Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Московский государственный технический университет имени Н.Э. Баумана
(национальный исследовательский университет)»
(МГТУ им. Н.Э. Баумана)

ФАКУЛЬТЕТ «Информатика и системы управления» (ИУ)

КАФЕДРА «Информационная безопасность» (ИУ8)

Отчёт

по лабораторной работе № 3
по дисциплине «Технологии и методы программирования»

Тема: «Криптографические примитивы в Java»

Вариант 4

Выполнил: А. В. Куликова, студент группы ИУ8-11М

Проверил: А. Ю. Быков

Москва, 2024

1. Постановка задачи

Разработать на основе ООП движок (достаточно продемонстрировать в консольном приложении) для системы аутентификации-идентификации на основе логина и пароля пользователя. Должен быть определен класс для описания пользователя с необходимыми полями и методами. Для хранения объектов (пользователей) в памяти выбрать подходящий контейнер.

Реализовать режимы: регистрация нового пользователя; вход пользователя (результат входа допуск или не допуск); смена пользователем пароля. Данные пользователей сохраняются на диске в безопасной форме.

Полезные классы: MessageDigest (пакет java.security) представляет криптографическую хеш-функцию; Cipher (пакет javax.crypto) представляет криптографический алгоритм; SecureRandom (пакет java.security) криптографический генератор псевдослучайных чисел.

2. Ход работы

Листинг 1 – Код программы user.java

```
import java.security.MessageDigest;

// Класс, представляющий пользователя
class User {
    private String username; // Имя пользователя
    private String passwordHash; // Хэш пароля

    // Конструктор для создания пользователя с заданным именем и паролем
    public User(String username, String password) {
        this.username = username;
        this.passwordHash = hashPassword(password); // Хэширование пароля
    }

    // Метод для получения имени пользователя
    public String getUsername() {
        return username;
    }

    // Метод для проверки введенного пароля
    public boolean checkPassword(String password) {
        return hashPassword(password).equals(passwordHash);
    }

    // Метод для изменения пароля пользователя
    public void changePassword(String newPassword) {
        this.passwordHash = hashPassword(newPassword);
    }

    // Метод для хэширования пароля с использованием SHA-256
    private String hashPassword(String password) {
        try {
            MessageDigest digest = MessageDigest.getInstance("SHA-256");
            byte[] hash = digest.digest(password.getBytes());
            StringBuilder hexString = new StringBuilder();
            for (byte b : hash) {
                String hex = Integer.toHexString(0xff & b);
                if (hex.length() == 1)
                    hexString.append('0');
                hexString.append(hex);
            }
            return hexString.toString();
        } catch (Exception e) {
            e.printStackTrace();
            return null;
        }
    }
}
```

Листинг 2 – Код программы auth.java

```
import java.util.HashMap;

class AuthenticationEngine {
    private HashMap<String, User> users; // Хранит пользователей и их данные

    public AuthenticationEngine() {
        users = new HashMap<>(); // Инициализация хранилища пользователей
    }

    // Регистрация нового пользователя
    public void registerUser(String username, String password) {
        if (!users.containsKey(username)) {
            users.put(username, new User(username, password)); // Создание нового
пользователя
            System.out.println("Пользователь " + username + " успешно
зарегистрирован.");
        } else {
            System.out.println("Пользователь " + username + " уже существует.");
        }
    }

    // Вход пользователя в систему
    public boolean loginUser(String username, String password) {
        if (users.containsKey(username)) {
            User user = users.get(username);
            if (user.checkPassword(password)) {
                System.out.println("Пользователь " + username + " успешно вошел в
систему.");
                return true;
            }
        }
        System.out.println("Ошибка входа. Неверное имя пользователя или
пароль.");
        return false;
    }

    // Изменение пароля пользователя
    public void changePassword(String username, String newPassword) {
        if (users.containsKey(username)) {
            User user = users.get(username);
            user.changePassword(newPassword);
            System.out.println("Пароль успешно изменен для пользователя " +
username);
        } else {
            System.out.println("Пользователь " + username + " не найден.");
        }
    }
}
```

Листинг 3 – Код программы main.java

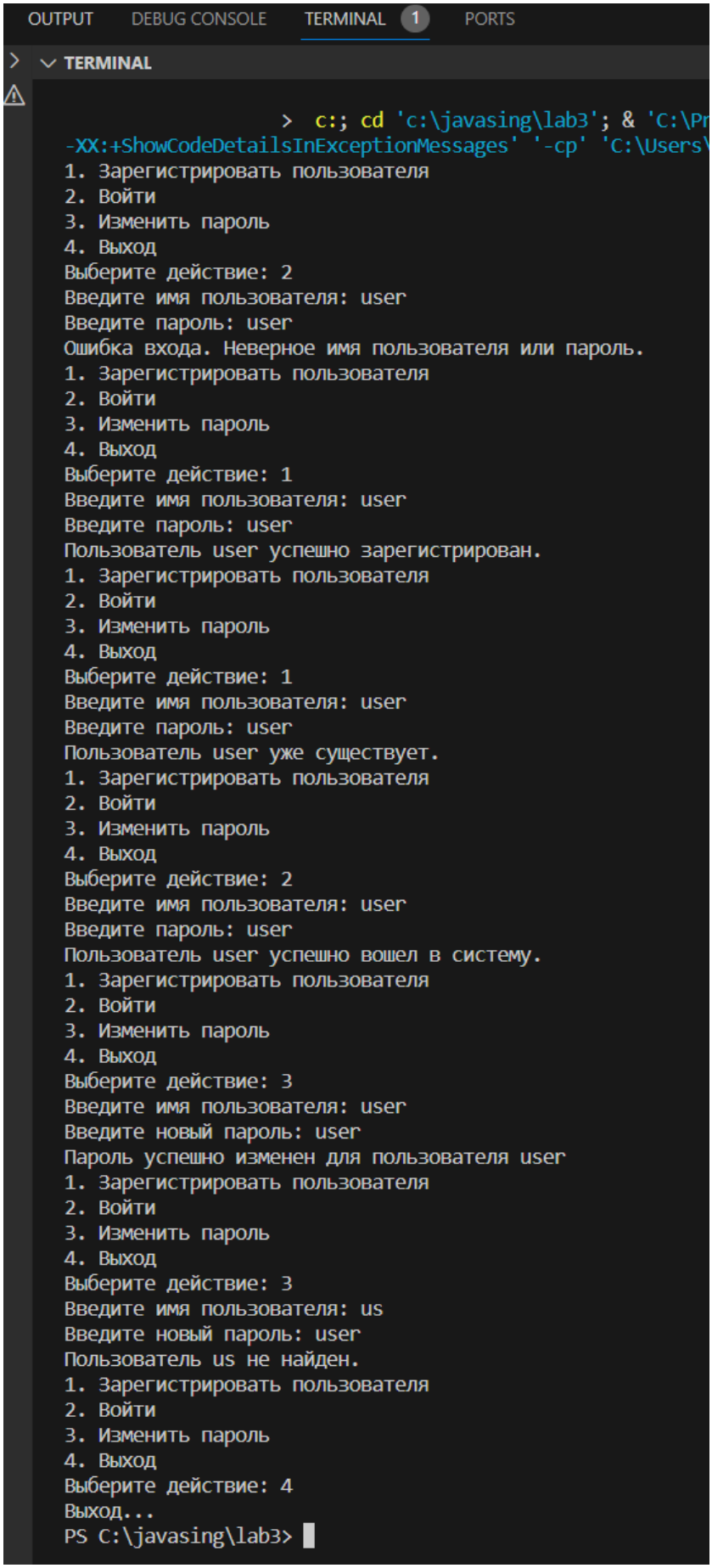
```
import java.util.Scanner;

// Класс, представляющий точку входа в программу
class Main {
    public static void main(String[] args) {
        AuthenticationEngine authEngine = new AuthenticationEngine();
        Scanner scanner = new Scanner(System.in);

        // Бесконечный цикл для работы с пользовательским вводом
        while (true) {
            System.out.println("1. Зарегистрировать пользователя");
            System.out.println("2. Войти");
            System.out.println("3. Изменить пароль");
            System.out.println("4. Выход");
            System.out.print("Выберите действие: ");
            int choice = scanner.nextInt();
            scanner.nextLine(); // считывание символа новой строки

            switch (choice) {
                case 1:
                    System.out.print("Введите имя пользователя: ");
                    String regUsername = scanner.nextLine();
                    System.out.print("Введите пароль: ");
                    String regPassword = scanner.nextLine();
                    authEngine.registerUser(regUsername, regPassword);
                    break;
                case 2:
                    System.out.print("Введите имя пользователя: ");
                    String loginUsername = scanner.nextLine();
                    System.out.print("Введите пароль: ");
                    String loginPassword = scanner.nextLine();
                    authEngine.loginUser(loginUsername, loginPassword);
                    break;
                case 3:
                    System.out.print("Введите имя пользователя: ");
                    String changeUsername = scanner.nextLine();
                    System.out.print("Введите новый пароль: ");
                    String newPassword = scanner.nextLine();
                    authEngine.changePassword(changeUsername, newPassword);
                    break;
                case 4:
                    System.out.println("Выход...");
                    System.exit(0);
                default:
                    System.out.println("Неверный выбор. Пожалуйста, попробуйте
снова.");
            }
        }
    }
}
```

Результат:


OUTPUT
DEBUG CONSOLE
TERMINAL 1
PORTS
TERMINAL
> c:; cd 'c:\javasing\lab3'; & 'C:\Pr
-XX:+ShowCodeDetailsInExceptionMessages' '-cp' 'C:\Users\
1. Зарегистрировать пользователя
2. Войти
3. Изменить пароль
4. Выход
Выберите действие: 2
Введите имя пользователя: user
Введите пароль: user
Ошибка входа. Неверное имя пользователя или пароль.
1. Зарегистрировать пользователя
2. Войти
3. Изменить пароль
4. Выход
Выберите действие: 1
Введите имя пользователя: user
Введите пароль: user
Пользователь user успешно зарегистрирован.
1. Зарегистрировать пользователя
2. Войти
3. Изменить пароль
4. Выход
Выберите действие: 1
Введите имя пользователя: user
Введите пароль: user
Пользователь user уже существует.
1. Зарегистрировать пользователя
2. Войти
3. Изменить пароль
4. Выход
Выберите действие: 2
Введите имя пользователя: user
Введите пароль: user
Пользователь user успешно вошел в систему.
1. Зарегистрировать пользователя
2. Войти
3. Изменить пароль
4. Выход
Выберите действие: 3
Введите имя пользователя: user
Введите новый пароль: user
Пароль успешно изменен для пользователя user
1. Зарегистрировать пользователя
2. Войти
3. Изменить пароль
4. Выход
Выберите действие: 3
Введите имя пользователя: us
Введите новый пароль: user
Пользователь us не найден.
1. Зарегистрировать пользователя
2. Войти
3. Изменить пароль
4. Выход
Выберите действие: 4
Выход...
PS C:\javasing\lab3>