**Тестирование требований**

Требования протестированы исходя из сравнения и сопоставления ожидаемых условий с реальным фактическим результатом, а также качества функционала.

Отметки:

* зеленым цветом выделены достоверные и полностью соблюденные требования;
* желтым цветом выделены частично соблюденные требования и некритические расхождения, включая опечатки и ошибки при составлении, в скобках указаны фактически присутствующие на сайте данные;
* красным цветом выделены критические расхождения с требованиями и серьезные дефекты, заведены баги в баг-репорте.

**Тестирование сайта**

Тестирование интерфейса страниц регистрации, авторизации и восстановления пароля в личном кабинете «Ростелеком» проведено исходя из отсутствия Личного кабинета у пользователя (тестировщик не является клиентом Ростелекома), а также без имеющегося тестового доступа к системе либо тестовых учетных данных, вследствие чего не все тестовые сценарии в требованиях могут быть покрыты тестами (особенно позитивными).

Проведено тестирование форм регистрации (разными способами), авторизации (разными способами) и восстановления пароля (разными способами).

Всего составлено 35 автоматизированных тестов, включая параметризованные 124 параметрами (отдельные кейсы), в т. ч.:

* Форма регистрации – 9 тестов и 28 параметров,
* Форма авторизации – 11 тестов и 40 параметров,
* Форма восстановления пароля – 15 тестов и 56 параметров.

**Техники тест-дизайна, используемые при составлении тестовых сценариев и тест кейсов:**

* разбиение на классы эквивалентности и анализ граничных значений;
* таблицы причинно-следственных решений, состояний и переходов;
* предугадывание ошибки;
* диаграмма пользовательских ролей;
* исследовательское и свободное тестирование.

**I. Регистрация**

**1.1. Основные шаги сценария**

1. Клиент переходит на страницу авторизации;
2. Клиент нажимает на ссылку "Зарегистрироваться";
   1. Система отображает форму регистрации, которая делится по вертикали на две половины;
   2. Правая часть содержит:
      * 1. Поле ввода имени (обязательное);
        2. Поле ввода фамилии (обязательное);
        3. Поле выбора региона (обязательное);
        4. Поле ввода email или мобильного телефона (обязательное);
        5. Поле ввода пароля (обязательное);
        6. Поле подтверждения пароля (обязательное);
        7. Кнопка "Продолжить";
        8. Ссылки на политику конфиденциальности и пользовательское соглашение;
   3. Левая часть содержит логотип и продуктовый слоган кабинета (отсутствуют);
3. Пользователь заполняет поле для ввода имени;
   1. Система проверяет на корректность введенные данные, поле ввода должно содержать минимум 2 символа состоящих из букв кириллицы или знака тире (-) – (не принимаются реальные валидные имена: двойное имя через пробел, имя из 1 буквы, имя с 2 и более тире, имя с апострофом);
4. Пользователь заполняет поле для ввода фамилии;
   1. Система проверяет на корректность введенные данные, поле ввода должно содержать минимум 2 символа состоящих из букв кириллицы или знака тире (-) – (не принимаются реальные валидные фамилии: двойная фамилия через пробел, фамилия из 1 буквы, фамилия с 2 и более тире, имя с апострофом).
5. Пользователь выбирает регион из выпадающего списка (по умолчанию Москва);
6. Пользователь вводит email или телефон;
   1. Система проверяет формат введенного адреса\телефона;
7. Пользователь вводит пароль и подтверждение пароля;
8. Система проверяет корректность пароля по правилам и при успешной проверке отображается следующая форма, иначе отображается ошибка - (поля «Пароль» и «Подтверждения пароля» принимают символы Юникод при соблюдении всех прочих условий для пароля):

8.1 Если пользователь ввел пароль менее 8 символов, ***"Длина пароля должна быть не менее 8 символов"*** под полем ***"Новый пароль"***

8.2 Если пользователь ввел пароль без заглавных букв, ***"Пароль должен содержать хотя бы одну заглавную букву"*** под полем ***"Новый пароль"***

8.3 Если пользователь ввел пароль не с латинскими буквами, ***"Пароль должен содержать только латинские буквы"*** под полем ***"Новый пароль"***

8.4 Если пользователь ввел в поле ***"Подтверждение пароля"*** пароль, отличный от пароля ***"Новый пароль",*** выводим ***"Пароли не совпадают"*** под полем ***"Подтверждение пароля"***

8.5 Если пользователь ввел пароль согласно парольной политике – переход на шаг 9.

1. Пользователь нажимает кнопку "Продолжить";
   1. Система отправляет код подтверждения на email или телефон;
   2. Система проверяет все обязательные к заполнению поля, валидацию телефона\email и отображает ошибку если какое-то поле не соответствует требованиям;
2. Система проверяет введенный email на уникальность, если введенный email привязан к имеющейся УЗ SSO, то отображается оповещающая форма, которая состоит из:
3. Кнопка "Войти" – редирект на форму авторизации.
4. Кнопка "Восстановить пароль" – редирект на форму восстановления пароля.
5. Кнопка "х" – закрыть всплывающее окно оповещения.
6. Система проверяет введенный телефон на уникальность, если введенный телефон привязан к имеющейся УЗ SSO, то отображается оповещающая форма, которая состоит из:
7. Кнопка "Зарегистрироваться" – телефон отвязывается от существующей УЗ и привязывается к УЗ, которая создается в процессе регистрации;
8. Кнопка "Отмена" – закрыть оповещающую форму;
9. Система перенаправляет пользователя на страницу ввода кода из смс или email, которая содержит:

(Маскированный номер телефона, если введен номер телефона при регистрации)

(Маскированная почта, если введена почта при регистрации)

1. Поля для ввода кода;
2. Кнопку "Получить код повторно"

(Повторная отправка смс с новым кодом, если введен номер телефона при регистрации);

(Повторная отправка письма с новым кодом, если введена почта при регистрации)

1. Кнопку **"Изменить номер"**(Если введен номер телефона при регистрации) (Переход на форму ввода регистрационных данных п.2, при этом необходимо отобразить все регистрационные данные, которые пользователь ввел до этого);

Кнопку **"Изменить почта" (**по факту: Изменить email**)** (Переход на форму ввода регистрационных данных п.2, при этом необходимо отобразить все регистрационные данные, которые пользователь ввел до этого);

1. При вводе неправильного кода отображается ошибка "Неверный код. Повторите попытку"
2. При вводе временного кода, срок времени которого закончился, отображается ошибка "Время жизни кода истекло"
3. Пользователь вводит корректный проверочный код (переход в п.11);
4. Пользователь перенаправляется в кабинет-инициатор.

***II. Стандартная авторизация по логину и паролю:***

1. Система отображает форму «Авторизация», разделенную вертикально на два блока и содержащую:
2. В левой части – (по факту: в правой части):
   1. Меню выбора типа аутентификации:
      1. Таб выбора аутентификации по номеру, "Номер" – (по факту: по номеру и паролю, «Телефон»)
      2. Таб выбора аутентификации по логину и паролю, "Почта" - (по факту: по почте и паролю)
      3. Таб выбора аутентификации по почте и паролю, "Логин" - (по факту: по логину и паролю)
      4. Таб выбора аутентификации по лицевому счету и паролю, "Лицевой счет"
   2. Форма ввода "Номер" или «Логин», или "Почта" или "Лицевой счет" (По умолчанию выбрана форма авторизации по телефону)
   3. Форма ввода "Пароль"
3. В правой части – (по факту: в левой части):
   1. Продуктовый слоган ЛК "Ростелеком ID".
   2. Вспомогательная информация для клиента – (по факту: отсутствует в правой части, присутствует в футере страницы).

При вводе номера телефона/почты/логина/лицевого счета – таб выбора аутентификации меняется автоматически – (по факту: не всегда корректно определяется тип аутентификации, также зависит от формата данных: при вводе почты, начинающейся с цифр, форма сохраняет в адресе автоматический префикс кода страны «7»).

***2.1 Сценарий авторизации клиента по номеру телефона, кнопка "Номер***" – (по факту: кнопка "Телефон")***:***

1. Клиент вводит номер телефона и пароль
2. Система:
   1. Проверяет корректность введенного номера;
   2. Проверяет связку Номер+Пароль;
   3. При успешной проверке Номера и пароля – система переходит к следующему шагу п.3, иначе клиенту отображается ошибка, сценарий начинается с пункта 1.
   4. При некорректном вводе связки Номер + Пароль, выводим сообщение "Неверный логин или пароль" и элемент "Забыл пароль" перекрашивается в оранжевый цвет.
3. Система:
   1. Выполняет успешный поиск УЗ по введенному номеру телефона;
   2. Аутентифицирует клиента;
   3. Выполняет перенаправление клиента на страницу redirect\_uri.

***2.2 Сценарий авторизации клиента по номеру телефона, кнопка "Почта" –*** (по факту: по почте и паролю):

1. Клиент вводит Почта и пароль
2. Система:
   1. Проверяет корректность введенной почты;
   2. Проверяет связку Почта+Пароль;
   3. При успешной проверке почты и пароля – система переходит к следующему шагу п.3, иначе клиенту отображается ошибка, сценарий начинается с пункта 1.
   4. При некорректном вводе связки Номер + Пароль ***–*** (по факту: Почта + Пароль), выводим сообщение "Неверный логин или пароль" и элемент "Забыл пароль" перекрашивается в оранжевый цвет.
3. Система:
   1. Выполняет успешный поиск УЗ по введенной почте;
   2. Аутентифицирует клиента;
   3. Выполняет перенаправление клиента на страницу redirect\_uri.

***2.3 Сценарий авторизации клиента по номеру телефона, кнопка "Логин" –*** (по факту: по логину и паролю):

1. Клиент вводит Логин и пароль
2. Система:
   1. Проверяет корректность введенного логина;
   2. Проверяет связку Логин+Пароль;
   3. При успешной проверке почты ***–*** (по факту: логина) и пароля – система переходит к следующему шагу п.3, иначе клиенту отображается ошибка, сценарий начинается с пункта 1.
   4. При некорректном вводе связки Номер + Пароль ***–*** (по факту: Логин + Пароль), выводим сообщение "Неверный логин или пароль" и элемент "Забыл пароль" перекрашивается в оранжевый цвет.
3. Система:
   1. Выполняет успешный поиск УЗ по введенному логину;
   2. Аутентифицирует клиента;
   3. Выполняет перенаправление клиента на страницу redirect\_uri.

***2.4 Сценарий авторизации клиента по номеру телефона, кнопка "Лицевой счет" –*** (по факту: по лицевому счету):

1. Клиент вводит Лицевой счет и пароль
2. Система:
3. Проверяет корректность введенного лицевого счета и ищет логин, связанный с лицевым счетом, в следующих шагах проверяется найденный логин;
4. Проверяет связку Логин+Пароль;
5. При успешной проверке логина и пароля – система переходит к следующему шагу п.3, иначе клиенту отображается ошибка, сценарий начинается с пункта 1.
6. При некорректном вводе связки Номер + Пароль ***–*** (по факту: Логин + Пароль), выводим сообщение "Неверный логин или пароль" и элемент "Забыл пароль" перекрашивается в оранжевый цвет.
7. Система:
8. Выполняет успешный поиск УЗ по Лицевому счету;
9. Аутентифицирует клиента;
10. Выполняет перенаправление клиента на страницу redirect\_uri.

***2.5 Авторизация по временному коду*** – (оценка не проводилась ввиду отсутствия доступа к авторизации про временному коду):

1. Система отображает форму «Авторизация по коду», содержащую:
2. Подсказку по работе с формой “Укажите контактный номер телефона или почту, на которые необходимо отправить код подтверждения”;
3. Поле ввода номера телефона или почты;
4. Кнопку "Получить код".
5. Клиент вводит номер телефона/почту и нажимает кнопку "Получить код";
6. Система:
7. Проверяет корректность введенного номера/почты;
8. Отправляет код на введенный номер телефон/почту;
9. Отображает форму ввода кода подтверждения, содержащую:
10. Номер телефона/Почту на который был отправлен код;
11. Ссылку "Изменить номер", если пользователь ввел телефон на 2 шаге или ссылку "Изменить почту", если пользователь ввел почту на шаге 2 (ссылка ведет на форму ввода номера телефона/почты);
12. Шесть отдельных полей для ввода кода подтверждения;
13. Текст с обратным отсчётом времени до повторной попытки отправки код, по завершении отсчёта отображается ссылка "Получить новый код";
14. Клиент начинает вводить полученный код;
15. Система:
16. После ввода каждой цифры переводит фокус ввода в следующее поле;
17. При событии заполнения всех 6 полей производит верификацию кода;
18. При успешной верификации кода система переходит к следующему шагу, иначе клиенту отображается ошибка, сценарий останавливается.
19. Система:
20. Выполняет поиск УЗ по введенному номеру телефона/почте:
21. Если УЗ с таким телефоном/почтой не найдена, то создает новую без пароля, ФИО, Региона после чего переход на шаг 8;
22. Если УЗ найдена – переход на шаг 8;
23. Аутентифицирует клиента;
24. Выполняет перенаправление клиента на страницу из redirect\_uri;

**III. Восстановление пароля**

**Окно выбора типа восстановления пароля:**

1. Система отображает форму «Восстановление пароля», содержащую:
   1. Меню выбора типа ввода контактных данных:
      1. Таб выбора восстановления пароля по номеру, "Номер" – (по факту: по номеру и паролю, «Телефон»)
      2. Таб выбора восстановления пароля по логину и паролю, "Почта" - (по факту: по почте и паролю)
      3. Таб выбора восстановления пароля по почте и паролю, "Логин" - (по факту: по логину и паролю)
      4. Таб выбора восстановления пароля по лицевому счету и паролю, "Лицевой счет"
   2. Форма ввода "Номер" или «Логин», или "Почта" или "Лицевой счет" (По умолчанию выбрана форма восстановления пароля по телефону)
   3. Форма ввода "Капча"
   4. Кнопка "Далее" – (по факту: Кнопка "Продолжить") переход в п.3. (Продолжить сценарий восстановления пароля)
2. Если к УЗ привязан только телефон, то переход в Сценарий восстановления пароля клиента по номеру телефона, кнопка "По SMS на номер телефона" - (по факту: "По номеру телефона")
3. Если к УЗ привязан только почту, то переход в Сценарий восстановления пароля клиента по номеру телефона, кнопка "По ссылке на почту" – (по факту: По email)
   1. Кнопка "Вернуться" (Вернуться на форму авторизации) - (по факту: "Вернуться назад")
4. После введения телефона, почты, логина или ЛС отображается форма выбора восстановления пароля:
   1. Выбор "По SMS на номер телефона" (Если телефон привязан к УЗ) - (по факту: "По номеру телефона")
   2. Выбор "По ссылке на почту" (Если почта привязана к УЗ) - (по факту: "По email")
   3. Кнопка "Продолжить" (Продолжить сценарий восстановления пароля)
   4. Кнопка "Вернуться назад" (Вернуться на форму ввода контактных данных п.1 для восстановления пароля)

***3.1 Сценарий восстановления пароля клиента по номеру телефона, кнопка "По SMS на номер телефона"*** - (по факту: "По номеру телефона")***:***

1. Пользователь выбирает восстановить по номеру телефона;
2. Система отправляет пользователю смс с кодом на номер привязанный к УЗ SSO;
3. Открывается форма с полем для ввода кода из СМС, которая содержит:

3.1 Кнопку "Получить код повторно" (Повторная отправка смс с новым кодом);

3.2 Кнопка "Вернуться назад" (Вернуться на шаг ввода контактных данных для восстановления доступа);

3.3 При вводе неправильного кода отображается ошибка "Неверный код. Повторите попытку"

3.4 При вводе временного кода, срок времени которого закончился, отображается ошибка "Время жизни кода истекло"

1. Пользователь вводит корректный проверочный код (переход в п.5);
2. После ввода корректного кода из смс – открывается форма для ввода нового пароля, состоящая из:

5.1 Поле ввода нового пароля

5.2 Поле ввода для подтверждения нового пароля

5.3 Кнопка "Сохранить" для подтверждения нового пароля (Переход в п.56)

5.4 Правила для создания пароля

1. Пользователь вводит новый пароль, подтверждение пароля и нажимает кнопку "Сохранить";
2. Система проверяет корректность пароля по правилам и при успешной проверке отображается следующая форма, иначе отображается ошибка:

7.1 Если пользователь ввел пароль менее 8 символов, "Длина пароля должна быть не менее 8 символов" под полем "Новый пароль"

7.2 Если пользователь ввел пароль без заглавных букв, "Пароль должен содержать хотя бы одну заглавную букву" под полем "Новый пароль"

7.3 Если пользователь ввел пароль не с латинскими буквами, "Пароль должен содержать только латинские буквы" под полем "Новый пароль"

7.4 Если пользователь ввел в поле "Подтверждение пароля" пароль, отличный от пароля "Новый пароль", выводим "Пароли не совпадают" под полем "Подтверждение пароля"

1. Если пользователь ввел пароль согласно парольной политике, система проверяет введенный пароль с тремя предыдущими:

8.1 Если пользователь ввел пароль, идентичный трем предыдущим, "Этот пароль уже использовался, укажите другой пароль"

8.2 Если пользователь ввел пароль, отличный от трех предыдущих, – переход на шаг 9.

1. Клиент перенаправляется на страницу авторизации.

***3.2 Сценарий восстановления пароля клиента по номеру телефона, кнопка "По ссылке на почту" -*** – (по факту: По email)***:***

1. Пользователь выбирает восстановить по почте;
2. Открывается форма, оповещающая пользователя об отправке письма на его почту, которая содержит:

2.1 Текст, оповещающий об отправке письма со ссылкой – (по факту: с кодом) на почту;

2.2 Кнопку "Вернуться назад" (Переход на форму авторизации) - (по факту: вернуться на шаг ввода контактных данных для восстановления доступа)

1. Пользователь открывает письмо и переходит по ссылке – (по факту: код для ввода в форму).
2. Система отображает форму, состоящую из:
   1. Поле ввода нового пароля
   2. Поле ввода для подтверждения нового пароля
   3. Кнопка "Сохранить" для подтверждения нового пароля (Переход в п.5)
   4. Правила для создания пароля
3. Система проверяет корректность пароля по правилам и при успешной проверке отображается следующая форма, иначе отображается ошибка:

5.1 Если пользователь ввел пароль менее 8 символов, "Длина пароля должна быть не менее 8 символов"

5.2 Если пользователь ввел пароль без заглавных букв, "Пароль должен содержать хотя бы одну заглавную букву"

5.3 Если пользователь ввел пароль не с латинскими буквами, "Пароль должен содержать только латинские буквы"

1. Если пользователь ввел пароль согласно парольной политике, система проверяет введенный пароль с тремя предыдущими:

6.1 Если пользователь ввел пароль, идентичный трем предыдущим, "Этот пароль уже использовался, укажите другой пароль"

6.2 Если пользователь ввел пароль, отличный от трех предыдущих, – переход на шаг 7.

1. Пользователь переходит на форму успешной смены пароля.
2. При нажатии на кнопку "Авторизоваться" пользователь перенаправляется на форму авторизации – (по факту: перенаправляется на страницу авторизации автоматически).