Лабораторна робота 11
ДОСЛІДЖЕННЯ ПРОЦЕСУ РОЗРОБКИ ДИСКРЕЦІЙНОЇ ПОЛІТИКИ БЕЗПЕКИ

Мета – дослідження процесів розробки дискреційної політики безпеки

ТЕОРЕТИЧНІ ВІДОМОСТІ

При розробці політики безпеки повинні бути враховані особливості організації, її розміщення, структура та корпоративна культура. Вона повинна враховувати вимоги сьогодення щодо необхідного рівня захисту та відповідати чинному законодавству. Політика безпеки повинна містити:

- загальний опис сфери діяльності підприємства;
- розподіл ролей і функцій, необхідних для вирішення конкретних питань, закріплення за певними співробітниками (фахівцями, керівниками) обов'язків по виконанню необхідної роботи з метою рішення завдань у рамках цієї політики безпеки.

У таблиці 11.1 представлено розподіл ролей одного із співробітників. Таблиця містить прізвище, ім’я, по-батькові співробітника, його посаду та опис функціональних обов’язків.

Таблиця 11.1.Розподіл ролей і функцій

№ з/п	ПІБ співробітника	Посада	Функціональні обов’язки
1.	Сидорчук Ольга Андріївна	Менеджер	Прийом замовлень від клієнтів, контроль за виконанням замовлень, аналіз запасів товарів і т.д.

Кожному працівнику організації необхідно присвоїти унікальний ідентифікатор та пароль для проведення аутентифікації при роботі з інформаційною системою.

Наступним є побудова матриці доступу до інформаційної системи підприємства, яка включає всі інформаційні ресурси, що представляють собою об’єкти інформаційної діяльності, O_n, перелік усіх користувачів інформаційної системи, S_m та визначені права щодо доступу до об’єктів інформаційної системи, P_i. Також слід визначити права користувачів щодо доступу до об’єктів інформаційної діяльності, як правило, це читання – 1, редагування – 2 та видалення – 3. Орієнтовний вигляд матриці доступу представлено у таблиці 11.2.

Таблиця 11.2 Матриця доступу до ресурсів інформаційної системи

	O_1	O_2	O_3	O_4
S_1	1	2	2	1
S_2	1	2	3	3

S_3	2	2	2	2
S_4	3	3	3	3
S_5	1	1	2	1

Для програмної реалізації розробленої політики безпеки першим етапом є розробка підсистеми аутентифікація користувачів, а другим – перевірка прав доступу до об’єктів інформаційної системи.

Приклад. Для наочності розглянемо підприємство, яке займається випуском кондитерської продукції. В інформаційній системі зберігаються дані про споживачів, постачальників, співробітників, структуру управління підприємством, конфіденційна та комерційна інформація про виробництво. Побудуємо таблицю розподілу ролей та функцій та представимо дані у формі таблиці 11.3.

Таблиця 11.3. Розподіл ролей і функцій

№ з/п	ПІБ співробітника	Посада	Функціональні обов’язки
1.	Талько В.С.	Директор	Управління керівництвом, працює з конфіденційною та комерційною інформацією
2.	Лайко О.В.	Секретар	Працює з неконфіденційною документацією, веде облік запису на прийом до директора
3.	Сарган О.В.	Оператор	Обслуговування технічних установок
4.	Сидорчук О.А.	Менеджер	Представлення виготовленої продукції на ринок
5.	Михайлова В.І.	Адміністратор	Підтримує нормальне функціонування інформаційної системи та бази та сайту підприємства

На наступному етапі кожному працівнику організації присвоїмо унікальний ідентифікатор та пароль для проведення аутентифікації при роботі з інформаційною системою. В межах прикладу використовуємо простий 4-хзначний цифровий пароль (в реальних системах використання такого паролю значно знижує рівень захищеності системи від зламу)

Таблиця 11.4. Ідентифікатори та паролі працівників

№ з/п	ПІБ співробітника	Ідентифікатор	Пароль
1.	Талько В.С.	director	111111
2.	Лайко О.В.	secretar	222222
3.	Сарган О.В.	operator	333333

4.	Сидорчук О.А.	meneger	444444
5.	Михайлова В.І.	admin	555555

Будуємо матрицю доступу до інформаційної системи підприємства, таблиця 11.5.

Таблиця 11.5. Матриця доступу до інформаційної системи

	O_1	O_2	O_3	O_4
S_1	2	2	2	2
S_2	4	1	1	1
S_3	4	1	1	1
S_4	4	1	2	2
S_5	4	3	3	3

S_1–директор;

S_2–секретар;

S_3–оператор;

S_4–менеджер;

S_5–адміністратор.

O_1–комерційна, конфіденційна інформація підприємства;

O_2–дані про робітників;

O_3–дані про споживачів;

O_4–дані про клієнтів.

P_i – права користувачів щодо доступу до об'єктів:

1) читання даних;
2) редагування;
3) видалення;
4) не має права доступу.

ЗАВДАННЯ ДО ВИКОНАННЯ

1. Ознайомитися з теоретичними відомостями.

2. Вибрати підприємство для дослідження процесів розробки політики безпеки.

3. Здійснити загальний опис сфери діяльності обраного підприємства.

4. Дослідити функціональні обов’язки співробітників та визначити їх роль та функції, необхідних для вирішення конкретних питань та виконання посадових обов’язків. Дані представити у вигляді таблиці 11.1 (таблиці 11.3).

5. Створити ідентифікатори та паролі кожному працівнику та представити їх у вигляді таблиці 11.4.

6. Визначити інформаційні ресурси підприємства, O_n та провести їх категоріювання. Привести перелік усіх користувачів інформаційної системи, S_m та визначені права щодо доступу до об’єктів інформаційної системи, P_i. Також

визначити права користувачів щодо доступу до об’єктів інформаційної діяльності.

7. Побудувати матрицю доступу до ресурсів інформаційної системи відповідно до таблиці 11.5.

8. Оформити звіт та дати відповіді на контрольні питання.

САМОСТІЙНА РОБОТА

Програмна реалізація розробленої політики безпеки дає можливість отримати +3 бали в рейтинг лист. Приклад лістингу програми знаходиться у Додатку 1. Приклад інтерфейсної частини на рис. 11.1 та рис.11.2.

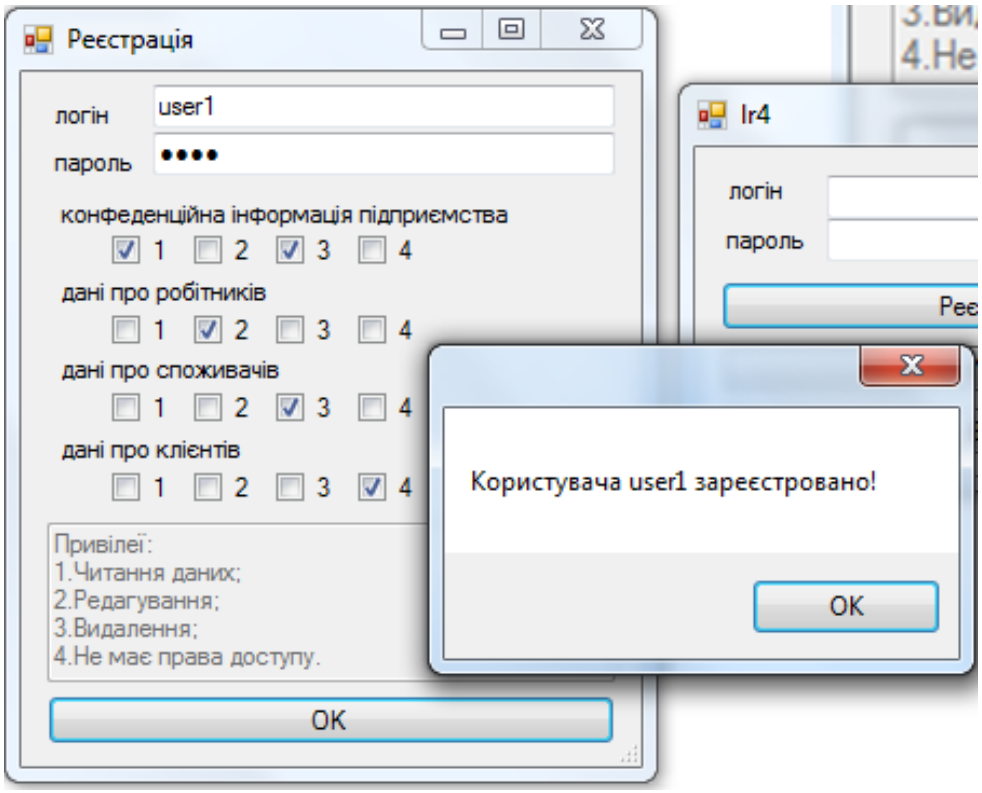

Рисунок 11.1. Вікно реєстрації користувачів

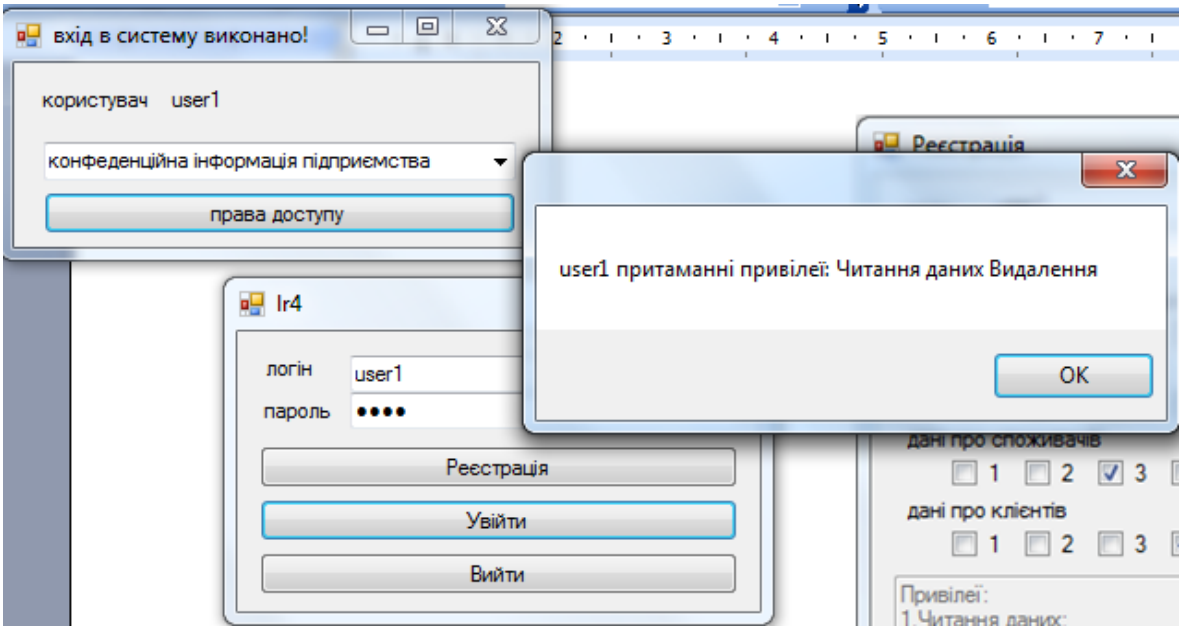

Рисунок 11.2. Перевірка прав доступу зареєстрованих користувачів

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Призначення політики безпеки на підприємстві.
2. Дайте визначення поняттю «дискреційна політика безпеки».
3. Назвіть переваги і недоліки дискреційної політики безпеки.
4. Дайте коротку характеристику мандатної політики безпеки.
5. Назвіть переваги і недоліки мандатної політики безпеки.
6. Дайте коротку характеристику рольової політики безпеки.
7. Назвіть переваги і недоліки рольової політики безпеки.
8. Назвіть етапи формального підходу до перевірки СЗІ на повноту і коректність.
9. Назвіть основні принципи захисту інформації від НСД.
10. Структура монітора звернень.
11. Основні характеристики моделі Белла-Ла Падула.
12. Дайте визначення поняттям «ідентифікація», «аутентифікація».
13. Перерахуйте засади, яким доцільно керуватися при формалізації політики захисту інформації.

```
namespace lr4
{
   public struct autent
   {
      public string user;
      public string pass;
      public byte[] privileges;
   };
   public partial class Form1 : Form
   {
      public Form1()
      {
         InitializeComponent();
      }
      public autent[] aunt = new autent [0];
      private void button2_Click(object sender, EventArgs e)
      {
         Close();
      }

      private void button3_Click(object sender, EventArgs e)
      {
         Form2 f2 = new Form2();
         f2.ShowDialog();
         if ((f2.user!="")||(f2.pass!=""))
         {
         Array.Resize(ref aunt, aunt.Length+1);
         aunt[aunt.Length-1].user = f2.user;
         aunt[aunt.Length-1].pass = f2.pass;
         aunt[aunt.Length - 1].privileges = f2.privileges;
         }
      }

      private void button1_Click(object sender, EventArgs e)
      {
         int k = 0;
         for (int i = 0; i < aunt.Length; i++)
         {
            if (textBox1.Text == aunt[i].user)
            {
               if (textBox2.Text == aunt[i].pass)
```

```
                {
                    k += 1;
                    Form3 f3 = new Form3();
                    f3.user = aunt[i].user;
                    f3.pass = aunt[i].pass;
                    f3.privileges = aunt[i].privileges;
                    f3.ShowDialog();
                }
            }
        }
        if (k==0)
        { MessageBox.Show("Невірний логін або пароль"); }

    }}}

namespace lr4
{
    public partial class Form2 : Form
    {
        public Form2()
        {
            InitializeComponent();
        }
        public string user;
        public string pass;
        public byte[] privileges = new byte[4];
        private void button1_Click(object sender, EventArgs e)
        {
            if ((textBox1.Text == "") || (textBox2.Text == ""))
                MessageBox.Show("Заповніть поля");
            else
            {
                user = textBox1.Text;
                pass = textBox2.Text;
                MessageBox.Show("Користувача " + user + " зареєстровано!");
                Close();
            }
        }

        private void checkBox5_CheckedChanged(object sender, EventArgs e)
        {
            if (checkBox5.Checked)
```

```
            {
                privileges[0] += 8;
            }
            else privileges[0] -= 8;
        }

        private void checkBox6_CheckedChanged(object sender, EventArgs e)
        {
            if (checkBox6.Checked)
            {
                privileges[0] += 4;
            }
            else privileges[0] -= 4;
        }

        private void checkBox7_CheckedChanged(object sender, EventArgs e)
        {
            if (checkBox7.Checked)
            {
                privileges[0] += 2;
            }
            else privileges[0] -= 2;
        }

        private void checkBox8_CheckedChanged(object sender, EventArgs e)
        {
            if (checkBox8.Checked)
            {
                privileges[0] += 1;
            }
            else privileges[0] -= 1;
        }}}
namespace lr4
{
    public partial class Form3 : Form
    {
        public Form3()
        {
            InitializeComponent();
        }
        public string user;
        public string pass;
```

```
    public string[] priv = { "Читання даних", "Редагування", "Видалення", "Не має права доступу" };
    public string vuvod;
    public byte bufer;
    public byte[] privileges = new byte[4];
    private void button1_Click(object sender, EventArgs e)
    {
       if (comboBox1.SelectedIndex == 0)
       {
          vuvod = "";
          bufer = 0;
          bufer = privileges[0];
          if (bufer >= 8)
             {
                bufer = (byte)(bufer - 8);
                vuvod += priv[0];
             }
          if (bufer >= 4)
             {
                bufer = (byte)(bufer - 4);
                vuvod += " ";
                vuvod += priv[1];

             }
          if (bufer >= 2)
             {
                bufer = (byte)(bufer - 2);
                vuvod += " ";
                vuvod += priv[2];

             }
          if (bufer == 1)
             {
                vuvod += " ";
                vuvod += priv[3];
             }
             MessageBox.Show(user + " притаманні привілеї: " + vuvod);
       }
private void Form3_Load(object sender, EventArgs e)
    {
       label2.Text = user;
    }}}
```