

2. ЛАБОРАТОРНАЯ РАБОТА № 2. МЕТОДЫ ПАРОЛЬНОЙ ЗАЩИТЫ. РАЗРАБОТКА ПРОГРАММНОЙ ПАРОЛЬНОЙ ЗАЩИТЫ

Цель работы: изучение технологии аутентификации пользователя на основе пароля.

2.1. Ход работы

1. Ознакомиться с теоретической частью данной работы.
2. Составить программу, представляющую собой форму доступа к определённым информационным ресурсам на основе пароля.
3. Составить отчет по проделанной работе.
4. Защитить работу.

2.2. Содержание отчета

- Тема.
- Цель работы.
- Ход работы.
- Постановка задачи.
- Листинг программы.
- Результат выполнения программы.

2.3. Теоретическая справка

Аутентификация — процедура проверки подлинности заявленного пользователя, процесса или устройства, например:

— проверка подлинности пользователя путём сравнения введённого им пароля с паролем, сохранённым в базе данных пользователей;

— подтверждение подлинности электронного письма путём проверки цифровой подписи письма по открытому ключу отправителя;

— проверка контрольной суммы файла на соответствие сумме, заявленной автором этого файла.

Эта проверка позволяет достоверно убедиться, что пользователь (процесс или устройство) является именно тем, кем себя объявляет. При проведении аутентификации проверяющая сторона убеждается в подлинности проверяемой стороны, при этом проверяемая сторона тоже активно участвует в процессе обмена информацией. Обычно пользователь подтверждает свою идентификацию, вводя в систему

уникальную, неизвестную другим пользователям информацию о себе (например, пароль или сертификат).

Идентификация — установление тождественности неизвестного объекта известному на основании совпадения признаков; опознание.

Идентификация в информационных системах — присвоение субъектам и объектам идентификатора и/или сравнение идентификатора с перечнем присвоенных идентификаторов. Например, идентификация по штрихкоду.

Идентификация и аутентификация являются взаимосвязанными процессами распознавания и проверки подлинности субъектов (пользователей). Именно от них зависит последующее решение системы, можно ли разрешить доступ к ресурсам системы конкретному пользователю или процессу. После идентификации и аутентификации субъекта выполняется его авторизация.

Аутентификацию не следует путать с авторизацией (процедурой предоставления субъекту определённых прав) и идентификацией (процедурой распознавания субъекта по его идентификатору).

Авторизация — процедура предоставления субъекту определенных полномочий и ресурсов в данной системе. Иными словами, авторизация устанавливает сферу действия субъекта и доступные ему ресурсы. Если система не может надёжно отличить авторизованное лицо от неавторизованного, конфиденциальность и целостность информации в ней могут быть нарушены. Организации необходимо четко определить свои требования к безопасности, чтобы принимать решения о соответствующих границах авторизации.

С процедурами аутентификации и авторизации тесно связана процедура администрирования действий пользователя.

Пароль — это то, что знает пользователь и что также знает другой участник взаимодействия. Для взаимной аутентификации участников взаимодействия может быть организован обмен паролями между ними.

2.4. Задание к лабораторной работе № 2

Разработать программу, представляющую собой форму доступа к определённым информационным ресурсам на основе пароля.

- В качестве информационного ресурса использовать любой файл или приложение.
- Доступ к ресурсу должен быть разрешен только санкционированным пользователям. Для этого в программе должны храниться имена пользователей и их пароли. При попытке доступа пользователя к ресурсу проверяется наличие его идентификатора

(имени) в системе и соответствие введенного пароля паролю, который хранится в системе.

- В системе должна храниться следующая информация о пользователе: ID или имя пользователя, пароль, ФИО, дата рождения, место рождения (город), номер телефона.

- Пользователь должен иметь возможность поменять пароль (таблица 2).

Таблица 2

Варианты заданий к лабораторной работе № 2

Номер варианта	Длина пароля (количество символов)	Используемые символы	Дополнительные средства защиты
1	6	Латиница (строчные буквы)	При смене пароля: проверка на отсутствие повторяющихся символов
2	7	Кириллица (строчные буквы)	При смене пароля: проверка на совпадение пароля с именем пользователя (если используется идентификационный номер, то в системе должны храниться имена каждого пользователя)
3	8	Цифры	Применение метода аутентификации на основе одноразовых паролей: каждый следующий пароль = предыдущий пароль+5
4	5	Цифры, знаки арифметических операций	При смене пароля: проверка на отсутствие повторяющихся символов
5	8	Цифры, знаки препинания	При смене пароля: проверка на совпадение пароля с датой рождения пользователя (хранится в системе) в формате дд.мм.гг или дд/мм/гг
6	10	Латиница (прописные буквы)	Применение метода аутентификации на основе одноразовых паролей: при каждой следующей попытке входа в систему последняя буква пароля меняется на следующую по алфавиту
7	11	Кириллица (прописные буквы)	При смене пароля: проверка на совпадение пароля с фамилией пользователя (если используется идентификационный номер, то в системе должны храниться имена каждого пользователя)

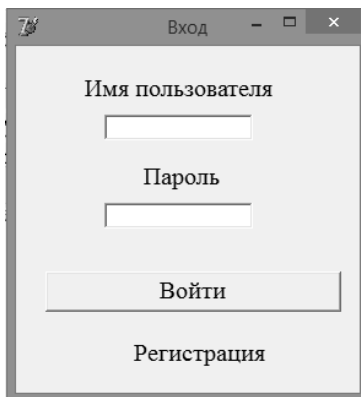
Номер варианта	Длина пароля (количество символов)	Используемые символы	Дополнительные средства защиты
8	10	Цифры, знаки препинания	При смене пароля: проверка на совпадение пароля с датой рождения пользователя (хранится в системе) в формате дд.мм.гггг или дд/мм/гггг
9	7	Цифры	Применение метода аутентификации на основе одноразовых паролей: к первой цифре каждого следующего пароля прибавляется 1
10	8	Кириллица (прописные и строчные буквы)	При смене пароля: проверка на отсутствие повторяющихся символов
11	5	Латиница (строчные и прописные буквы)	Применение метода аутентификации на основе одноразовых паролей: после ввода пользователем пароля к нему добавляется «случайная» величина, такая же величина добавляется к паролю, который хранится в системе, после чего производится сравнение (в качестве «случайной» величины использовать «Аbc»)
12	9	Кириллица (прописные буквы)	При смене пароля: проверка на совпадение пароля с отчеством пользователя
13	10	Цифры	При смене пароля: проверка на совпадение пароля с номером телефона пользователя в формате: xxxxxxxxxx
14	7	Кириллица (прописные буквы)	При смене пароля: проверка на совпадение пароля со словами в словаре (в качестве словаря использовать массив названий месяцев)
15	6	Латиница (строчные и прописные буквы)	При смене пароля: проверка на отсутствие повторяющихся символов

Номер варианта	Длина пароля (количество символов)	Используемые символы	Дополнительные средства защиты
16	7	Кириллица (строчные буквы)	Применение метода аутентификации на основе одноразовых паролей: после ввода пользователем пароля в его начало добавляется «случайная» величина, такая же величина добавляется к паролю, который хранится в системе, после чего производится сравнение (в качестве «случайной» величины использовать «АБВ»)
17	4	Цифры	При смене пароля: проверка на совпадение пароля с годом рождения пользователя
18	5	Цифры	Применение односторонней (хэш) функции: сложение всех цифр пароля. Такая же функция должна быть применена к паролю, который хранится в системе. Затем проводится сравнение паролей
19	9	Кириллица (строчные буквы)	Шифрование пароля (в качестве алгоритма шифрования применить метод перестановки: поменять местами первую и последнюю букву пароля). Тот же алгоритм должен быть применен к паролю, который хранится в системе. Затем проводится сравнение паролей
20	10	Кириллица (прописные буквы)	При смене пароля: проверка на совпадение пароля с местом рождения пользователя
21	13	Цифры, знаки препинания	При смене пароля: проверка на совпадение пароля с номером телефона пользователя в формате: xxx-xxx-xx-xx
22	6	Латиница (строчные буквы)	При смене пароля: проверка на совпадение пароля со словами в словаре (в качестве словаря использовать массив названий дней недели)

Номер варианта	Длина пароля (количество символов)	Используемые символы	Дополнительные средства защиты
23	7	Кириллица (прописные буквы)	При смене пароля: проверка на совпадение пароля с именем пользователя, записанным в обратном порядке
24	8	Цифры, знаки препинания	При смене пароля: проверка на совпадение пароля с текущей датой в формате дд.мм.гг или дд/мм/гг
25	5	Цифры	Применение односторонней (хэш) функции: перемножение всех цифр пароля. Такая же функция должна быть применена к паролю, который хранится в системе. Затем проводится сравнение паролей
26	6	Цифры	Шифрование пароля (в качестве алгоритма шифрования применить метод замены: к каждой цифре пароля прибавить по цифре из даты рождения пользователя соответственно). Тот же алгоритм должен быть применен к паролю, который хранится в системе. Затем проводится сравнение паролей
27	10	Кириллица (прописные буквы)	При смене пароля: проверка на совпадение пароля со словами в словаре (в качестве словаря использовать массив из любых 10 слов, длиной в 10 символов)
28	4	Кириллица (строчные и прописные буквы)	При смене пароля: проверка на совпадение пароля с месяцем рождения пользователя
29	10	Цифры, знаки препинания	При смене пароля: проверка на совпадение пароля с текущей датой в формате дд.мм.гггг или дд/мм/гггг
30	9	Цифры	При смене пароля: проверка на отсутствие повторяющихся символов

2.5. Пример реализации лабораторной работы

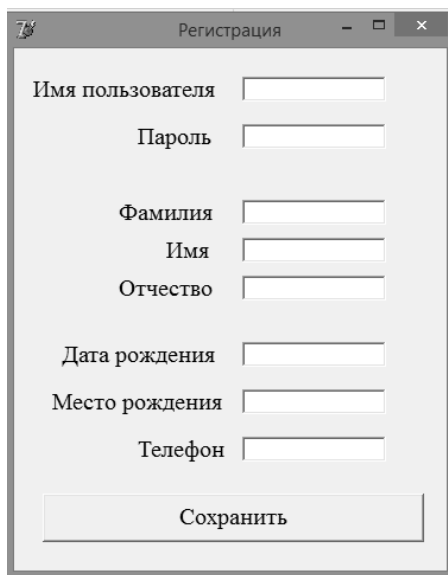
Примерный интерфейс программы представлен на рисунках 2, 3, 4.



The screenshot shows a window titled "Вход" (Login). It contains two text input fields: "Имя пользователя" (Username) and "Пароль" (Password). Below these fields is a "Войти" (Login) button. At the bottom of the window is a "Регистрация" (Registration) link.

Рис. 2

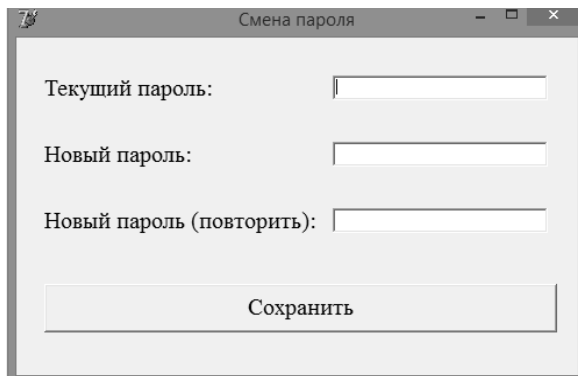
Форма авторизации пользователя



The screenshot shows a window titled "Регистрация" (Registration). It contains several text input fields: "Имя пользователя" (Username), "Пароль" (Password), "Фамилия" (Surname), "Имя" (Name), "Отчество" (Patronymic), "Дата рождения" (Date of birth), "Место рождения" (Place of birth), and "Телефон" (Phone). At the bottom of the window is a "Сохранить" (Save) button.

Рис. 3

Форма регистрации пользователя



Смена пароля

Текущий пароль:

Новый пароль:

Новый пароль (повторить):

Рис. 4
Форма смены пароля

Контрольные вопросы

1. Дать определение аутентификации. Привести примеры.
2. Дать определение идентификации в информационных системах.
3. Дать определение авторизации пользователя.
4. Дать определение пароля.