Лекція 12

ОСНОВНІ МОДЕЛІ ТЕОРІЇ ЗАХИСТУ ІНФОРМАЦІЇ

ПЛАН

1. Рівні інформаційно-комунікаційної системи
2. Несанкціонований доступ на різних рівнях інформаційно-комунікаційної системи
3. Моделі загроз і потенційного порушника.
4. Причини порушення безпеки.

1. Рівні інформаційно-комунікаційної системи

Рівень мережі – відповідає за взаємодію вузлів ІКС.

Елементами ІКС, що належать до цього рівня, є модулі, які реалізують стеки протоколів мережної взаємодії, наприклад TCP/IP. Також на цьому рівні функціонує специфічна апаратура – мережне обладнання.

Рівень операційних систем – відповідає за обслуговування програмного забезпечення, яке реалізує більш високі рівні, і його взаємодію з обладнанням.

Серед типових представників цього рівня можна назвати такі поширені ОС, як Microsoft Windows, Sun Solaris і Linux.

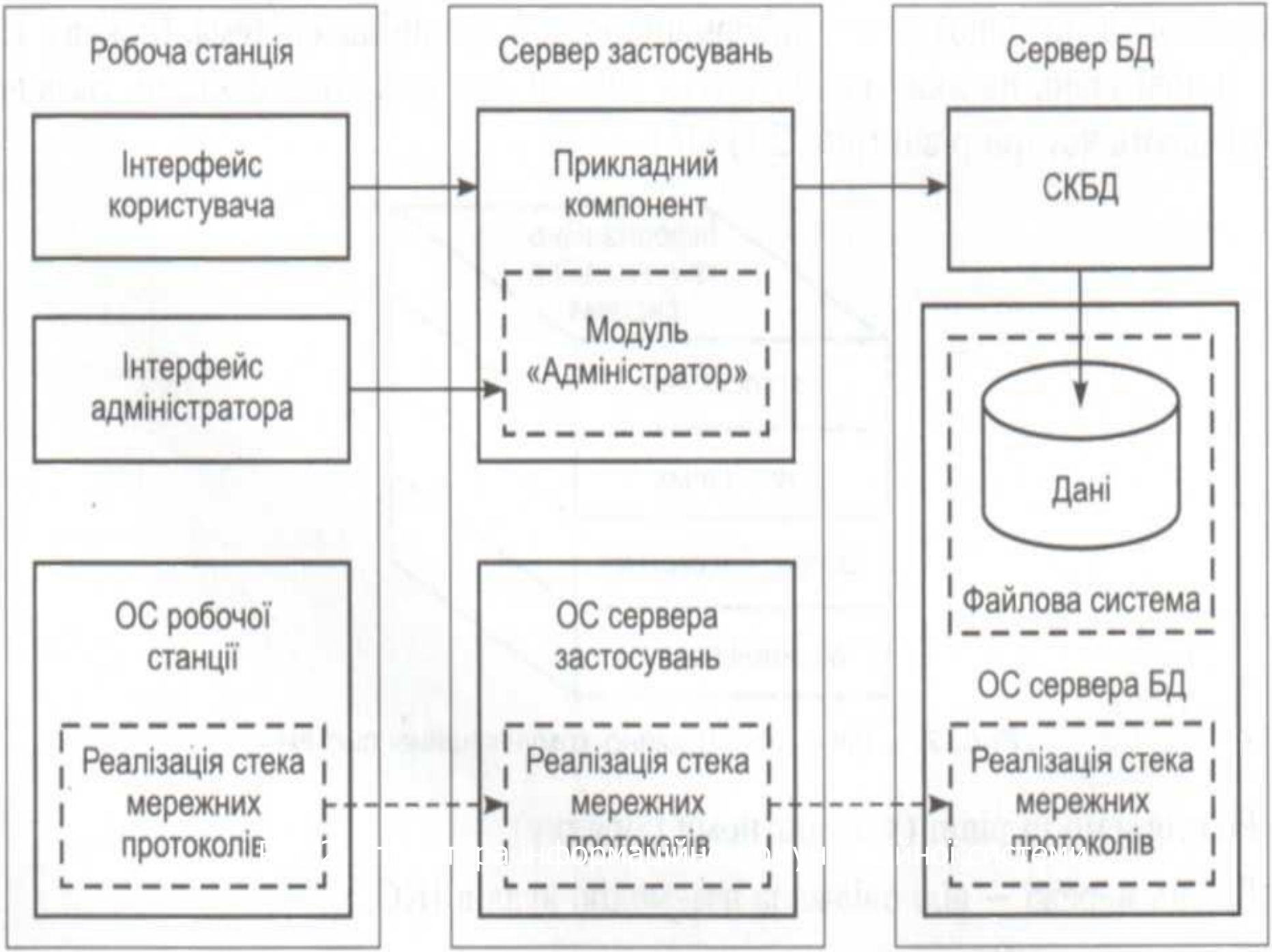
Рівень систем керування базами даних (СКБД) – відповідає за зберігання та оброблення даних.

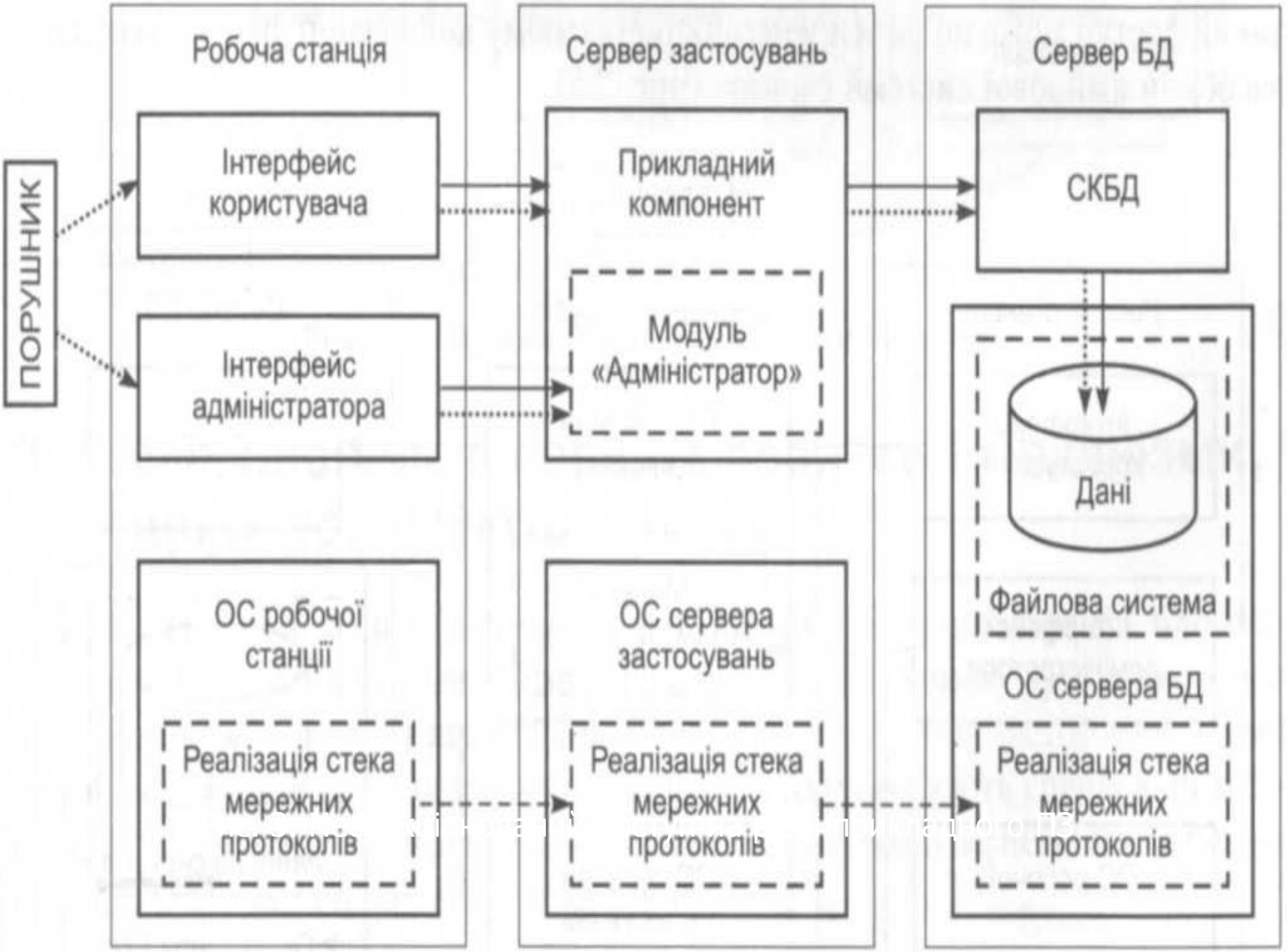
Серед типових представників цього рівня можна назвати СКБД Oracle, а також MS SQL Server. Іноді СКБД є центральним елементом ІКС, а іноді виконує допоміжні функції, зокрема для зберігання технологічної інформації самої ІКС.

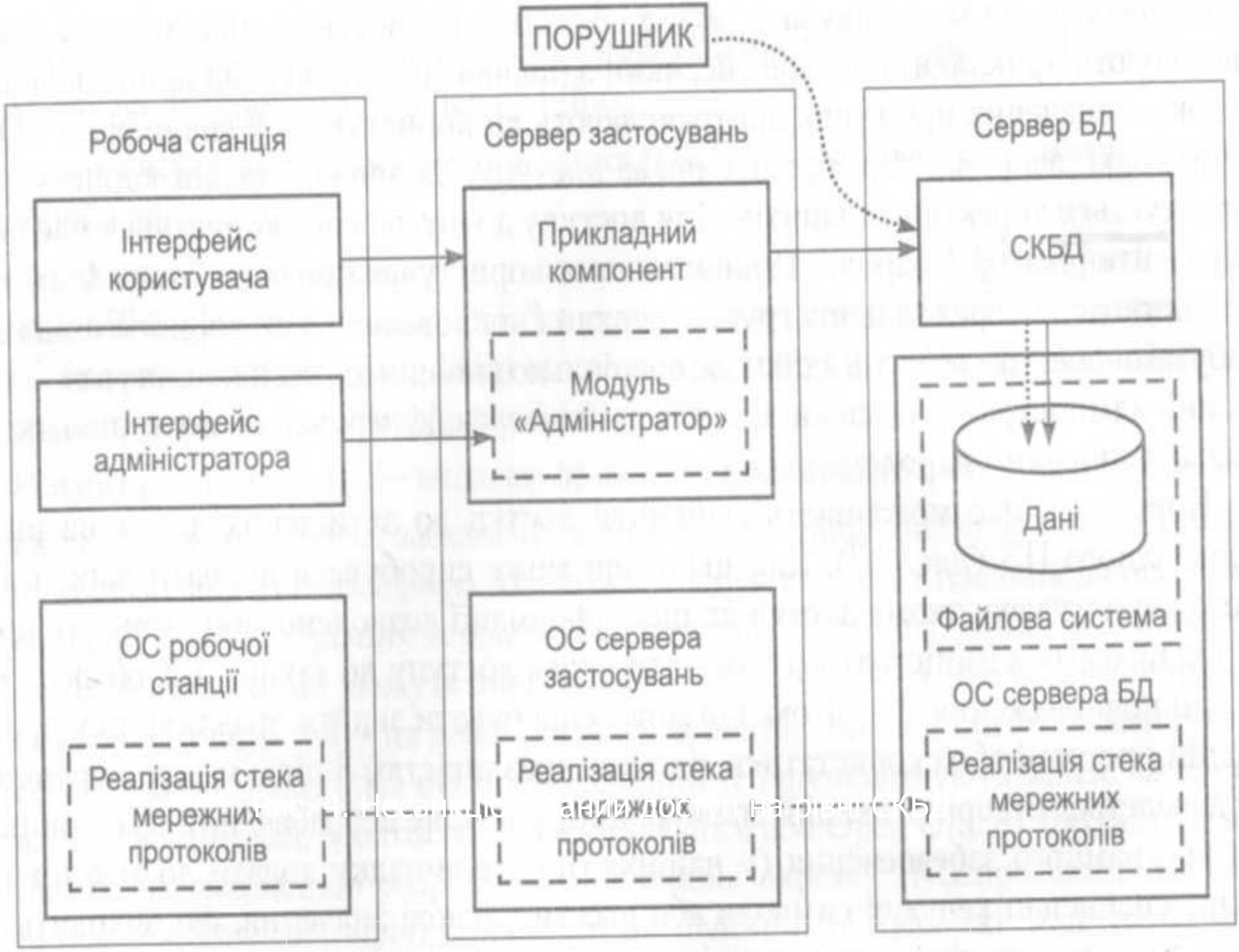
Рівень прикладного ПЗ – включає прикладний компонент і компонент подання.

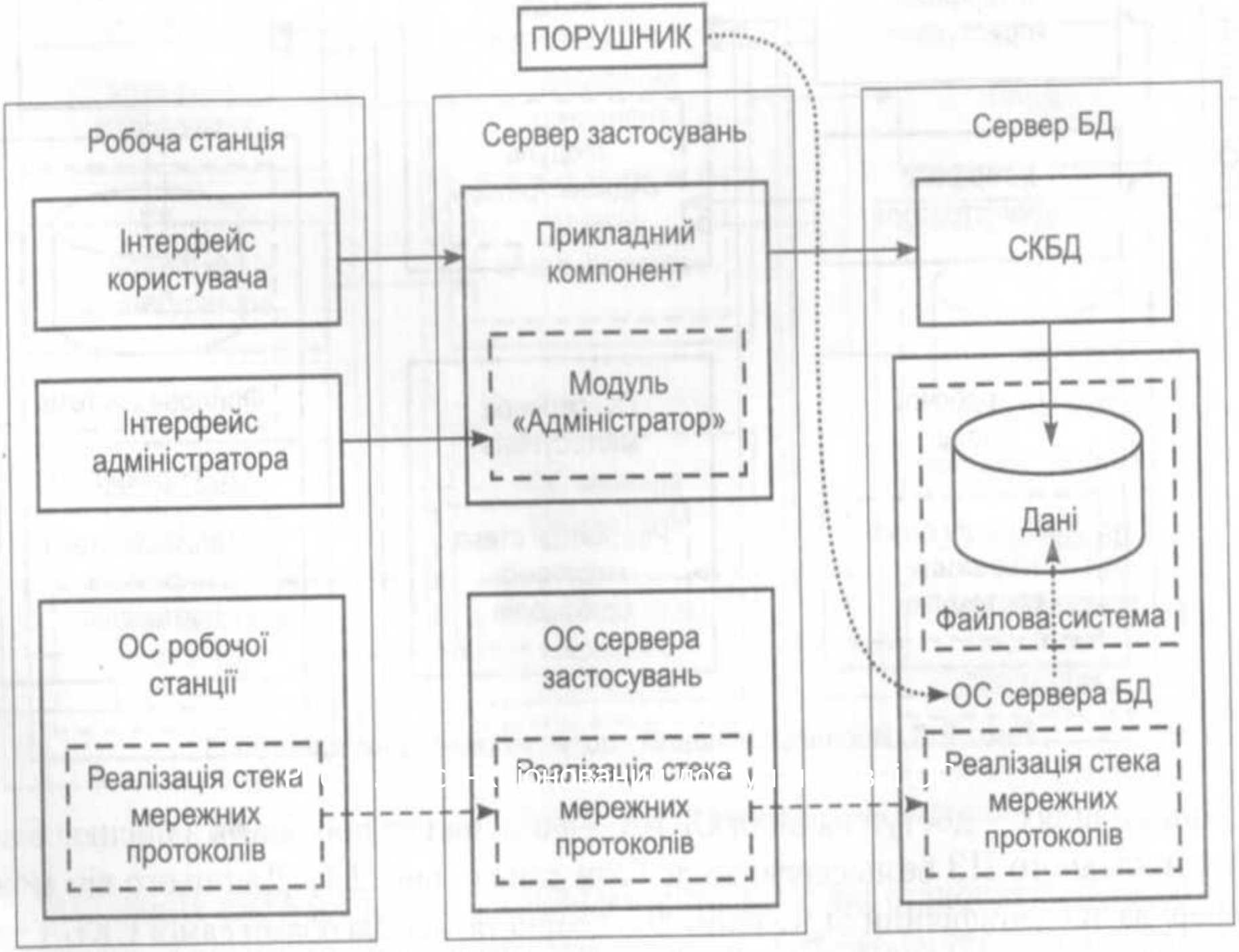
Прикладний компонент забезпечує виконання специфічних функцій ІКС. Компонент подання відповідає за взаємодію з користувачем і подання даних у необхідній формі. У різних варіантах архітектури ІКС прикладний компонент і компонент подання можуть міститися на одному або на різних комп'ютерах (компонент подання – на робочій станції клієнта, прикладний компонент – на сервері застосувань).

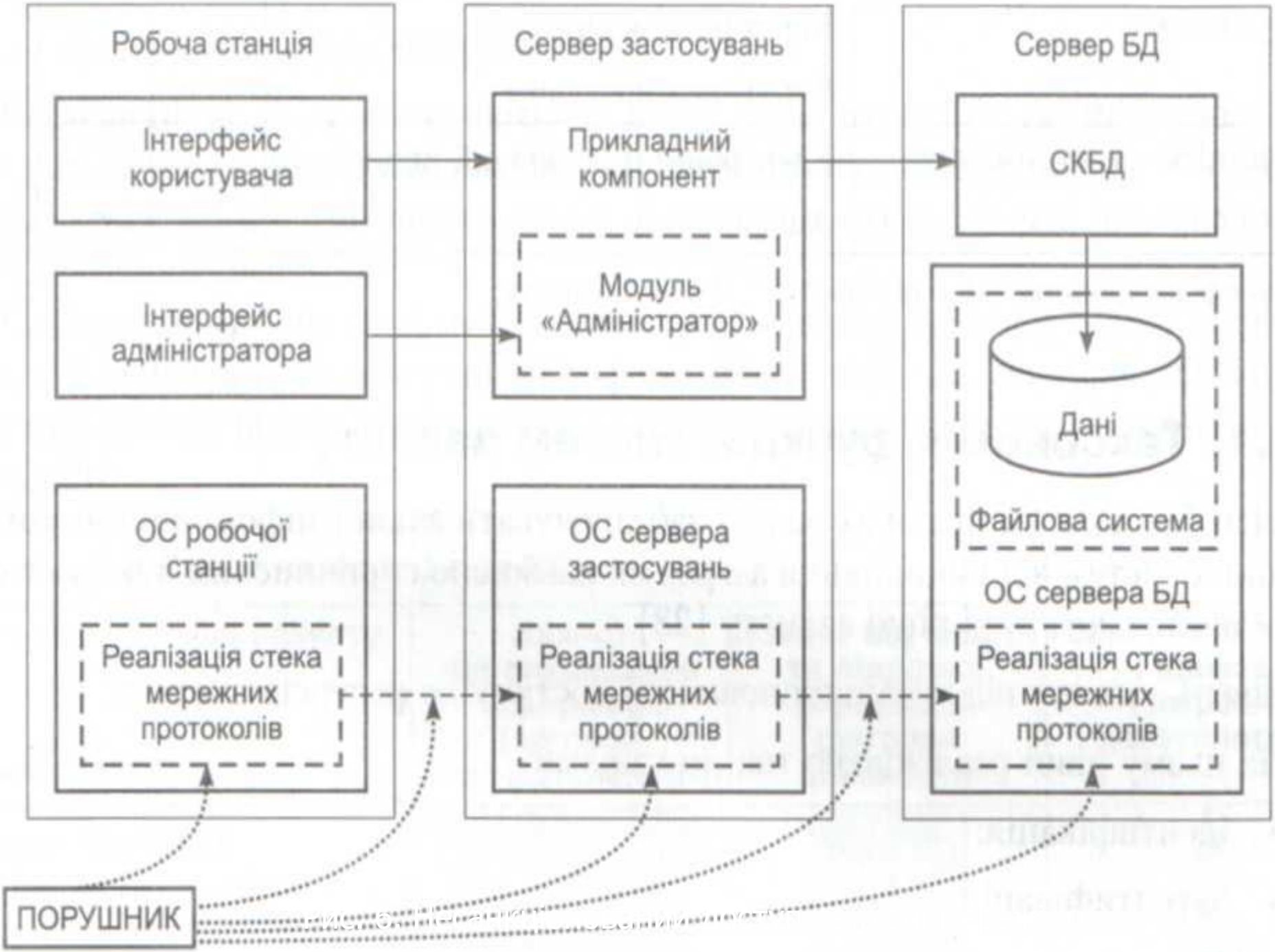
2.Несанкціонований доступ на різних рівнях інформаційно-комунікаційної системи


Робоча станція
Інтерфейс користувача
Інтерфейс адміністратора
ОС робочої станції
Реалізація стека мережних протоколів
Сервер застосувань
Прикладний компонент
Модуль «Адміністратор»
ОС сервера застосувань
Реалізація стека мережних протоколів
Сервер БД
СКБД
Дані
Файлова система
ОС сервера БД
Реалізація стека мережних протоколів


Робоча станція
Сервер застосувань
Сервер БД
ПОРУШНИК
Інтерфейс користувача
Інтерфейс адміністратора
Прикладний компонент
Модуль «Адміністратор»
СКБД
Дані
Файлова система
ОС робочої станції
ОС сервера застосувань
ОС сервера БД
Реалізація стека мережних протоколів
Реалізація стека мережних протоколів
Реалізація стека мережних протоколів


ПОРУШНИК
Робоча станція
Інтерфейс користувача
Інтерфейс адміністратора
ОС робочої станції
Реалізація стека мережних протоколів
Сервер застосувань
Прикладний компонент
Модуль «Адміністратор»
ОС сервера застосувань
Реалізація стека мережних протоколів
Сервер БД
СКБД
Дані
Файлова система
ОС сервера БД
Реалізація стека мережних протоколів


ПОРУШНИК
Робоча станція
Інтерфейс користувача
Інтерфейс адміністратора
ОС робочої станції
Реалізація стека мережних протоколів
Сервер застосувань
Прикладний компонент
Модуль «Адміністратор»
ОС сервера застосувань
Реалізація стека мережних протоколів
Сервер БД
СКБД
Дані
Файлова система
ОС сервера БД
Реалізація стека мережних протоколів


Робоча станція
Інтерфейс користувача
Інтерфейс адміністратора
ОС робочої станції
Реалізація стека мережних протоколів
Сервер застосувань
Прикладний компонент
Модуль «Адміністратор»
ОС сервера застосувань
Реалізація стека мережних протоколів
Сервер БД
СКБД
Дані
Файлова система
ОС сервера БД
Реалізація стека мережних протоколів
ПОРУШНИК

3.Моделі загроз і потенційного порушника

Основними завданнями захисту можуть бути:

1. організація і координація робіт із захисту інформації, яка обробляється та передається засобами АС;
2. визначення, класифікація ресурсів АС, що підлягають захисту;
3. забезпечення визначених конфіденційності, цілісності, доступності інформації під час створення та експлуатації АС, недопущення витоку інформації з обмеженим доступом (ІзОД) та втрати її матеріальних носіїв;
4. створення механізму та умов оперативного реагування на загрози для безпеки інформації;

Основними завданнями захисту можуть бути:

5. ефективне попередження, своєчасне виявлення та знешкодження загроз для ресурсів АС, причин та умов, які спричиняють або можуть привести до порушення її функціонування;
6. організація служби захисту інформації;
7. організація та впровадження системи допуску особового складу (користувачів) до роботи з інформацією, яка потребує захисту;
8. керування засобами захисту інформації, керування доступом користувачів до ресурсів АС, контроль за їхньою роботою з боку персоналу служби захисту інформації, оперативне сповіщення про спроби НСД до ресурсів АС;

Основними завданнями захисту можуть бути:

9. створення умов для максимально можливого відшкодування та локалізації збитків, що завдаються неправомірними та несанкціонованими діями порушників, зменшення негативного впливу наслідків порушення безпеки на функціонування АС;
10. забезпечення режиму секретності під час обробки секретної інформації;
11. розробка організаційно-розпорядчої і робочої документації, що визначає вимоги і порядок захисту та обробки ІзОД;
12. організація обліку, зберігання, обігу інформації, яка потребує захисту, та її матеріальних носіїв;
13. реєстрація, збір, зберігання, обробка даних про всі події в системі, які мають відношення до безпеки інформації;
14. здійснення контролю за забезпеченням захисту ІзОД та за збереженням її матеріальних носіїв.

Модель загроз складається для конкретної АС та повинна враховувати особливості функціонування, склад АС, технологію обробки інформації та ін.

Для кожної з загроз необхідно визначити:

- ✓ на порушення яких властивостей інформації або АС вона спрямована (рекомендується користуватись чотирма основними градаціями – порушення конфіденційності, цілісності, доступності інформації, а також порушення спостереженості та керованості АС);
- ✓ джерела виникнення (які суб'єкти АС або суб'єкти, зовнішні по відношенню до неї, можуть ініціювати загрозу);
- ✓ можливі способи здійснення загроз.

Порушник – це особа, яка може отримати доступ до роботи з включеними до складу АС засобами. Вона може помилково, унаслідок необізнаності, цілеспрямовано, свідомо чи несвідомо, використовуючи різні можливості, методи та засоби, здійснити спробу виконати операції, які призвели або можуть призвести до порушення властивостей інформації, що визначені політикою безпеки.

Модель порушника – це абстрактний формалізований або неформалізований опис порушника.

Модель порушника відображає його практичні та потенційні можливості, апріорні знання, час та місце дії тощо.

При розробці моделі порушника визначаються:

- припущення щодо категорії осіб, до яких може належати порушник;
- припущення щодо мотивів дій порушника (цілей, які він має);
- припущення щодо рівня кваліфікації та обізнаності порушника і його технічної оснащеності (щодо методів та засобів, які використовуються при здійсненні порушень);
- обмеження та припущення щодо характеру можливих дій порушників (за часом та місцем дії та інші).

Серед *зовнішніх* порушників виділяють такі:

- добре озброєна й оснащена силова група, що діє і ззовні швидко і напролом;
- поодинокий порушник, що не має допуску на об’єкт і намагається діяти потайки й обережно, оскільки він усвідомлює, що сили реагування мають над ним переваги.

Серед потенційних *внутрішніх* порушників можна відзначити:

- допоміжний персонал об’єкта, що допущений на об’єкт, але недопущений до життєво важливого центру (ЖВЦ) АСУ;
- основний персонал, що допущений до ЖВЦ (найбільш небезпечний тип порушників);
- співробітників служби безпеки, які часто формально і не допущені до ЖВЦ, але реально мають достатньо широкі можливості для збору необхідної інформації і вчинення акції.

Серед внутрішніх порушників можна виділити такі ***категорії персоналу***:

- користувачі (оператори) системи;
- персонал, що обслуговує технічні засоби (інженери, техніки);
- співробітники відділів розробки та супроводження ПЗ (прикладні та системні програмісти)
- технічний персонал, що обслуговує будівлю (прибиральниці, електрики, сантехніки та інші співробітники, що мають доступ до будівлі та приміщення, де розташовані компоненти АС);
- співробітники служби безпеки;
- керівники різних рівнів та посадової ієрархії.

Сторонні особи, що можуть бути порушниками:

- ✓ клієнти (представники організацій, громадяни);
- ✓ відвідувачі (запрошені з якого-небудь приводу);
- ✓ представники організацій, що займаються забезпеченням життєдіяльності організації (енерго-, водо-, теплопостачання і т. д.);
- ✓ представники конкуруючих організацій (іноземних служб) або особи, що діють за їхнім завданням;
- ✓ особи, які випадково або навмисно порушили пропускний режим (не маючи на меті порушити безпеку);
- ✓ будь-які особи за межами контрольованої зони.

Можна виділити також три основні мотиви порушень:

- безвідповідальність,
- самоствердження
- корисна мета.

Усіх порушників можна класифікувати *за рівнем знань про АС*:

- знає функціональні особливості АС, основні закономірності формування в ній масивів даних і потоків запитів до них, уміє користуватися штатними засобами;
- має високий рівень знань і досвід роботи з технічними засобами системи і їх обслуговуванням;
- має високий рівень знань у галузі програмування й обчислювальної техніки, проектування й експлуатації автоматизованих інформаційних систем;
- знає структуру, функції і механізм дії засобів захисту, їх сильні і слабкі сторони.

За рівнем можливостей (методами та засобами, що використовуються):

- застосовує суто агентурні методи отримання відомостей;
- застосовує пасивні засоби (технічні засоби перехоплення без модифікації компонент системи);
- використовує тільки штатні засоби та недоліки системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні магнітні носії інформації, які можуть бути потайки пронесені через пости охорони;
- застосовує методи та засоби активного впливу (модифікація та підключення додаткових технічних засобів, підключення до каналів передавання даних, впровадження програмних закладок та використання спеціальних інструментальних та технологічних програм).

За часом дії:

- у процесі функціонування (під час роботи компонент системи);
- у період неактивності системи (у неробочий час, під час планових перерв у її роботі, перерв для обслуговування і ремонтів і т.д.);
- як у процесі функціонування, так і в період неактивності компонент системи.

За місцем дії:

- ✓ без доступу на контрольовану територію організації;
- ✓ з контрольованої території без доступу до будівель та споруд;
- ✓ усередині приміщень, але без доступу до технічних засобів;
- ✓ з робочих місць кінцевих користувачів (операторів);
- ✓ з доступом у зону даних (баз даних, архівів тощо);
- ✓ з доступом у зону управління засобами забезпечення безпеки

Класи безпеки:

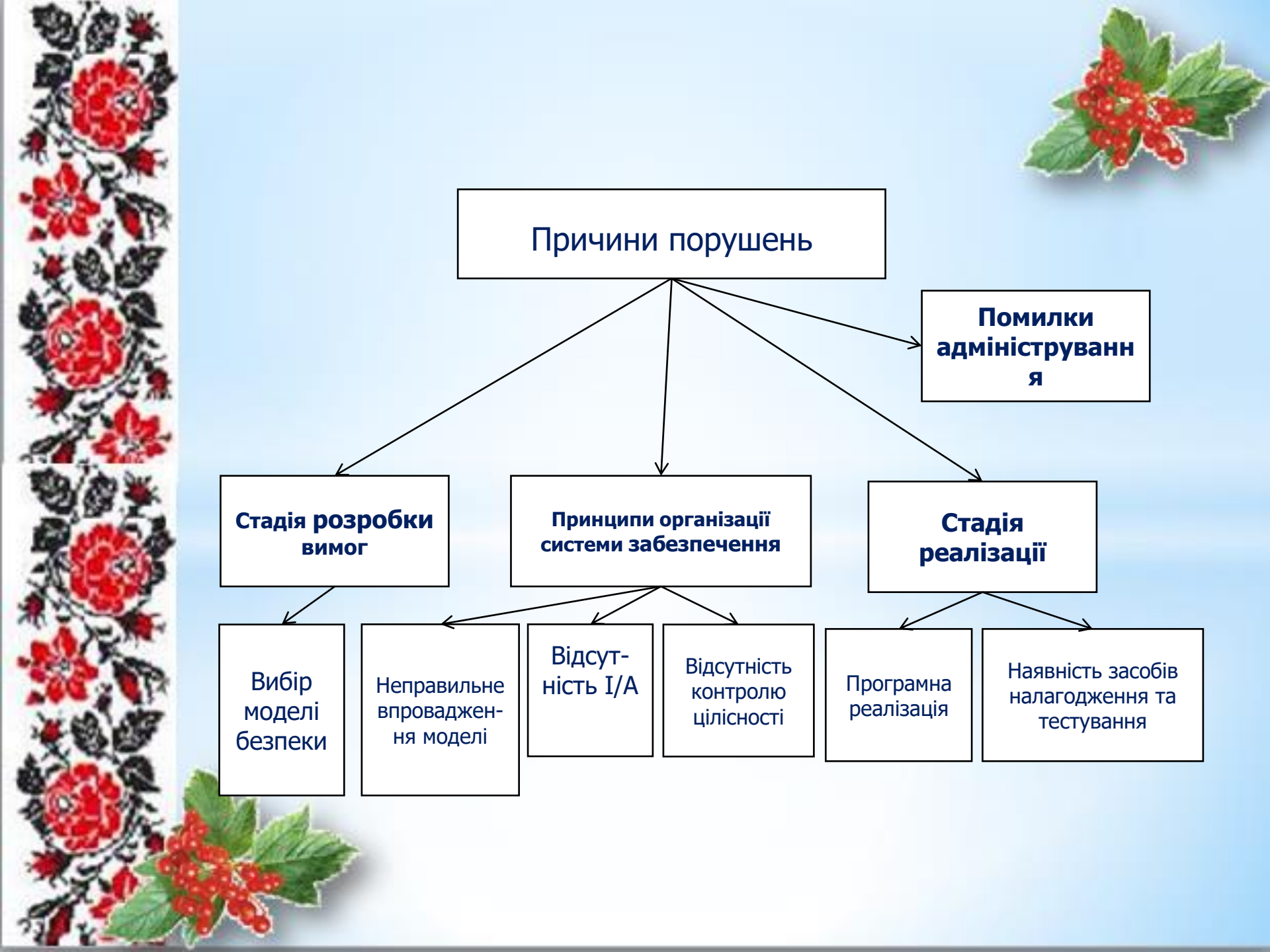
1-й клас – для захисту життєво важливої інформації, витік, руйнування або модифікація якої можуть призвести до втрат для користувача. Міцність розрахована на порушника – професіонала.

2-й клас – використовується для захисту важливої інформації при роботі декількох користувачів, що мають доступ до різних масивів даних або формуючих свої файли, недоступні іншим користувачам. Міцність розрахована на порушника високого класу, але непрофесіонала.

3-й клас рекомендується для захисту щодо важливої інформації, постійний НСД до якої шляхом її нагромадження може привести до витоку і більш важливої інформації. Міцність захисту при цьому повинна бути розрахована на відносно кваліфікованого порушника – непрофесіонала.

4-й клас рекомендується для захисту іншої інформації, що не представляє інтересу для серйозних порушників. Однак його необхідність диктується дотриманням технологічної дисципліни обліку й обробки інформації службового користування з метою захисту від НСД.

4. Причини порушення безпеки


Причини порушень
Помилки адміністрування
Стадія розробки вимог
Принципи організації системи забезпечення
Стадія реалізації
Вибір моделі безпеки
Неправильне впровадження моделі
Відсутність І/А
Відсутність контролю цілісності
Програмна реалізація
Наявність засобів налагодження та тестування

Висновки:

1. Доцільно розглядати чотири рівні інформаційно-комунікаційної системи: прикладний рівень, рівень СКБД, рівень ОС і рівень мережних сервісів. На кожному з цих рівнів можуть існувати певні вразливості та шляхи несанкціонованого доступу, відтак механізми захисту необхідно впроваджувати на всіх рівнях інформаційно-комунікаційної системи.

2. Функціональний сервіс безпеки – це визначений набір функцій, які дають можливість протистояти певній загрозі або певній множині загроз. Для реалізації функціональних сервісів в інформаційно-комунікаційній системі впроваджують специфічні механізми.

3. Розглядають такі рівні захисту:

- рівень захисту від НСД до ресурсів системи;
- рівень захисту від несанкціонованого використання ресурсів системи;
- рівень захисту від некоректного використання ресурсів системи;
- рівень внесення інформаційної та функціональної надлишковості.

Перші два рівні захищають від несанкціонованих дій користувачів і програмних засобів, що здебільшого є реалізацією навмисних загроз. Решта рівнів захищають від некоректних і помилкових дій користувачів, а також від реалізації випадкових загроз.

4.До комплексу засобів захисту належать окремі підсистеми, що забезпечують необхідні сервіси безпеки. Типовий перелік підсистем КЗЗ:

- підсистема керування доступом;
- підсистема ідентифікації та автентифікації;
- підсистема аудита;
- підсистема забезпечення цілісності;
- антивірусна підсистема;
- криптографічні функції.

Контрольні запитання та завдання:

1. Назвіть типові рівні інформаційно-комунікаційної системи.
2. Дайте визначення функціонального сервісу безпеки.
3. Які механізми захисту впроваджують на рівні захисту від НСД до ресурсів системи?
4. Які механізми захисту впроваджують на рівні захисту від несанкціонованого використання ресурсів системи?
5. Які механізми захисту впроваджують на рівні захисту від некоректного використання ресурсів системи?
6. Які механізми захисту впроваджують на рівні внесення інформаційної та функціональної надлишковості?
7. Який рівень захисту забезпечує захист конфіденційності інформації?
8. Назвіть типові підсистеми КЗЗ.
9. Яке завдання виконує підсистема ідентифікації та автентифікації?