загальні відомості 67](#_Toc30032422)

[3.3 Робота з програмою 71](#_Toc30032423)

[ВИСНОВКИ 77](#_Toc30032424)

[СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ ВИКОРИСТАНИХ ДЖЕРЕЛ 78](#_Toc30032425)

[Додаток А. Програмна реалізація розподіленої системи резервного копіювання (p2pclient.java) 79](#_Toc30032426)

# 

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

АВ – Аварійне відновлення;

ВД – Відновлення даних;

ЗД – Захист даних;

ЗІ – Захист інформації;

ІД – Інформаційна діяльність;

КД – Критичні дані;

ОС – Операційна система;

РК – Резервне копіювання.

# 

# ВСТУП

**Актуальність**. Різні технології захисту даних (ЗД) від втрати або пошкодження за допомогою створення резервних копій використовуються давно і успішно запобігають матеріальному (а часто і моральному) збитку власників інформації, починаючи від звичайних користувачів автоматизованих систем, і закінчуючи великими світовими корпораціями. Терабайти даних копіюються і зберігаються на різноманітних носіях, будь то ваш особистий жорсткий диск або флешка, спеціально виділена машина, яка виконує роль сервера резервного копіювання у вашій мережі, або навіть так звана «хмара», яка по суті також є сервером (частіше - декількома серверами), наданим третьою стороною.

Однак, ціна на подібне «задоволення» від надійних вендорів навіть для невеликої компанії може досягати декількох тисяч доларів США. Самостійне додавання спеціального сервера в мережу для зберігання важливих даних, а також його налагодження та обслуговування, вимагає чималих зусиль і спеціальних знань з боку системного адміністратора. Поява такого сервера підвищує навантаження на мережу і частина обчислювальних ресурсів і систем зберігання даних випадає з продуктивного використання. Виникає питання: чи можна зберегти цінну інформацію, не звертаючись до дорогих комерційних рішень і не використовуючи спеціалізовані системи?

Таким чином, актуальність задачі забезпечення захищеності даних за допомогою резервного копіювання пов’язана з необхідністю отримати можливість резервного копіювання та відновлення даних (ВД) без використання спеціальних серверів та послуг, що надаються сторонніми компаніями.

Маємо однорангову (peer-to-peer) мережу резервного копіювання з трьох або більше комп'ютерів. Учасники мережі резервного копіювання не мають централізованого управління і не залежать від виділеного сервера. Цінна інформація співробітників компанії зберігається окремо на закріплених за ними системах і контролюється особисто користувачами систем. Адміністратор мережі резервного копіювання відсутній.

Рішення: проводити резервне копіювання (РК) за допомогою розподілу інформації, що копіюється, між доступними системами в мережі (або порівну, або в залежності від вільної пам'яті на кожному окремо взятому комп'ютері) за допомогою спеціального програмного забезпечення.

**Метою роботи є** вирішення задачі зберігання та відновлення даних без використання спеціальних серверів та послуг, що надаються сторонніми компаніями, а також розробка програмного додатку для обміну резервними копіями між комп’ютерами локальної мережі peer-to-peer.

**Галузь застосування** є інформаційні технології.

**Об’єктом дослідження** дані або сукупності даних, процес створення резервних копій та відновлення даних.

**Предметом дослідження** є захищеність даних від втрати, що забезпечується завдяки резервному копіюванню.

**Методи дослідження** аналіз, порівняння.

**Новизна одержаних результатів полягає в наступному:** проаналізовано існуючі рішення задачі резервного копіювання в мережах peer-to-peer, розроблено програмний додаток, що дозволяє створювати резервні копії файлів та зберігати їх на інших комп’ютерах мережі у зашифрованій формі.

# РОЗДІЛ 1

# ОСНОВНІ ШЛЯХИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ.

В Інтернеті відбувається переплетіння величезного потоку користувачів. Тому сьогодні мережа Інтернет стала універсальним способом і засобом зберігання інформації. Процес обміну даними став набагато простішим, швидшим та в багатьох випадках безкоштовним.

Проте чи замислювалися ви над питанням, скільки різної інформації розміщується в соціальних мережах кожного дня: починаючи з дати та місця народження, навчання, роботи та завершуючи тим, де ви проводите свої вихідні та відпочиваєте? Сьогодні ми ділимося з Інтернетом майже всіма аспектами нашого життя. Та чи можемо ми бути впевнені, що наші персональні дані в мережі Інтернет стовідсотково будуть захищенні?

Цікаво, що Іспанія гарантує своїм громадянам право на доступ до Інтернету в будь-якому місці. Мобільні безкоштовні точки доступу розміщені в багатьох містах. Також подібні права існують в Естонії, Франції, Фінляндії та Греції. Здатність людей отримувати доступ до інформації через використання інформаційних технологій – це найважливіша передумова для участі в інформаційному суспільстві.

Однак враховуючи весь обсяг інформації, що ми розміщуємо у популярних мережах. Мережеві гіганти зберігають та контролюють більше даних про повсякденне життя та соціальні взаємодії людей, ніж свого часу мали тоталітарні уряди XX століття. Тому наразі стає популярним питання захисту персональних даних особи.

Право на захист персональних даних та конфіденційність є старим основоположним правом людини, яке отримало нову та особливу актуальність з поширенням і розвитком інформаційних технологій. Саме це право нам гарантує Закон «Про захист персональних даних», у поточній редакції від 01 січня 2017 року.

Суть проблеми полягає в тому, що при використанні Інтернету або мобільних телефонів значні обсяги персональних даних часто обробляються, а буває і передаються, без чіткої згоди чи навіть інформування про їх обробку.

Яскравим прикладом є пошукова система: одного разу здійснивши пошук готелю в іншому місті, Інтернет пропонуватиме вам різноманітні готелі вже на інших сайтах у вигляді реклами. Таке запам’ятовування наших рухів у мережі значно полегшує подальше життя. Водночас є негативні аспекти: існує величезна кількість потенційних зловживань за допомогою володіння нашими даними, які можуть коливатися від прямого визначення змісту нашої інформації за допомогою цільової реклами до свідомої та зловмисної маніпуляції з тим, що ми бачимо та здійснюємо в Інтернеті, що призводить до впливу на нашу свідомість, як споживача.

Забезпечення кібербезпеки почало врегульовуватися на національному рівні. Нещодавно світ побачив новий Закон України «Про основні засади забезпечення кібербезпеки України». Метою цього закону є створення національної системи кібербезпеки, яка сприятиме захисту важливих інтересів суспільства та держави. Закон оперує важливими поняттями, визначає основні об’єкти такого захисту та виділяє ключових осіб, які повинні слідкувати за реалізацією такого захисту. Проте після ознайомлення з текстом цього закону виникає питання, чи захищатиме закон інтереси окремої особи як індивіда? Основна увага закону зосереджена на захисті прав суспільства та держави в кіберпросторі, однак саме людина як індивід зазнає найбільших негативних впливів у сучасному інформаційному просторі. Насамперед, важливою складовою такої проблеми є відсутність розуміння того, що саме повинно захищатися в контексті інформаційної безпеки людини.

Також яскравим прикладом дієвості механізмів захисту персональних даних особи є Естонія. Кожен громадянин цієї країни має спеціальніідентифікаційні картки, які містять багато важливої інформації про її власника. Ці картки використовуються не лише для ідентифікації особи, а ще й для здійснення різних фінансових операцій, включаючи проїзд у транспорті. Вся інформація про особу зберігається у спеціальній базі даних, до якої мають доступ правоохоронні органи та спеціальні служби. Враховуючи цей факт, кожна особа має можливість переглянути, хто цікавиться особистою інформацією про неї, а також має право вимагати пояснень, з яких підстав та чи інша особа або спецслужба цікавиться ним.

Отже, основною вимогою є те, що зібрані особисті дані мають бути достатньо захищеними, персональні дані повинні збиратися, використовуватися та надаватися зі знанням та згодою особи, а також особа повинна мати доступ до особистих даних, що збираються про неї, включаючи можливість виправлення або видалення неправильних даних.

Для тих, хто незаконно збирає, зберігає, знищує та поширює конфіденційну інформацію про особу передбачена Стаття 182 (Порушення недоторканості приватного життя) Кримінального кодексу. Покарання за таку діяльність становить від 8500 до 17000 гривень, а за повторні злочини – навіть

позбавлення волі на строк від 3 до 5 рокі.

Таким чином, необхідно пам’ятати, що в умовах сучасності інформаційне суспільство не повинно відокремлюватися від реального світу, в якому ми зараз живемо. Цей принцип повинен стати основою для формування цінностей сучасного інформаційного суспільства.

## 1.1 Основні шляхи забезпечення безпеки інформації.

### 1.1.1 Концепція захисту інформації

Вразливість інформації в автоматизованих комплексах обумовлена великою концентрацією обчислювальних ресурсів, їх територіальною розподіленністю, довгостроковим збереженням великого об’єму даних на магнітних та оптичних носіях, одночасним доступом до ресурсів багатьох користувачів. У цих умовах необхідність вживання заходів захисту, напевно, не викликає сумнівів. Однак існують певні труднощі:

* немає єдиної теорії захисту систем;
* виробники засобів захисту, в основному, пропонують окремі

компоненти для рішення приватних задач, залишаючи питання формування системи захисту і сумісності цих засобів на розсуд споживачів;

* для забезпечення надійного захисту необхідно розв’язати цілий

комплекс технічних і організаційних проблем і розробити відповідну документацію.

Для подолання перерахованих вище труднощів, необхідна координація дій всіх учасників інформаційного процесу як на окремому підприємстві, так і на державному рівні.

Концепція захисту інформації - офіційно прийнята система поглядів на проблему інформаційної безпеки і шляхи її рішення з урахуванням сучасних тенденцій. Вона є методологічною основою політики розробки практичних заходів для її реалізації. На базі сформульованих у концепції цілей, задач і можливих шляхів їх рішення формуються конкретні плани забезпечення інформаційної безпеки.[1]

### 1.1.2 Стратегія та архітектура захисту інформації

В основі комплексу заходів щодо інформаційної безпеки повинна бути стратегія захисту інформації. У ній визначаються мета, критерії, принцип і процедури, необхідні для побудови надійної системи захисту.

Найважливішою особливістю загальної стратегії інформаційного захисту є дослідження системи безпеки. Можна виділити два основних напрямки:

* аналіз засобів захисту;
* визначення факту вторгнення.

На основі концепції безпеки інформації розробляються стратегія безпеки інформації та архітектура системи захисту інформації, а далі – політика безпеки інформації (рис.1.1).

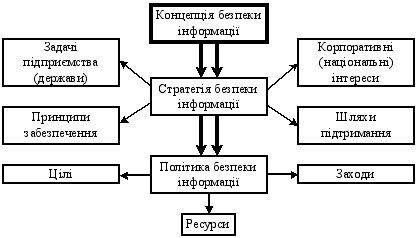


Рис. 1.1 Ієрархічний підхід до забезпечення безпеки інформації

Розробку концепції захисту рекомендується проводити в три етапи (рис. 1.2).

На першому етапі повинна бути чітко визначена цільова установка захисту, тобто які реальні цінності, виробничі процеси, програми, масиви даних необхідно захищати. На цьому етапі доцільно диференціювати по значимості окремі об'єкти, що вимагають захисту.

На другому етапі повинен бути проведений аналіз злочинних дій, що потенційно можуть бути зроблені стосовно об'єкта, що захищається. Важливо визначити ступінь реальної небезпеки таких найбільш широко розповсюджених злочинів, як економічне шпигунство, саботаж, крадіжки зі зломом. Потім потрібно проаналізувати найбільш ймовірні дії зловмисників стосовно основних об'єктів, що потребують захисту. [2]

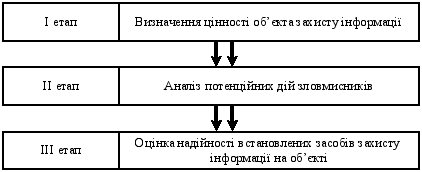


Рис. 1.2 Етапи розробки концепції захисту інформації

Головною метою третього етапу є аналіз обставин, у тому числі місцевих специфічних умов, виробничих процесів, уже встановлених технічних засобів захисту.

Концепція захисту повинна містити перелік організаційних, технічних і інших заходів, що забезпечують максимальну безпеку при заданому залишковому ризику і мінімальні витрати на їх реалізацію.

Політика захисту - це загальний документ, де перераховуються правила доступу, визначаються шляхи реалізації політики та описується базова архітектура середовища захисту.

Сам по собі документ складається з декількох сторінок тексту. Він формує основу фізичної архітектури мережі, а інформація, що знаходиться в ньому, визначає вибір продуктів захисту. При цьому, документ може і не включати список необхідних закупок, але вибір конкретних компонентів після його складання повинен бути очевидним.

Політика захисту повинна обов'язково відображати наступне:

* контроль доступу (заборона на доступ користувача до матеріалів, яким

йому не дозволено користуватися);

* ідентифікацію та аутентифікацію (використання паролів або інших

механізмів для перевірки статусу користувача);

* облік (запис усіх дій користувача в мережі);
* контрольний журнал (журнал дозволяє визначити, коли і де відбулося

порушення захисту);

* акуратність (захист від будь-яких випадкових порушень);
* надійність (запобігання монополізації ресурсів системи одним

користувачем);

* обмін даними (захист усіх комунікацій).

Один з найпростіших способів реалізувати захист - доручити зайнятися цим спеціалізованій компанії. [3]

### 1.1.3 Політика безпеки інформації

При розробці політики безпеки інформації, у загальному випадку, спочатку визначають об'єкти, які треба захистити, і їх функції. Потім оцінюють ступінь інтересу потенційного супротивника до цих об'єктів, ймовірні види нападу і спричинений ними збиток. Нарешті, визначають вразливі для впливу області, в яких наявні засоби протидії не забезпечують достатнього захисту. При цьому, розробка політики безпеки інформації повинна проводитися з урахуванням задач, рішення яких забезпечить реальний захист даного об'єкта (рис. 1.3).

Автоматизований комплекс можна вважати захищеним, якщо всі операції виконуються у відповідності з чітко визначеними правилами (рис. 1.4), що забезпечують безпосередній захист об'єктів, ресурсів і операцій. Основу для формування вимог до захисту складає список загроз. Коли такі вимоги відомі, можуть бути визначені відповідні правила забезпечення захисту. Ці правила, в свою чергу, визначають необхідні функції і заходи захисту. Чим суворіші вимоги до захисту і більше відповідних правил, тим ефективніші його механізми і тим більш захищеним виявляється автоматизований комплекс.

Отже, захист інформації в комп'ютерній мережі ефективніший в тому випадку, коли проектування і реалізація системи захисту відбувається в три етапи:

* аналіз ризику;
* реалізація політики безпеки;
* підтримка політики безпеки. [4]

На першому етапі аналізуються вразливі елементи комп'ютерної мережі, визначаються й оцінюються загрози і підбираються оптимальні засоби захисту. Аналіз ризику закінчується прийняттям політики безпеки. Політикою безпеки (Security Policy) називається комплекс взаємозалежних засобів, спрямованих на забезпечення високого рівня безпеки. У теорії захисту інформації вважається, що ці засоби повинні бути спрямовані на досягнення наступних цілей:

* конфіденційність (засекречена інформація повинна бути доступна

тільки тому, кому вона призначена);

* цілісність (інформація, на основі якої приймаються рішення, повинна

бути достовірною і повною, а також захищена від можливих ненавмисного і злочинного перекручувань);

* готовність (інформація і відповідні автоматизовані служби повинні

бути доступні та, у разі потреби, готові до обслуговування).

Визначення об’єктів, які захищаються: призначення; вартість заміни; можливість зміни.

Визначення критичності: аналіз призначення; стан в певний момент; простота зміни.

Визначення загроз: шпіонаж; саботаж; тероризм; кримінальні злочинці; незадоволені робітники. Враховується: вартість об’єкта; мета агресій; заходи усування наслідків; ризик.

Визначення можливості нападу: так; ні.

Визначення видів нападу: таємний вхід; підрив; розвідка; демонстрація; напад з повітря; напад з зони недосяжності; крадіжка; руйнування; засмічення; несанкціонований доступ.

Визначення загрози нападу: інструмент; зброя.

Визначення вразливості: можливості сил захисту; захист від проникнення; можливості оцінки; можливості виявлення; контроль доступу; контроль процедур; вимоги до будівлі; таємність дій.

Визначення обмежень: фінансові; оперативні.

Визначення вимог захисту: зовнішній периметр; внутрішній периметр; на об’єкті.[5]

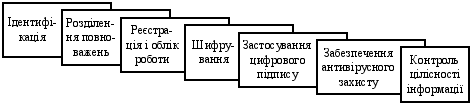


Рис. 1.3 Основні правила забезпечення політики безпеки інформації

Вразливість означає невиконання хоча б однієї з цих властивостей. Для комп'ютерних мереж можна виділити наступні ймовірні загрози, які необхідно враховувати при визначенні політики безпеки:

* несанкціонований доступ сторонніх осіб, що не належать до числа

службовців і ознайомлення зі збереженою конфіденційною інформацією;

* ознайомлення своїх службовців з інформацією, до якої вони не повинні

мати доступу;

* несанкціоноване копіювання програм і даних;
* перехоплення та ознайомлення з конфіденційною інформацією,

переданої по каналах зв'язку;

* крадіжка магнітних носіїв, що містять конфіденційну інформацію;
* крадіжка роздрукованих документів;
* випадкове або навмисне знищення інформації;
* несанкціонована модифікація службовцями документів і баз даних;
* фальсифікація повідомлень, переданих по каналах зв'язку;
* відмова від авторства повідомлення, переданого по каналах зв'язку;
* відмовлення від факту одержання інформації;
* нав'язування раніше переданого повідомлення;
* помилки в роботі обслуговуючого персоналу;
* руйнування файлової структури через некоректну роботу програм або апаратних засобів;
* руйнування інформації, викликане вірусними впливами;
* руйнування архівної інформації, що зберігається на магнітних носіях;
* крадіжка устаткування;
* помилки в програмному забезпеченні;
* відключення електроживлення;
* збої устаткування. [6]

Оцінка імовірності появи даних погроз і очікуваних розмірів втрат - важка задача. Ще складніше визначити вимоги до системи захисту. Політика безпеки повинна визначатися наступними заходами:

* ідентифікація, перевірка дійсності і контроль доступу користувачів на

об'єкт, у приміщення, до ресурсів автоматизованого комплексу;

* поділ повноважень користувачів, що мають доступ до обчислювальних

ресурсів;

* реєстрація та облік роботи користувачів;
* реєстрація спроб порушення повноважень;
* шифрування конфіденційної інформації на основі криптографічних

алгоритмів високої стійкості;

* застосування цифрового підпису для передачі інформації по каналах

зв'язку;

* забезпечення антивірусного захисту (у тому числі і для боротьби з

невідомими вірусами) і відновлення інформації, зруйнованої вірусними впливами;

* контроль цілісності програмних засобів і оброблюваної інформації;
* відновлення зруйнованої архівної інформації, навіть при значних

втратах;

* наявність адміністратора (служби) захисту інформації в системі;
* вироблення і дотримання необхідних організаційних заходів;
* застосування технічних засобів, що забезпечують безперебійну роботу

устаткування. [7]

Другий етап - реалізація політики безпеки - починається з проведення розрахунку фінансових витрат і вибору відповідних засобів для виконання цих задач. При цьому, необхідно врахувати такі фактори як: безконфліктність роботи обраних засобів, репутація постачальників засобів захисту, можливість одержання повної інформації про механізми захисту і надані гарантії. Крім того, варто враховувати принципи, в яких відображені основні положення по безпеці інформації:

* економічна ефективність (вартість засобів захисту повинна бути меншою,ніж розміри можливого збитку);
* мінімум привілей (кожен користувач повинен мати мінімальний набір

привілей, необхідних для роботи);

* простота (захист буде тим ефективніший, чим легше користувачеві з

ним працювати);

* відключення захисту (при нормальному функціонуванні захист не

повинен відключатися, за винятком особливих випадків, коли співробітник зі спеціальними повноваженнями може мати можливість відключити систему захисту);

* відкритість проектування і функціонування механізмів захисту

(таємність проектування і функціонування засобів безпеки - кращий підхід до захисту інформації тому, що фахівці, які мають відношення до системи захисту, повинні цілком уявляти собі принципи її функціонування та, у випадку виникнення скрутних ситуацій, адекватно на них реагувати);

* незалежність системи захисту від суб'єктів захисту (особи, що

займалися розробкою системи захисту, не повинні бути в числі тих, кого ця система буде контролювати);

* загальний контроль (будь-які виключення з безлічі контрольованих

суб'єктів і об'єктів захисту знижують захищеність автоматизованого комплексу);

* звітність і підконтрольність (система захисту повинна надавати досить

доказів, що показують коректність її роботи);

* відповідальність (особиста відповідальність осіб, що займаються

забезпеченням безпеки інформації);

* ізоляція і поділ (об'єкти захисту доцільно розділяти на групи таким

чином, щоб порушення захисту в одній з груп не впливало на безпеку інших груп);

* відмова за замовчуванням (якщо відбувся збій засобів захисту і

розроблювачі не передбачили такої ситуації, то доступ до обчислювальних ресурсів повинен бути заборонений);

* повнота і погодженість (система захисту повинна бути цілком

специфікована, протестована і погоджена);

* параметризація (захист стає більш ефективним і гнучкішим, якщо він

допускає зміну своїх параметрів з боку адміністратора);

* принцип ворожого оточення (система захисту повинна проектуватися в

розрахунку на вороже оточення і припускати, що користувачі мають найгірші наміри, що вони будуть робити серйозні помилки і шукати шляхи обходу механізмів захисту);

* залучення людини (найбільш важливі і критичні рішення повинні

прийматися людиною, тому що комп'ютерна система не може передбачити всі можливі ситуації);

* відсутність зайвої інформації про існування механізмів захисту

(існування механізмів захисту повинно бути по можливості приховане від користувачів, робота яких контролюється).

Підтримка політики безпеки - третій, найбільш важливий, етап. Заходи, проведені на даному етапі, вимагають постійного спостереження за вторгненнями у мережу зловмисників, виявлення «дір» у системі захисту об'єкта інформації, обліку випадків несанкціонованого доступу до конфіденційних даних.

При цьому основна відповідальність за підтримку політики безпеки мережі лежить на системному адміністраторі, що повинен оперативно реагувати на усі випадки злому конкретної системи захисту, аналізувати їх і використовувати необхідні апаратні і програмні засоби захисту з урахуванням максимальної економії фінансових засобів.[8]

### 1.1.4 Види забезпечення безпеки інформації

В даний час комп'ютерні злочини надзвичайно різноманітні. Це несанкціонований доступ до інформації, що зберігається в комп'ютері, введення в програмне забезпечення логічних бомб, розробка і поширення комп'ютерних вірусів, розкрадання комп'ютерної інформації, недбалість у розробці, виготовленні та експлуатації програмно-обчислювальних комплексів, підробка комп'ютерної інформації.

Всі заходи протидії комп'ютерним злочинам, що безпосередньо забезпечують безпеку інформації, можна підрозділити на:

* правові;
* організаційно-адміністративні;
* інженерно-технічні. [9]

До правових заходів (рис. 1.5) варто віднести розробку норм, що встановлюють відповідальність за комп'ютерні злочини, захист авторських прав програмістів, удосконалювання карного і цивільного законодавства, а також судочинства. До них відносяться також питання суспільного контролю за розроблювачами комп'ютерних систем і прийняття відповідних міжнародних договорів про обмеження, якщо вони впливають або можуть уплинути на військові, економічні і соціальні аспекти країн. Тільки в останні роки з'явилися роботи з проблем правової боротьби з комп'ютерними злочинами. А зовсім недавно і вітчизняне законодавство стало на шлях боротьби з комп'ютерною злочинністю.

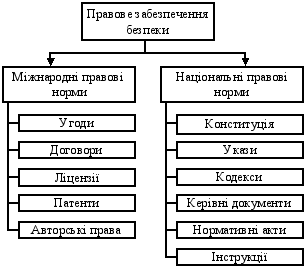


Рис. 1.5 Правові норми забезпечення безпеки інформації

До організаційно-адміністративних заходів (рис. 1.6) відносяться: охорона комп'ютерних систем, підбір персоналу, виключення випадків ведення особливо важливих робіт тільки однією людиною, наявність плану відновлення працездатності центру після виходу його з ладу, обслуговування обчислювального центру сторонньою організацією або особами, незацікавленими в приховуванні фактів порушення роботи центру, універсальність засобів захисту від усіх користувачів (включаючи вище керівництво), покладання відповідальності на осіб, що повинні забезпечити безпеку центру, вибір місця розташування центру і т.п. [10]

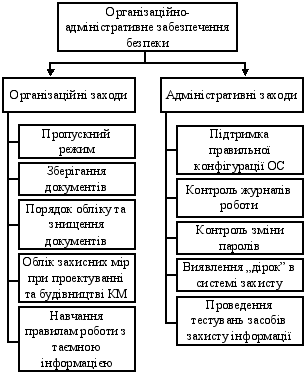


Рис. 1.6 Основні організаційні та адміністративні заходи по захисту інформації в мережі.

До інженерно-технічних заходів (рис. 1.7) можна віднести захист від несанкціонованого доступу до комп'ютерної системи, резервування важливих комп'ютерних систем, забезпечення захисту від розкрадань і диверсій, резервне електроживлення, розробку і реалізацію спеціальних програмних і апаратних комплексів безпеки тощо.

Фізичні засоби містять у собі різні інженерні засоби, що перешкоджають фізичному проникненню зловмисників на об'єкти захисту і захищаючий персонал, особисті засоби безпеки, матеріальні засоби і фінанси, інформацію від протиправних дій.

До апаратних засобів відносяться прилади, пристрої, пристосування та інші технічні рішення, які використовуються в інтересах забезпечення безпеки. У практиці діяльності будь-якої організації знаходить широке застосування різна апаратура: від телефонного апарату до розроблених автоматизованих інформаційних систем, що забезпечують її виробничу діяльність. Основна задача апаратних засобів - стійка безпека комерційної діяльності.

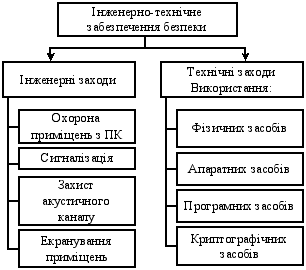


Рис. 1.7 Основні інженерні та технічні заходи по захисту інформації в мережі

Програмні засоби - це спеціальні програми, програмні комплекси і системи захисту інформації в інформаційних системах різного призначення і засобах обробки даних.

Криптографічні засоби - ця спеціальні математичні та алгоритмічні засоби захисту інформації, переданої по мережах зв'язку, збереженої та обробленої на комп'ютерах з використанням методів шифрування. [11]

## 1.2 Нормативно-правова база у сфері захисту інформації

### 1.2.1 Закон України «Про інформацію»

Цей Закон регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, ЗІ.

Стаття1. Визначення термінів

У цьому Законі наведені нижче терміни вживаються в такому значенні:

* документ - матеріальний носій, що містить інформацію, основними

функціями якого є її збереження та передавання у часі та просторі;

* захист інформації (ЗІ) - сукупність правових, адміністративних,

організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї;

* інформація - будь-які відомості та/або дані, які можуть бути збережені

на матеріальних носіях або відображені в електронному вигляді;

* суб'єкт владних повноважень - орган державної влади, орган місцевого

самоврядування, інший суб'єкт, що здійснює владні управлінські функції відповідно до законодавства, у тому числі на виконання делегованих повноважень.

Стаття2. Основні принципи інформаційних відносин

Основними принципами інформаційних відносин є:

* гарантованість права на інформацію;
* відкритість, доступність інформації, свобода обміну інформацією;
* достовірність і повнота інформації; свобода вираження поглядів

переконань;

* правомірність одержання, використання, поширення, зберігання та ЗІ;
* захищеність особи від втручання в її особисте та сімейне життя.

Стаття3. Державна інформаційна політика

Основними напрямами державної інформаційної політики є:

* забезпечення доступу кожного до інформації;
* забезпечення рівних можливостей щодо створення, збирання,

одержання, зберігання, використання, поширення, охорони, ЗІ; створення умов для формування в Україні інформаційного суспільства; забезпечення відкритості та прозорості діяльності суб'єктів владних повноважень;

* створення інформаційних систем і мереж інформації, розвиток

електронного урядування;

* постійне оновлення, збагачення та зберігання національних

інформаційних ресурсів; забезпечення інформаційної безпеки України;

* сприяння міжнародній співпраці в інформаційній сфері та входженню

України до світового інформаційного простору.

Стаття4. Суб'єкти і об'єкт інформаційних відносин

Суб'єктами інформаційних відносин є:

* фізичні особи;
* юридичні особи;
* об'єднання громадян;
* суб'єкти владних повноважень.

Об'єктом інформаційних відносин є інформація.

Стаття5. Право на інформацію

Кожен має право на інформацію, що передбачає можливість вільного одержання, використання, поширення, зберігання та ЗІ, необхідної для реалізації своїх прав, свобод і законних інтересів.

Реалізація права на інформацію не повинна порушувати громадські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи і законні інтереси інших громадян, права та інтереси юридичних осіб.

Стаття6. Гарантії права на інформацію

Право на інформацію забезпечується: створенням механізму реалізації права на інформацію;

* створенням можливостей для вільного доступу до статистичних даних,

архівних, бібліотечних і музейних фондів, інших інформаційних банків, баз даних, інформаційних ресурсів;

* обов'язком суб'єктів владних повноважень інформувати громадськість

та засоби масової інформації про свою діяльність і прийняті рішення;

* обов'язком суб'єктів владних повноважень визначити спеціальні

підрозділи або відповідальних осіб для забезпечення доступу запитувачів до інформації; здійсненням державного і громадського контролю за додержанням законодавства про інформацію;

* встановленням відповідальності за порушення законодавства про

інформацію.

Право на інформацію може бути обмежене законом 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.

Стаття7. Охорона права на інформацію

Право на інформацію охороняється законом. Держава гарантує всім суб'єктам інформаційних відносин рівні права і можливості доступу до інформації.

Ніхто не може обмежувати права особи у виборі форм і джерел одержання інформації, за винятком випадків, передбачених законом.

Суб'єкт інформаційних відносин може вимагати усунення будь-яких порушень його права на інформацію.

Забороняється вилучення і знищення друкованих видань, експонатів, інформаційних банків, документів з архівних, бібліотечних, музейних фондів, крім встановлених законом випадків або на підставі рішення суду.

Право на інформацію, створену в процесі діяльності фізичної чи юридичної особи, суб'єкта владних повноважень або за рахунок фізичної чи юридичної особи, Державного бюджету України, місцевого бюджету, охороняється в порядку, визначеному законом.

Стаття8. Мова інформації

Мова інформації визначається законом про мови, іншими актами законодавства в цій сфері, міжнародними договорами та угодами, згода на обов'язковість яких надана Верховною Радою України.

Стаття9. Основні види інформаційної діяльності (ІД)

Основними видами ІД є створення, збирання, одержання, зберігання, використання, поширення, охорона та ЗІ.

Стаття10. Види інформації за змістом

За змістом інформація поділяється на такі види:

* 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.

Стаття11. Інформація про фізичну особу

Інформація про фізичну особу (персональні дані) - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

Не допускаються збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та захисту прав людини. До конфіденційної інформації про фізичну особу належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження.

Кожному забезпечується вільний доступ до інформації, яка стосується його особисто, крім випадків, передбачених законом.

Стаття12. Інформація довідково-енциклопедичного характеру

Інформація довідково-енциклопедичного характеру - систематизовані, документовані, публічно оголошені або іншим чином поширені відомості про суспільне, державне життя та навколишнє природне середовище.

Основними джерелами інформації довідково-енциклопедичного характеру є: енциклопедії, словники, довідники, рекламні повідомлення та оголошення, путівники, картографічні матеріали, електронні бази та банки даних, архіви різноманітних довідкових інформаційних служб, мереж та систем, а також довідки, що видаються уповноваженими на те органами державної влади та органами місцевого самоврядування, об'єднаннями громадян, організаціями, їх працівниками та автоматизованими інформаційно-телекомунікаційними системами.

Правовий режим інформації довідково-енциклопедичного характеру визначається законодавством та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

Стаття13. Інформація про стан довкілля (екологічна інформація)

Інформація про стан довкілля (екологічна інформація) - відомості та/або дані про:

* стан складових довкілля та його компоненти, включаючи генетично

модифіковані організми, та взаємодію між цими складовими;

* фактори, що впливають або можуть впливати на складові довкілля

(речовини, енергія, шум і випромінювання, а також діяльність або заходи, включаючи адміністративні, угоди в галузі навколишнього природного середовища, політику, законодавство, плани і програми);

* стан здоров'я та безпеки людей, умови життя людей, стан об'єктів

культури і споруд тією мірою, якою на них впливає або може вплинути стан складових довкілля;інші відомості та/або дані.

Правовий режим інформації про стан довкілля (екологічної інформації) визначається законами України та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

Інформація про стан довкілля, крім інформації про місце розташування військових об'єктів, не може бути віднесена до інформації з обмеженим доступом.

Стаття14. Інформація про товар (роботу, послугу)

Інформація про товар (роботу, послугу) - відомості та/або дані, які розкривають кількісні, якісні та інші характеристики товару (роботи, послуги).

Інформація про вплив товару (роботи, послуги) на життя та здоров'я людини не може бути віднесена до інформації з обмеженим доступом.

Правовий режим інформації про товар (роботу, послугу) визначається законами України про захист прав споживачів, про рекламу, іншими законами та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

Стаття15. Науково-технічна інформація

Науково-технічна інформація - будь-які відомості та/або дані про вітчизняні та зарубіжні досягнення науки, техніки і виробництва, одержані в ході науково - дослідної, дослідно-конструкторської, проектно-технологічної, виробничої та громадської діяльності, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

Правовий режим науково-технічної інформації визначається Законом України "Про науково-технічну інформацію" (3322-12), іншими законами та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

Науково-технічна інформація є відкритою за режимом доступу, якщо інше не встановлено законами України.

Стаття16. Податкова інформація

Податкова інформація - сукупність відомостей і даних, що створені або отримані суб'єктами інформаційних відносин у процесі поточної діяльності і необхідні для реалізації покладених на контролюючі органи завдань і функцій у порядку, встановленому Податковим кодексом України (2755-17).

Правовий режим податкової інформації визначається Податковим кодексом України (2755-17) та іншими законами.

Стаття17. Правова інформація

Правова інформація - будь-які відомості про право, його систему, джерела, реалізацію, юридичні факти, правовідносини, правопорядок, правопорушення і боротьбу з ними та їх профілактику тощо.

Джерелами правової інформації є Конституція України (254к/96-ВР), інші законодавчі і підзаконні нормативно-правові акти, міжнародні договори та угоди, норми і принципи міжнародного права, а також ненормативні правові акти, повідомлення засобів масової інформації, публічні виступи, інші джерела інформації з правових питань.

З метою забезпечення доступу до законодавчих та інших нормативних актів фізичним та юридичним особам держава забезпечує офіційне видання цих актів масовими тиражами у найкоротші строки після їх прийняття.

Стаття18. Статистична інформація

Статистична інформація - документована інформація, що дає кількісну характеристику масових явищ та процесів, які відбуваються в економічній, соціальній, культурній та інших сферах життя суспільства.

Офіційна державна статистична інформація підлягає систематичному оприлюдненню.

Держава гарантує суб'єктам інформаційних відносин відкритий доступ до офіційної державної статистичної інформації, за винятком інформації, доступ до якої обмежений згідно із законом.

Правовий режим державної статистичної інформації визначається Законом України "Про державну статистику" (2614-12), іншими законами та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

Стаття19. Соціологічна інформація

Соціологічна інформація - будь-які документовані відомості про ставлення до окремих осіб, подій, явищ, процесів, фактів тощо.

Правовий режим соціологічної інформації визначається законами та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

Стаття20. Доступ до інформації

За порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом.

Будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом.

Стаття21. Інформація з обмеженим доступом

Інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація.

Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом.

Відносини, пов'язані з правовим режимом конфіденційної інформації, регулюються законом.

Порядок віднесення інформації до таємної або службової, а також порядок доступу до неї регулюються законами.

До інформації з обмеженим доступом не можуть бути віднесені такі відомості:

* про стан довкілля, якість харчових продуктів і предметів побуту;
* про аварії, катастрофи, небезпечні природні явища та інші надзвичайні

ситуації, що сталися або можуть статися і загрожують безпеці людей;

* про стан здоров'я населення, його життєвий рівень, включаючи

харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально - демографічні показники, стан правопорядку, освіти і культури населення;

* про факти порушення прав і свобод людини і громадянина;
* про незаконні дії органів державної влади, органів місцевого

самоврядування, їх посадових та службових осіб;

* інші відомості, доступ до яких не може бути обмежено відповідно до

законів та міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України.

Стаття27. Відповідальність за порушення законодавства про інформацію

Порушення законодавства України про інформацію тягне за собою дисциплінарну, цивільно-правову, адміністративну або кримінальну відповідальність згідно із законами України.

Інформація не може бути використана для закликів до повалення конституційного ладу, порушення територіальної цілісності України, пропаганди війни, насильства, жорстокості, розпалювання міжетнічної, расової, релігійної ворожнечі, вчинення терористичних актів, посягання на права і свободи людини.

Стаття29. Поширення суспільно необхідної інформації

Інформація з обмеженим доступом може бути поширена, якщо вона є суспільно необхідною, тобто є предметом суспільного інтересу, і право громадськості знати цю інформацію переважає потенційну шкоду від її поширення.

Предметом суспільного інтересу вважається інформація, яка свідчить про загрозу державному суверенітету, територіальній цілісності України; забезпечує реалізацію конституційних прав, свобод і обов'язків; свідчить про можливість порушення прав людини, введення громадськості в оману, шкідливі екологічні та інші негативні наслідки діяльності (бездіяльності) фізичних або юридичних осіб тощо.

Стаття30. Звільнення від відповідальності

Ніхто не може бути притягнутий до відповідальності за висловлення оціночних суджень.

Оціночними судженнями, за винятком наклепу, є висловлювання, які не містять фактичних даних, критика, оцінка дій, а також висловлювання, що не можуть бути витлумачені як такі, що містять фактичні дані, зокрема з огляду на характер використання мовно-стилістичних засобів (вживання гіпербол, алегорій, сатири). Оціночні судження не підлягають спростуванню та доведенню їх правдивості.

Якщо особа вважає, що оціночні судження або думки принижують її гідність, честь чи ділову репутацію, а також інші особисті немайнові права, вона вправі скористатися наданим їй законодавством правом на відповідь, а також на власне тлумачення справи у тому самому засобі масової інформації з метою обґрунтування безпідставності поширених суджень, надавши їм іншу оцінку. Якщо суб'єктивну думку висловлено в брутальній, принизливій чи непристойній формі, що принижує гідність, честь чи ділову репутацію, на особу, яка таким чином та у такий спосіб висловила думку або оцінку, може бути покладено обов'язок відшкодувати завдану моральну шкоду.

Суб'єкти інформаційних відносин звільняються від відповідальності за розголошення інформації з обмеженим доступом, якщо суд встановить, що ця інформація є суспільно необхідною.

Додаткові підстави звільнення від відповідальності засобів масової інформації та журналістів встановлюються законами України "Про друковані засоби масової інформації (пресу) в Україні" (2782-12), "Про телебачення і радіомовлення" (3759­12), "Про інформаційні агентства" (74/95-ВР) та іншими.

Стаття31. Відшкодування матеріальної та моральної шкоди

У разі якщо порушенням права на свободу інформації особі завдано матеріальної чи моральної шкоди, вона має право на її відшкодування за рішенням суду.

Суб'єкти владних повноважень як позивачі у справах про захист честі, гідності та ділової репутації вправі вимагати в судовому порядку лише спростування недостовірної інформації про себе і не мають права вимагати відшкодування моральної (немайнової) шкоди. Це не позбавляє посадових і службових осіб права на захист честі, гідності та ділової репутації в суді [12].

### 1.2.2 Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»

Цей Закон регулює відносини у сфері ЗІ в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах (далі - система).

Стаття1**.** Визначення термінів

У цьому Законі наведені нижче терміни вживаються в такому значенні:

* блокування інформації в системі - дії, внаслідок яких

унеможливлюється доступ до інформації в системі;

* виток інформації - результат дій, внаслідок яких інформація в системі

стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї;

* володілець інформації - фізична або юридична особа, якій належать

права на інформацію;

* власник системи - фізична або юридична особа, якій належить право

власності на систему;

* доступ до інформації в системі - отримання користувачем можливості

обробляти інформацію в системі;

* ЗІ в системі - діяльність, спрямована на запобігання несанкціонованим

діям щодо інформації в системі;

* знищення інформації в системі - дії, внаслідок яких інформація в

системі зникає;

* інформаційна (автоматизована) система - організаційно-технічна

система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів;

* інформаційно-телекомунікаційна система - сукупність інформаційних

та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле;

* комплексна система ЗІ - взаємопов'язана сукупність організаційних та

інженерно-технічних заходів, засобів і методів ЗІ;

* користувач інформації в системі (далі - користувач) - фізична або

юридична особа, яка в установленому законодавством порядку отримала право доступу до інформації в системі;

* криптографічний ЗІ - вид ЗІ, що реалізується шляхом перетворення

інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо;

* несанкціоновані дії щодо інформації в системі - дії, що проводяться з

порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства;

* обробка інформації в системі - виконання однієї або кількох операцій,

зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів;

* порушення цілісності інформації в системі - несанкціоновані дії щодо

інформації в системі, внаслідок яких змінюється її вміст;

* порядок доступу до інформації в системі - умови отримання

користувачем можливості обробляти інформацію в системі та правила обробки цієї інформації;

* 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;

* технічний ЗІ - вид ЗІ, спрямований на забезпечення за допомогою

інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації.

Стаття 2. Об'єкти захисту в системі

Об'єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації.

Стаття 3. Суб'єкти відносин

Суб'єктами відносин, пов'язаних із захистом інформації в системах, є:

* володільці інформації;
* власники системи;
* користувачі;
* спеціально уповноважений центральний орган виконавчої влади з

питань організації спеціального зв'язку та ЗІ і підпорядковані йому регіональні органи;

На підставі укладеного договору або за дорученням власник системи може надати право розпоряджатися системою іншій фізичній або юридичній особі - розпоряднику системи.

Стаття 4. Доступ до інформації в системі

Порядок доступу до інформації, перелік користувачів та їх повноваження стосовно цієї інформації визначаються володільцем інформації.

Порядок доступу до державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, перелік користувачів та їх повноваження стосовно цієї інформації визначаються законодавством.

У випадках, передбачених законом, доступ до інформації в системі може здійснюватися без дозволу її володільця в порядку, встановленому законом.

Стаття 5. Відносини між володільцем інформації та власником системи

Власник системи забезпечує ЗІ в системі в порядку та на умовах, визначених у договорі, який укладається ним із володільцем інформації, якщо інше не передбачено законом.

Власник системи на вимогу володільця інформації надає відомості щодо ЗІ в системі.

Стаття 6. Відносини між власником системи та користувачем

Власник системи надає користувачеві відомості про правила і режим роботи системи та забезпечує йому доступ до інформації в системі відповідно до визначеного порядку доступу.

Стаття 7. Відносини між власниками систем

Власник системи, яка використовується для обробки інформації з іншої системи, забезпечує захист такої інформації в порядку та на умовах, що визначаються договором, який укладається між власниками систем, якщо інше не встановлено законодавством.

Власник системи, яка використовується для обробки інформації з іншої системи, повідомляє власника зазначеної системи про виявлені факти несанкціонованих дій щодо інформації в системі.

Стаття 8. Умови обробки інформації в системі

Умови обробки інформації в системі визначаються власником системи відповідно до договору з володільцем інформації, якщо інше не передбачено законодавством.

Державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням комплексної системи ЗІ з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством.

Для створення комплексної системи захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, використовуються засоби ЗІ, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері технічного та/або криптографічного ЗІ. Підтвердження відповідності та проведення державної експертизи цих засобів здійснюються в порядку, встановленому законодавством.

Стаття 9. Забезпечення ЗІ в системі

Відповідальність за забезпечення ЗІ в системі покладається на власника системи.

Власник системи, в якій обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, утворює службу ЗІ або призначає осіб, на яких покладається забезпечення ЗІ та контролю за ним.

Про спроби та/або факти несанкціонованих дій у системі щодо державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, власник системи повідомляє відповідно спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та ЗІ або підпорядкований йому регіональний орган.

Стаття 10. Повноваження державних органів у сфері ЗІ в системах

Вимоги ([373-2006-п](http://zakon3.rada.gov.ua/laws/show/373-2006-%D0%BF)) до забезпечення захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, встановлюються Кабінетом Міністрів України.

Спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та ЗІ:

* розробляє пропозиції щодо державної політики у сфері ЗІ та забезпечує

її реалізацію в межах своєї компетенції;

* визначає вимоги та порядок створення комплексної системи захисту

державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

* організовує проведення державної експертизи комплексних систем ЗІ,

експертизи та підтвердження відповідності засобів технічного і криптографічного ЗІ;

* здійснює контроль за забезпеченням захисту державних інформаційних

ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

* здійснює заходи щодо виявлення загрози державним інформаційним

ресурсам від несанкціонованих дій в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах та дає рекомендації з питань запобігання такій загрозі.

Державні органи в межах своїх повноважень за погодженням відповідно із спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та ЗІ або підпорядкованим йому регіональним органом встановлюють особливості захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом.

Особливості ЗІ в системах, які забезпечують банківську діяльність, встановлюються Національним банком України.

Стаття 11. Відповідальність за порушення законодавства про ЗІ в системах

Особи, винні в порушенні законодавства про ЗІ в системах, несуть відповідальність згідно із законом.

Стаття 12. Міжнародні договори

Якщо міжнародним договором, згода на обов'язковість якого надана Верховною Радою України, визначено інші правила, ніж ті, що передбачені цим Законом, застосовуються норми міжнародного договору [13].

## 1.3 Висновки по розділу

Основою правового регулювання у сфері інформаційної безпеки є Закон України «Про інформацію», який встановлює загальні правові засади основних видів ІД, таких як одержання, використання, поширення, зберігання інформації тощо. Даний закон визначає основні принципи інформаційних відносин, гарантує право громадян на інформацію, встановлює режим доступу до інформації та його контроль, дає визначення інформації з обмеженим доступом.

Пряме відношення до теми даної дипломної роботи має Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», оскільки він регулює відносини у сфері ЗІ в інформаційних (автоматизованих) системах. Згідно з цим законом об’єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації. Закон встановлює порядок доступу до інформації в системі, умови її обробки, забезпечення захищеності даних засобами технічного та/або криптографічного ЗІ. Закон також встановлює відповідальність за порушення законодавства про ЗІ в системах.

# РОЗДІЛ 2

# РЕЗЕРВНЕ КОПІЮВАННЯ ТА ВІДНОВЛЕННЯ ДАНИХ. ЗАХИСТ ДАНИХ

В даній роботі термін «захист даних» використовується у значенні зберігання інформації таким чином, що її буде легко знайти та відновити, не зважаючи на те, де саме вона знаходиться в архівах резервних копій. «Аварійне відновлення» означає відновлення серверу, робочої станції або цілого центру обробки даних після масштабної проблеми.

## 2.1 Визначення даних

Через те, що дані приймають багато форм, легко заплутатися в тому, які саме дані потребують захисту та можливості легкого відновлення. Вважається, що захищеними повинні бути дані, які мають цінність.

Те, що нелегко замінити, - це суттєва конкурентна перевага, яка зберігається у файлах та базах даних у комп'ютерних системах. Ця критична інформація міститься в бухгалтерських файлах, списках клієнтів, списках деталей, кресленнях робіт тощо. Ця інформація є унікальною для будь-якої компанії; саме це робить компанію особливою для постачальників та клієнтів. На відміну від фізичних активів, інформацію важко, якщо не неможливо, відновити після того, як вона зникне. [14]

## 2.2 Резервне копіювання

Резервне копіювання— процес створення копії даних з носія (жорсткого диска, дискети тощо), призначений для відновлення цих даних у разі їх пошкодження або видалення.

Створення резервної копії даних надає можливість виконати відновлення інформації при втраті оригіналу, з якого було створено резервну копію. При цьому під втратою треба розуміти настання події, що призвела до зміни даних, після чого вони втратили цінність або були видалені з носія. Приклад: умисне завдання шкоди через видалення важливої для підприємства інформації. [15]

### 2.2.1Об'єкти резервного копіювання

Об'єкти резервного копіювання — це дані або сукупність даних, з яких можна створити резервну копію. Приклади об'єктів: файли або теки, дані прикладних програм, дані операційної системи чи сама ОС (наприклад Windows System State або AIX System Backup), образи віртуальних машин та дисків віртуальних машин, файлові системи тощо.[40]

### 2.2.2Вимоги для відновлення даних.

Для визначення вимог для швидкості відновлення та періодичності створення резервних копій, використовують наступні визначення:

* Recovery Point Objective (RPO) - Цільова точка відновлення. Визначає

періодичність створення резервних копій. У разі пошкодження або видалення даних і потребу відновити "найсвіжішу" копію, це можливо зробити лише на останню RPO. В залежності від технологій, що були використані під час створення резервних копій, відновлення можливе також у період між різними RPO, така технологія називається Point In Time Restore та властива СУБД.

* Recovery Time Objective (RTO) - Цільовий час відновлення. Визначає

час, який повинен пройти з початку і до кінця відновлення даних з резервної копії. Час з моменту втрати даних до початку роботи спеціаліста по відновленню, а також час з моменту відновлення з резервної копії до початку використання даних користувачами, може не включатися до RTO.

Для можливості відновлення під час катастрофи (відмова сайту або парна відмова зарезервованих компонентів) існують також такі визначення:

* Disaster Recovery Point Objective (DRPO) - Цільова точка відновлення

під час катастрофи. RPO у разі настання катастрофи.

* Disaster Recovery Time Objective (DRTO) - Цільовий час відновлення під

час катастрофи. RTO у разі настання катастрофи. [17]

### 2.2.3Рівні 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.

* Lx (розшифровується як Level X) — Це один із стандартів описання

методів резервного копіювання. Оскільки різні джерела можуть по різному тлумачити поняття диференційного та додаткового резервного копіювання, може використовуватись нотація Lx, що для перелічених типів буде означати L1 та L2 відповідно. Рівень Lx завжди залежить від попереднього Lx-1 або Lx-n, якщо він був останнім. Наприклад, у разі наступної послідовності резервних копій L0, L5, L3, L2, L4, процедура відновлення на останню найсвіжішу резервну копію буде відбуватись у такій послідовності: L0, L2, L4.[18]

### 2.2.4 Ціліснісність резервних копій даних.

Цілісність резервної копій даних — це відповідність даних резервної копії та оригіналу на момент створення копії. Якщо було вибрано неправильний метод створення резервної копії, неможливо буде відновити дані у разі потреби. Для забезпечення цілісності резервних копій використовують різні методи, в залежності від об'єкта резервного копіювання. Загалом, необхідно виконати декілька дій:

* Забезпечити незмінність даних під час створення копії, інакше

неможливо буде перевірити відповідність створеної копії: контрольні суми збереженої копії та оригіналу будуть відрізнятися.

* Зозблокувати дані для можливості читання — ОС може блокувати

навіть спроби читання файлів з носія.

* Виконати запис змін, що були зроблені в оперативній пам'яті, на

жорсткий диск (в Linux — команда sync) — інакше деякі частини об'єкту резервного копіювання можуть не відповідати змінам, які вже були виконані.[19]

Приклади:

Під час створення резервної копії файлів ОС Windows неможливо отримати доступ до деяких системних файлів, які використовуються в системі, але, завдяки технології VolumeShadowCopyServices, перед початком копіювання може бути виконана процедура створення тіньової копії тома, таким чином, для копіювання буде використовуватись не оригінальний том, а його тіньова копія.

При створенні копії образу віртуальної машини VMwarevSphere, щоб досягти цілісності, використовується програмне забезпечення VMwareTools, яке «повідомляє» операційну систему про необхідність підготовки її даних для початку резервного копіювання. З боку ОС, якщо використовується ОС Windows, це також ініціює запуск компонентів VSS. [20]

### 2.2.5 Методи передачі резервних копій.

З використанням агента. — Копіювання даних здійснюється за допомогою частини програмного забезпечення, що встановлюється з боку системи, дані якої потрібно захистити. Такий метод є обтяжливий для адміністрування, оскільки потребує контролю за встановленням та оновленням такого програмного забезпечення, але надає змогу щільно інтегруватись у програмне середовище, що використовується на клієнтській системі. Для інших методів також може використовуватись агент, оскільки необхідно координувати процеси всередині операційної системі під час створення резервної копії.

Off-host — Метод, що дозволяє створення резервної копії без значного навантаження на клієнтську систему. Зазвичай дані передаються безпосередньо зі сховища даних на сервер резервного копіювання.

Serverless — Метод, що дозволяє передавати дані від клієнта у сховище резервних копій без участі сервера резервного копіювання. При цьому сервер резервного копіювання отримує від клієнта необхідну інформацію про об'єкти, що їх було скопійовано в сховище. Цей метод використовується для зменшення навантаження на сервер резервного копіювання. [21]

### 2.2.6 Методи створення копії даних.

Тіньова копія (Shadow Copy) — Створення миттєвої копії з дискового розділу операційної системи, при цьому використовується властивості файлової системи.

Snapshot дисків — Замороження змін на основному диску та перенаправлення їх у окремий файл під час створення резервної копії.

Snapshot дискового розділу — створення миттєвої копії даних безпосередньо на дисковому масиві, використовується можливості дискових масивів. [22]

### 2.2.7 Зберігання резервної копії.

Резервні копії можуть зберігатись на різних носіях у залежності від конкретних потреб. Зазвичай використовується сервер резервного копіювання, який координує процеси резервного копіювання та керує сховищами. Сховища можуть бути такими:

* Стрічкова бібліотека або стример — запис резервних копій

відбувається на магнітну стрічку стримера. Перевагами цього методу є: швидкість запису та читання; відносно мала вартість зберігання одиниці інформації; можливість збереження off-line (тобто стрічки можна виймати та зберігати в сейфі). Недоліки: необхідність створення штучної надмірності (redundancy); повільний доступ до файлів; обмежена здатність компресії; обмежена кількість одночасних операцій оскільки обмежена кількість стримерів та роботів (picker, що вставляють та виймають стрічки).

* Дискове сховище — Запис резервних копій відбувається на диски, що

можуть бути об'єднані в RAID або на дискову систему збереження. Переваги цього методу: швидкість доступу до інформації; необмежена кількість одночасних операцій; можливість використання технологій усунення дуплікації, що значно зменшує потреби в просторі (в залежності від типу даних від 1,5 і більше разів) та також прискорює запис даних, оскільки дублікати не записуються а відкидаються. Недоліками є: менша (у порівнянні з стрічками) швидкість запису та читання інформації; відносно більша вартість 1 ГБ.

* Virtual Tape Library — запис резервних копій на диски, але саме

сховище виглядає для клієнта як стрічкова бібліотека. Перевагами цього методу є: можливість використання технології усунення дуплікації, значно збільшена кількість одночасних операцій, велика швидкість доступу до даних.

* "Хмарний" бекап — запис резервних даних за «хмарною» технологією

через онлайн-служби спеціальних провайдерів. Сервер резервного копіювання також може використовувати як сховище "Хмару". Перевагами цього методу є: низька вартість обслуговування, швидке розгортання та масштабування, можливість використання Pay-as-you-Go. Недоліки: занадто низька швидкість запису та читання, недостатня безпека доступу до даних. [23]

## 2.3 Відновлення даних

Відновлення даних— процес порятунку або відновлення доступу до даних, що зберігаються на будь-якому носії пристрою запам'ятовування, коли вони не можуть бути доступні у звичайному режимі.

У професійних лабораторіях фахівці часто здатні відновити дані, втрачені у найважчих випадках, таких як пожежа або повінь. Для відновлення даних потрібні знання електроніки, робототехніки та автоматизації, фізики, програмування і різноманітних методів зберігання даних: систем баз даних, файлових систем та криптології.

Відновлення даних включає:

* Відновлення пошкоджених чи видалених файлів та каталогів.
* Реконструкцію пошкоджених файлових систем після пошкодження або

форматування.

* Відновлення інформації за сигнатурами.

Термін «відновлення даних» також використовується в контексті судово-медичних програм або розвідки, коли відновлюється дані, які були не пошкоджені, а зашифровані або приховані. [24]

### 2.3.1 Способи відновлення.

В даний час існує два основних способи відновлення даних. Спосіб вибирається залежно від виниклої несправності накопичувача. Програмно-апаратний метод застосовують в тих випадках. коли програмний спосіб не дасть результату.

1. Програмний спосіб.

Програмний спосіб — це відновлення даних без фізичного втручання в пристрій накопичувача, а також у функціонування прошивки й структуру модулів службової інформації. Даний спосіб застосовується у випадках, коли збережена працездатність самого накопичувача, але з тієї чи іншої причини доступ до даних, що зберігаються на ньому, втрачений.

Причиною цього може стати форматування логічних дисків, невдала зміна логічної геометрії накопичувача, видалення інформації, часткове, або повне руйнування файлової системи, як інформації про структуру розміщення даних на накопичувачі. Найчастіше в перерахованих випадках вдається відновити більшу частину даних, проте трапляються випадки, коли відновлення втрачених даних неможливо (окремим випадком можна вважати перезапис даних). Для автоматизації процесу відновлення написано безліч програм, в тому числі й безкоштовних.[25]

1. Відновлення структури файлової системи.

У разі форматування логічного диска або розділу, структура та атрибути даних не порушуються, але змінюється або інвентаризується (наводиться в початковий стан) інформація про розташування даних на даному накопичувачі. При швидкому форматуванні оновлюється мала частина файлової таблиці, частина службових записів залишається, необхідно лише інтерпретувати її та прочитати дані в потрібному порядку.

Повне форматування може оновити всю файлову таблицю, тому відновлення структури файлів і тек не завжди можливо. Для відновлення даних без інформації про структуру можна використовувати відновлення файлів по сигнатурам.

Якщо сталося пошкодження файлової системи в результаті програмного збою або несправності носія, програми для відновлення даних можуть відновити частину інформації, що залежить від обсягу пошкоджень. [26]

1. Відновлення видалених даних файлової системи.

При видаленні даних, насправді, дані фізично залишаються на накопичувачі, проте в файловій системі більше не показуються, а місце на носії, де вони розташовуються, позначається як вільний і готове до запису нової інформації. У цьому випадку атрибути файлів змінюються. У разі запису в даний розділ або логічний диск може статися часткове або повне заміщення даних, помічених, як віддалені.

Подібні файли можна легко прочитати та відновити з усіма атрибутами та інформацією про розташування, прочитавши службові записи файлової системи. Існують як програми тільки для відновлення видалених даних, так і комплексні рішення, де відновлення видалених даних — лише одна з функцій.

Також існують спеціальні програми — «шредери», призначені для знищення даних. Після правильного використання таких програм відновлення неможливо. [27]

1. Відновлення за сигнатурами.

У разі, коли реконструкція файлової системи неможлива в силу будь-яких причин, деякі файли все ще можна відновити, використовуючи відновлення по сигнатурах. При даному типі відновлення відбувається по секторне сканування накопичувача на предмет наявності відомих сигнатур файлів.

Основний принцип роботи алгоритмів сигнатурного пошуку такий же, як у найперших антивірусів. Як антивірус сканує файл в пошуках ділянок даних, які збігаються з відомими фрагментами коду вірусів, так і алгоритми сигнатурного пошуку, що використовуються в програмах для відновлення даних, зчитують інформацію з поверхні диска в надії зустріти знайомі ділянки даних. Заголовки багатьох типів файлів містять характерні послідовності символів. Наприклад, файли у форматі JPEG містять послідовність символів «JFIF», архіви ZIP починаються з символів «PK», а документи PDF починаються з символів «% PDF-». [28]

Деякі файли (наприклад, текстові та HTML файли) не володіють характерними сигнатурами, але можуть бути визначені за непрямими ознаками, тому що містять тільки символи з таблиці ASCII.

|  |  |
| --- | --- |
| **Файл** | **Починається з сигнатури** |
| avi | 5249 |
| bmp | 424D |
| tif | 4949 |
| doc | D0CF |
| docx | 504B |
| jpeg | FFD8 |
| png | 8950 |

За результатами сканування видається, найчастіше, список файлів, відсортованих за типом. Інформація про розташування файлів не відновлюється.

Даний тип відновлення добре застосовувати для відновлення фотографій з карт пам'яті, бо дані на карті однотипні та записуються, в загальному випадку, суворо послідовно, без фрагментації. [29]

1. Змішане відновлення.

Більшість програм дозволяють застосувати одночасно кілька способів відновлення за одне сканування. В результаті видається максимально можливий результат при використанні даної програми.

Найнадійніший, простий і дешевий спосіб відновлення інформації — відновлення інформації з раніше зроблених резервних копій. Для створення резервних копій використовується спеціалізоване ПО, яке в тому числі може виконувати відновлення даних. [30]

1. **Програмно-апаратний спосіб.**

Програмно-апаратний спосіб потрібно при фізичному пошкодженні накопичувача. Тут необхідно загострити увагу на типі накопичувача: гнучкий це магнітний диск (НГМД), жорсткий магнітний диск (НЖМД), флеш (накопичувач NAND-Flash) або CD / DVD / BD. Розглянемо основні типи носіїв і їх несправності.

Накопичувач на гнучкому магнітному диску (НГМД).Основною несправністю є так зване «розмагнічування».

Зустрічається найчастіше при проходженні магнітних детекторів в магазинах, метро, ​​аеропортах. Відновити дані вдається тільки з не розмагніченого областей накопичувача. Так само зустрічаються несправності, пов'язані з фізичним ушкодженням носія, такими як подряпини, сильне забруднення. Кожен випадок необхідно розглядати індивідуально і тільки після цього прогнозувати результат відновлення інформації.[10]

### 

1. **Відновлення видалених даних.**

При видаленні даних вони фізично залишаються на накопичувачі, проте в файловій системі більш не показуються, а місце на носії, де вони розташовуються, позначається як вільне і готове до запису нової інформації. У випадку запису в даний розділ або логічний диск може статися часткове або повне заміщення даних, помічених як вилучені.

Подібні файли можна прочитати і відновити з усіма атрибутами та інформацією про розташування, прочитавши службові записи файлової системи. Існують як програми тільки для відновлення видалених даних, так і комплексні рішення, де відновлення видалених даних — лише одна з функцій. [32]

## 2.4 Захист даних

Існує два типи ризиків для інфраструктури, яка підтримує активи даних: (1) фізична втрата через несправність пристрою або катастрофу на його місцеположенні та (2) логічна втрата, спричинена програмою або помилкою користувача. Фізична втрата є менш вірогідною з двох, але вона потенційно наносить найбільші пошкодження. Вона включає в себе такі випадки, як несправність жорсткого диска, збій сервера або екологічна катастрофа, така як пожежа або повінь. Вона може вплинути на місцеположення частково або повністю. Фізичні втрати становлять приблизно 20 відсотків усіх інцидентів, що впливають на ресурси інформаційних технологій. На відміну від них, логічна втрата включає такі випадки, як помилки програми, помилки користувачів або порушення безпеки. Логічні збої складають приблизно 80 відсотків усіх випадків. Логічну помилку може бути легше відновити, але вона може залишатись непоміченою протягом деякого часу [33].

Основні елементи, які потребують захисту:

* Дані для завантаження (Bootstrap data): дані для завантаження

використовуються для запуску машини. Це програма, яка запускається першою після ввімкнення або перезавантаження системи. Без дійсного завантажувача система ніколи не стане робочою.

* Метадані файлової структури (File-structure metadata): метадані

файлової структури описують де розташовані всі файли та папки, а також завантажувальні дані, операційна система (ОС) та драйвери. Вони зберігають інформацію про те, які блоки на диску використовуються і які є вільними, зв'язують кожен каталог та ім'я файлу з певним розташуванням на диску. Цей тип даних також містить списки дозволу і доступу, які запобігають несанкціонованим операціям читання або записування шляхом перевірки цих списків.

* У деяких системах спеціальні журнали зберігають записи як

контрольний журнал змін. Ці журнали використовуються для відновлення після збоїв електроживлення та інших різких зупинок. Всі ці метадані важливі, коли потрібно відновити цілу систему.

* Двійкові файли драйверів (Driver binaries): ці файли контролюють

пристрої, що читають з дисків, стрічок або мережі. Драйвери часто є частиною ОС, і вони повинні бути сумісними з рештою системи. Вони часто поставляються з придбаними пристроями і не входять до ОС від початку.

* Операційна система (Operating system): код ОС, як правило,

поставляється на фізичному диску. Виробник зазвичай випускає оновлення через мережу, тому початковий диск рано чи пізно застаріває. Важливо створювати резервні копії ОС після встановлення оновлень, щоб у користувача завжди була поточна версія для відновлення. Якщо не зберігати оновлену версію, доведеться повторно застосувати всі оновлення після відновлення системи, а це – схильний до помилок, трудомісткий процес.

* Файли конфігурації (Configuration files): Файлів конфігурації дуже

багато. Деякі з них є настільки ж простими, як файл, що містить назву системи або часовий пояс; інші є такими ж складними, як реєстр Windows - великий файл, що містить тисячі одиниць інформації. Файли паролів - це, наприклад, файли конфігурації. Деякі програми настільки захищені, що, якщо файл пароля буде втрачено, дані не зможуть бути відновлені. Крім того, у багатьох додатках є складні конфігураційні файли, в яких зберігаються всі види інформації, які є особливими для системи.

* Програмні додатки (Application programs): Компанії купують багато

додатків, які вони використовують, від третіх осіб, але деякі компанії розробляють свої власні програми. Один з найбільш трагічних випадків втрачання даних відбувається, коли програма розробляється внутрішньовідомчо, а потім втрачається вихідний код. Якщо компанія втрачає ці програмні файли, вона не може використовувати будь-які збережені дані. Наявність даних, а не програм, які використовують ці дані, рівносильна втраті даних. Підприємства повинні захищати програми з тією самою ретельністю, як вони захищають самі програмні дані.

* Файли даних (Data files): файли даних - це дуже портативні файли, які

використовуються багатьма програмами, наприклад, такими як електронні таблиці та PDF-документи. Інші файли даних є унікальними для конкретних програм, такі як файли журналу та бази даних. Ці файли можуть бути короткими, постійними, великими або швидко змінюватися, а будь-який сервер компанії може містити їх у кількості сотень тисяч або навіть мільйонів.

Бази даних (Databases): Хоча базу даних можна вважати іншою

програмою з файлами даних, існують спеціальні міркування з захисту баз даних для забезпечення постійності. Будь-який резервний процес не обов'язково захищає бази даних [34].

## 2.4.1 Оцінка ризику

Дані є чутливими до втрати або пошкодження з кількох джерел. Деякі основні причини втрати даних включають:

* Віруси. Ці шкідливі програми можуть проникнути в систему в будь

який час і вдарити, коли користувач найменше цього очікує. Як тільки один пристрій зазнає зараження, вірус може поширюватися від системи до системи, знищуючи дані на цьому шляху.

* Стихійні лиха. Пожежі, повені та сильні вітри можуть призвести до

фізичного пошкодження систем і зробити дані недоступними або нечитабельними.

* Переривання роботи. Системи можуть бути пошкоджені внаслідок

раптової втрати потужності або, ще гірше, невелика частина потоку даних може бути втрачена, що призведе до пошкоджень, які можуть бути невиразними.

* Поломка жорсткого диску. Питання полягає не в тому, чи зламається

жорсткий диск, але коли саме він зламається. Ймовірність аварії жорсткого диску вища протягом 90 днів після введення в експлуатацію та після приблизно трьох років середнього використання.

* Втрата або крадіжка ноутбуків або смартфонів. Значення даних, що

зберігаються на ноутбуці або іншому портативному пристрої, зазвичай набагато перевищує вартість заміни апаратного забезпечення.

* Несправності програмного забезпечення. Мережеве програмне

забезпечення для ОС і мереж може призвести до збою, пошкоджуючи наявні дані.

* Несправності додатків. Програмні додатки не мають гарантії на

відсутність помилок; помилка в додатку може призвести до неповно або неправильно відформатованих або розрахованих даних, які будуть записані у файли.

* Помилка постачальника. При розміщенні електронної комерції або

інших додатків з постачальником SaaS (SoftwareasaService, програмне забезпечення як сервіс), дані можуть опинитися під загрозою, якщо постачальник раптом збанкрутує. [35]

## 2.4.2 Створення плану ВД

Подібно до будь-якого іншого проекту, існує кілька різних кроків, необхідних для розробки плану для успішного ВД після катастрофи. Рекомендовані кроки показано на рис. 2.1:

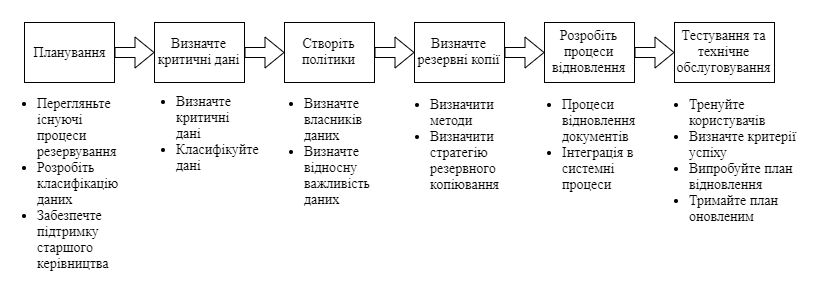


Рис. 2.1 Етапи ВД

1. Планування.
2. Визначення критичних даних (КД).
3. Створення політик.
4. Визначення типів резервних копій.
5. Розробка процесів відновлення.
6. Тестування та технічне обслуговування. [36]

### Планування

Як і в будь-якому проекті, успішний план ВД починається з належного планування. Першим кроком має стати перегляд очікувань щодо ВД із ключовими зацікавленими сторонами. Які їх потреби в бізнесі і чи є нормативні вимоги, в яких вони зацікавлені? Дуже мала кількість організацій не розробляє план ВД, тому наступним кроком має стати перегляд існуючих стратегій резервного копіювання та відновлення. Що саме зараз копіюють і як часто? Чи існують процедури для періодичного тестування резервних копій? Як резервні копії транспортуються та зберігаються? Які нові системи з'явилися в мережі з моменту останнього оновлення документації з резервного копіювання? Чи створюються резервні копії старих файлів, які можна було б архівувати та вилучити з робочих систем?

Необхідно вивчати найбільш дієві та ефективні способи зберігання даних для резервного копіювання. Можливо, компанія має кілька об'єктів, які можуть зберігати дані один одного. Важливо переконатися, що збережені дані не будуть знищені в одній катастрофі.

Також потрібно планувати аналіз та класифікацію даних. В чому цінність резервного копіювання для кожної фірми? Вартість захисту даних повинна бути пропорційною вартості самих даних. Немає сенсу витрачати багато часу і ресурсів, захищаючи дані, які легко відновити іншими засобами.

Є численні стратегії резервного копіювання та ВД. Вони включають в себе традиційні методи зберігання в автономному режимі, такі як роздруківка з паперу, магнітна стрічка, CD-ROM, портативні жорсткі диски тощо. Проте онлайн-методи, що включають дзеркальне відображення дисків та РК в Інтернеті, дозволяють швидше відновити дані. Оцінка та вибір відповідних стратегій мають вирішальне значення для успіху плану відновлення. Також слід враховувати те, чи є використовувані резервні апаратні та програмні засоби останніми версіями від виробника. Багато фірм зазнали аварії та з'ясували, що програмне забезпечення, необхідне для читання їх резервних носіїв, було застарілим, важким і дорогим, або просто більше не було доступним.

Інше важливе питання: де саме будуть зберігатися дані компанії? Найзручніше, якщо фірма має декілька місць, які можуть зберігати дані одне одного. Також можна підписати взаємну угоду з іншою неконкурентоспроможною фірмою для зберігання даних один для одного. Звичайно, потрібно бути достатньо впевненими в тому, що обидва місця не будуть зачепленими однією самою катастрофою. Потрібно переконатися, що обидва учасника можуть обробляти додаткове навантаження, якщо один з них не працює. Цей варіант важко керувати, і на практиці він не завжди добре працює.

ВД у найкоротші терміни дозволить мінімізувати втрату доходів, спричинену пошкодженням або втратою даних. "Час до даних" ̶ критичний показник, який потрібно оцінити при створенні плану відновлення, він визначається як час, потрібний для того, щоб користувачі могли отримати доступ до своїх даних після аварії. [37]

### Визначення КД

Перша проблема, яка виникає при створенні свого плану ВД, - це пошук даних. Кількість даних, що виробляються підприємствами сьогодні, швидко зростає. Це не лише дані, які зберігаються в традиційних базах даних, але також графіка, текстові файли, електронні таблиці, звукові записи та інші поширені форми даних. У багатьох організаціях розмір традиційних баз даних вимірюється в терабайтах (близько 1 трильйона байт); бази даних розміром більше петабайта (1024 терабайт) скоро стануть буденністю. Папір як і раніше є важливим сховищем даних; паперові файли зберігаються у файлові шафи, настінні шухляди тощо. Для даних, які зберігаються в електронному вигляді, є продукти для автоматичного пошуку файлів і баз даних у всій мережі.

Наступне питання після того, як дані були знайдені, полягає в категоризації даних. Як і в паперових файлах, на більшу частину електронних даних, що створюються, більше ніколи не посилаються. Потрібно визначити КД, необхідні для відновлення критичних бізнес-операцій, допоміжні дані, документацію та дані, які необхідно зберегти в силу юридичних вимог.

Значна частина того, що зберігається на файлових серверах користувачами, ̶ це дані, які не є необхідними для роботи компанії. Це дані, які просто витрачають простір, такі як файли електронної пошти, файли кешу в Інтернеті та особисті файли, такі як цифрові зображення. Ці несуттєві дані можуть різко збільшити вартість резервного копіювання та відновлення. При створенні повного дублікату системи буде використано більше дискового простору. РК за допомогою стрічок або компакт ̶ дисків для створення резервних копій вимагатиме додаткові носії. Реплікації на віддаленому місці, для підтримки всіх цих файлів, може знадобитися додаткова пропускна здатність.

Для початку зменшення обсягу непотрібних файлів потрібно створити політику, яка забороняє зберігання особистих файлів на серверах компанії. Суворе дотримання цих правил може суттєво зменшити обсяг даних резервних копій. Також слід розглянути питання про обмеження кількості місць зберігання, доступних кожному користувачеві, що змусить їх ретельно замислитись на тим, що зберігати в їхніх особистих папках.

### Створення необхідних політик та процедур

Більшість компаній не мають політик та процедур для зберігання та класифікації даних. І багато хто з тих, хто має політику, виконують погану роботу з її застосування. Якщо політика не застосовується, це може спричинити помилкове відчуття безпеки, що може бути гірше, ніж взагалі відсутність політики.

Першим кроком у створенні політики зберігання та класифікації даних є визначення власників інформації. Усі дані в компанії повинні мати визначеного власника, який відповідає за розуміння важливості та використання даних.

Коли власники даних були ідентифіковані, розробляється політика для визначення відносної важливості даних та будується схема класифікації інформації. Деякі категорії, які можна використовувати, включають критичну для бізнесу, уразливу, юридично необхідну та некритичну.

* Критична для бізнесу. Це дані, необхідні для ведення бізнесу. Вони

можуть включати в себе списки клієнтів, бухгалтерські файли, креслення тощо.

* Уразлива. Це дані, які не повинні бачити конкуренти компанії. Вони

можуть включати в себе списки клієнтів, списки працівників, документацію з виробництва та інше.

* Юридично необхідна. Це інформація, необхідна для дотримання

державних правил, таких як вимоги законодавства щодо охорони праці та охорони здоров'я, інформація про охорону довкілля, дані щодо найму працівників тощо.

* Некритична. Це інформація, без якої компанія можете існувати. До 90

відсотків всієї інформації, що зберігається в шафах та базах даних, ніколи не використовується знову, тому ця категорія містить велику кількість даних.[38]

### Визначення типу (типів) резервних копій

Різні типи даних та різні вимоги до "часу до даних" вимагають різних процесів резервного копіювання та носіїв. Види резервних копій включають:

* Регулярне РК на стрічку або інший змінюваний носій.
* Віддалене дзеркальне відображення.
* "Електронне сховище" в широкосмуговій мережі або Інтернеті.

### Розробка процесів відновлення

Останній крок ̶ розробка та документування процесу резервування та ВД. Необхідно розробити розклад, щоб забезпечити своєчасне створення резервних копій. Деякі критерії, які слід враховувати при оцінці методів відновлення:

* RTO (Recovery Time Objective - мета часу відновлення). Наскільки

швидко дані повинні бути відновлені, до того як бізнес зазнає негативного впливу?

* RPO (Recovery Point Objective - цільова точка відновлення). Скільки

даних фірма може дозволити собі втратити, до того як бізнес зазнає негативного впливу?

* Доступність. Чи може система бути вимкненою під час створення

резервних копій?

* Відновлення. Наскільки впевненими потрібно бути у спроможності

компанії відновити дані?

* Значення. Скільки коштує ЗД?
* Ефективність. Які вимоги до ефективності програми?

Потрібно також брати до уваги, наскільки ефективно кожен метод відновлення захищає від різних типів втрат. Кожен бізнес-процес може мати свій особливий процес відновлення. [39]

### 

### Варіанти збереження даних

Існує безліч варіантів зберігання даних, кожен з яких має свої переваги та недоліки.

* **РК на стрічку.**

РК на стрічку майже таке ж старе, як самі обчислення. Стрічка має низьку вартість за гігабайт і її відносно легко переносити та зберігати. Стрічка була надійним носієм для зберігання та архівування важливих даних, але вона не є повністю захищеною. Стрічки можуть вийти з ладу, тому критично важливо, щоб резервні копії періодично перевірялися. Аудит слід проводити шляхом випадкового вибору стрічки та перевірки, чи можна читати та відновлювати данні, використовуючи інше обладнання, аніж те, що використовувалося для запису. Надзвичайна ситуація ̶ це не найкращий час, щоб виявити, що касети не зчитуються або їх можна прочитати лише за допомогою обладнання, яке використовувалося для створення резервної копії.

* **Дзеркальне відображення диска.**

За допомогою віддзеркалювання дисків дані записуються на два різних диска, щоб створити дві ідентичні копії для збільшення шансів, що принаймні одна копія даних буде доступна у потрібний час. Основний диск, який використовується для зберігання даних, називається захищеним диском, а диск, на який дані реплікуються, називається резервним диском. Ці два диски можуть зберігатися в одному або в різних місцях. Якщо резервний диск знаходиться в іншому місці від захищеного диску, для доступу до нього використовується WAN. Зберігання резервної копії в іншому місці забезпечує захист від катастрофи, яка виникає на місцезнаходженні захищеного диску. Хоча цей метод є ефективним, він також сильно впливає на мережевий трафік. [40]

* **RAID.**

RAID (Redundant Array of Inexpensive (Independent) Disks) - абревіатура, що означає «резервний масив недорогих (або незалежних) дисків» і використовується для забезпечення відмовостійкості систем зберігання дисків. RAID працює шляхом об'єднання набору дисків у логічний масив дисків за допомогою спеціального контролера дисків, який не вимагає роботи всіх елементів масиву для забезпечення цілісності даних. Він може бути реалізований за допомогою апаратного або програмного забезпечення. RAID-накопичувачі розглядаються ОС як окремі пристрої. RAID також збільшує продуктивність та надійність дисків, поширюючи зберігання даних на кількох, а не на одному диску.

Терміни, що використовуються при описі реалізації RAID:

* Дуплекс (Duplex). Дуплексний диск передбачає використання двох

RAID-контролерів, які одночасно записують однакові дані на два окремих диска. Система, що використовує дуплекс, може пережити невдачу будь-якого контролера диска або жорсткого диска.

* Дзеркальне відображення (Mirroring). Дзеркалювання диска

передбачаєвикористання одного RAID-контролера, який одночасно записує однакові дані на два окремих диска. Система, що використовує дзеркальне відображення, може пережити невдачу жорсткого диска. Як дуплекс, так і дзеркальне відображення можуть знизити продуктивність системи, оскільки дані записуються двічі.

* Чергування (Striping). Чергування полягає у розділенні даних на більш

дрібні частини та записуванні різних частин на декількох дисках. Дані можуть бути розбиті на біти, байти або блоки залежно від використовуваної реалізації RAID. Метод чергування є швидшим за дуплекс або дзеркальне відображення.

* Паритет (Parity). Паритет - це спосіб досягнення надмірності даних без

накладних витрат на дзеркальне відображення на диску за допомогою зберігання логічної інформації про записані дані для полегшення відновлення. Паритет використовується із чергуванням і вимагає принаймні трьох дисків. Інформація паритету зберігається на декількох або на окремому диску.

Існує декілька рівнів експлуатації RAID, кожен з яких має власний баланс надмірності, відмовостійкості, вартості та складності.

* RAID 0. Ця реалізація RAID використовує дискове чергування. Дані

діляться між кількома дисками, що забезпечує хорошу продуктивність, але не забезпечує надмірність. Цей рівень не забезпечує захист від втрати даних, якщо диск перестає працювати, і не рекомендується для ВД.

* RAID 1. Цей рівень RAID передбачає дзеркальне відображення або

дуплекс даних за допомогою двох або більше дисків. Це забезпечує надмірність у разі відмови диску. Продуктивність менша, ніж при використанні RAID 0, особливо під час запису даних. Цей рівень простий і недорогий в реалізації, але 50 відсотків об'єму пам'яті буде втрачено через дублювання даних.

* RAID 2. Бітове чергування. Цей рівень послідовно чергує біти даних по

декількох дисках і використовується з дисками без вбудованого виявлення помилок. Оскільки більшість сучасних дисків мають вбудовані засоби виявлення помилок, цей рівень RAID рідко використовується на сьогоднішній день.

* RAID 3. Байтове чергування. Цей рівень чергує байти даних по

декількох дисках, при цьому інформація про паритет зберігається на окремому диску. Диск з паритетом може бути використаний для ВД у разі аварії. Паритетна інформація знаходиться під загрозою, оскільки вона зберігається тільки на одному диску.

* RAID 4. Блокове чергування. Цей рівень RAID чергує дані на рівні

блоків. Так само, як при RAID 3, інформація про паритет зберігається на окремому диску. Продуктивність більша, ніж у RAID 2 або 3, оскільки дані обробляються блоками.

* RAID 5. Чергування з розподіленим паритетом. Цей рівень подібний до

RAID 4, за винятком того, що інформація про паритет зберігається на доступних дисках. RAID 5 ̶ це поширена реалізація RAID.

* RAID 10. Дзеркальне чергування. Цей рівень RAID (іноді називається

RAID 0 + 1) являє собою поєднання рівнів RAID 0 і 1. Дані чергуються на декількох дисках, а також відображаються у дзеркалі. Це забезпечує найкращу відмовостійкість з усіх рівнів RAID, але, очевидно, даний метод є найдорожчим.[41]

* **Балансування навантаження.**

Балансування навантаження використовується для динамічного розподілу мережевого трафіку по всій групі серверів, що працюють із будь-якою програмою, щоб запобігти перевантаженню сервера. При балансуванні навантаження, група серверів відображається в мережі як окремий сервер. Процес балансування навантаження є частиною мережевої ОС; процес контролює кожен сервер, щоб визначити найкращий шлях для трафіку в мережі для підвищення продуктивності та доступності. Балансування навантаження також дозволяє програмі продовжувати роботу, навіть якщо один з серверів виходить з ладу. Поки принаймні один сервер доступний, програма буде продовжувати працювати.

* **Мережеве сховище.**

Мережеве сховище (NAS - Network Attached Storage) ̶ це загальна область зберігання для декількох серверів. Середовища NAS корисні для зберігання даних або для файлових серверних програм, таких як поштовий та веб-сервіси. Сервер NAS працює з мінімальною ОС і оптимізований для полегшення переміщення та зберігання даних. Використання середовища NAS створює централізовано керований фонд з даними, який дозволяє додавати нові пристрої зберігання без необхідності простою в мережі. Обсяги зберігання з аварійного серверу можна легко переназначити, або, якщо потрібно, можна легко додати новий обсяг пам'яті. Гнучкість, надана середовищем NAS, збільшує доступність і надійність мережевого зберігання, додаючи вартість до стратегії на випадок надзвичайних ситуацій.

* **Мережі зберігання.**

Мережа зберігання (SAN - Storage Area Network) ̶ це високошвидкісна високопродуктивна мережа, яка дозволяє комп'ютерам, що працюють з кількома ОС, зберігати дані на одному віртуальному пристрої зберігання даних. SAN призначена для обробки резервного трафіку більш ефективно, ніж середовище NAS. SAN може бути локальною або віддаленою, і зазвичай зв'язується з сервером за допомогою оптоволоконного каналу. Переміщенням сховища з локальної мережі досягається РК без впливу на продуктивність програм у локальній мережі.

* **РК онлайн.**

Онлайн ̶ зберігання даних стає популярним, оскільки програмне забезпечення як служба (SaaS) все частіше використовується для надання послуг користувачам. За допомогою онлайн ̶ сховища даних зміни до даних поставляються через Інтернет до постачальника послуг. Це дозволяє зберігати дані в безпечному, професійно керованому місці, на відстані від будь ̶ яких небезпек для місцеположення пристроїв з даними.

* **Розподілене РК.**

Розподілене РК - це крок вперед від загального резервного копіювання на мережевому сервері до бездротової системи розподіленої системи резервного копіювання, яка розподіляє резервні дані по всій мережі. Логічно, всі комп'ютери всередині мережі спільно створюють віртуальний сервер, до якого може отримати доступ будь-який клієнт, але фізично, центрального сховища даних немає.

Переваги розподіленого резервного копіювання:

* Технологія розподіленого резервного копіювання легко і послідовно

інтегрується в архітектуру будь-якої мережі невеликих та середніх розмірів та надає численні переваги, що робить її одним з кращих мережевих резервних рішень для підприємств:

* Віртуальний сервер, створений комп'ютерами в системі розподіленого

резервного копіювання, усуває необхідність створення резервних пристроїв зберігання даних: це дозволяє забути про спеціальні диски, схеми їх вилучення, зберігання та чергування. Після налаштування, він забезпечує надійний спосіб резервного копіювання мережевих комп'ютерів.

* Концепція розподіленого (peer-to-peer) резервного копіювання

забезпечує найефективніший спосіб експлуатації вільного дискового простору працівників, забезпечує надійне зберігання даних і дозволяє кожному комп'ютеру отримувати доступ до всіх резервних файлів, навіть якщо деякі машини недоступні.

* Колективний дисковий простір може бути набагато більшим, ніж будь

який жорсткий диск, доступний на ринку, і забезпечує більшу надійність за нижчою ціною.

* Всі дані, що зберігаються на машинах учасників, повторюються кілька

разів за допомогою алгоритму розподіленого рандомізованого розміщення. Усі важливі дані можна подвоїти, потроїти і т. д. відповідно до коефіцієнта реплікації, визначеного адміністратором. Це гарантує безпеку даних, навіть якщо комп'ютер не працює.

* Розподілене РК зберігає всі функції звичайного серверного мережевого

резервного копіювання: забезпечує ефективний захист всіх важливих даних, може бути запланованим і легко поширюватися на будь-яку кількість комп'ютерів [42].

## 2.5 Висновки по розділу

На підставі розглянутого теоретичного матеріалу по захисту даних від втрати за допомогою резервного копіювання можна зробити наступні висновки:

1. Одними із головних цілей описаного виду захисту даних є: здатність

служб до повернення до нормальної роботи так швидко, наскільки це є фізично можливим після виходу з ладу або програмної помилки будь-якого з компонентів; надання можливості отримання даних де це необхідно та коли це необхідно; відповідь нормативним вимогам, а також вимогам зі збереження бізнес-даних; досягнення цілей відновлення та повернення бізнесу на належний операційний рівень у разі стихійного лиха.

1. Кроки, необхідні для досягнення даних цілей, включають в себе:

створення копій всієї значущої інформації, незалежно від типу або структури платформи, на якій зберігаються дані, або програми, яка є джерелом цих даних; управління носіями, які містять у собі ці копії, незалежно від їх числа та місцезнаходження; надання можливості створення додаткових копій даних; здатність розширювати систему резервного копіювання разом із збільшенням об’ємів даних підприємства.

1. При розробці стратегії захисту потрібно враховувати такі критерії,

як: об’єм даних підприємства; критичну важливість даних; складність даних; складність інфраструктури зберігання, в тому числі NAS, SAN, RAID та інші структури; мету часу відновлення (RTO) та цільову точку відновлення (RPO).

# 

# РОЗДІЛ 3

# РОЗРОБКА ПРОГРАМНОГО ДОДАТКУ

## 3.1 Платформа реалізації

Основним критерієм до вибору платформи послугувала можливість кросплатформності у використанні технологійпобудови мережевого зв’язку. Оскільки дана методологія дозволяє абстрагуватися від властивостей і технологій, використаних при створенні графічного інтерфейсу. Тож серед усіх відомих мов програмування вибір падає саме на Java. Віртуальна машина Java забезпечує кросплатформність, що поширюється на усі існуючі на сьогодні найбільш популярні платформи – Windows, Linux, Mac.

Окрім кросплатформності сильними сторонами мови Java є також висока надійність роботи, розвиненість мови. Java була зароджена як об’єктно-орієнтована мова програмування, і надійність цього підходу з роками виправдала себе. Парадигма ООП наділяє мову такою прекрасною властивістю як масштабованість, що дає змогу без особливих труднощів багаторазово розширювати систему. Мова Java створена так, щоб бути максимально простою танадійною. Наприклад, в ній забороняється використовувати множинне наслідування, для запобігання уникнення неоднозначності при зверненні до батьківського класу. Натомість було впроваджено поняття інтерфейсу, який вже не є класом, проте містить загальні рекомендації до створення класів і надає можливість множинного наслідування.

Окремою темою є безпека мови, на якій розробники сконцентрували найбільшу увагу. Тому щоб створити просту, безпечну і безвідмовну мову програмування, в Java існує система винятків або ситуацій, коли програма зустрічається з неочікуваними труднощами, наприклад:

* операції над елементом масиву поза його межами або над порожнім

елементом;

* читання з недоступного каталогу або неправильної адреси URL;
* ввід недопустимих даних користувачем.

Одна з особливостей концепції віртуальної машини полягає в тому, що помилки (виключення) не призводять до повного краху системи. Крім того, існують інструменти, які «приєднуються» до середовища періоду виконання і кожен раз, коли сталося певне виключення, записують інформацію з пам'яті для відлагодження програми. Ці інструменти автоматизованої обробки виключень надають основну інформацію щодо виключень в програмах на Java.

Для ефективного керування пам'яттю під час життєвого циклу об'єкта Java використовує автоматичний збирач сміття. Програміст вирішує, коли створювати об'єкти, а віртуальна машина відповідальна за звільнення пам'яті після того, як об'єкт стає непотрібним. Коли до певного об'єкта вже не залишається посилань, збирач сміття може автоматично прибирати його із пам'яті. Проте, витік пам'яті все ж може статися, якщо код, написаний програмістом, має посилання на вже непотрібні об'єкти, наприклад на об'єкти, що зберігаються у діючих контейнерах. Збирання сміття дозволене у будь-який час. В ідеалі воно відбувається під час бездіяльності програми. Збірка сміття автоматично форсується при нестачі вільної пам'яті в купі для розміщення нового об'єкта, що може призводити до зависання. Тому існують реалізації віртуальної машини Java з прибиральником сміття спеціально створеним для програмування систем реального часу.

Java не має підтримки вказівників у стилі C/C++. Це зроблено задля безпеки й надійності, аби дозволити збирачу сміття переміщувати вказівникові об'єкти.

## 3.2 Загальні відомості

Для реалізації графічного інтерфейсу (GUI) в Java існують два основних пакети класів:

* Abstract Window Toolkit (AWT)
* Swing

Перевагами першого є простота використання, інтерфейс подібний до інтерфейсу ОС та дещо краща швидкодія, оскільки базується на засобах ОС, щоправда має обмежений набір графічних елементів. Другий пакет Swing реалізує власний Java інтерфейс.

При написанні даного програмного продукту був використаний пакет Swing.Даний пакет створювався на основі AWT, і має набагато більше можливостей та більшу кількість графічних елементів. Swing-компоненти ще називають полегшеними (англ. lightweight), оскільки вони написані повністю на Java і, через це, є платформонезалежними.Пропонуються наступні компоненти:

|  |  |  |
| --- | --- | --- |
| № | Компонент | Призначення компонента |
| 1 | JLabel | «Мітка» - виведення однорядкового неформатованого тексту |
| 2 | JButton | «Кнопка» - кнопка з текстом і/або з картинкою |
| 3 | JToggleButton | «Западаюча кнопка» - кнопка з фіксацією. Може бути однією з декількох таких кнопок у групі, у цьому випадку натискання однієї кнопки викликає відпускання іншої. Робота групи забезпечується компонентом ButtonGroup |
| 4 | JCheckBox | «Чекбокс» - пункт вибору з незалежною фіксацією. |
| 5 | JRadioButton | "Радиокнопка» - пункт вибору із залежною фіксацією, повинен бути одним з декількох у групі. Робота групи забезпечується компонентом ButtonGroup. |
| 6 | ButtonGroup | Забезпечує роботу груп компонентів JToggleButton або JradioButton. |
| 7 | JComboBox | «Комбобокс» - список, що випадає. |
| 8 | JList | «Прокручуваний список» |
| 9 | JTextField | «Текстове поле» - однорядковий пункт введення й редагування тексту. |
| 10 | JTextArea | «Текстова область» - багаторядковий пункт введення й редагування тексту |
| 11 | JPanel | «Панель» - компонент, що дозволяє розташовувати на собі інші компоненти. Пересування панелі переміщає разом з нею всі розташовані на ній компоненти. За замовчуванням властивість layout (розміщення) встановлено як FlowLayout – «у вигляді потоку». Для простих задач замість цього компонента краще використовувати JLayeredPane |
| 12 | JTabbedPane | «Панель із закладками» - кожний покладений на неї компонент показується в окремій закладці |
| 13 | JScrollBar | Незалежна смуга прокручування. Використовується рідко - для програмно керованого прокручування вмісту компонентів, для яких відсутнє вбудоване прокручування. |
| 14 | JScrollPane | «Панель зі смугами прокручування» |
| 15 | JMenuBar | «Меню форми» - призначено для розташування в ньому компонентів типу JMenu (заголовків меню) |
| 16 | JPopupMenu | «Контекстне меню» - призначено для розташування в ньому компонентів типу JMenuItem (пунктів меню) |
| 17 | JSlider | «Повзунок» - використовується для плавного регулювання числових величин, а також пов'язаних з ними програмно регульованих змін |
| 18 | JProgressBar | «Прогресбар» - смуга показу частки виконання задачі. Показує рівень, що відбиває частку виконання задачі |
| 19 | JSplitPane | «Панель із роздільником» - панель, що складаєтьсяз двох частин, між якими є лінія роздільника, яку можна перетаскувати мишею, змінюючи взаємний розмір частин |
| 20 | JFormattedTextField | «Поле введення форматованого тексту» |
| 21 | JPasswordField | «Поле введення пароля» - уводиться текст, що, відображається зірочками. |
| 22 | JSpinner | «Спіннер» - поле введення числа із кнопками збільшення/зменшення |
| 23 | JSeparator | «Сепаратор» - роздільна лінія. Використовується в декоративних цілях для поділу робочих областей форми й інших компонентів, що групують |
| 24 | JTextPane | «Текстова панель» - за замовчуванням автоматично переносить текст на новий рядок. А не розташовує в один рядок з показом горизонтального скролера, як це робить JTextArea |
| 25 | JEditorPane | «Панель текстового редактора» |
| 26 | JTree | «Дерево» - показує дерево, у якому кожна галузь може бути з іконками й текстом |
| 27 | JTable | «Таблиця» - показ текстової таблиці. Має можливість заповнення значеннями за замовчуванням на етапі проектування |
| 28 | JToolBar | «Тулбар» - панель інструментів. Звичайно на ньому розміщують кнопки JToggleButton, для яких призначені іконки |
| 29 | JInternalFrame | «Дочірнє вікно» - вікно багатовіконного додатка. Його можна переміщувати в межах батьківського вікна - головного вікна додатка |
| 30 | JLayeredPane | «Панель із абсолютним позиціонуванням елементів» |
| 31 | JDesktopPane | «Панель - робочий стіл». Ще один тип панелі з абсолютним позиціонуванням елементів |
| 32 | JOptionPane | «Діалогова панель» - призначена для відображення діалогових форм. На відміну від більшості інших компонентів робота йде за допомогою методів класу |
| 33 | JColorChooser | «Діалог вибору кольору» |
| 34 | JFileChooser | «Діалог вибору файлу» |
| 35 | JFrame | «Екранна форма» |
| 36 | JDialog | «Діалогова форма» |

Вікно верхнього рівня (таке, що не містить в середині іншого вікна) в мові Java називається фреймом (frame - каркас). В бібліотеці Swing для цього вікна призначений клас JFrame.

Фрейм - це контейнер в який поміщають всі інші компоненти (меню, кнопки, прапорці та інші елементи графічного елементу). Сам клас JFrame, який реалізує фрейм, складається з чотирьох областей (pane), що накладаються одна на одну: коренева область (root pane), область шару (layered pane), прозора область (glass pane) та область вмісту (content pane). Перші три застосовують для створення та обслуговування меню. Для роботи з графічними елементами застосовується область вмісту, в яку і додають компоненти.

Обробка подій

Натиснення кнопки, закриття вікна, клацання мишкою – все це є прикладами подій, які отримує ОС і передає відповідній програмі на обробку. Програміст повинен передбачити як потрібно обробляти дані події.

В Java запропонована, так звана, модель делегування подій (event delegation model). Джерело події (event source) породжує подію, після чого вона передається в обробник подій (event listener – дослівно слухач події). При цьому будь-який об’єкт може бути призначеним як обробник деякої події. Така модель доволі гнучка, оскільки кожен програміст може вибрати зручний для нього спосіб обробки події (де саме її обробляти), проте інколи текст програми може бути дещо заплутаним для тих хто не звик до такої моделі.

Інформація про подію інкапсулюється у об’єкті події (event object). Всі події описуються підкласами java.util.EventObject. Як приклади можна навести підкласи ActionEvent та WindowEvent. Перші об’єкти породжують кнопки, а другі вікна.

Джерела подій містять методи, які дозволяють зв’язати його з обробниками подій. Коли виникає подія, джерело повідомляє про неї усіх зареєстрованих обробників. Обробники подій на основі інформації у об’єкті події визначає як реагувати на ту чи іншу подію.

При розробці графічного інтерфейсу розробнику необхідного здійснити наступне:

* Створити клас, який оброблятиме подію чи ряд подій і, який

реалізовуватиме відповідний інтерфейс;

* Створити джерела подій (вікно, кнопки, смугу прокрутки тощо);
* Зв’язати джерела подій з обробниками подій.

## 3.3 Робота з програмою

Головна форма містить наступні компоненти:

* Кнопки для швидкої роботи з програмою:
  + - 1. Кнопка «Host Info» призначена для отримання програмою

інформації про клієнта. Інформація містить у собі ім’я клієнта, його IP-адресу у локальній мережі, порт, на якому виконується програма, та повну адресу каталогу, в якому будуть зберігатися резервні копії.

* + - 1. Кнопка «Discover peers» знаходить комп’ютери в мережі, готові

приймати або віддавати резервні копії.

* + - 1. Кнопка «Choose file to save» викликає інтерфейс файлового

менеджеру для вибору файлу, що потребує збереження.

* + - 1. Кнопка «Save» зберігає файл на обраному комп’ютері в мережі.
      2. Кнопка «Get list of backups» відображає список резервних копій,

що містяться на обраному комп’ютері в мережі.

* + - 1. Кнопка «Remove» видаляє обрану резервну копію з комп’ютера.
      2. Кнопка «Restore» відновляє файл з обраної резервної копії.
* Елементи для відображення результатів роботи програми (списки, текстові поля).

Скріншот головного вікна програми в системі представлено на рисунку 3.1.

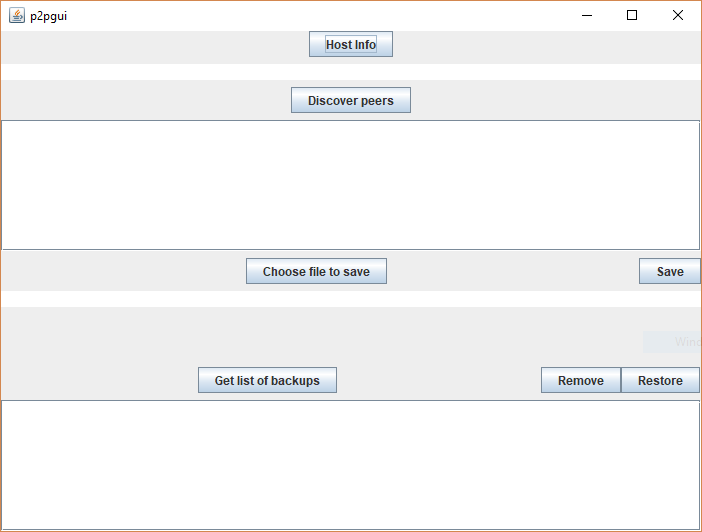


Рис. 3.1 Головне вікно програми резервного копіювання.

Розглянемо більш детально роботу з програмою резервного копіювання.

Перед початком роботи користувачу необхідно відредагувати файл конфігурації *ini.txt*, що містить у собі ім’я клієнта, його IP-адресу у локальній мережі, порт, на якому виконується програма, та повну адресу каталогу, в якому будуть зберігатися резервні копії. Скріншот вмісту конфігураційного файлу в системі, відкритого для перегляду в програмі «Блокнот» представлено на рисунку 3.2.

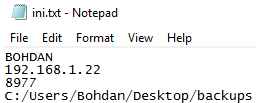


Рис. 3.2 Вміст конфігураційного файлу

При натисканні на кнопку «Host Info» програма зчитує необхідну для коректної роботи інформацію з даного файлу та відображає її у текстовому полі.

Наступним кроком є встановлення складу учасників обміну резервними копіями. Для цього програмі необхідна інформація про IP-адресу мережі, а також номер порту, через який буде встановлюватись з’єднання з іншими «пірами». Скріншот елементу головного вікна програми, що відображає отримані про комп’ютер дані, представлено на рисунку 1.3.

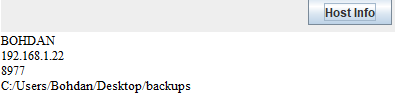


Рис. 3.3 Інформація про комп’ютер, відображена на інтерфейсі

При натисканні на кнопку «Discover peers» виконується алгоритм пошуку клієнтів програми у локальній мережі:

* з отриманої раніше IP-адреси вилучається адреса мережі;
* на кожен комп’ютер у мережі надсилається запит на отримання

інформації про нього;

* комп’ютер, що отримав запит, повідомляє програмі-ініціатору своє

ім’я, яке відображається у списку знайдених «пірів» нижче разом із IP-адресою;

* програма створює об’єкт класу Peer для кожного знайденого

комп'ютера, зберігаючи таким чином інформацію про нього для подальшого обміну.

Скріншот елементу головного вікна програми, що відображає знайдені «піри», представлено на рисунку 3.4.



Рис. 3.4 Список комп’ютерів-учасників обміну резервними копіями

Після цього користувач має обрати комп’ютер в мережі (шляхом обирання його зі списку), на якому він бажає зберегти резервну копію того чи іншого файлу та натиснути на кнопку «Choose file to save». У вікні файлового менеджеру потрібно обрати файл. Скріншот вікна файлового менеджеру представлено на рисунку 3.5.

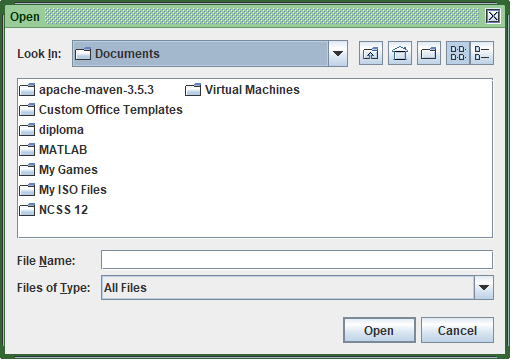


Рис. 3.5 Файловий менеджер.

По натисканню на кнопку «Open»ім’я файлу відобразиться у текстовому полі під кнопкою «Save», після натискання на яку файл буде піддається шифруванню алгоритмом AES та посилається по мережі до обраного комп’ютера. Скріншот елементу головного вікна програми, що відображає ім’я обраного файлу, представлено на рисунку 3.6.



Рис. 3.6 Обраний для збереження файл.

На приймаючому комп’ютері байти записуються у файл з розширенням *.file*, якому надається унікальне ім’я, що складається з імені комп’ютера-власника файлу, дати відправки та часового коду. Також створюється допоміжний файл з аналогічним ім’ям, але з закінченням *.info.txt*, що містить у собі повний шлях до файлу в системі комп’ютера-власника файлу. Це необхідно для того, щоб у майбутньому відновити файл у тому ж місці, де він знаходився з самого початку. Скріншот зі списком збережених копій в системі представлено на рисунку 3.7.



Рис. 3.7 Збережена у системі резервна копія та її допоміжний файл

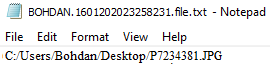


Рис. 3.8 Вміст допоміжного файлу

По натисканню на кнопку «Get list of backups»на обраний комп’ютер в мережі надсилається запит на отримання списку збережених на ньому резервних копій, що належать цьому клієнту. Комп’ютер обирає файли, ім’я яких містить у собі ім’я комп’ютера, що запитує, та відсилає список з унікальними іменами копій та початковими іменами файлів у відповідь. Отриманий список відображається у відповідному полі. Скріншот елементу головного вікна програми, що відображає список резервних копій, збережених на обраному «пірі» представлено на рисунку 3.9.



Рис. 3.9 Список резервних копій, доступних для відновлення

За допомогою кнопок «Remove» та «Restore»користувач може видалити копію з комп’ютера або відновити файл відповідно. Після відправленого запиту на відновлення файлу комп’ютер-власник отримує повну адресу файлу, створює його за даною адресою та записує отримані байти до створеного файлу, попередньо дешифрувавши їх.

3.4 Висновки по розділу

В результаті проведеної роботи по розробці сервісу для зберігання даних шляхом створення резервних копій на інших комп’ютерах локальної мережі вдалося створити зручний та простий у використанні програмний додаток. Програма підтримує різноманітні версії сучасних ОС.

Всі цілі і задачі даної роботи були досягнуті. За час роботи був отриманий досвід розробки додатків мовою Java з використанням сторонніх бібліотек.

Був реалізований основний функціонал, якого достатньо для швидкого та безпечного обміну резервними копіями. До основного функціоналу відноситься можливість обирання, шифрування, та зберігання файлів. Також є можливість відновлення файлу з резервної копії та видалення старих резервних копій. Для продуктивної роботи з додатком не потрібно переміщатись між вкладками та вікнами, інтерфейс є інтуїтивно зрозумілим, що дозволяє максимально ефективно використати місце на екрані та сконцентрувати увагу користувача на потрібних функціях.

Програма була протестована та показала свою працездатність на реальних пристроях на платформі Windows (стаціонарний ПК та ноутбук).

# ВИСНОВКИ

Постійно зростаючий попит на комп'ютерну техніку, глобальна комп'ютеризація суспільства, в даний час невипадкові. Все більше різних послуг населенню надаються за допомогою електронних терміналів, основною частиною яких є персональний комп'ютер. Дуже багато завдань з управління різними процесами на виробництві, по організації роботи і контролю за громадським транспортом, організації перевезень також покладено на обчислювальні машини. Якщо в будь-якому з процесів будуть перебої, то наслідки можуть виявитися непередбачуваними. Тому питання щодо захисту і резервного копіювання інформації в даний час стоїть досить гостро. Подальший розвиток технології та інформатизації спричинить за собою сильне зростання кількості інформації, що зберігається. Тому дослідження в сфері зберігання та резервного копіювання інформації в даний час дуже затребувані, і в подальшому будуть розвиватися, а програмні продукти вдосконалюватися і підлаштовуватися під потреби суспільства.

В роботi звернено увагу на необхiднiсть проведення резервного копiювання з точки зору iнформацiйної безпеки, коротко проаналiзовано iснуючi методи резервного копiювання.

У даній роботі описані етапи розробки власного програмного забезпечення, що реалізує механізм резервного копіювання таВД.Реалізовано можливістьвідновлення окремого файлу або цілої папки на вказаний момент часу. Крім того, створено зручний для користувача інтерфейс.

Основною перевагою даної програми є економія дискового простору на локальній машині за рахунок збереження копій на віддаленій машині. Безпека передачі даних на віддалену машину забезпечена за допомогою шифрування резервних копій перед відправкою.

Розроблене програмне забезпечення є готовим продуктом, який може використовуватися як рядовими користувачами, так і комерційними організаціями з метою збереження і ЗІ.

# СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Грайворонський М. В. Безпека інформаційно-комунікаційних систем / М. В. Грайворонський, О. М. Новіков. – К. : Видавнича група BHV, 2009. – 608 с.
2. Дорошенко А. Н. Информационная безопасность. Методы и средства защиты информации в компьютерных системах : учебн. пособ. / А. Н. Дорошенко, Л. Л. Ткачев. – М. : МГУПИ, 2006. – 143 с.
3. Кузнецов О. О. Захист інформації в інформаційних системах / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2011. – 512 с.
4. Потий А. В. Стандартизация и сертификация в сфере защиты информации. Стандарты механизмов безопасности : учебн. пособ. / А. В. Потий. – Х. : ХНУРЕ, 2002. – 80 с.
5. Хорошко В. А. Методы и средства зашиты информации / В. А. Хорошко, А. А. Чекатков. – К. : Юниор, 2003. – 504 с.
6. Щеглов А. Ю. Защита компьютерной информации от несанкционированного доступа / А. Ю. Щеглов. – СПб. : Наука и Техника, 2004. – 384 с.
7. Ведеев Д. Захист даних в комп'ютерних мережах. Відкриті системи / Д. Ведеев– М.:Спарк, 2004. – 120 c.
8. Поповский В. В. Защита информации в телекоммуникационных системах : учебник / В. В. Поповский, А. В. Персиков. – Х. : ООО "Компания СМИТ", 2006. – Т. 1. – 292 с.
9. Казарин О. В. Безопасность программного обеспечения компьютерных систем / О. В. Казарин. – М. : МГУЛ, 2003. – 212 с.
10. Галицкий А. В. Защита информации в сети – анализ технологий и синтез решений / А. В. Галицкий, С. Д. Рябко, В. Ф. Шаньгин. – М. : ДМК Пресс, 2004. – 616 с.
11. Левин В.К. Защита информации в информационно-вычислительных cистемах и сетях // Программирование. - 1994. - N5. - C. 5-16.
12. Про інформацію : Закон України від 2 жовтня 1992 р. № 2657-ХІІ // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650.
13. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 5 липня 1994 р. № 80/94-ВР // Відомості Верховної Ради України. – 1994. – № 31. – Ст. 286.
14. Joel Berman. Backup For Dummies, Acronis Special Edition. - Hoboken, NJ: John Wiley & Sons, Inc., 2014.
15. Макарова Н.В. /Інформатика. – СПб: Пітер, 2009. - 684 с.
16. ПоспєловД.А. /Інформатика: Енциклопедичний словник. - М.:Педагогика-Пресс, 2006. – 342 с.
17. Сухова С.В. /Система безпеки мережі. - М.: Видавничий центр, 2002. – 672 с.
18. Гайдамакин Н.А. /Розмежування доступу до інформацією комп'ютерних системах. – СПб: Пітер, 2005. – 688 с.
19. Daemen J. AES Proposal: Rijndael, AES Algorithm Submission [Electronic resource] / J. Daemen, V. Rijmen. – Access mode : <http://www.docstoc.com/docs/14641406/AES-Implementation-and-Performance-Evaluationon-8-bit-Microcontrollers>.
20. Distributed backup solution for corporate networks [Електронний ресурс]. URL: <https://www.handybackup.net/distributed-backup-system.shtml>.
21. Баранов В М. и др. Защита информации в системах и средствах информатизации и связи. Учебное пособие. – СПб.: 1996. – 111 с.
22. Назарова З. /Комп'ютерні технології обробки інформації. – М.:Росстат, 2006. – 384 с.
23. Касперски До. /Відновлення даних. Практичне керівництво. – М.:Бук-пресс, 2006. - 224 с.
24. Феоктисов Г.Г. / Інформаційна безпеку суспільства, особистість і засоби інформації Інформатика і обчислювальної техніки. – М.: Пітер, 2003. – 379 с.
25. Department of Defense Trusted Computer System Evaluation Criteria [Electronic resource]. – Access mode : http://www.dynamoo.com /orange/fulltext.htm.
26. Гультяев О.К. /Відновлення даних. — СПб.: Пітер, 2006. — 379 с.
27. Millan W. Boolean function design using hill climbing methods / W. Millan, A. Clark, E. Dawson // In 4th Australasian Conference on Information, Security and Privacy. – 1999. – Num. 1587. – P. 1–11.
28. Дергачова Є.В. /Роль інформаційного протиборства у сучасних умовах. Інформатика і обчислювальної техніки. – М.: Москва, 2002. – 188 с.
29. Потий А. В. Стандартизация и сертификация в сфере защиты информации. Стандарты механизмов безопасности : учебн. пособ. / А. В. Потий. – Х. : ХНУРЕ, 2002. – 80 с.
30. Мельников В.В. Защита информации в компьютерных системах. М.: Финансы и статистика. – 1997. – 364 с.
31. Шафрин Ю.Д. /Інформаційні технології: у двох частинах. – М.:Бином, лабораторія знань, 2009. – 704 с.
32. Michael Wallace, Lawrence Webber. The disaster recovery handbook: a step-by-step plan to ensure business continuity and protect vital operations, facilities, and assets, Second Edition. - New York, NY: AMACOM, 2011.
33. Cheswick W.R., Bellovin S.M. Firewalls and Internet Security: Repelling the Wily Hacker. - Addison-Wesley, 1994. - 275 c.
34. Герасименко В. А. Основы теории защиты информации в автоматизированных системах обработки данных / В. А. Герасименко. – М. : Деп. в ВИНИТИ, 1991. – 410 с.
35. Основи інформаційної безпеки / С. В. Кавун, О. А. Смірнов, В. Ф. Столбов – Кіровоград : Вид. КНТУ, 2012. – 414 с.
36. Основы информационной безопасности : учебн. пособ. для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков и др. – М. : Горячая линия – Телеком, 2006. – 544 с.
37. Трубачев А. П. Оценка безопасности информационных технологий / А. П. Трубачев ; под общ. ред. В. А. Галатенко. – М. : СИП РИА, 2001. – 356 с.
38. Концепція технічного захисту інформації в Україні. – [Електронний ресурс]. – Режим доступу : http://zakon1.rada.gov.ua/cgibin/laws /main.cgi?nreg=1126-97-%EF.
39. An Introduction to Computer Security: The NIST Handbook. Draft. - National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, 1994. - 310 c.
40. Г. Король. – Х. : Вид. ХНЕУ, 2010. – 316 с.
41. Основи захисту інформації : навч. посібн. / О. А. Смірнов, Л. Г. Віхрова, С. І. Осадчий та ін. – Кіровоград, 2010. – 322 с.
42. Украинский ресурс по безопасности [Електронний ресурс]. – Режим доступа : <http://kiev-security.org.ua>.

# Додаток А. Програмна реалізація розподіленої системи резервного копіювання(p2pclient.java)

importjavax.swing.\*;

import java.awt.event.ActionEvent;

import java.awt.event.ActionListener;

import java.io.File;

import java.util.List;

public class p2pgui {

public static Host host;

private List<Peer> peers;

private File selectedFile;

private Manager manager = new Manager();

private String [] backupsArray;

private JButton discoverPeersButton;

private JButton hostInfoButton;

private JTextArea hostInfoTextArea;

private JPanel gui;

private JList peersList;

private JScrollPane peersListScrollPane;

private JButton chooseFileToSaveButton;

private JTextArea selectedFileTextArea;

private JButton saveFileButton;

private JButton getListOfBackupsButton;

private JList backupsList;

private JScrollPane backupsListScrollPane;

private JButton restoreButton;

private JButton removeButton;

private JFileChooser fileChooser;

public p2pgui() {

hostInfoButton.addActionListener(new ActionListener() {

@Override

public void actionPerformed(ActionEvent e) {

InfoManager infoManager = new InfoManager();

host = new Host(infoManager.readIniFile());

hostInfoTextArea.append(host.toString());

}

});

discoverPeersButton.addActionListener(new ActionListener() {

@Override

public void actionPerformed(ActionEvent e) {

InitialStart initialStart = new InitialStart();

initialStart.start();

peers = initialStart.getPeers();

DefaultListModel listModel = new DefaultListModel();

for (Peer peer : peers) {

listModel.addElement(peer);

}

peersList.setModel(listModel);

peersList.setSelectedIndex(0);

}

});

chooseFileToSaveButton.addActionListener(new ActionListener() {

@Override

public void actionPerformed(ActionEvent e) {

fileChooser = new JFileChooser();

int returnValue = fileChooser.showOpenDialog(null);

if (returnValue == fileChooser.APPROVE\_OPTION) {

selectedFile = fileChooser.getSelectedFile();

selectedFileTextArea.append(selectedFile.getName());

}

}

});

saveFileButton.addActionListener(new ActionListener() {

@Override

public void actionPerformed(ActionEvent e) {

manager.saveFile(peers.get(peersList.getSelectedIndex()), selectedFile);

selectedFileTextArea.setText(null);

JOptionPane.showMessageDialog(null, "File was saved successfully!");

}

});

getListOfBackupsButton.addActionListener(new ActionListener() {

@Override

public void actionPerformed(ActionEvent e) {

String backups = manager.getListOfBackups(peers.get(peersList.getSelectedIndex()));

backupsArray = backups.split("\\r?\\n");

DefaultListModel listModel = new DefaultListModel();

for (String backup : backupsArray) {

listModel.addElement(backup);

}

backupsList.setModel(listModel);

backupsList.setSelectedIndex(0);

}

});

restoreButton.addActionListener(new ActionListener() {

@Override

public void actionPerformed(ActionEvent e) {

String selectedBackup = backupsArray[backupsList.getSelectedIndex()];

String[] file = selectedBackup.split("\\s+");

manager.restoreFile(peers.get(peersList.getSelectedIndex()), file[0]);

JOptionPane.showMessageDialog(null, "File was restored successfully!");

}

});

removeButton.addActionListener(new ActionListener() {

@Override

public void actionPerformed(ActionEvent e) {

DefaultListModel listModel = (DefaultListModel) backupsList.getModel();

int selected = backupsList.getSelectedIndex();

listModel.remove(selected);

}

});

}

public static void main(String[] args) {

JDialog.setDefaultLookAndFeelDecorated(true);

JFrame frame = new JFrame("p2pgui");

frame.setContentPane(new p2pgui().gui);

frame.setDefaultCloseOperation(JFrame.EXIT\_ON\_CLOSE);

frame.pack();

frame.setVisible(true);

}