# ЛАБОРАТОРНАЯ РАБОТА № 3

# АНАЛІЗ ВИМОГИ БЕЗПЕКИ

**Мета роботи:** ознайомитись з різними шифрами простої заміни (шифрами підстановки) та методами їх дешифрування.

# Короткі теоретичні відомості

Для досягнення ефективного захисту інформації потрібно правильно спроектувати підсистему захисту та застосувати відповідні методи та засоби захисту. Правильність проектування визначається виконанням усіх вимог до системи захисту, тому на початковому етапі необхідно сформулювати вимоги безпеки до системи захисту. Потім на основі цих вимог вибираються та розробляються рішення, що застосовуються для захисту інформації.

Результатом аналізу вимог є перелік ресурсів, загрози та вразливості, що виникають у системі, вимоги до застосовуваних механізмів захисту, попередня оцінка ризику та захищеності, що досягається.

Для вивчення процесу аналізу використається математична модель інформаційної системи. Модель інформаційної системи розширена моделями елементів, що використовуються при побудові засобів захисту інформації: загрози, засоби захисту та ін.

Математична модель представляє статичний стан та описує такі елементи:

- інформаційні ресурси;

- активні процеси, що виконують обробку та доступ до даних;

- уразливості, які є в інформаційній системі;

- загрози порушення безпеки;

- засоби та методи захисту інформації.

## Методи та засоби захисту інформації

Для протидії загрозам використовується сукупність заходів безпеки:

- правові чи законодавчі заходи;

- морально-етичні заходи;

- адміністративні заходи;

- фізичні;

- апаратно-програмні заходи.

До апаратно-програмних методів відносять електронні пристрої та програми, які в комплексі дозволяють протистояти зазначеним загрозам.

Розрізняють два підходи захисту інформаційних систем, що доповнюють один одного: формальне моделювання політики безпеки та криптографічні методи захисту інформації. Формальні моделі безпеки надають розробникам систем основні принципи, що визначають концепції побудови систем. Криптографія дає методи забезпечення конфіденційності, цілісності, обмеження доступу до даних. Формальна модель безпеки є дуже важливою для отримання безпечної системи, оскільки вона визначає основні принципи та концепції забезпечення безпеки, які використовуються на рівні взаємодії елементів системи.

Формальна модель будується на основі вимог, які пред'являються до системи. Для теоретичного підтвердження безпеки системи слід проводити формальний доказ безпеки. Криптографія є сукупністю алгоритмів і протоколів захисту інформації.

Розглянемо види криптографічних блоків, що використовуються у системах захисту інформації:

- ідентифікація;

- автентифікація;

- шифрування;

- контроль цілісності.

Призначенням ідентифікації є розмежування доступу користувачів чи процесів до даних у системі.

Аутентифікація використовується для автентифікації користувача. p align="justify">

Метод шифрування є основним для побудови захищених систем, на його основі реалізується більшість інших методів забезпечення безпеки.

Метод контролю цілісності призначений протистояти загрозам порушення цілісності.

Захищена система будується на основі застосування всіх видів криптографічних методів, і лише комплекс заходів дозволяє з необхідною впевненістю протистояти певним загрозам.

У криптографії використовуються алгоритми:

- симетричне шифрування даних;

- шифрування з відкритим ключем;

- хешування даних.

Алгоритм симетричного шифрування даних заснований на тому, що використовується один секретний ключ, який передається захищеним каналом відправнику та одержувачу.

У разі шифрування з відкритим ключем не потрібна передача захищеним каналом секретного ключа. Використовується дві пари ключів, шифрування виконується за допомогою відкритого ключа, а зворотне перетворення – за допомогою секретного ключа.

Алгоритми хешування призначені для отримання стисненого образу даних, якими не можна відновити дані, але можна перевірити їх цілісність.

Ключі, що використовуються в криптографічних алгоритмах, повинні задовольняти певні вимоги, і для цього розроблені алгоритми генерації ключів.

При розгляді сучасних рішень потрібно з'ясувати схему роботи, основні можливості та характеристики, переваги та недоліки засобів та застосовуваних методів для захисту інформації.

## Аналіз захищеності

Оцінка захищеності є вкрай важливою при розробці підсистеми захисту інформації, так як така оцінка дозволяє виявити помилки в конфігурації, небезпечні вразливості, оцінити ризик порушення доступу до інформації, можливі втрати при використанні різноманітних засобів та методів захисту інформації.

Існують різні підходи до оцінки захищеності:

- статистичний;

- метод мінімізації витрат на засоби захисту та суми збитків при успішному здійсненні загроз;

- неформальні методи.

Зазначені вище підходи аналізу захищеності розрізняються за ефективністю, мають суттєві обмеження щодо застосування.

Статистичний підхід ґрунтується на обчисленні ризиків, пов'язаних із успішною реалізацією загроз. Недоліком статистичного підходу є складність визначення ймовірнісних характеристик подій в інформаційній системі, а також складність оцінки величин збитків та ступеня опірності механізмів захисту.

Мінімізація витрат дозволяє розробити оптимальну систему захисту сумарних витрат. У ряді випадків, коли безпека інформації має більшого значення, ніж вартість використання засобів захисту недоцільно застосовувати метод мінімізації витрат.

Методи аналізу ризиків та мінімізації вартості є формальними та дозволяють на основі відомих вихідних даних про елементи системи визначити точні значення ризиків, витрат, захищеності.

Неформальні методи ґрунтуються на класифікації елементів у системі. Підхід не дає точних оцінок захищеності, а дозволяє визначити категорію захищеності. Методи, засновані на класифікації, мають ширше коло застосування, ніж формальні методи.

Для вивчення процесу аналізу захищеності використовуються формальні методи. Ці методи дозволяють на основі моделі системи виконати аналіз, розрахунок та порівняння захищеності.

Статична модель системи, яка враховує вплив загроз на елементи інформаційної системи, застосування механізмів захисту описується такими визначеннями:

а)  - система складається з 6 множин;

б)  - безліч суб'єктів;

в)  - безліч ресурсів;

г)  - безліч загроз;

д)  - безліч уразливостей;

е) - безліч механізмів захисту;

ж)  - безліч бар'єрів;

з)  - безліч відносин між елементами;

і) відношення,  що належать безлічі, як значення можуть мати порожнє значення, значення — не можуть бути порожніми;

## Хід роботи

1. Статична модель згідно з варіантом зображено на рисунку 1.2.

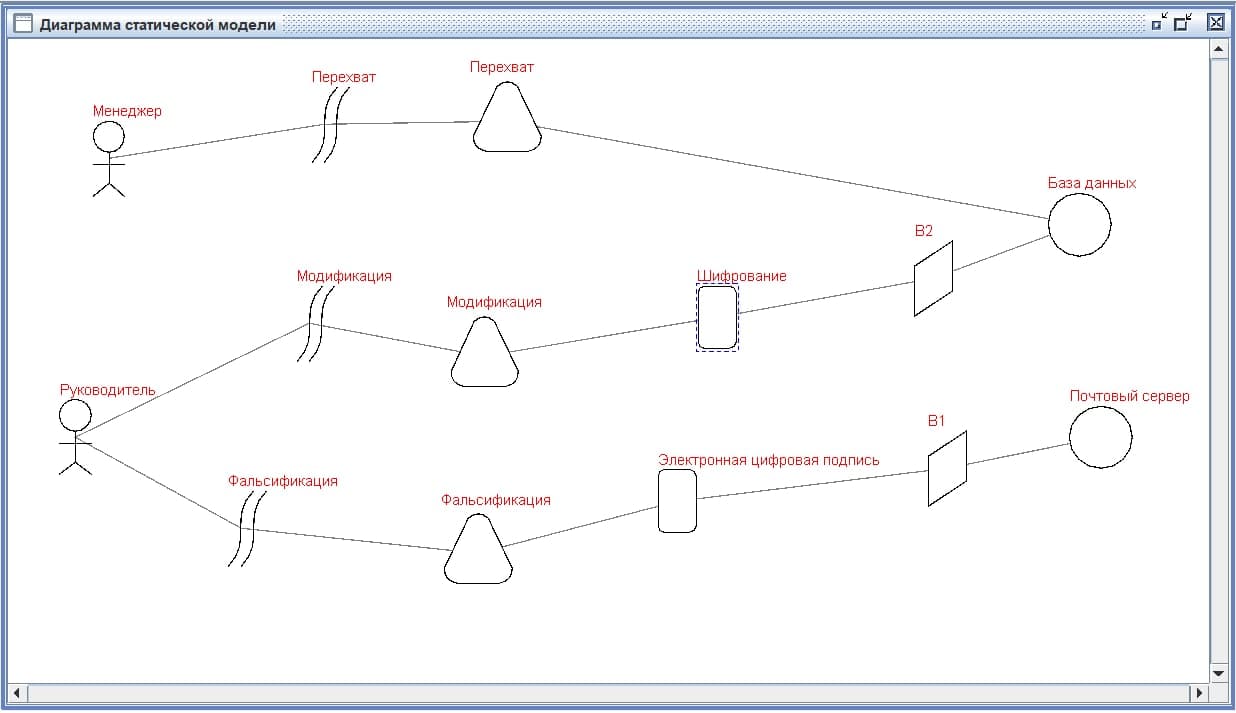


Рисунок 1.2 – Статична модель

2. Вікна редагування ресурсів, суб'єктів, загроз, уразливостей, засобів захисту зображено на рисунку 1.3 – 1.7.

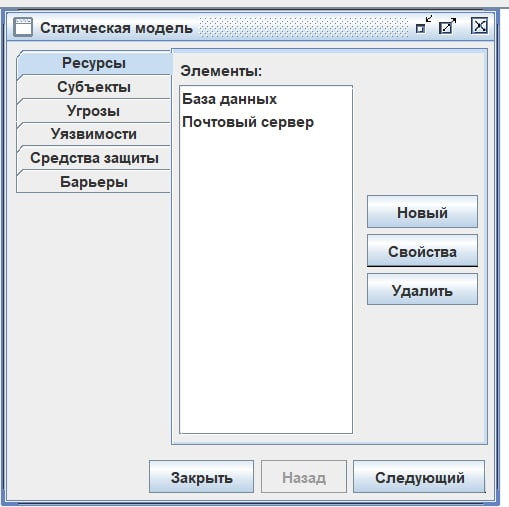


Рисунок 1.3 – Вікно редагування ресурсів

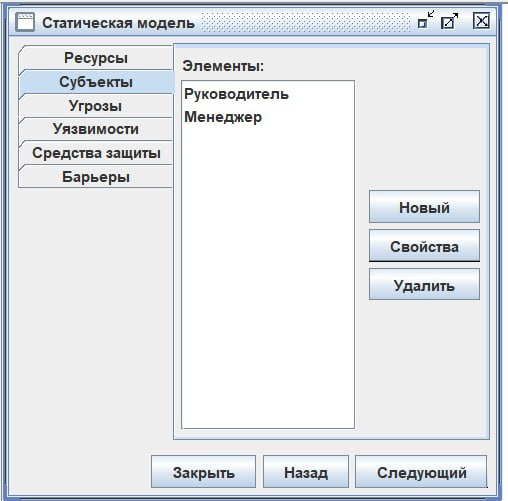


Рисунок 1.4 – Вікно редагування суб’єктів

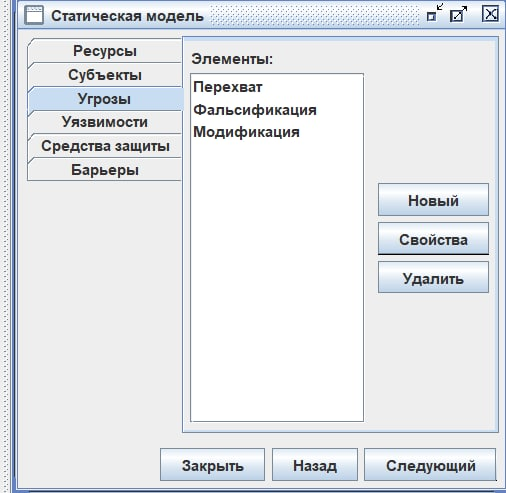


Рисунок 1.5 – Вікно редагування загрози

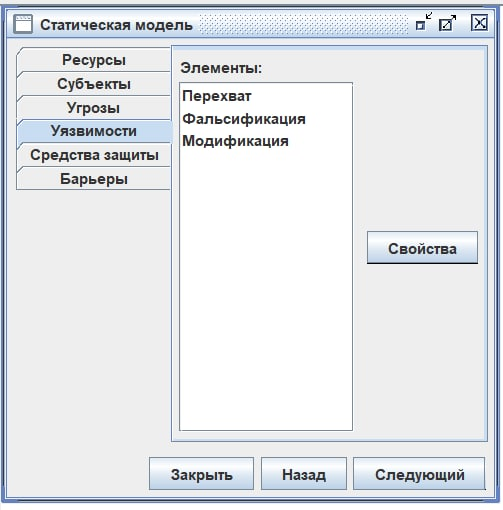


Рисунок 1.6 – Вікно редагування вразливостей

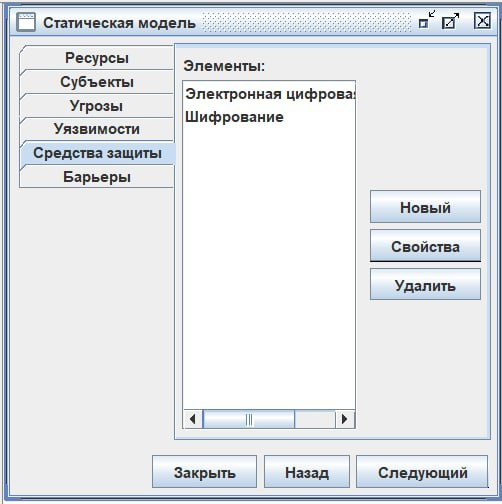


Рисунок 1.7 – Вікно редагування засобів захисту

3. Аналіз захищеності зображено на рисунку 1.8

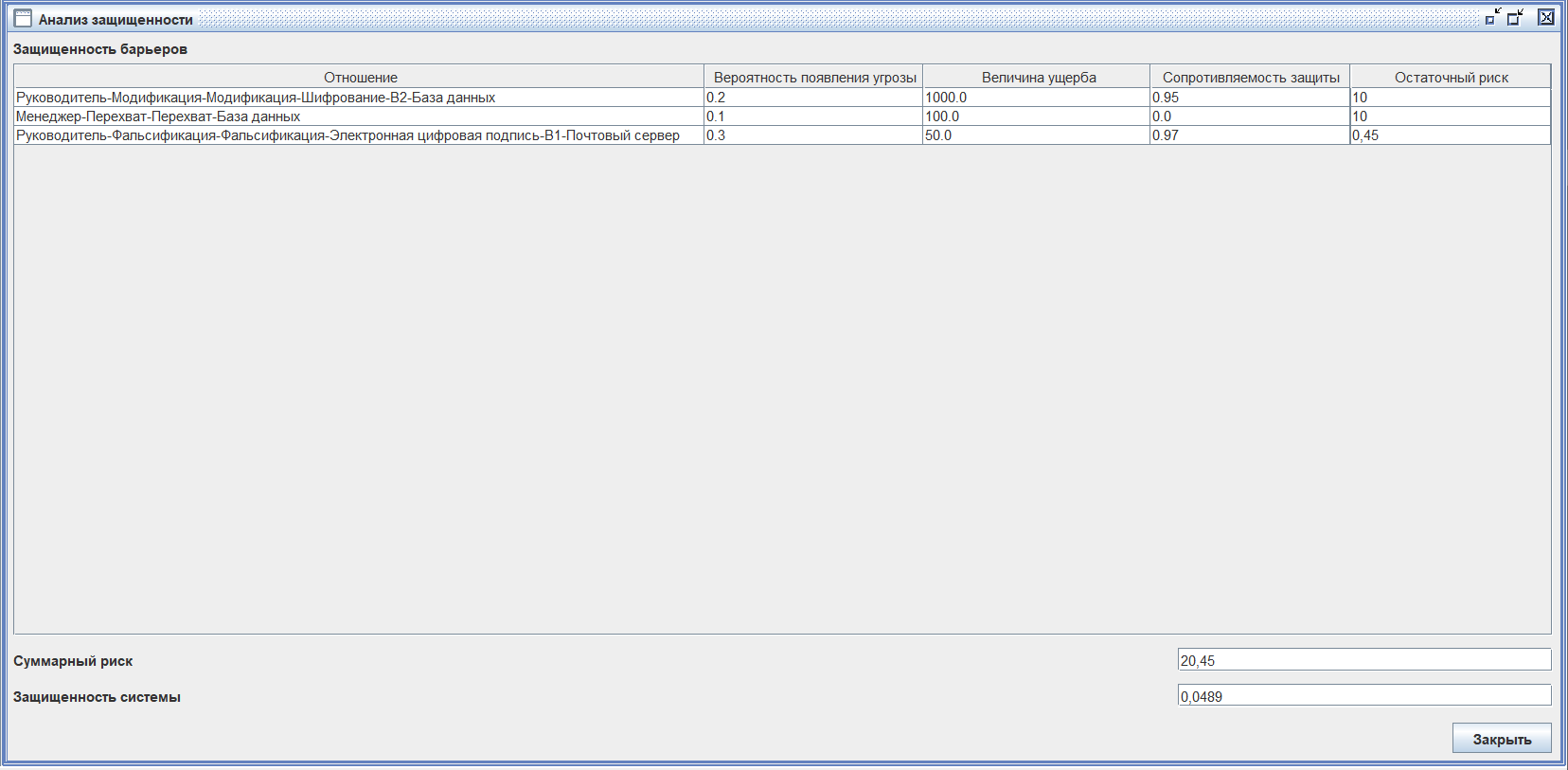


Рисунок 1.8 – Вікно аналізу захищеності

**Висновок:** ознайомились з формування елементів системи створили статистичну модель та модель суб'єкту також налаштували модель уразливостей, налаштували вікно редагування властивостей механізму захисту.