МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ АЛТАЙСКОГО КРАЯ
КРАЕВОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«ЯРОВСКОЙ ПОЛИТЕХНИЧЕСКИЙ ТЕХНИКУМ»

Практическая работа №11
Тема: Оценка необходимого количества тестов.
Цель: Получить навыки разработки тестовых сценариев.

Работу выполнил(и):	Крутиков С.В и Сухих А.Н Студенты группы ИСиП-21
Работу проверил:	Олюшин В.В

Яровое 2025

Анализ авторизации пользователя-туриста

Классы эквивалентности входных данных

Логин/Email:

- Валидный класс: корректный email-адрес (содержит @, домен)
- Невалидный класс 1: некорректный формат email
- Невалидный класс 2: пустая строка
- Невалидный класс 3: слишком короткий/длинный email

Пароль:

- Валидный класс: пароль соответствует требованиям (длина, символы)
- Невалидный класс 1: пароль короче минимальной длины
- Невалидный класс 2: пароль длиннее максимальной длины
- Невалидный класс 3: пароль без специальных символов
- Невалидный класс 4: пустая строка

Граничные значения

Для email:

- Минимальная длина допустимого email
- Максимальная длина допустимого email
- Email с одним символом до @
- Email с одним символом после @

Для пароля:

- Пароль минимальной длины
- Пароль максимальной длины
- Пароль на 1 символ короче минимального
- Пароль на 1 символ длиннее максимального

Зависимости от состояний системы

1. Аккаунт активен:
- Успешная авторизация
- Неверный пароль
- Неверное имя пользователя
2. Аккаунт заблокирован:
- Попытка авторизации
- Сообщение о блокировке
3. Аккаунт неактивен:
- Требуется активация
- Письмо с инструкциями
4. Многократные неудачные попытки:
- Временная блокировка
- Уведомление пользователю
5. Смена пароля:
- Запрос на восстановление
- Временный пароль
- Новый пароль

Рекомендации по тестированию

1. Проверить все комбинации классов эквивалентности
2. Протестировать все граничные значения
3. Учесть все состояния системы
4. Проверить обработку ошибок
5. Протестировать восстановление после ошибок
6. Проверить работу системы при высокой нагрузке
7. Убедиться в корректности сообщений об ошибках

Такой подход позволит обеспечить полное покрытие тестами всех возможных сценариев авторизации пользователя-туриста и выявить потенциальные проблемы на ранних этапах.

Элемент для тестирования	Классы эквивалентности / Граничные значения	Ожидаемое количество тестов	Обоснование
Поле “Email”	Валидный формат: user@example.com Невалидный формат отсутствует user@, user, @example.com	4 теста	Проверка корректного формата, обработка самых частых ошибок ввода(отсутствие@, отсутствие домена) и обязательность поля.
Поле”Пароль”	Валидный пароль: Qw123! (соответствует политике) Неверный пароль: wrongrass Пустое значение: (пустая строка)	3 теста	Проверка корректного пароля, обработка неверного пароля и обязательность поля.
Состояние учётной записи	Учётная запись существует и активна. Учётная запись не существует. Учётная запись существует, но заблокирована.	3 теста	Проверка логики системы, зависящей от состояния(например, разное сообщение об ошибке для “Неверный аккаунт”). Это требует отдельных тестовых данных

Граничные значения для длины пароля	Минимальная длина (6 символов): 123Ab ! Ниже минимума (5 символов): 123 aB Максимальная длина (64 символа): Ab1! +60 символов Выще максимума (65 символов): Ab1!+61 символ	4 теста	Проверка корректности проверки граничных значений политики безопасности паролей (например, минимальная длина 6 символов).
Функционал ьные кнопки	Кнопка “Войти”(основное действие) Ссылка ”Забыли пароль?” Ссылка “Регистрация”	3 теста	Проверка доступности и работоспособности всех элементов управления на форме авторизации.
	ИТОГО примерное количество тестов	~17 тестов	Это оценка для минимального позитивного/ негативного покрытия. На практике тестов может быть больше за счёт комбинаций (например, валидный email+неверный пароль +заблокированный аккаунт).

2. Разработка тестовых сценариев

Тестовый сценарий 1 (позитивный)

ID:	TC_AUTH_01
Название:	Проверка успешной авторизации с валидными данными активного пользователя.
Предусловия:	1.Пользователь с email test_user@example.com и паролем SecurePass123! Зарегистрирован в системе. 2.Учётная запись пользователя активна.
Шаги:	1.Открыть страницу авторизации. 2.В поле”Email” ввести test_user@eexample.com. 3.В поле “Пароль” ввести SecurePass123!. 4.Нажать кнопку “Войти”.
Ожидаемый результат:	Происходит перенаправление на главную страницу личного кабинета системы. В шапке страницы отображается приветствие: ”Добро пожаловать, test_user”.
Фактический результат:	[Заполняется тестировщиком во время выполнения]
Статус:	[Passed/Failed/Blocked-заполняется тестировщиком]

Тестовый сценарий 2 (Негативный-обработка ошибки)

ID:	TC_AUTH_02
Название:	Проверка обработки попытки входа с неверным паролем.
Предусловия:	1.Пользователь с email test_user@example.com зарегистрирован в системе.
Шаги:	1.Открыть страницу авторизации. 2.В поле”Email” ввести test_user@eexample.com. 3.В поле “Пароль” ввести WrongPassword456. 4.Нажать кнопку “Войти”.
Ожидаемый результат:	1.Авторизация не происходит. 2.Отображается сообщение об ошибке красным цветом:

	”Неверный email или пароль”. 3.Поле “Пароль” очищается. 4.Пользователь остаётся на странице авторизации.
Фактический результат:	[Заполняется тестировщиком во время выполнения]
Статус:	[Passed/Failed/Blocked-заполняется тестировщиком]

Тестовый сценарий 3 (Проверка граничного значения)

ID:	TC_AUTH_03
Название:	Проверка ввода пароля минимальной допустимой длины.
Предусловия:	1.Политика безопасности системы требуют минимальную длину пароля в 6 символов. 2.Пользователь с email short_pass_user@example.com т паролемAb1! 23(ровно 6 символов) зарегистрирован и активен.
Шаги:	1.Открыть страницу авторизации. 2.В поле”Email” ввести short_pass_user@eexample.com. 3.В поле “Пароль” ввести A123!. 4.Нажать кнопку “Войти”.
Ожидаемый результат:	Авторизация проходит успешно. Происходит перенаправление на главную страницу личного кабинета.
Фактический результат:	[Заполняется тестировщиком во время выполнения]
Статус:	[Passed/Failed/Blocked-заполняется тестировщиком]

3. Описание выполненных действий

1. Выбор модуля: Был выбран ключевой модуль ”Авторизация пользователя” из-за его важности для безопасности и функциональной системы.

2. Анализ входных данных: Для каждого поля ввода (Email,Пароль) были определены классы эквивалентности (валидные/ невалидные данные) и граничные значения(минимальная /максимальная длина пароля).
3. Анализ зависимостей от состояния: Учтены различные состояния учётной записи (активна, не существует, заблокирована), которые критически влияют на поведение модуля.
4. Оценка количества тестов: На основе проведённого анализа была составлена таблица, где для каждого элемента тестирования обосновано необходимое количество проверок. Итоговая оценка – около 17 тестов для базового покрытия.
5. Разработка тестовых сценариев: Созданы три подробных тест-кейса в заданном формате, которые покрывают:

- Позитивный сценарий (TC_AUTH_01): Успешный вход в систему.
- Негативный сценарий (TC_AUTH_02): Обработка системой ошибки (неверный пароль) с проверкой корректного сообщения и поведения UI.
- Проверку граничного значения (TC_AUTH_03): Проверка корректной работы с паролем минимально допустимой длины.

Этот отчёт представляет собой структурированный план тестирования для модуля авторизации, который можно использовать для дальнейшей практической реализации тестов.