# Тема 4

**СТРУКТУРА ТА БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ**

# ПЛАН

1. Структура інформаційних систем.

2. Безпека інформаційних систем.

# 1. Структура інформаційних систем.

Інформаційні системи належать до об’єктів, що складаються з багатьох компонентів – підсистем. Підсистема ІС являє собою її частину, виділену за певною ознакою, наприклад, за видом забезпечення – ресурсу або за функціональним призначенням.

Практично всі різновиди інформаційних систем незалежно від сфери застосування включають один і той же набір *компонентів:*

* функціональні компоненти;
* компоненти системи опрацювання даних;
* організаційні компоненти (рис. 4.1).



Рис. 4.1 Структура інформаційної системи

Під *функціональними компонентами* мають на увазі систему функцій управління – повний набір (комплекс) взаємопов'язаних у часі й просторі робіт з управління, необхідних для досягнення поставлених перед підприємством цілей. Декомпозиція інформаційної системи за функціональною ознакою містить у собі виділення її окремих частин, які мають назву функціональних підсистем (функціональні модулі, бізнес-додатки), що реалізують систему функцій управління. Функціональні підсистеми істотно залежать від предметної області (сфери застосування) інформаційних систем. Специфічні особливості кожної функціональної підсистеми містяться в так званих «функціональних завданнях» підсистеми. Із появою нових інформаційних технологій поняття «*завдання*» розглядається ширше – як закінчений комплекс опрацювання інформації, що забезпечує або видачу прямих керуючих впливів на хід виробничого процесу, або видачу необхідної інформації для прийняття рішень управлінським персоналом.

Вибір складу функціональних завдань функціональних підсистем управління здійснюється звичайно з урахуванням основних фаз управління: *планування*; *обліку, контролю і аналізу; регулювання* (*виконання*).

Наприклад, інформаційна система управління персоналом туристичного підприємства може містити такі функціональні підсистеми:

* планування чисельності персоналу підприємства;
* розрахунок фонду заробітної плати персоналу;
* планування та організація навчання персоналу;
* управління кадровими переміщеннями;
* статистичний облік і звітність;
* довідки за запитом.

Вибір та обґрунтування складу функціональних задач є одним з найважливіших елементів створення інформаційних систем.

*Компоненти системи опрацювання даних*

Основна функція системи опрацювання даних – це реалізація таких типових операцій опрацювання даних:

* збір, реєстрація і перенесення інформації на машинні носії;
* передача інформації в місця її збереження й опрацювання;
* уведення інформації в ЕОМ, контроль уведення та компонування інформації в пам'яті комп'ютера;
* створення і ведення внутрішньомашинної інформаційної бази;
* опрацювання інформації на ЕОМ (накопичення, сортування коригування, вибірка, арифметичне і логічне опрацювання) для вирішення функціональних задач системи (підсистеми) управління об'єктом;
* вивід інформації для здійснення функцій управління;

- організація, управління (адміністрування) обчислювальним процесом (планування, облік, контроль, аналіз реалізації ходу обчислень в обчислювальних мережах).

*Система опрацювання даних* (СОД) призначена для інформаційного обслуговування фахівців різних органів управління підприємства, що приймають управлінські рішення.

Виділення типових операцій опрацювання даних дозволили створити спеціалізовані програмно-апаратні комплекси, що їх реалізують (різні периферійні пристрої, оргтехніку, стандартні набори програм, у тому числі пакети прикладних програм – ППП за допомогою яких реалізують функціональні задачі ІС.

Практично всі системи опрацювання даних інформаційних систем незалежно від сфери застосування їх включають один і той самий набір складових (компонентів), що називаються видами забезпечення. Прийнято виділяти *інформаційне*, *програмне*, *технічне*, *правове*, *лінгвістичне* та ін. забезпечення.

*Інформаційне забезпечення –* це сукупність даних та правил їх отримання, організації структури та зміст інформаційних сукупностей, зберігання та оновлення даних, методи класифікації і кодування інформації, способи організації нормативно-довідкової інформації, побудови банків даних, зокрема побудови та ведення інформаційної бази і т. ін.

*Програмне забезпечення –* сукупність програм постійного користування, що створюють бібліотеки програм, а саме системні програми, пакети прикладних програм, системи управління базами даних (СУБД). Воно являє собою сукупність програм на носіях даних і програмних документів, які призначені для налагодження, функціонування і перевірки працездатності ІС.

*Технічне забезпечення* представляє собою комплекс технічних засобів, що використовується для вводу, обробки, підготовки, збереження, використання та передачі даних; методичні та керівні матеріали; комплект технічної документації; персонал, що обслуговує технічні засоби.

*Правове забезпечення –* це сукупність законодавчих актів, правових норм та нормативів, які регламентують правові відносини під час функціонування ІС та юридичний статус результатів такого функціонування.

*Лінгвістичне забезпечення –* це сукупність мовних засобів, що використовуються на різних стадіях створення та експлуатації СОД для підвищення ефективності розробки і забезпечення спілкування людини і ЕОМ.

*Організаційно-методичне забезпечення –* це сукупність правил, документів, інструкцій та положень, які забезпечують створення системи та взаємодію її складових, описують технологію функціонування ІС, методи вибору і застосування користувачами технологічних прийомів для одержання конкретних результатів під час функціонування ІС.

*Ергономічне забезпечення* являє собою сукупність вимог, що спрямовані на узгодження психологічних та фізіологічних особливостей людини з технічними характеристиками засобів обчислювальної техніки та параметрами робочого місця, середовища, а також створювати найсприятливіші умови праці людини в ІС. Загалом робоче місце має відповідати нормативним значенням рівня освітленості, шуму, випромінення, температури, вологості.

Під *організаційними компонентами ІС* мають на увазі сукупність методів і засобів, що дозволяють удосконалити організаційну структуру об'єктів і управлінські функції, які виконуються структурними підрозділами; визначити штатний розклад і чисельний склад кожного структурного підрозділу; розробити посадові інструкції персоналу управління в умовах функціонування СОД. Впровадження інформаційних систем сприяє удосконаленню організаційних структур, оскільки передбачає визначення розрахункової, тобто науково обґрунтованої, чисельності апарату управління по структурних підрозділах.

# 2. Безпека інформаційних систем.

Широке впровадження інформаційних технологій у життя сучасного суспільства привело до необхідності вирішення проблеми інформаційної безпеки.

*Інформаційна безпека організації* – цілеспрямована діяльність її органів та посадових осіб з використанням дозволених сил і засобів по досягненню стану захищеності інформаційного середовища організації, що забезпечує її нормальне функціонування і динамічний розвиток.

Говорячи про інформаційну безпеку, часто мають на увазі інформаційну безпеку в найзагальнішому сенсі, як комплекс заходів, покликаний зменшити число ймовірних шкідливих сценаріїв чи розмір збитків, яких може зазнати підприємство у разі розголошення конфіденційної інформації. З цієї точки зору інформаційна безпека – це економічний параметр, який повинен враховуватися у роботі підприємства, а інформацію (або дані) можна розглядати як певний товар або цінність, що підлягає захисту, а відтак вона має бути доступною лише для авторизованих користувачів чи програм

*Інформаційна безпека* – стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації.

Надійний захист можливий лише за умови проведення комплексу взаємодоповняльних заходів, з яких можна виділити три основні складові:

* + нормативно-правові засоби;
  + адміністративні заходи;
  + спеціальне обладнання та програмне забезпечення.

*Політика інформаційної безпеки –* це формальний виклад правил, яких повинні дотримуватися особи, що одержують доступ до корпоративних технологій та інформації.

Перелік об'єктів, що можуть підлягати захисту включає:

* + апаратне забезпечення;
  + програмне забезпечення;
  + дані: збережені в реальному режимі, резервні копії і архіви, бази даних, паролі та записи обліку користувачів;

При розробці політики інформаційної безпеки важливим є визначення переліку потенційних загроз:

* + несанкціонований доступ до ресурсів і/або інформації;
* ненавмисне розкриття інформації (наприклад, випадкове ознайомлення з паролем);
* відмова в обслуговуванні користувачів інформаційної системи тими чи іншими видами сервісу – мережевими, WWW, e-mail та ін.;
* різні види атак, що дозволяють проникнути в мережу або перехопити управління мережею;
* комп'ютерні віруси та ін.

*Захист інформації* – сукупність методів і засобів, що забезпечують *цілісність*, *конфіденційність* і *доступність* інформації за умов впливу на неї загроз природного або штучного характеру, реалізація яких може призвести до завдання шкоди власникам і користувачам інформації.

*Сервіс інформаційної безпеки* – це сукупність механізмів, процедур та інших заходів управління для зменшення ризиків, пов'язаних з загрозою втрати або розкриття даних.

*Основними сервісами інформаційної безпеки є:*

* сервіс автентифікації;
* сервіс конфіденційності;
* сервіс цілісності;
* сервіс дотримання зобов'язань.

Першим етапом на шляху захисту ресурсів інформаційної

системи є організація перевірки, чи є користувач, який входить в систему, тим, за кого він себе видає. Сама процедура перевірки носить назву *автентифікації* користувача. Як правило, процедура автентифікації складається з двох кроків: *ідентифікації* та *верифікації*.

Під *ідентифікацією* розуміють процедуру представлення користувача системі. Звичайно це відбувається шляхом уведення імені, під яким користувач зареєстрований в цій системі.

*Верифікація –* це процедура яку система виконує для того, щоб переконатися, що користувач, який входить в систему, є саме тим, чиє ім'я він ввів при ідентифікації. Для цього користувачу пропонується ввести пароль *(password),* який буде порівняний з паролем в записі обліку цього користувача*.*

Серед альтернативних методів автентифікації варто відзначити *біометричні*. У наш час вони стають поширеними не лише у надсекретних організаціях, а й системах масового користування.

*Конфіденційність* означає, що доступ до інформації може бути наданий тільки тим суб'єктам, що мають на це право. Якщо необхідно, для забезпечення конфіденційності використовується *шифрування даних*.

*Сервіс цілісності даних* забезпечує захист від навмисної або випадкової зміни даних.

*Сервіс дотримання зобов'язань* гарантує, що учасники інформаційного обміну не зможуть заперечити факт своєї участі в ньому. Тобто, наприклад, відправник не зможе відмовитися від факту передачі даних, адресат – від факту їх прийому. Цей сервіс може бути реалізований за рахунок використання *цифрового підпису*.

*Шифрування* – це перетворення даних у форму, що не дає можливості безпосереднього сприйняття зашифрованої інформації.

Шифрування здійснюється з використанням *криптографічного ключа* (key), з використанням ключа здійснюється і зворотна процедура *дешифрування*.

*Криптографія –* це наука засекречування інформації, тобто перетворення її в форму, яка недоступна для прочитання без наявності ключа.

Прикладом застосування криптографії є банківські послуги і платежі в діалоговому режимі. Електронний бізнес може існувати тільки за умови конфіденційності інформації, одним з найкращих методів забезпечення якої є криптографія.

Якщо відправник і одержувач користуються одним і тим же ключем, тобто для шифрування і дешифрування використовується один ключ, то така методика шифрування називається *симетричною криптографією.*

*Асиметрична криптографія* передбачає використання для шифрування і дешифрування двох різних ключів.

Алгоритми асиметричного шифрування використовуватись для створення цифрових підписів, базуючись на двох положеннях:

- таємний ключ захищений і доступ до нього має тільки власник;

- єдиний спосіб створити цифровий підпис – це використати секретний ключ.

*Цифровий підпис* є унікальним для повідомлення. Кожна комбінація повідомлення і таємного ключа буде видавати різні підписи.

*Цифровий підпис* – це конкретна реалізація криптографічної системи з відкритим ключем. Існує ще поняття електронного підпису.

*Електронний підпис* – це будь-який знак або процедура, реалізовані електронними засобами та призначені для зв'язання запису з зобов'язаннями або завірення справжності запису. Прикладами електронного підпису може бути вихідний сигнал складного біометричного пристрою, який працює на розпізнаванні відбитків пальців.

*Захист апаратних пристроїв*

Комп'ютер може вийти з ладу не тільки внаслідок збою операційної системи, дій користувача чи зловмисника, а й в результаті збою аппаратною пристрою.

Для захисту від збоїв апаратури необхідно вживати наступні заходи:

* забезпечення безперебійного живлення;
* резервування апаратного забезпечення;
* резервування даних.

*Захист мереж від зовнішніх втручань*

Для захисту від зовнішнього вторгнення сьогодні існує безліч систем, які є різного роду фільтрами, що допомагають виявити спроби несанкціонованого втручання на ранніх етапах і по можливості не допустити зловмисників у систему через зовнішні мережі.

*Захист від комп 'ютерних вірусів*

Прикладом одного з найбільш поширених типів втручання в роботу мережі, яким не можна нехтувати, є комп'ютерний вірус. Добра безпека передбачає своєчасне виявлення вірусів і негайну реакцію на них.

Інформаційна безпека часто залежить від так званого *людського фактору,* пов'язаного з тим, що інформаційні системи створюються, модернізуються і керуються людьми, і від їхньої чесності, професійних якостей і майстерності залежить довіра споживачів та загальний успіх усього підприємства. Результати безлічі досліджень показують, що найбільше занепокоєння в організаціях викликає саме внутрішня загроза – навмисні чи ненавмисні дії власних працівників.

У проблемі захисту від внутрішніх загроз розрізняють два аспекти: технічний і організаційний.

*Технічний аспект* полягає в прагненні виключити будь-яку імовірність несанкціонованого доступу до інформації.

*Організаційний аспект* полягає в розробці раціональної політики внутрішнього захисту:

* + введення загальної культури дотримання безпеки в компанії;
  + створення системи делегування повноважень і колективної відповідальності;
  + проведення періодичних тренінгів для персоналу з питань безпеки і кіберзлочинності та ін.